实 Clifford+CH 量子电路的完备等式理论

Alexandre Clément 巴黎萨克雷大学、巴黎萨克雷高等师范学院、法国国家科学研究中心、法国国家信息与自动化研究院、LMF，91190，法国吉夫叙尔伊韦特
alexandre.clement@inria.fr

摘要

我们为由实 Clifford 门和双量子比特受控 Hadamard 门生成的量子电路片段提出一种完备等式理论。也就是说，我们给出该片段中电路之间的一组简单等式，并证明所有其他成立的方程都可由这些等式推导得出。这是首个针对有限生成的量子电路通用片段的此类完备性结果，该片段不含参数化门，也不需要辅助量子比特。

1 引言

量子电路构成了量子计算的基础语言，处于其核心位置。它们在实践中所发挥的作用，有时被比作经典计算中的汇编语言。不过从形式上看，它们实际上是布尔电路的量子对应物。与布尔电路一样，它们由一系列量子门组成，这些量子门作用于量子数据；量子数据通常以量子比特的形式存在，是比特的量子对应物。

量子计算可以先验地在具有各种特性的多种物理平台上实现；目前，基本上无法预测哪种物理实现最终会是最佳选择，也不清楚某一种技术是否会完全取代其他技术。因此，形式化研究各种不同类别的量子电路先验地都具有意义。即使仅限于最标准的量子计算模型（其中数据编码在量子比特中），也有若干量子电路语言的片段值得考察；这些片段对应于用于构建电路的特定基本量子门集合。其中一些片段受到了特别关注，例如著名的 Clifford+T 和 Toffoli-Hadamard 片段。门集的一项重要特性是计算通用，也就是说，原则上能够以任意小的误差实现任何量子程序。Clifford+T 和 Toffoli-Hadamard 之所以引人关注，一个原因是它们既具有通用性，又由非常小且简单的一组量子门生成；此外，它们或许也适用于超导电路等前景良好的实现方案。

量子计算中的一项核心任务是操作量子电路，尤其是将电路转换为在某些标准下更优的等价电路：这有各种实际应用，例如优化、满足硬件约束、量子纠错或验证。操作量子电路的一种前景广阔的方法是通过图形重写。近年来，已有若干图形语言被提出，用于形式化地操作量子电路（以及量子过程的其他方面），其中包括 ZX、ZW、ZH 和 ZXW 演算 [2, 12, 16, 19, 29]。一个核心问题是此类语言形式化中的一个核心问题，是其等式理论的完备性，也就是说，配备的重写规则集是否足够强大，能够实现任何在语义上有意义的变换。另一个相关的重要问题是，尽可能简化完备等式理论；如果可能，最终还要证明它是极小的，即所有冗余都已被化简消除。目前，图形语言已有多种完备等式理论 [20, 23–25, 35], , 其中一些是极小的 [14] 或接近极小的 [3, 4, 32–35]。

量子电路的语言本身可以被视为一种图形语言，与依赖 ZX 演算等外部辅助语言相比，为其寻找完备等式理论具有额外的价值。例如，对量子电路应用任意 ZX 变换都可能生成一个 ZX 图，而从该图中恢复量子电路可能会很困难 [13, 16]。尽管为量子电路寻找完备等式理论的问题早在21世纪初就已提出 [22, 26], , 第一套完备等式理论直到几年前才被发现 [11], , 随后又进行了简化并证明了其最小性 [9, 10]。这些结果针对的是量子比特设定下的完整量子电路语言。也就是说，门集非常简单，但仍包含一个参数化门；而最小等式理论相对简单，却涉及对参数进行非平凡的计算。

本文研究量子电路的一个有限生成片段，该片段不包含参数化门，具体而言，它由实 Clifford 门——Hadamard 门 H、Pauli Z 门和受控-Z 门 CZ——以及受控 Hadamard 门 CH 生成。我们将这一片段称为 *Real-Clifford+CH*。这是 Clifford + T 的一个子片段，其中包含 Toffoli-Hadamard [1]，因而具有通用性。据我们所知，这是首个针对由有限门集生成且不含参数化门的量子电路片段的完备性结果。

与 [11], 类似，我们的结果基于与一种辅助语言之间的双向转换；该辅助语言已知具有完备性结果，即由单级和双级矩阵 [17] 生成的矩阵群 $U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 的一个表示。这些单级和双级矩阵的结构与 [11]中使用的光学线路相似。

相关工作。除了前文提到的图形语言外，其他用于量子计算的语言也配备了完备的等式理论 [15, 17, 21]。主要区别在于，这些语言配备了控制构造子（或等价的构造），使其能够表达任意多重控制量子门，这意味着从量子电路的角度来看，它们并非有限生成的。

[1]但不包括无辅助量子比特的三量子比特电路这一情况。

等价构造）使人们能够表示任意多重控制门，这意味着从量子电路的角度来看，它们不是有限生成的。

本文组织如下：在第2.1节，我们正式介绍实-Clifford+CH 量子电路，并定义一些有用的宏。在第3节，我们介绍将要证明其完备性的等式理论。在第4节，我们陈述本结果所依赖的完备性结果 [17],，并对其加以调整，从而将完备性推广到量子电路。在第5节和6节，我们进一步阐释完备性证明。在第7节，我们证明该等式理论对于作用于 1 个和 2个量子比特的电路是完备的。最后，在第8节，我们证明一般情形下的完备性。

2 实-Clifford+CH 量子电路

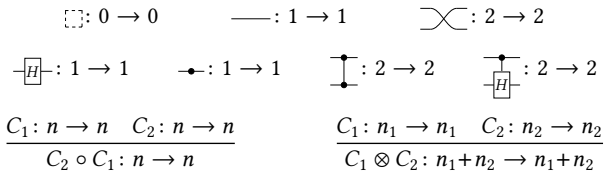
2.1 实-Clifford+CH 量子电路的 PROP

我们考虑由以下门集生成的不含辅助量子比特的量子电路实-Clifford+CH 片段：

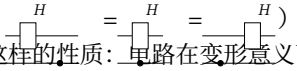

(A)

沿着 [9–11],，我们利用 PROP 的结构对 Real-Clifford+CH 量子电路进行严谨的形式化。PROP 源自范畴论， [28, 36] 但也可以纯粹视为一种代数结构 [8]。我们首先定义原始电路 [11],，它们是由（A）的生成元、空电路、单量子比特单位元和交换，通过顺序复合∘ 以及并行复合 ⊗自由构造而成的项：

定义 2.1。原始 *Real-Clifford+CH* 电路的集合$\mathbf{QC}_{\mathbf{raw}}$ 按如下方式归纳定义：



定义 2.2。*Real-Clifford+CH* 电路的 *PROP*，记作$\mathbf{QC}$，通过对$\mathbf{QC}_{\mathbf{raw}}$ 按 *PROP* 公理取商得到，如图*1*所示。

粗略来说，方程（a）至（e）是必要的公理，用于保证具有相同图形表示的两个电路实际上相等，并且导线的长度无关紧要（例如，  ）。方程（f）和（g）还赋予我们这样的性质：电路在变形意义下定义。

注 1。仅通过以下方程对 $\mathbf{QC}_{\mathbf{raw}}$ 进行商得到的结构称为 *PRO*。根据具体情境，将量子电路建模为 *PRO* 而非 *PROP* 可能更合适（例如考虑交换门代价高昂的实现时），反之亦然。请注意，只需将方程 (a) 至 (e) 加入图 *4* 所示的完备等式理论中，我们的完备性结果便可直接调整为适用于 *PRO* 设置。此外，方程 (f) 和 (g) 实际上无需进行参数化*4*。而且，方程 (f) 实际上无需进行参数化为任意电路 C：只需假设它对生成元成立即可，也就是说，方程 (f) 可以替换为图 *2* 中的方程*2*，因为结合 *PROP* 的其他公理，便可由这些方程推出原方程。因此，只需在完备等式理论中增加四个方程，即可使其适用于 *PRO* 设置。

注记 2. 其他标准实 *Clifford* 门都可以由 (A) 中的门构造出来（见图*3*）。另请注意，交换门可以由 (A) 的生成元表示（见方程 (8)）。

定义 2.3（语义）。对于任意 n 量子比特电路 C，令 $[\![C]\!]: \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$ 为其语义，并按如下方式归纳定义：

$$
\begin{aligned}
[\![C_2 \circ C_1]\!] &= [\![C_2]\!] \circ [\![C_1]\!] \\
[\![C_1 \otimes C_2]\!] &= [\![C_1]\!] \otimes [\![C_2]\!] \\
[\![\ \ ]\!] &= 1 \mapsto 1 \\
[\![\text{——}]\!] &= |x\rangle \mapsto |x\rangle \\
[\![\text{╳}]\!] &= |x,y\rangle \mapsto |y,x\rangle \\
[\![\text{—●—}]\!] &= |x\rangle \mapsto (-1)^x |x\rangle \\
[\![\text{—H—}]\!] &= |x\rangle \mapsto \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}} \\
[\![\text{●—●}]\!] &= |x,y\rangle \mapsto (-1)^{xy} |x,y\rangle \\
[\![\text{●—H}]\!] &= |x,y\rangle \mapsto \begin{cases} |0,y\rangle \mapsto |0,y\rangle \\ |1,y\rangle \mapsto \frac{|1,0\rangle + (-1)^y |1,1\rangle}{\sqrt{2}} \end{cases}
\end{aligned}
$$

注记 3. 严格来说，$[\![\cdot]\!]$定义在原始电路上。不过，可以验证它在图 *1*的方程下保持不变，因此在（非原始）电路上定义良好。

2.2 简写

现在我们定义若干简写，它们将在本文余下部分派上用场，其中一些对应于标准门。请注意，从形式上说，本文中绘制的所有电路仍被视为仅由（A）中的门组成；这些简写只是表示特定电路的一种便捷方式。

首先，我们将使用受控非门，以及量子门的标准变体，这些变体定义在图 3中。

其次，考虑一个将 H 对角化为 Z 的换基矩阵会特别有用：我们将使用如下矩阵：[2]

$$P \coloneqq R_Y(\tfrac{\pi}{4})Z = e^{-i\frac{\pi}{8}} SHTHS = \begin{pmatrix} \cos(\frac{\pi}{8}) & \sin(\frac{\pi}{8}) \\ \sin(\frac{\pi}{8}) & -\cos(\frac{\pi}{8}) \end{pmatrix}.$$

可以验证 $P^2 = I$和 $PZP = H$。注意， P 无法 用实数克利福德+CH 电路表示，因为它不属于该群

[2] where H, Z, S, T and R_Y are the matrices corresponding to the standard gates: $H = [\![\text{—H—}]\!] = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, $Z = [\![\text{—●—}]\!] = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$, $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{smallmatrix}\right)$, and $R_Y(\theta) = \left(\begin{smallmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{smallmatrix}\right)$

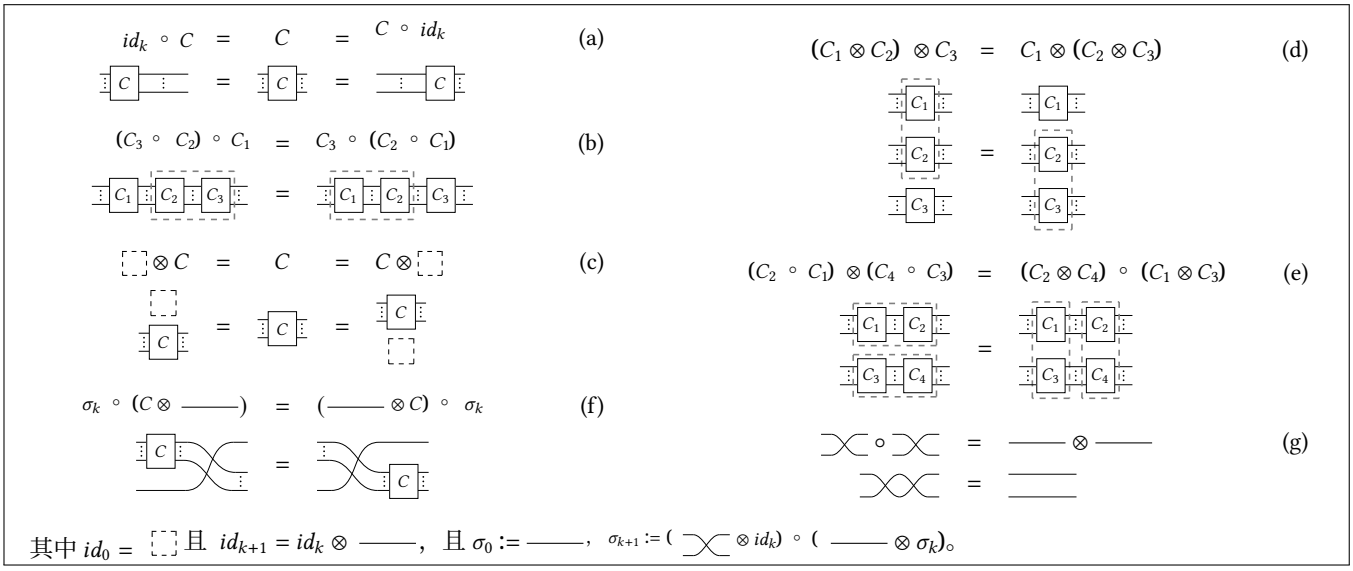


图 1：PROP公理。

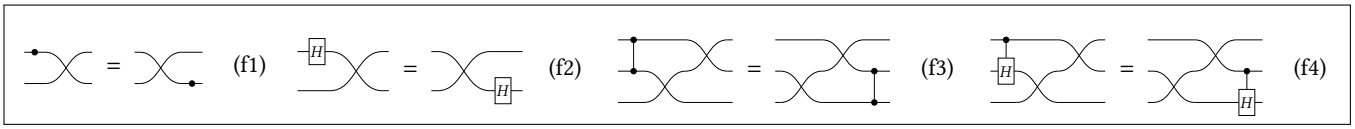
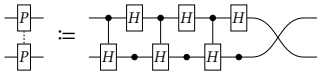


图 2：方程 (f) 的替代形式。

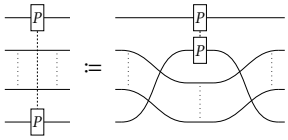
$U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$。然而，有

$$P \otimes P = \frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{2}+1 & 1 & 1 & \sqrt{2}-1 \\ 1 & -\sqrt{2}-1 & \sqrt{2}-1 & -1 \\ 1 & \sqrt{2}-1 & -\sqrt{2}-1 & -1 \\ \sqrt{2}-1 & -1 & -1 & \sqrt{2}+1 \end{pmatrix}$$

它属于该群，且可由实 Clifford+CH 电路表示。我们用略带虚线的线条绘制此简写，以便标明它实际上是由双量子比特门定义的：



表示一对作用于非相邻量子比特的 P 门也很有用：



最后，与 [11], 类似，另一类特别有用的简写是多受控门。

一方面，我们将使用多重控制的 Z 和 H 量子门。注意，对于 $n \geq 3$，无法将 n量子比特的多重控制

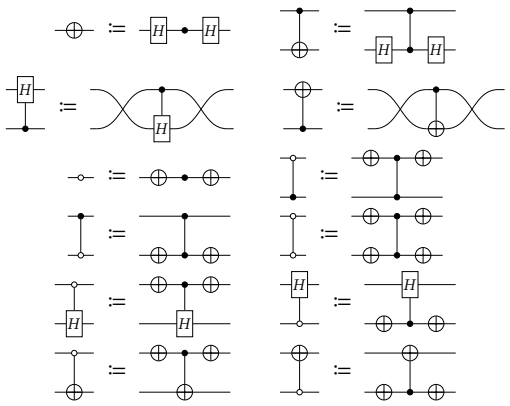


图 3：定义为简写的标准单量子比特门和双量子比特门。

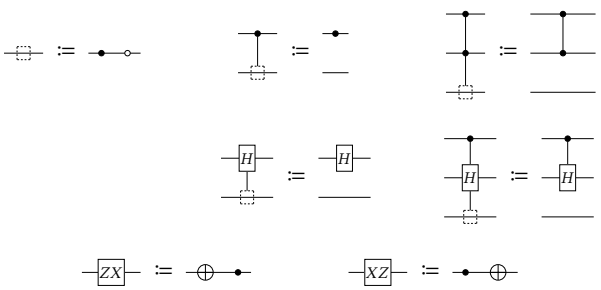
Z或 H 量子门表示为 n量子比特的实 Clifford+CH 电路。[3] 不过，可以将与单量子比特恒等门张量积的（$n-1$）量子比特多重控制 Z或 H 量子门表示出来。

另一方面，我们还会使用多受控 ZX和 XZ门（其中 ZX和 XZ 只是 Z门和 X门按两种顺序相乘的结果），它们不受此类限制。

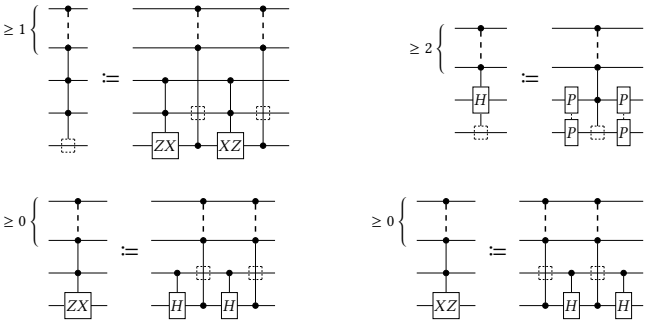
[3]这是因为它的行列式为 -1，而且我们只处理实矩阵。另请参阅第 4 节。

定义如下，通过相互归纳给出。注意，我们用一个小的虚线框来绘制多受控 Z 和 H 门，以便记录这一事实：该快捷方式实际上比多受控门本身多使用一个量子比特。[4]

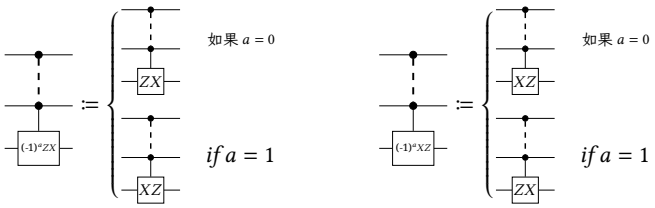
定义 2.4（多重控制的 Z、H、ZX 和 XZ 门）。基例如下：



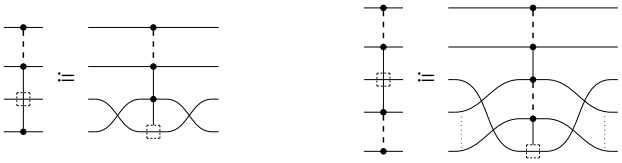
递归步骤如下：



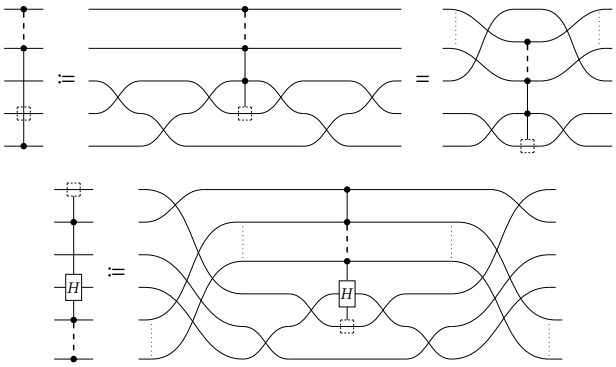
请注意，从语义上讲，$XZ = -ZX$。由此引出以下记号：对于 $a \in \{0,1\}$，



此外，考虑作用于非相邻量子比特上的多重受控门，或目标量子比特不在末端的情况也很有用（注意，我们在上面的归纳定义中已经使用过这种记号）。与 $P \otimes P$ 门类似，这些门通过与交换门共轭来定义。例如：

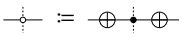


[4]对于多受控 Z 量子门，可以将虚线框理解为表示一个单量子比特 $-I$ 量子门，而我们的图示则表示一个多受控 $-I$ 量子门。类似地，可以将与单位元张量积的多受控 H 视为一个多受控 $H \otimes I$ 量子门。

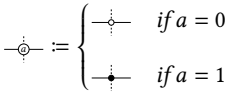


注意，由于电路是按照拓扑规则定义的，因此无需指定多重受控门两侧交换门的具体网络，只需指定它们实现的整体置换即可。唯一可能存在歧义的是控制位的顺序：按照惯例，我们总是采用保持控制位垂直顺序的置换。

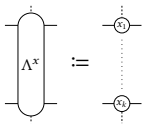
此外，我们还将考虑带有负控制位的多重控制量子门（即相对于 $|0\rangle$ 而非 $|1\rangle$），并采用白色控制的常用记号来表示。它们通过与 X 量子门共轭来定义：



进一步地，我们还定义参数化控制位，其颜色取决于一个布尔参数：



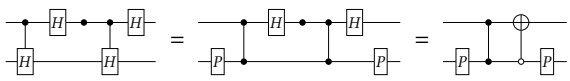
最后，我们按如下方式表示一系列参数化控制位，仿照 *[11]*中使用的记号：对于任意 $x = x_1 \ldots x_k \in \{0,1\}^k$，



3 等式理论

我们声称完备的方程集 QC 在图4中给出。我们记 $\mathsf{QC} \vdash C_1 = C_2$，当 C_1 与 C_2 可以通过这些方程相互变换时。[5]

方程（1）至（10）以及（12）至（15）相对而言较为标准。方程（16）和（17）也表达了一个广为人知的性质，即正控制电路与负控制电路相互对易。方程（11）本质上也表达了这一性质，但视角是 H的特征基：从纯语义的角度推理，可以非正式地写作



[5]也就是说，$\mathsf{QC} \vdash \cdot = \cdot$ 是满足图5中方程的、电路上的最小同余。

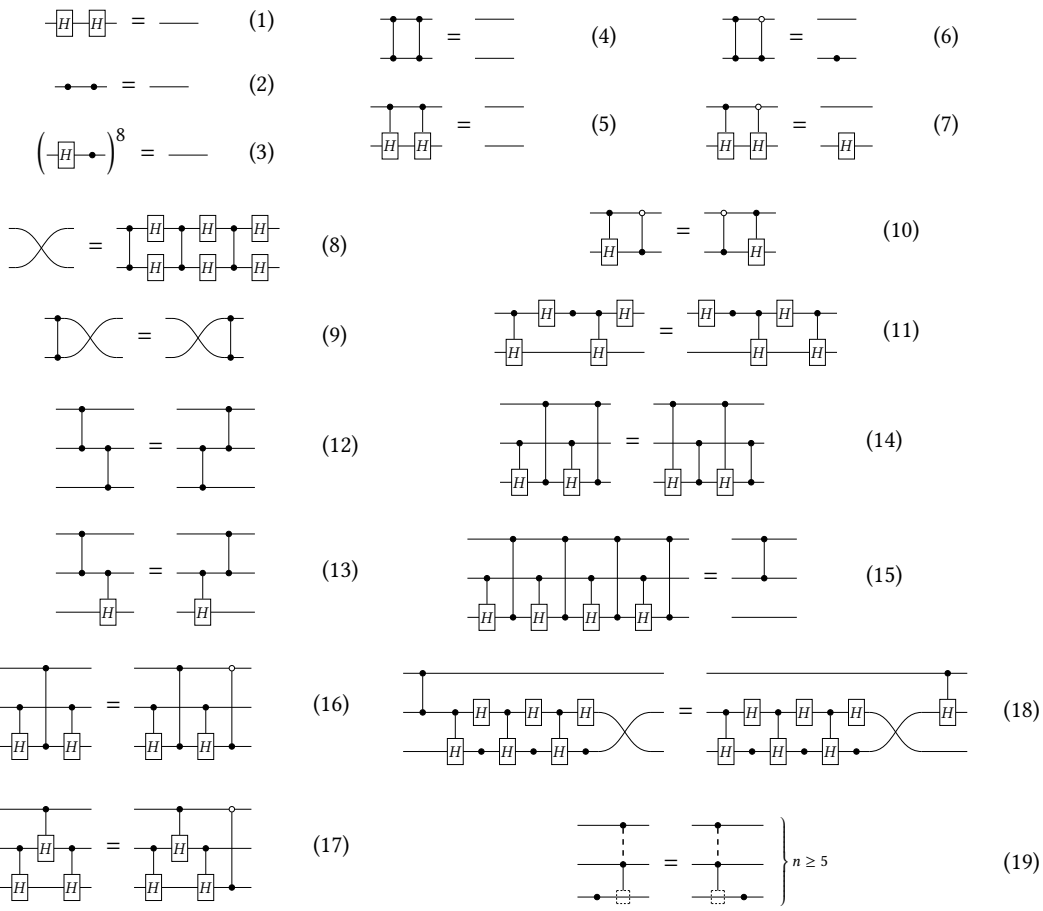


图 4：实 Clifford+CH 量子电路的完备等式理论。方程（19）是一个方程模式，由一个关于 n 个量子比特的方程组成，每个 $n \geq 5$。方程（6）、（7）、（14）至（17），以及（19）使用了第 2.2 节中定义的简写。

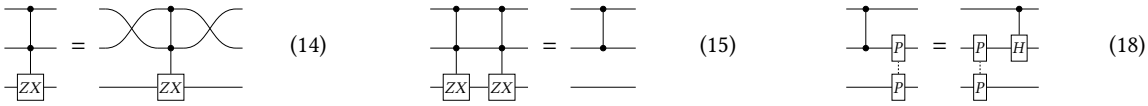


图 5：图 4中的部分方程，采用了更多简写。

这使对易关系显而易见。最后，方程（18）P表明，其顶部部分确实表现得像一个 P 门（见图P5），而方程（19）在一定程度上证明了这个捷径的行为就好像它没有触及底部的量子比特。

命题 3.1（可靠性）。对于任意电路 C_1，$C_2 \in \mathbf{QC}$，

$$\textit{if}\, \mathrm{QC} \vdash C_1 = C_2 \textit{ then } [\![C_1]\!] = [\![C_2]\!].$$

证明。 语义具有复合性，因此只需检查每个方程两边的语义是否相同。方程 (1) 至 (18) 可通过直接计算验证，方程 (19) 则可通过简单的归纳法验证。 □

4 辅助语言

本文主要依赖 [17] 的一项结果，该结果给出了群 $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 的一个表示（即一组生成元及其完备等式理论），该群由 N 维酉元矩阵，其元素属于 $\mathbb{Z}[\frac{1}{\sqrt{2}}]$。[11] 类似，我们将通过一种往返编码，把该完备等式理论转化为量子电路的等式理论。然而，与 [11]，中的情况不同，由实数-Clifford+CH 电路表示的矩阵集合并不恰好是 $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$，而是它的一个子群，我们需要先对其加以刻画。

$$(-1)_{[a]}^2 \approx \varepsilon \tag{a1}$$
$$X_{[a,b]}^2 \approx \varepsilon \tag{a2}$$
$$H_{[a,b]}^2 \approx \varepsilon \tag{a3}$$

$$(-1)_{[a]}(-1)_{[b]} \approx (-1)_{[b]}(-1)_{[a]} \tag{b1}$$
$$(-1)_{[a]}X_{[b,c]} \approx X_{[b,c]}(-1)_{[a]} \tag{b2}$$
$$X_{[a,b]}X_{[c,d]} \approx X_{[c,d]}X_{[a,b]} \tag{b3}$$
$$(-1)_{[a]}H_{[b,c]} \approx H_{[b,c]}(-1)_{[a]} \tag{b4}$$
$$X_{[a,b]}H_{[c,d]} \approx H_{[c,d]}X_{[a,b]} \tag{b5}$$
$$H_{[a,b]}H_{[c,d]} \approx H_{[c,d]}H_{[a,b]} \tag{b6}$$

$$(-1)_{[a]}X_{[a,b]} \approx X_{[a,b]}(-1)_{[b]} \tag{c1}$$
$$X_{[b,c]}X_{[a,b]} \approx X_{[a,b]}X_{[a,c]} \tag{c2}$$
$$X_{[a,c]}X_{[b,c]} \approx X_{[b,c]}X_{[a,b]} \tag{c3}$$
$$H_{[b,c]}X_{[a,b]} \approx X_{[a,b]}H_{[a,c]} \tag{c4}$$
$$H_{[a,c]}X_{[b,c]} \approx X_{[b,c]}H_{[a,b]} \tag{c5}$$

$$(-1)_{[a]}(-1)_{[b]}H_{[a,b]} \approx H_{[a,b]}(-1)_{[a]}(-1)_{[b]} \tag{d1}$$
$$(-1)_{[b]}H_{[a,b]} \approx H_{[a,b]}X_{[a,b]} \tag{d2}$$
$$(H_{[c,d]}H_{[a,c]}H_{[b,d]})^4 \approx H_{[a,b]}H_{[c,d]} \tag{d3}$$
$$(H_{[a,c]}H_{[b,d]}H_{[a,b]}H_{[a,c]}H_{[b,d]}X_{[c,e]}X_{[d,f]})^3 \approx H_{[c,e]}H_{[d,f]}H_{[e,f]}H_{[c,e]}H_{[d,f]}X_{[c,e]}X_{[d,f]} \tag{d4}$$

$$X_{[c,b]} \approx X_{[b,c]} \tag{e1}$$
$$H_{[c,b]} \approx X_{[b,c]}H_{[b,c]}X_{[b,c]}. \tag{e2}$$

图 6：给出的完备等式理论见 [17]。在每个方程中，所有指标必须互不相同。在方程（e1）和（e2）中，我们要求 $b < c$；在其他所有方程中，每个 H 或 X 的两个指标都必须按递增顺序排列。

$$(-1)_{[0]}^2 \approx \varepsilon \tag{a1*}$$
$$X_{[a,b]}^2 \approx \varepsilon \tag{a2}$$
$$H_{[a,b]}^2 \approx \varepsilon \tag{a3}$$

$$(-1)_{[0]}(-1)_{[1]} \approx (-1)_{[1]}(-1)_{[0]} \tag{b1*}$$
$$(-1)_{[1]}H_{[0,2]} \approx H_{[0,2]}(-1)_{[1]} \tag{b4*}$$
$$H_{[0,1]}H_{[2,3]} \approx H_{[2,3]}H_{[0,1]} \tag{b6*}$$

$$(-1)_{[a]}X_{[a,b]} \approx X_{[a,b]}(-1)_{[b]} \tag{c1}$$
$$H_{[a,c]}X_{[b,c]} \approx X_{[b,c]}H_{[a,b]} \tag{c5}$$

$$(-1)_{[b]}H_{[a,b]} \approx H_{[a,b]}X_{[a,b]} \tag{d2}$$

$$H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]} \approx H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]}H_{[0,1]} \tag{d3*}$$

$$H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]} \approx H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]} \tag{d4*}$$

$$H_{[c,b]}X_{[b,c]} \approx X_{[b,c]}H_{[b,c]} \tag{e2*}$$

图 7：更简单的等式理论，与图 6等价。在每个方程中，所有指标必须互不相同，但顺序不限。

4.1 Real-Clifford+CH 电路的表达能力

首先，回顾一下 $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 的相关生成集，它由所谓的*1* 级和 *2* 级 矩阵构成：

定义 4.1 ([1, 17])。 设 M 是一个 $m \times m$ 矩阵，设 $m < N$，且设 $0 \le a_1, ..., a_m \le N-1$。类型为 M 的 m 级矩阵是由 $M_{[a_1,...,a_m]}$ 定义的 $N \times N$ 矩阵

$$(M_{[a_1,...,a_m]})_{i,j} = \begin{cases} M_{i',j'} & \text{if } i = a_{i'} \text{ and } j = a_{j'} \\ \delta_{i,j} & \text{otherwise.} \end{cases}$$

命题 4.2 ([1])。 对于 $N \ge 1$，一个矩阵属于群 $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$，当且仅当它可以表示为由以下生成元构成的乘积

$$\mathcal{G}_N := \left\{ (-1)_{[a]}, X_{[a,b]}, H_{[a,b]} \;\middle|\; a, b \in \{0, ..., N-1\},\ a \neq b \right\}.$$

现在可以陈述 [17] 的完备性结果：

定义 4.3。 由 $\mathcal{G}_N$ 生成的自由幺半群（即 $\mathcal{G}_N$ 上的词幺半群）记作 $\mathcal{G}_N^*$。空词记作 ϵ。与字 $w = G_1 G_2 ... G_k \in \mathcal{G}_N^*$ 相关联的矩阵称为其语义，记作 $[\![w]\!] := G_1 \cdot G_2 \cdot ... \cdot G_k$。

我们将 $\approx$ 满足图 6 中方程的最小同余记作 $w_1,\ w_2 \in \mathcal{G}_N^*$。也就是说，对于任意两个字 $w_1 \approx w_2$ 当且仅当w_1，并且 w_2 可以使用图 6中的方程相互转换。

定理 4.4（$\approx$关于$\mathcal{G}_N^*$ [17]的可靠性与完备性）。设 $w_1,\ w_2 \in \mathcal{G}_N^*$。那么 $[\![w_1]\!] = [\![w_2]\!]$ 当且仅当 $w_1 \approx w_2$。

请注意，与 [17],不同，我们并未先验地要求$a < b$ 在 $X_{[a,b]}$ 或 $H_{[a,b]}$中成立，因此图6的说明中包含了额外条件；此外，方程（e1）和（e2）在此被视为公理，而在 [17] 中，它们只是快捷定义。

现在，我们可以给出刻画实 Clifford+CH 电路所张成的矩阵群所需的奇偶性条件：

引理 4.5。对于任意 $A \in U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$，在任意将 A 分解为$\mathcal{G}_N$ 中生成元之积的方式中，形如 $H_{[a,b]}$ 的生成元数量的奇偶性（形如 $(-1)_{[a]}$ 或 $X_{[a,b]}$ 的生成元数量的奇偶性）仅取决于 A。

证明。 根据定理 4.4，将 A 分解为来自 $\mathcal{G}_N$ 的生成元之积的任意两种分解，都可以使用图 6中的方程相互转换。可以验证，所有这些方程都保持以下两者的奇偶性：形如$H_{[a,b]}$的生成元数量的奇偶性，以及形如 $(-1)_{[a]}$ 或 $X_{[a,b]}$的生成元数量的奇偶性。 □

下文中，任意分解中 A 的 $H_{[a,b]}$ 数量的奇偶性将称为 A的 H-奇偶性 ，而此类分解中 $(-1)_{[a]}$ 与 $X_{[a,b]}$ 的总数量的奇偶性将称为 A的 ZX-奇偶性 。

命题 4.6。 对于 $N \geq 1$，一个矩阵属于群 $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$，且具有偶数的 ZX-奇偶性和 H-奇偶性，当且仅当它可以表示为来自

$$\mathcal{P}_N \coloneqq \left\{ \left((-1)_{[a]}(-1)_{[c]}\right), \left((-1)_{[a]}X_{[c,d]}\right), \left(X_{[a,b]}X_{[c,d]}\right), \left(H_{[a,b]}H_{[c,d]}\right) \;\middle|\; a,b,c,d \in \{0,\ldots,n-1\},\ a \neq b \wedge c \neq d \right\}.$$

证明。将 $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$中的给定元素分解为 P_N 的生成元之积的 [17] 算法，可以略作修改，使其输出仅由一串$H_{[a,b]}$ 以及随后的一串 $(-1)_{[a]}$ 和 $X_{[a,b]}$ 组成（修改后的算法见附录 A.1）。根据引理 4.5，这两串的长度均为偶数，因此我们可以分别将其中的生成元两两分组。最后，只需通过注意到以下事实来消去形如$\left(X_{[c,d]}(-1)_{[a]}\right)$的生成元对：当 $a \notin \{c,d\}$时，它在语义上等价于$\left((-1)_{[a]}X_{[c,d]}\right)$；当 $a = c$时，等价于 $\left((-1)_{[d]}X_{[c,d]}\right)$；当 $a = d$ 时，等价于 $\left((-1)_{[c]}X_{[c,d]}\right)$。 □

引理 4.7。 对于 $n = 2$，可以由 n 个量子比特的实 *Clifford+CH* 电路表示的矩阵集合恰好是 $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$。对于 $n \geq 3$，该集合是 $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 的子集，其中包含具有偶数 ZX 奇偶性和 H 奇偶性的矩阵。

证明。首先，根据语义的定义可知，任何实数-Clifford+CH 电路都表示 $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 的一个元素。

对于 $n = 2$，我们需要证明 $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 中的任意元素都可以由一个实数-Clifford+CH 电路表示。为此，只需为 $\mathcal{G}_N$ 的每个生成元给出一个具有相应语义的电路。这在定义 7.3 中完成。

对于 $n \geq 3$，同样地，只需将 $\mathcal{P}_N$ 的每个生成元表示为实 Clifford+CH 电路即可。这在定义 8.3 中完成。 □

4.2 $\mathcal{P}_N^*$ 的完整等式理论

因此，对于 $n \geq 3$，由 n 个量子比特的实 Clifford+CH 电路表示的矩阵构成 $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 的一个子群，其指数为 4。

虽然我们讨论的是群，但请注意，下面我们实际上只会使用幺半群结构。事实上，这并不会从根本上改变表示，因为所有逆元都可以由原始生成元轻松表示；而且从量子电路的角度来看，这样也更合理。

当整个群的完备等式理论已知时，可以利用 *Reidemeister-Schreier* 定理 [30, 31]这一标准技术来获得其子群的完备等式理论。该定理已被推广到幺半群（见 [6]），并用于获得 2 量子比特 Clifford+T [6] 和 3 量子比特 Clifford+CS [7] 量子电路的完备等式理论。这种技术的一个缺点是，它往往会导致组合爆炸，造成高昂的计算成本，即使是在相对简单的情形下也是如此。因此， [7] 的完备性结果仅限于 3 个量子比特，而底层矩阵群的表示先验地适用于任意维度。

我们不直接将 Reide- meister-Schreier 定理应用于 [17], 的等式理论，以试图获得实数 Clifford+CH 量子电路的完备等式理论，而是采用分两步进行的替代方法：

- 首先，我们使用 Reidemeister-Schreier 定理，得到由 P_N 生成的 $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 子幺半群的一个表示
- 然后，我们使用与 [11] 中类似的往返编码，将该表示转化为实数 Clifford+CH 电路的完备等式理论。

此外，我们在每一步之前和之后都对等式理论进行了一些简化。具体而言，我们首先对 [17] 的等式理论稍作简化；简化后的完备等式理论见图 7。

命题 4.8（图 7 中等式理论相对于 $\approx$ 的可靠性与完备性）。对于任意 $w_1,\ w_2 \in \mathcal{G}_N^*$，有 $w_1 \approx w_2$ 当且仅当 w_1 和 w_2 可以使用图 7 中的方程相互转换。换言之，$\approx$ 是满足图 7 中关系的最小同余。

证明。 可以验证，图 7 中的方程在语义上是正确的。因此，根据定理 4.4，它们可以由图 6中的方程推导得出。反过来，仍需证明图 6 中的方程可以由图 7中的方程推导得出。这将在附录 A.2中完成。 □

关于我们如何使用 Reidemeister-Schreier 定理的详细说明见附录 A.3.1。应用 Reidemeister-Schreier 定理得到的原始完备等式理论见附录A.3.2。请注意，其中包含许多方程，这些方程

未必适合下一步使用第 8 节中定义的解码函数进行转换；因此，在进行往返编码之前，我们先将该等式理论简化为一个较小的理论，如图 8 所示。图 8中的等式理论从人类读者的角度来看其实并非最简形式（尽管它比附录 A.3.2 中的理论简单得多），但经过优化，以便简化解码步骤。

这给出了如下完备性结果：

定义4.9。 由$\mathcal{P}_N$生成的自由幺半群（即$\mathcal{P}_N$上的词幺半群）记为$\mathcal{P}_N^*$。空词记为 ϵ。与字 $w = P_1P_2...P_k \in \mathcal{P}_N^*$相关联的矩阵称为其语义，并记为 $[\![w]\!] := P_1 \cdot P_2 \cdot ... \cdot P_k$。

我们用 $\approx$ 表示满足图8中方程的最小同余。也就是说，对于任意两个字 w_1， $w_2 \in \mathcal{P}_N^*$，有 $w_1 \approx w_2$ 当且仅当w_1 与 w_2 可以通过图8中的方程相互变换。

定理 4.10（$\approx$ 对$\mathcal{P}_N^*$的可靠性与完备性）。设w_1， $w_2 \in \mathcal{P}_N^*$，且 $N \geq 8$。则 $[\![w_1]\!] = [\![w_2]\!]$ 当且仅当 $w_1 \approx w_2$。

证明。 为证明可靠性，只需验证图 8 中的所有方程均保持语义。完备性的证明见附录 A.3 和 A.4。 □

5 多重受控门的辅助方程/性质

类似于 [11],，针对 Real-Clifford+CH 电路、借助第 7 节和第 8 节所述来回编码技术而朴素得到的完备等式理论，主要由涉及大量（可能无界）多重受控门的方程构成。本文的主要贡献之一，是从如图 4 所示的简单得多的等式理论推导出这些方程。为此，我们将依赖辅助方程，这些辅助方程由图 4 在附录 B 和 D 中的相应方程推导得到。请注意，如同 [11], 中那样，多重受控门的基本性质起着关键作用。

特别地，可以看出 [11],中所用的主要辅助性质，即单个多受控门的不同控制位作用相同，因而可以交换（方程 (307)、(313) 和 (353)）；正控制门可以与同一门的负控制版本合并（方程 (309)、(310) 和 (354)）；并且正控制门总是与由同一量子比特负控制的门对易（方程 (335) 至 (352)）。方程 (311)、(312)、(317) 和 (355) 可视为 [11] 的可加性与周期性性质的类似形式。

其他值得注意的辅助方程更具体地适用于实数 Clifford+ +CH 片段，尤其包括这样一个事实：多重控制 Z和 H量子门的虚线框确实仅表现为一条恒等线（方程（274）和（277），以及引理 D.9 和 D.11，还有此前在引理 D.8中证明的各种特殊情形）。

注 4。可以证明，方程 (19) 尤其可以从方程 (272) 或从方程 (274)推导得出。因此，方程 (272)和 (274) 是两个可相互替代的公理模式，每个都可以替代方程 (19) 加入图 4中的等式理论，而不会影响其完备性。

注 5. 特别地，方程 (272) 的四量子比特情形是显然的，因为它可由拓扑规则推出。因此，方程 (19) 的四量子比特情形可由其他方程推导出来（见附录 (154) 中的方程 D.3）。这在一定程度上解释了一个或许令人惊讶的事实：图 4 的等式理论不包含任何针对四个量子比特的公理。

请注意，在完备性的证明中，我们实际上将分别证明每个 n量子比特电路的完备性。因此，我们也可以对 n 进行归纳推理 n （基例由引理 7.1 和 7.6给出）。这不会改变完备性证明本身的做法，但有助于证明辅助方程。这可以表述为我们可以使用以下引理：

引理 5.1（完备性证明的归纳假设）。对于任意实 *Clifford+CH* 电路 C_1， C_2，若 $[\![C_1]\!] = [\![C_2]\!]$ 则$\mathbf{QC} \vdash (\otimes C_1) = (\otimes C_2)$ 且$\mathbf{QC} \vdash (C_1 \otimes) = (C_2 \otimes)$。

6 序列化电路范畴

正如我们所说，完备性的证明将基于一种往返翻译，类似于 [11], 实 Clifford+CH 电路的 PROP 与幺半群 $\mathcal{G}_N^*$ 和$\mathcal{P}_N^*$之间的翻译。然而，实 Clifford+CH 电路具有更丰富的结构：它们不仅构成幺半群（对每个特定数量的量子比特而言），这对应于图 1 中的方程（a）和（b），1；它们还满足 PROP 的其他相干关系。因此，我们不能直接将电路编码为字，因为这些关系无法得到保留，编码也就定义不良。相反，我们将使用所谓的序列化电路，即范畴$\mathbf{QC}^{\mathbf{seq}}$ 中的元素；该范畴由原始电路构成，并仅对方程（a）和（b）取商。

通常实数-克利福德**量子电路**PROP+的通常实数-克利福德 +CH 电路，可通过对剩余拓扑规则取商得到，即方程 (c) 至 (g)。[6] 给定一个序列化电路 $C \in \mathbf{QC}^{\mathbf{seq}}$，我们将其经由典范投影映射到 $|C|$ 上的像记为$\mathbf{QC}$。反过来，任意电路 $C \in \mathbf{QC}$ 都有多个代表元 C' 属于 $\mathbf{QC}^{\mathbf{seq}}$，并满足 $|C'| = C$。

现在我们已经准备好证明本文的主要结果。具体如下：首先，在第 7.1 节中，我们利用标准形证明单量子比特电路的完备性，这很容易做到；然后，在第 $\mathcal{G}_4^*$ 节中，通过往返编码到 7.2，我们证明双量子比特电路的完备性。最后，在第 $n \geq 3$ 节中，通过往返编码到 $\mathcal{P}_{2^n}^*$，我们证明作用于 8 个量子比特的电路的完备性。请注意，尽管编码函数需要定义在序列化电路上，解码函数却可以直接定义到 PROP $\mathbf{QC}$ 中。

[6]更确切地说，对方程 (c) 至 (g) 的变体取商，这些变体是根据典范投影 $\mathbf{QC}_{\mathbf{raw}} \to \mathbf{QC}_{\mathbf{raw}}/\{(a),(b)\}$，分别投影每个方程两边而得到的。

$$((-1)_{[a]}(-1)_{[a]}) \approx \epsilon \quad (20)((-1)_{[a]}(-1)_{[b]}) \approx ((-1)_{[b]}(-1)_{[a]}) \quad (21)((-1)_{[a]}(-1)_{[b]})\,((-1)_{[b]}(-1)_{[c]}) \approx ((-1)_{[a]}(-1)_{[c]}) \quad (22)((-1)_{[a]}(-1)_{[a+1]}) \approx ((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[a]}X_{[a,a+1]}) \quad (23)$$

$$((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[a+1]}X_{[a+1,a+2]})\,((-1)_{[a]}X_{[a,a+1]}) \approx ((-1)_{[a+1]}X_{[a+1,a+2]})\,((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[a+1]}X_{[a+1,a+2]}) \quad (24)((-1)_{[a]}X_{[a,c]}) \approx ((-1)_{[a+1]}X_{[a,a+1]})\,((-1)_{[a+1]}X_{[a+1,c]})\,((-1)_{[a]}X_{[a,a+1]}) \quad a+1<c,\ c-a\text{奇数} \quad (25)((-1)_{[c]}X_{[a,c]}) \approx ((-1)_{[a+1]}X_{[a,a+1]})\,((-1)_{[c]}X_{[a+1,c]})\,((-1)_{[a]}X_{[a,a+1]}) \quad a+1<c,\ c-a\text{奇数} \quad (26)((-1)_{[a]}X_{[a,c]}) \approx ((-1)_{[c-1]}X_{[c-1,c]})\,((-1)_{[a]}X_{[a,c-1]})\,((-1)_{[c]}X_{[c-1,c]}) \quad a+1<c,\ c-a\text{偶数} \quad (27)((-1)_{[c]}X_{[a,c]}) \approx ((-1)_{[c-1]}X_{[c-1,c]})\,((-1)_{[c-1]}X_{[a,c-1]})\,((-1)_{[c]}X_{[c-1,c]}) \quad a+1<c,\ c-a\text{偶数} \quad (28)((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[a+1]}X_{[a,a+1]}) \approx \epsilon \quad (29)((-1)_{[c]}X_{[a,b]}) \approx ((-1)_{[c]}(-1)_{[a]})\,((-1)_{[a]}X_{[a,b]}) \quad c \neq a,\ b \quad (30)((-1)_{[a+1]}(-1)_{[c]})\,((-1)_{[a]}X_{[a,a+1]}) \approx ((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[a]}(-1)_{[c]}) \quad c \neq a,\ a+1 \quad (31)((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[b]}X_{[b,b+1]}) \approx ((-1)_{[b]}X_{[b,b+1]})\,((-1)_{[a]}X_{[a,a+1]}) \quad a+1<b \quad (32)((-1)_{[b]}X_{[a,b]}) \approx ((-1)_{[b]}X_{[b,a]}) \quad (33)(X_{[a,b]}X_{[c,d]}) \approx ((-1)_{[a]}X_{[a,b]})\,((-1)_{[b]}X_{[c,d]}) \quad (34)(H_{[a,b]}H_{[c,d]}) \approx \Sigma_{a,\ b,\ c,\ d} \circ (H_{[0,1]}H_{[3,2]}) \circ \Sigma'_{a,\ b,\ c,\ d}\text{见图注} \quad (35)(H_{[a,b]}H_{[c,d]}) \approx \mathsf{W}_1\text{见图注} \quad (36)(H_{[a,b]}H_{[c,d]}) \approx \mathsf{W}_2\text{见图注} \quad (37)((-1)_{[a]}X_{[a,a+1]})\,(H_{[0,1]}H_{[3,2]}) \approx (H_{[0,1]}H_{[3,2]})\,((-1)_{[a]}X_{[a,a+1]}) \quad a \geq 4 \quad (38)((-1)_{[0]}(-1)_{[1]})\,(H_{[0,1]}H_{[3,2]}) \approx (H_{[0,1]}H_{[3,2]})\,((-1)_{[0]}(-1)_{[1]}) \quad (39)((-1)_{[3]}(-1)_{[4]})\,(H_{[0,1]}H_{[3,2]}) \approx (H_{[0,1]}H_{[3,2]})\,((-1)_{[3]}(-1)_{[4]})\,((-1)_{[2]}X_{[2,3]}) \quad (40)(H_{[0,1]}H_{[3,2]})\,(H_{[0,1]}H_{[3,2]}) \approx \epsilon \quad (41)(H_{[a,b]}H_{[e,f]})\,(H_{[e,f]}H_{[c,d]}) \approx (H_{[a,b]}H_{[c,d]})\text{见图注} \quad (42)$$

$$(H_{[0,1]}H_{[3,2]})\,(H_{[3,2]}H_{[4,5]}) \approx (X_{[0,3]}X_{[1,2]})\,(H_{[3,2]}H_{[4,5]})\,(X_{[0,3]}X_{[1,2]}) \quad (43)(X_{[0,3]}X_{[1,2]})\,(H_{[0,1]}H_{[3,2]}) \approx (H_{[0,1]}H_{[3,2]})\,(X_{[0,3]}X_{[1,2]}) \quad (44)$$

$$(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)_{[0]}(-1)_{[1]})\,(H_{[0,3]}H_{[1,2]}) \approx (H_{[0,3]}H_{[1,2]})\,((-1)_{[0]}(-1)_{[1]})\,(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})$$

$$(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[3,2]}H_{[4,5]})\,(H_{[7,6]}H_{[4,5]})\,((-1)_{[2]}(-1)_{[3]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]}) \approx (H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)_{[2]}(-1)_{[3]})\,(H_{[7,6]}H_{[4,5]})\,(H_{[3,2]}H_{[4,5]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})$$

(45)

(46)

图 8：当维度至少为 8 时，这个更简单的等式理论与附录 A.3.2 中的等式理论等价（因此是完备的）。在公式 (36) 中，我们要求元组 $(G_n(a)\ G_n(b)\ G_n(c)\ G_n(d))$ 具有形式 $(x0y0z, x1y0z, x0y1z, x1y1z)$，其中 x、y、z 是某些比特串；在公式 (37) 中，我们要求它具有形式 $(x0y0z, x0y1z, x1y0z, x1y1z)$；在方程 (35) 中，我们要求它不具有这两种形式中的任何一种。Σ_a、$_b$、$_c$、$_d$ 和 Σ'_a、$_b$、$_c$、$_d$ 在定义 8.3 中定义。在方程（42）中，我们要求 $|\{a,b,c,d\}| \leq 3$，并且 $e < f$ 是 $\{0,\ldots,2^n-1\} \setminus \{a,b,c,d\}$ 中最小的两个元素。公式（36）和（37）的右侧是专门设计的字，旨在使其在解码时表现良好（参见定义 8.3 和 2.4 以及附录 E.5）；它们在附录 A.4.1 中定义。

7 单量子比特和双量子比特完备性

7.1 单量子比特完备性

引理 7.1（单量子比特完备性）。对于任意作用于 $\{\square, \bullet\}$ 上的单量子比特量子电路 $C_1 \multimap C_2$，如果 $[\![C_1]\!] = [\![C_2]\!]$，那么 $\mathrm{QC} \vdash C_1 = C_2$。

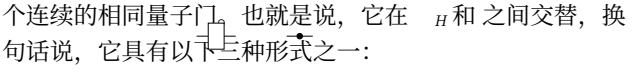
证明。我们称一个单量子比特电路为规范形，如果它具有以下形式

$$\left(-\boxed{H}\!\bullet-\right)^k \qquad \text{or} \qquad -\boxed{H}- \circ \left(-\boxed{H}\!\bullet-\right)^k$$

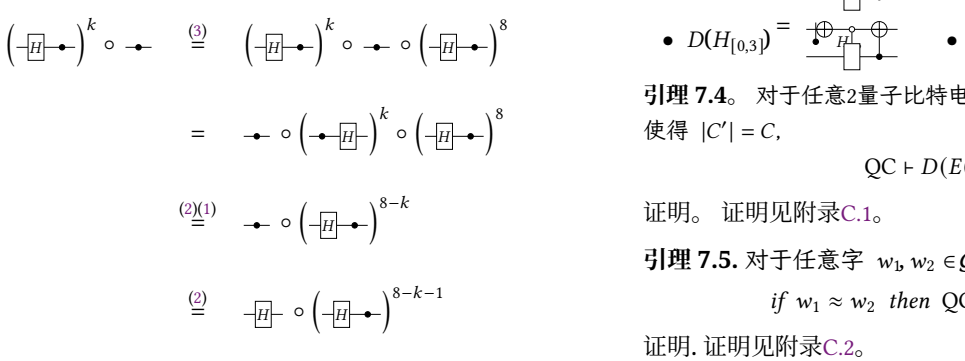
其中 $k \in \{0、\ldots\ldots、7\}$。

通过直接计算可以验证，如果两个标准形式电路具有相同的语义，那么它们相等。因此，还需证明任意单量子比特电路都可以化为标准形。

注意，单量子比特电路只是由 H 和量子门组 $\mathbb{T}$ 的序列。通过反复应用方程（1）和（2），我们可以确保其中不包含两个连续的相同量子门。也就是说，它在 H 和 之间交替，换句话说，它具有以下三种形式之一：



通过应用方程（3）$\lfloor \frac{k}{8} \rfloor$次，我们可以确保 $k \in \{0, \ldots, 7\}$。因此，如果电路属于前两种形式之一，那么它就是标准形。如果它属于第三种形式，那么我们进行如下变换：



由此得到一个标准形电路。 □

7.2 双量子比特完备性

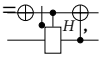
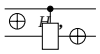
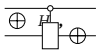
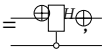
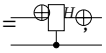
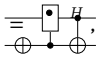
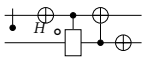
定义 7.2（双量子比特编码）。令 $E : \mathbf{QC}_{\mathbf{seq}}^{(2)} \to \mathcal{G}_4^*$ 定义如下：对于任意2量子比特序列化电路 C，令 $E(C) = E_{0,0}(C)$，其中 $E_{k,\ell}$ 定义在满足 $k + m + \ell = 2$ 的任意 m量子比特序列化电路上，归纳定义如下：

- $E_{k,\ell}(C_1 \otimes C_2) = E_{k+n_1,\ell}(C_2) \circ E_{k,\ell+n_2}(C_1)$, *where* C_1 *(resp.* C_2*) is acting on* n_1 *(resp.* n_2*) qubits;*
- $E_{k,\ell}(C_2 \circ C_1) = E_{k,\ell}(C_2) \circ E_{k,\ell}(C_1)$;

以及生成元：

- $E_{k,\ell}(\,\vdots\,) = \epsilon$,
- $E_{k,\ell}(\text{——}) = \epsilon$,
- $E_{0,0}(\times) = X_{[1,2]}$,
- $E_{1,0}(-H-) = H_{[0,1]}H_{[2,3]}$,
- $E_{0,1}(-H-) = H_{[0,2]}H_{[1,3]}$,
- $E_{1,0}(\bullet) = (-1)_{[1]}(-1)_{[3]}$,
- $E_{0,1}(\bullet) = (-1)_{[2]}(-1)_{[3]}$,
- $E_{0,0}(\,\vdots\,) = (-1)_{[3]}$,
- $E_{0,0}(\,\vdots\,H) = H_{[2,3]}$.

定义 7.3（双量子比特解码）。令 $D: \mathcal{G}_4^* \to \mathbf{QC}^{(2)}$ 为如下定义在生成元上的幺半群同态：

- $D((-1)_{[0]}) =$  ,
- $D((-1)_{[1]}) =$  ,
- $D((-1)_{[2]}) =$  ,
- $D((-1)_{[3]}) =$  ,
- $D(X_{[2,3]}) = D(X_{[3,2]}) =$  ,
- $D(X_{[0,1]}) = D(X_{[1,0]}) =$  ,
- $D(X_{[0,2]}) = D(X_{[2,0]}) =$  ,
- $D(X_{[1,3]}) = D(X_{[3,1]}) =$  ,
- $D(X_{[1,2]}) = D(X_{[2,1]}) =$  ,
- $D(X_{[0,3]}) = D(X_{[3,0]}) =$  ,
- $D(H_{[2,3]}) =$ 
- $D(H_{[0,1]}) =$ 
- $D(H_{[0,2]}) =$ 
- $D(H_{[1,3]}) =$ 
- $D\left(H_{[2,1]}\right) =$ 
- $D(H_{[0,3]}) =$
- $D(H_{[3,2]}) =$ 
- $D(H_{[1,0]}) =$ 
- $D(H_{[2,0]}) =$ 
- $D(H_{[3,1]}) =$ 
- $D\left(H_{[1,2]}\right) =$ 
- $D(H_{[3,0]}) =$ 

引理 7.4。对于任意2量子比特电路 C，以及任意序列化电路 C'，使得 $|C'| = C$，

$$\mathrm{QC} \vdash D(E(C')) = C.$$

证明。 证明见附录C.1。 □

引理 7.5. 对于任意字 $w_1, w_2 \in \mathcal{G}_4^*$，

$$\textit{if } w_1 \approx w_2 \textit{ then } \mathrm{QC} \vdash D(w_1) = D(w_2).$$

证明. 证明见附录C.2。 □

引理 7.6（双量子比特完备性）。对于任意两个量子比特的实 *Clifford+CH* 量子电路 C_1, C_2，

$$\textit{if } [\![C_1]\!] = [\![C_2]\!] \textit{ then } \mathrm{QC} \vdash C_1 = C_2.$$

证明。设 C_1', C_2' 是 $\mathrm{QC}_{\mathbf{seq}}^{(2)}$ 中分别代表 C_1 和 C_2 的代表元，因此 $|C_1'| = C_1$ 且 $|C_2'| = C_2$。由于 $[\![C_1]\!] = [\![C_2]\!]$ 且编码保留语义，可得 $[\![E(C_1')]\!] = [\![E(C_1')]\!]$。因此，根据定理 4.4，可得 $E(C_1') \approx E(C_2')$。由引理 7.5 可知，这意味着 $\mathrm{QC} \vdash D(E(C_1')) = D(E(C_2'))$。进而，由引理 7.4 可知，这意味着 $\mathrm{QC} \vdash C_1 = C_2$。 □

8 一般情形下的完备性

为了定义 n量子比特电路与表示 2^n维矩阵的$\mathbb{P}_{2^n}$ 元素之间的往返编码，像在 [11], 中那样，将整数$0, \ldots\ldots 2^n - 1$编码为长度为 n的比特串会很有帮助；这里不使用通常的二进制编码，而是使用格雷码，其优点是两个连续整数的编码始终恰好相差一个比特：

定义8.1（格雷码 [11]）。整数 $k \in \{0, \ldots, 2^n - 1\}$ 的 n 比特格雷码是字 $G_n(k) \in \{0, 1\}^n$，归纳定义为 $G_0(0) = \epsilon$ 和

$$G_n(k) = \begin{cases} 0G_{n-1}(k) & \textit{if } k < 2^{n-1}, \\ 1G_{n-1}(2^n - 1 - k) & \textit{if } k \geq 2^{n-1}. \end{cases}$$

容易验证， $G_n: \{0, ..., 2^n - 1\} \to \{0,1\}^n$ 是一个双射。

定义 8.2（编码）。对于任意 $n \geq 3$，令 E： $\mathbf{QC}^{\mathbf{seq}} \to \mathcal{P}_{2^n}^*$ 定义如下：对于任意 n-量子比特序列化电路 C，令 $E(C) = E_{0,0}(C)$，其中 $E_{k,\ell}$ 定义在满足 $k + m + \ell = n$ 的任意 m-量子比特序列化电路上，并归纳定义如下（乘积的顺序未予指定，因为这不会影响证明）：

- $E_{k,\ell}(C_1 \otimes C_2) = E_{k+n_1,\ell}(C_2) \circ E_{k,\ell+n_2}(C_1)$，其中 C_1（分别为 C_2）作用于 n_1（分别为 n_2）个量子比特；
- $E_{k,\ell}(C_2 \circ C_1) = E_{k,\ell}(C_2) \circ E_{k,\ell}(C_1)$；
- $E_{k,\ell}($  $) = \epsilon$；
- $E_{k,\ell}($  $) = \epsilon$；

若 $\ell \geq 1$，则

- $E_{k,\ell}($  $) = \prod_{x \in \{0,1\}^k} \{\}_{y \in \{0,1\}^{\ell-1}} \left((-1)_{[G_n^{-1}(x10y)]} (-1)_{[G_n^{-1}(x11y)]} \right)$；
- $E_{k,\ell}($ $) = \prod_{x \in \{0,1\}^k} \{\}_{y \in \{0,1\}^{\ell-1}} \left((-1)_{[G_n^{-1}(x110y)]} (-1)_{[G_n^{-1}(x111y)]} \right)$；
- $E_{k,\ell}($  $) = \prod_{x \in \{0,1\}^k} \{\}_{y \in \{0,1\}^{\ell-1}} \left(H_{[G_n^{-1}(x00y)\, G_n^{-1}(x10y)]} H_{[G_n^{-1}(x01y)\, G_n^{-1}(x11y)]} \right)$；
- $E_{k,\ell}($  $) = \prod_{x \in \{0,1\}^k} \{\}_{y \in \{0,1\}^{\ell-1}} \left(H_{[G_n^{-1}(x100y)\, G_n^{-1}(x110y)]} H_{[G_n^{-1}(x101y)\, G_n^{-1}(x111y)]} \right)$；

并且如果 $\ell = 0$（注意，由于条件 $k + m + \ell = n$，在这种情况下我们必然有 $k \geq 1$），那么

- $E_{k,0}($  $) = \prod_{x \in \{0,1\}^{k-1}} \left((-1)_{[G_n^{-1}(0x1)]} (-1)_{[G_n^{-1}(1x1)]} \right)$；
- $E_{k,0}($ $) = \prod_{x \in \{0,1\}^{k-1}} \left((-1)_{[G_n^{-1}(0x11)]} (-1)_{[G_n^{-1}(1x11)]} \right)$；
- $E_{k,0}($ $) = \prod_{x \in \{0,1\}^{k-1}} \left(H_{[G_n^{-1}(0x0), G_n^{-1}(0x1)]} H_{[G_n^{-1}(1x0), G_n^{-1}(1x1)]} \right)$；
- $E_{k,0}($ $) = \prod_{x \in \{0,1\}^{k-1}} \left(H_{[G_n^{-1}(0x10), G_n^{-1}(0x11)]} H_{[G_n^{-1}(1x10), G_n^{-1}(1x11)]} \right)$；

最后，对于任意 $\ell \geq 0$，

- $E_{k,\ell}($  $) = E_{k,\ell}($  $) \circ$

$$\prod_{\substack{x \in \{0,1\}^k \\ y \in \{0,1\}^\ell}} \left((-1)_{[G_n^{-1}(x11y)]} X_{[G_n^{-1}(x10y), G_n^{-1}(x11y)]} \right) \circ$$

$$\prod_{\substack{x \in \{0,1\}^k \\ y \in \{0,1\}^\ell}} \left((-1)_{[G_n^{-1}(x01y)]} X_{[G_n^{-1}(x01y), G_n^{-1}(x11y)]} \right) \circ$$

$$\prod_{\substack{x \in \{0,1\}^k \\ y \in \{0,1\}^\ell}} \left((-1)_{[G_n^{-1}(x11y)]} X_{[G_n^{-1}(x10y), G_n^{-1}(x11y)]} \right).$$

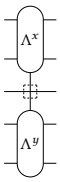
定义 8.3（解码）。对于任意 $n \geq 3$，令 D： $\mathcal{P}_{2^n}^* \to \mathbf{QC}$ 为由下列生成元上的定义所确定的幺半群同态：

($(-1)_{[a]}$ $(-1)_{[b]}$) 的情况。

- 对于任意 $a \in \{0, ..., 2^n - 1\}$，我们定义

$$D((-1)_{[a]}(-1)_{[a]}) \coloneqq (\text{———})^{\otimes n}.$$

- 对于任意 $a \in \{0, ..., 2^n - 2\}$，我们定义

$$D\left((-1)_{[a]}(-1)_{[a+1]}\right) \coloneqq$$ 

其中 $\beta \in \{0, 1\}$， $x \in \{0, 1\}^k$，以及 $y \in \{0, 1\}^{n-k-1}$ 满足 $G_n(a) = x\beta y$ 且 $G_n(a+1) = x\bar{\beta}y$.[7]

- 如果 $a \leq b$，那么我们定义[8]

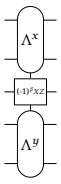
$$D\left((-1)_{[a]}(-1)_{[b]}\right) \coloneqq \overleftarrow{\prod_{k=a}^{b-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right)$$

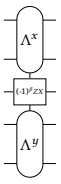
这里我们使用如下记号 $\overleftarrow{\prod_{k=n}^{m}} C_k \coloneqq C_m \circ \cdots \circ C_n$ 以及 $\overrightarrow{\prod_{k=n}^{m}} C_k \coloneqq C_n \circ \cdots \circ C_m$，约定当乘积为空时，其值为单位元（即当 $m < n$ 时）。

- 最后，如果 $a > b$，我们定义 $D\left((-1)_{[a]}(-1)_{[b]}\right) \coloneqq D\left((-1)_{[b]}(-1)_{[a]}\right)$。

$\left((-1)_{[c]}X_{[a,b]}\right)$的情形。

- 对于任意 $a \in \{0, ..., 2^n - 2\}$，我们定义

$D\left((-1)_{[a]}X_{[a,a+1]}\right) \coloneqq$ 

， $D\left((-1)_{[a+1]}X_{[a,a+1]}\right) \coloneqq$ 

其中 $\beta \in \{0、1\}$、 $x \in \{0、1\}^k$ 和 $y \in \{0、1\}^{n-k-1}$ 满足 $G_n(a) = x\beta y$ 以及 $G_n(a+1) = x\bar{\beta}y$。

- 如果 $a < b$，则我们在 $b - a$ 上进行归纳定义（以前一种情况作为基础情形）：
  - *if $b - a$ is odd,* $D\left((-1)_{[a]}X_{[a,b]}\right) \coloneqq D\left((-1)_{[a+1]}X_{[a,a+1]}\right) \circ D\left((-1)_{[a+1]}X_{[a+1,b]}\right) \circ D\left((-1)_{[a]}X_{[a,a+1]}\right)$

and $D\left((-1)_{[b]}X_{[a,b]}\right) \coloneqq D\left((-1)_{[a+1]}X_{[a,a+1]}\right) \circ D\left((-1)_{[b]}X_{[a+1,b]}\right) \circ D\left((-1)_{[a]}X_{[a,a+1]}\right)$;

  - *if $b - a$ is even,* $D\left((-1)_{[a]}X_{[a,b]}\right) \coloneqq D\left((-1)_{[b-1]}X_{[b-1,b]}\right) \circ D\left((-1)_{[a]}X_{[a,b-1]}\right) \circ D\left((-1)_{[b]}X_{[b-1,b]}\right)$

and $D\left((-1)_{[b]}X_{[a,b]}\right) \coloneqq D\left((-1)_{[b-1]}X_{[b-1,b]}\right) \circ D\left((-1)_{[b-1]}X_{[a,b-1]}\right) \circ D\left((-1)_{[b]}X_{[b-1,b]}\right)$.

- 如果 $a > b$，则我们定义

$$D\left((-1)_{[a]}X_{[a,b]}\right) \coloneqq D\left((-1)_{[a]}X_{[b,a]}\right),$$
$$D\left((-1)_{[b]}X_{[a,b]}\right) \coloneqq D\left((-1)_{[b]}X_{[b,a]}\right).$$

[7] β， x， y 根据格雷码的性质，它们必然存在。[8] 请注意，当 $b = a + 1$ 时，该定义是一致的。

- 最后，如果 $c \neq a$、b，则我们定义[9]

$$D\left((-1)_{[c]}X_{[a,b]}\right) \coloneqq D\left((-1)_{[c]}(-1)_{[a]}\right) \circ D\left((-1)_{[a]}X_{[a,b]}\right).$$

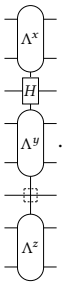
当 $(X_{[a,b]}X_{[c,d]})$.对于任意 a, b, c, d，满足 $a \neq b$且 $c \neq d$，我们定义

$$D\left(X_{[a,b]}X_{[c,d]}\right) \coloneqq D\left((-1)_{[a]}X_{[a,b]}\right) \circ D\left((-1)_{[b]}X_{[c,d]}\right).$$

情形 $\left(H_{[a,b]}H_{[c,d]}\right)$。

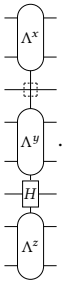
- 如果存在 x, y, z，使得 $G_n(a) = x0y0z$, $G_n(b) = x1y0z$,$G_n(c) = x0y1z$，且 $G_n(d) = x1y1z$，那么我们定义

$$D\left(H_{[a,b]}H_{[c,d]}\right) \coloneqq$$



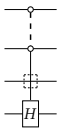
- 如果存在 x, y, z，使得 $G_n(a) = x0y0z$, $G_n(b) = x0y1z$,$G_n(c) = x1y0z$，且 $G_n(d) = x1y1z$，那么我们定义

$$D\left(H_{[a,b]}H_{[c,d]}\right) \coloneqq$$



- 在其他满足 $|\{a, b, c, d\}| = 4$ 的情形中，我们定义：

$$D\left(H_{[a,b]}H_{[c,d]}\right) \coloneqq D(\Sigma_{a,b,c,d}) \circ$$



$\circ\, D(\Sigma'_{a,b,c,d})$

其中 $\Sigma_{a,b,c,d}$ 和 $\Sigma'_{a,b,c,d}$ 是 $\mathcal{P}_N$ 上的字，且不包含任何形式为 $\left(H_{[e,f]}H_{[g,h]}\right)$ 的生成元，并且 $\left[\!\left[\Sigma'_{a,b,c,d}\right]\!\right] = \left[\!\left[\Sigma_{a,b,c,d}\right]\!\right]^{-1}$

并且以下二者之一成立：$[\![\Sigma_{a,b,c,d}]\!] = \sigma$ 或 $[\![\Sigma_{a,b,c,d}]\!] = \sigma \circ [\![(-1)_{[\mu]}]\!]$，其中 $\mu \notin \{0, 1, 3, 2\}$，$\sigma$ 是一个置换矩阵，分别将 $|0\rangle$ $|1\rangle$ $|3\rangle$ $|2\rangle$ 映射到 $|a\rangle$ $|b\rangle$ $|c\rangle$ $|d\rangle$。

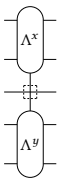
注意，$\Sigma_{a、b、c、d}$ 和 $\Sigma'_{a、b、c、d}$ 的精确定义在证明中并不重要。不过，附录 *E.1* 中给出了可能定义的一个示例

- 最后，如果 $|\{a, b, c, d\}| < 4$，那么我们定义 $D\left(H_{[a,b]}H_{[c,d]}\right)$:=$D\left(H_{[a,b]}H_{[e,f]}\right) \circ D\left(H_{[e,f]}H_{[c,d]}\right)$，其中 e、f $with$ $e < f$ 是 $\{0, \ldots, 2^n - 1\} \setminus a$、$b$、$c$、$d\}$ 中最小的两个元素。

[9] ~~注意，由于 D~~ $((-1)_{[a]}(-1)_{[a]})$ 被定义为单位元，因此即使 $a = c$ 或 $a = d$，等式仍然成立。

引理 8.4。对于任意比特串 $x \in \{0、1\}^k$ 和 $y \in \{0、1\}^\ell$，满足 k、$\ell \geq 0$ 和 $k + \ell = n - 1$,

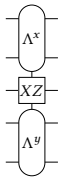
$$\mathrm{QC} \vdash D\left((-1)_{[G_n^{-1}(x0y)]}(-1)_{[G_n^{-1}(x1y)]}\right) =$$



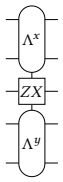
证明。证明见附录 E.2。 □

引理 8.5。对于任意比特串 $x \in \{0、1\}^k$ 和 $y \in \{0、1\}^\ell$，满足k、$\ell \geq 0$ 和 $k + \ell = n - 1$,

$$\mathrm{QC} \vdash D\left((-1)_{[G_n^{-1}(x0y)]}X_{[G_n^{-1}(x0y),G_n^{-1}(x1y)]}\right) =$$



$$\mathrm{QC} \vdash D\left((-1)_{[G_n^{-1}(x1y)]}X_{[G_n^{-1}(x0y),G_n^{-1}(x1y)]}\right) =$$



证明。证明见附录 E.3。 □

引理 8.6。对于任意 n量子比特电路 $C \in \mathbf{QC}$、任意 $C' \in \mathbf{QC^{seq}}$ 使得 $|C'| = C$，以及任意 k、ℓ使得 $k + n + \ell \geq 3$,

$$\mathrm{QC} \vdash D(E_{k,\ell}(C')) = id_k \otimes C \otimes id_\ell.$$

证明。证明见附录 E.4。 □

引理 8.7。对于任意满足 $n \geq 3$ 的 n 量子比特电路 $C \in \mathbf{QC}$，以及任意满足 $|C'| = C$ 的$C' \in \mathbf{QC^{seq}}$，

$$\mathrm{QC} \vdash D(E(C')) = C.$$

证明。这可由引理8.6直接得出。 □

引理 8.8。对于任意满足 $n \geq 3$ 的 w_1、$w_2 \in \mathcal{P}^*_{2^n}$，

$$if\ w_1 \approx w_2\ \ then\ \ \mathrm{QC} \vdash D(w_1) = D(w_2).$$

证明。证明见附录 E.5。 □

，**定理 8.9（完备性）**。对于任意电路 C_1，$C_2 \in \mathbf{QC}$,

$$if [\![C_1]\!] = [\![C_2]\!]\ then\ \mathrm{QC} \vdash C_1 = C_2.$$

证明。令 C_1，C_2 为满足 $[\![C_1]\!] = [\![C_2]\!]$ 的 n 量子比特电路。

若 $n = 0$，则结论显然成立，因为它⬚唯一的0量子比特电路。若 $n = 1$ 或 $n = 2$，则结论分别由引理7.1 和7.6 给出。

若 $n \geq 3$，令 C'_1, C'_2 为 $\mathbf{QC^{seq}}$ 中分别代表 C_1 和 C_2 的代表元，使得 $|C'_1| = C_1$ 和 $|C'_2| = C_2$。由于 $[\![C_1]\!] = [\![C_2]\!]$ 且编码保留语义，因此有 $[\![E(C'_1)]\!] = [\![E(C'_1)]\!]$。于是，根据定理 4.10，有 $E(C'_1) \approx E(C'_2)$。根据引理 8.8，这意味着 $\mathrm{QC} \vdash D(E(C'_1)) = D(E(C'_2))$。进而，根据引理 8.7，这意味着 $\mathrm{QC} \vdash C_1 = C_2$。 □

9 结论与展望

我们为门集 $\left\{ \square, , , \begin{smallmatrix}\bullet\\ \square\end{smallmatrix} \right\}$ 上的酉量子电路提出了一套完备等式理论。据我们所知，这是第三个获得完备公理化的酉量子电路通用片段，也是第一个有限生成的通用片段。值得注意的是，我们的完备等式理论与 [9],的等式理论颇为相似，后者已被证明是最小的：两种等式理论都由若干个简单方程组成，这些方程至多涉及 3个量子比特，此外还包含一个方程模式，其中每种量子比特数量对应一个方程；在这两种情形下，该方程模式都有平凡的语义解释，其意义在于多受控门是由 1 个和 2 个量子比特门构成的宏。我们的等式理论与 [9] 的等式理论有一点不同：由于我们采用离散设置，因此无需处理连续参数。

未来工作的一个显而易见的问题是，方程（19）中的无界方程模式是否确有必要，或者能否由有限个方程推导得出。若是后一种情况，就需要找到它的推导；若是前一种情况，则需要找到论证来证明其必要性。请注意， [9]中使用的必要性论证并不适用于我们的情况。

我们的结果针对的是不含辅助量子比特的酉电路。可以按照 [10] 中的方法，将等式理论及其完备性扩展到包含量子比特初始化、辅助量子比特和量子比特丢弃（即偏迹）的电路。如果方程（19）最终被证明在酉情形下是必要的，那么另一个尚待解决的问题是，在存在辅助量子比特时能否推导出该方程，类似于 [9, 10] 中的做法。

另一个开放问题是为量子电路的其他相关片段寻找完备等式理论。具体而言，原则上可以按照本文采用的相同方法，利用分别见于 [27] 和 [5]的相应矩阵群表示，为 Toffoli-Hadamard 和 Clifford+CS 片段导出完备等式理论。若要对 Clifford+T 采用同样的方法，则首先需要将 [18] 的表示扩展到任意维度。

致谢

本研究部分由法国国家研究署（ANR）资助，资助框架为“法国2030计划”，具体包括研究项目 EPIQ ANR-22-PETQ-0007、HQI-Acquisition ANR-22-PNCQ-0001 和 HQI-R&D ANR-22-PNCQ-0002。

参考文献

[1] Matthew Amy、Andrew N. Glaudell 和 Neil J. Ross。某些受限 Clifford+T 电路的数论刻画。*Quantum*，4:252，2020 年 4 月。doi:10.22331/q-2020-04-06-252。[2] Miriam Backens 和 Aleks Kissinger。ZH：一种用于涉及经典非线性之量子计算的完备图形演算。*Electronic Proceedings in Theoretical Computer Science*，287:23–42，2019 年 1 月。doi:10.4204/eptcs.287.2。[3] Miriam Backens、Simon Perdrix 和 Quanlong Wang。简化的稳定子 ZX 演算。载于 Ross Duncan 和 Chris Heunen 编，第 *13* 届量子物理与逻辑国际会议论文集，*QPL 2016*，苏格兰格拉斯哥，*2016* 年 *6* 月 *6–10* 日，第 236 卷，收录于*EPTCS*，第 1–20 页，2016 年。doi:10.4204/EPTCS.236.1。[4] Miriam Backens、Simon Perdrix 和 Quanlong Wang。迈向最小稳定子 ZX 演算。*Log. Methods Comput. Sci.*，16(4)，2020 年。doi:10.23638/LMCS-16(4:19)2020。

[5] Xiaoning Bian 和 Peter Selinger。un(z[1/2,i]) 的生成元与关系。载于 Chris Heunen 和 Miriam Backens 编，《第18届国际量子物理与逻辑会议论文集》，格但斯克（波兰）及线上会议，2021年6月7日至11日，Electronic Proceedings in Theoretical Computer Science 第343卷，第145–164页。开放出版协会，2021年。doi:10.4204/EPTCS.343.8。[6] Xiaoning Bian 和 Peter Selinger。2量子比特 Clifford+T 算子的生成元与关系。载于 Stefano Gogioso 和 Matty Hoban 编，《第19届国际量子物理与逻辑会议论文集》，QPL 2022，牛津沃尔夫森学院（英国），2022年6月27日至7月1日，EPTCS 第394卷，第13–28页，2022年。doi:10.4204/EPTCS.394.2。[7] Xiaoning Bian 和 Peter Selinger。3量子比特 Clifford+CS 算子的生成元与关系。载于 Shane Mansfield、Benoît Valiron 和 Vladimir Za-mdzhiev 编，《第二十届国际量子物理与逻辑会议论文集》，QPL 2023，巴黎（法国），2023年7月17日至21日，EPTCS 第384卷，第114–126页，2023年。doi:10.4204/EPTCS.384.7。[8] Titouan Carette 和 Emmanuel Jeandel。量子图形语言的构造方法。载于 Artur Czumaj、Anuj Dawar 和 Emanuela Merelli 编，《第47届自动机、语言与编程国际研讨会》（ICALP 2020），莱布尼茨国际信息学论文集（LIPIcs）第168卷，第118:1–118:17页，德国达格施图尔，2020年。达格施图尔城堡—莱布尼茨信息学中心。URL: https://drops.dagstuhl.de/opus/volltexte/2020/12525，doi: 10.4230/LIPIcs.ICALP.2020.118。[9] Alexandre Clément、Noé Delorme 和 Simon Perdrix。量子电路的最小等式理论。载于 LICS '24：《第39届年度 ACM/IEEE计算机科学逻辑研讨会论文集》，第27号，第1–14页，爱沙尼亚塔林，2024年7月。ACM。URL: https://hal.science/hal-04399210，arXiv:2311.07476，doi:10.1145/3661814.3662088。[10] Alexandre Clément、Noé Delorme、Simon Perdrix 和 Renaud Vilmart。量子电路完备性：扩展与简化。载于《第32届EACSL计算机科学逻辑年会》（CSL 2024），意大利那不勒斯，2024年2月。URL: https://hal.science/hal-04016498，arXiv:2303.03117，doi: 10.4230/LIPIcs.CSL.2024.20。[11] Alexandre Clément、Nicolas Heurtel、Shane Mansfield、Simon Perdrix 和 Benoît Valiron。量子电路的完备等式理论。载于《2023年第38届年度 ACM/IEEE计算机科学逻辑研讨会》（LICS），第1–13页，美国波士顿，2023年6月。IEEE。URL: https://hal.science/hal-03926757，arXiv:2206.10577，doi:10.1109/LICS56636.2023.10175801。[12] Bob Coecke 和 Ross Duncan。交互量子可观测量：范畴代数与图示。《新物理学杂志》，13(4):043016，2011年。doi: 10.1088/1367-2630/13/4/043016。[13] Niel de Beaudrap、Aleks Kissinger 和 John van de Wetering。ZX 图的电路提取可能是 #P 难的。arXiv 预印本，2022年。arXiv:2202.09194。[14] Marc de Visme 和 Renaud Vilmart。有限维 ZW 演算的最小性。arXiv 预印本，2024年。已被 CSL 2025 接收。URL: https://hal.science/hal-04496193，arXiv:2401.16225。[15] Noé Delorme 和 Simon Perdrix。以控制为构造子的图示推理及其在量子电路中的应用。arXiv 预印本，2025年。arXiv: 2508.21756。[16] Ross Duncan、Aleks Kissinger、Simon Perdrix 和 John Van De Wetering。利用 ZX 演算对量子电路进行图论简化。Quantum，4:279，2020年。[17] Wang Fang、Chris Heunen 和 Robin Kaarsgaard。Hadamard-pi：等式量子编程。《ACM编程语言学报》，10(POPL)，2026年1月。arXiv:2506.06835，doi:10.1145/3776647。[18] Seth Eveson Murray Greylyn。群 $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ 的生成元与关系。理学硕士论文，达尔豪斯大学，2014年。可从 arXiv 获取：1408.6204。[19] Amar Hadzihasanovic。量子比特纠缠的图示公理化。载于《2015年第30届年度 ACM/IEEE计算机科学逻辑研讨会》，第573–584页，2015年。doi:10.1109/LICS.2015.59。[20] Amar Hadzihasanovic、Kang Feng Ng 和 Quanlong Wang。纯态量子比特量子计算的两种完备公理化。载于 Anuj Dawar 和 Erich Grädel 编，《第33届年度 ACM/IEEE计算机科学逻辑研讨会论文集》，第502–511页。ACM，2018年。doi:10.1145/3209108. 3209128。[21] Chris Heunen、Robin Kaarsgaard 和 Louis Lemonnier。一种适用于所有情形的环。arXiv 预印本，2025年。arXiv:2510.05032。[22] Kazuo Iwama、Yahiko Kambayashi 和 Shigeru Yamashita。用于设计基于 CNOT 的量子电路的变换规则。载于《第39届设计自动化会议论文集》，第419–424页，2002年。[23] Emmanuel Jeandel、Simon Perdrix 和 Renaud Vilmart。Clifford+T 量子力学的 ZX 演算完备公理化。载于《第33届年度 ACM/IEEE计算机科学逻辑研讨会论文集》，第 – 页，2018年。URL: https://hal.science/hal- doi: . / . . [24] Emmanuel Jeandel、Simon Perdrix 和 Renaud Vilmart。超越 Clifford+T 量子力学的图示推理。载于《第33届年度 ACM/IEEE计算机科学逻辑研讨会论文集》，第569–578页，2018年。

[25] Emmanuel Jeandel、Simon Perdrix 和 Renaud Vilmart。ZX 演算的完备性。《计算机科学中的逻辑方法》，第16卷，第2期，2020年6月。URL: https://lmcs.episciences.org/6532，doi:10.23638/LMCS-16(2:11)2020。 [26] Yves Lafont。迈向布尔电路的代数理论。《纯粹与应用代数杂志》，184(2):257–310，2003年。doi:10.1016/S0022-4049(03)00069-0。 [27] Sarah Meng Li、Neil J. Ross 和 Peter Selinger。群 on(z[1/2]) 的生成元与关系。载于 Chris Heunen 和 Miriam Backens 编，《第18届国际量子物理与逻辑会议论文集》，格但斯克（波兰）及线上会议，2021年6月7日至11日，Electronic Proceedings in Theoretical Computer Science 第343卷，第210–264页。开放出版协会，2021年。doi: 10.4204/EPTCS.343.11。[28] Saunders MacLane。范畴代数。《美国数学学会通报》，71(1):40–106，1965年。doi:10.1090/S0002-9904-1965-11234-4。 [29] Boldizsár Poór、Quanlong Wang、Razin A. Shaikh、Lia Yeh、Richie Yeung 和 Bob Coecke。ZXW 演算在任意有限维数下的完备性：一种统一演算。载于《2023年第38届年度 ACM/IEEE计算机科学逻辑研讨会》（LICS）。IEEE，2023年6月。doi:10.1109/lics56636.2023.10175672。 [30] Kurt Reidemeister。《纽结与群》。汉堡大学数学研讨会论文集，5(1):7–23，1927年。doi:10.1007/BF02952506。 [31] Otto Schreier。自由群的子群。汉堡大学数学研讨会论文集，5(1):161–183，1927年。doi: 10.1007/BF02952517。[32] Borun Shi。迈向 Clifford+T ZX 演算的最小性。硕士论文，牛津大学，2018年。 [33] John van de Wetering 和 Sal Wolffs。无相位 ZH 演算的完备性。arXiv 预印本 arXiv:1904.07545，2019年。 [34] Thomas van Ouwerkerk、Aleks Kissinger 和 Freek Wiedijk。研究 ZH 演算的最小性。2019年。 [35] Renaud Vilmart。纯量子比特量子力学 ZX 演算的近最小公理化。载于《2019年第34届年度 ACM/IEEE计算机科学逻辑研讨会》（LICS），第1–10页。IEEE，2019年。 [36] Fabio Zanasi。交互Hopf代数——线性系统理论。博士论文，里昂高等师范学院 - ENS LYON，2015年10月。URL: https://tel.archives-ouvertes.fr/tel-01218015，arXiv:1805.03032。

附录目录

A 辅助语言 A.1 修改后的精确综合算法 A.2 [17]完备等式理论的略微简化 A.3 应用 Reidemeister-Schreier 定理 A.3.1 幺半群 Reidemeister-Schreier 定理的要素 A.3.2 Reidemeister-Schreier 定理的原始输出 A.4 简化 Reidemeister-Schreier 定理的输出 A.4.1 关于公式（36）和（37）的细节 A.4.2 $\approx$对 P_N^*的完备性证明 B 一些辅助方程和有用性质 B.1 电路的一些有用的一般性质 B.2 一量子比特和二量子比特辅助方程 C 双量子比特完备性 C.1 引理 7.4 的证明 C.2 引理 7.5 的证明 D 其他辅助方程及多重受控门的性质 D.1 二量子比特上的其他辅助方程 D.2 三量子比特上的辅助方程 D.3 四量子比特上的辅助等式 D.4 五量子比特上的辅助方程 D.5 n 量子比特上的基本辅助方程及多重受控门的性质 D.6 n 量子比特上的更多辅助方程及多重受控门的性质 D.7 多重受控门的对易性质 D.8 多重受控 ZX 和 XZ 门的性质 D.9 n 量子比特上的其他有用辅助方程 E 一般情形下的完备性 E.1 $\Sigma_{a,\ b,\ c,\ d}$ 和 $\Sigma'_{a,\ b,\ c,\ d}$的定义 E.2 引理 8.4 的证明 E.3 引理 8.5 的证明 E.4 引理 8.6 的证明 E.5 引理 8.8 的证明

15 15 15 21 21 23 27 27 28 55 55 56 62 62 62 66 66 66 79 136 153 183 189 234 237 244 244 245 247 250 252

A 辅助语言

A.1 修改后的精确合成算法

A.2 对 [17] 的完备等式理论的略微简化

引理 A.1. 图 *6* 中的方程可由图 *7* 中的方程推导得出。

证明。 严格来说，除方程 (e1) 和 (e2) 外，我们只需考虑每个生成元的两个指标按递增顺序排列的情形。不过，为了简化起见，我们在不作此限制的情况下证明每个方程的一般情形（请注意，每个生成元的两个指标仍需互不相同）。

方程证明 (a1):

- 如果 $a = 0$，那么方程 (a1) 就是方程 (a1*)。
- 如果 $a \neq 0$:

$$
\begin{aligned}
(-1)^2_{[a]} &\overset{(a2)}{\approx} X^2_{[0,a]}(-1)^2_{[a]} \\
&\overset{(c1)}{\approx} X_{[0,a]}(-1)^2_{[0]}X_{[0,a]} \\
&\overset{(a1^*)}{\approx} X^2_{[0,a]} \\
&\overset{(a2)}{\approx} \epsilon
\end{aligned}
$$

算法 1 精确合成 $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$（参见 [17]）。

输入： $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$中的一个元素 A

输出： 一个序列 $\mathbf{W}_1$、……、$\mathbf{W}_\ell$，由 G_N 上的字组成，使得 $\mathbf{W}_\ell \cdots \mathbf{W}_1 A = I$

$B \leftarrow A$
对于 $j \leftarrow N-1,\ N-2$、……、0 **执行**
  $k \leftarrow \mathrm{lde}(Be_j)$ ▷ 关于 lde 的定义，请参见 [17]
  当 $k > 0$ **时执行**
    令 i_1 为满足 $\sqrt{2}^{-k} B[i_1, j] \equiv 1$（模 2）或 $\equiv 1 + \sqrt{2}^{-}$（模 2）的最小整数
    令 i_2 为满足 $\sqrt{2}^{-k} B[i_2, j] \equiv \sqrt{2}^{k} B[i_1, j]$（模 2）的最小整数 $> i_1$ ▷ 参见 [1]，了解 i_1 和 i_2 的存在性
    $\mathbf{W} \leftarrow H_{[i_1,i_2]}$
    输出 $\mathbf{W}$
    $B \leftarrow \mathbf{W}B, k \leftarrow \mathrm{lde}(Be_j)$
  结束 while 循环
结束 for 循环 ▷ $\mathrm{lde}(Be_j) = 0$ 对所有 j 都成立，因此 B 现在是一个置换矩阵
对 $j \leftarrow N-1, N-2, \ldots, 0$ **执行**
  $v \leftarrow Be_j$
  如果 $v \neq e_j$，**则**
    存在 $a \leq j$ 和 $\tau \in \{0,1\}$，使得 $v = (-1)^\tau e_a$。
    如果 $a = j$，**则** $\mathbf{W} \leftarrow (-1)^\tau_{[a]}$
    如果 $a < j$，**则** $\mathbf{W} \leftarrow X_{[a,j]}(-1)^\tau_{[a]}$
    输出 $\mathbf{W}$
    $B \leftarrow \mathbf{W}B$
  结束 if
结束 for

方程证明 (e1)：

$$
\begin{aligned}
X_{[b,c]} &\overset{(a2)}{\approx} X_{[b,c]}X_{[b,c]}X_{[b,c]} \\
&\overset{(a3)}{\approx} X_{[b,c]}H_{[b,c]}H_{[b,c]}X_{[b,c]}X_{[b,c]} \\
&\overset{(d2)}{\approx} X_{[b,c]}H_{[b,c]}(-1)_{[c]}H_{[b,c]}X_{[b,c]} \\
&\overset{(e2^*)}{\approx} H_{[c,b]}X_{[b,c]}(-1)_{[c]}H_{[b,c]}X_{[b,c]} \\
&\overset{(c1)}{\approx} H_{[c,b]}(-1)_{[b]}X_{[b,c]}H_{[b,c]}X_{[b,c]} \\
&\overset{(e2^*)}{\approx} H_{[c,b]}(-1)_{[b]}H_{[c,b]}X_{[b,c]}X_{[b,c]} \\
&\overset{(a2)}{\approx} H_{[c,b]}(-1)_{[b]}H_{[c,b]} \\
&\overset{(d2)}{\approx} H_{[c,b]}H_{[c,b]}X_{[c,b]} \\
&\overset{(a3)}{\approx} X_{[c,b]}
\end{aligned}
$$

方程证明 (e2)：

$$
\begin{aligned}
H_{[c,b]} &\overset{(a2)}{\approx} H_{[c,b]}X_{[b,c]}X_{[b,c]} \\
&\overset{(e2^*)}{\approx} X_{[b,c]}H_{[b,c]}X_{[b,c]}
\end{aligned}
$$

方程证明 (c3)：

$$
\begin{aligned}
X_{[b,c]}X_{[a,b]} &\overset{(a3)}{\approx} X_{[b,c]}H_{[a,b]}H_{[a,b]}X_{[a,b]} \\
&\overset{(d2)}{\approx} X_{[b,c]}H_{[a,b]}(-1)_{[b]}H_{[a,b]}
\end{aligned}
$$

$$\begin{aligned}
&\overset{(c5)}{\approx} && H_{[a,c]}X_{[b,c]}(-1)_{[b]}H_{[a,b]}\\
&\overset{(a2)}{\approx} && H_{[a,c]}X_{[b,c]}(-1)_{[b]}X_{[b,c]}X_{[b,c]}H_{[a,b]}\\
&\overset{(c1)}{\approx} && H_{[a,c]}X_{[b,c]}X_{[b,c]}(-1)_{[c]}X_{[b,c]}H_{[a,b]}\\
&\overset{(a2)}{\approx} && H_{[a,c]}(-1)_{[c]}X_{[b,c]}H_{[a,b]}\\
&\overset{(c5)}{\approx} && H_{[a,c]}(-1)_{[c]}H_{[a,c]}X_{[b,c]}\\
&\overset{(d2)}{\approx} && H_{[a,c]}H_{[a,c]}X_{[a,c]}X_{[b,c]}\\
&\overset{(a3)}{\approx} && X_{[a,c]}X_{[b,c]}
\end{aligned}$$

方程证明 (c2):

$$\begin{aligned}
X_{[a,b]}X_{[a,c]} &\overset{(e1)}{\approx} X_{[a,b]}X_{[c,a]}\\
&\overset{(c3)}{\approx} X_{[c,b]}X_{[a,b]}\\
&\overset{(e1)}{\approx} X_{[b,c]}X_{[a,b]}
\end{aligned}$$

方程证明 (c4):

$$\begin{aligned}
X_{[a,b]}H_{[a,c]} &\overset{(a2)}{\approx} X_{[a,b]}H_{[a,c]}X_{[c,a]}X_{[c,a]}\\
&\overset{(e2^*)}{\approx} X_{[a,b]}X_{[c,a]}H_{[c,a]}X_{[c,a]}\\
&\overset{(c3)}{\approx} X_{[c,b]}X_{[a,b]}H_{[c,a]}X_{[c,a]}\\
&\overset{(c5)}{\approx} X_{[c,b]}H_{[c,b]}X_{[a,b]}X_{[c,a]}\\
&\overset{(c3)}{\approx} X_{[c,b]}H_{[c,b]}X_{[c,b]}X_{[a,b]}\\
&\overset{(e2^*)}{\approx} H_{[b,c]}X_{[c,b]}X_{[c,b]}X_{[a,b]}\\
&\overset{(a2)}{\approx} H_{[b,c]}X_{[a,b]}
\end{aligned}$$

以下方程 (c2)、(c4)、(c5) 和 (d2) 的变体将有助于证明其余方程:

$$X_{[a,b]}X_{[b,c]} \approx X_{[a,c]}X_{[a,b]} \tag{c2†}$$
$$X_{[a,b]}H_{[b,c]} \approx H_{[a,c]}X_{[a,b]} \tag{c4†}$$
$$X_{[b,c]}H_{[a,c]} \approx H_{[a,b]}X_{[b,c]} \tag{c5†}$$
$$H_{[a,b]}(-1)_{[b]} \approx X_{[a,b]}H_{[a,b]} \tag{d2†}$$

方程证明 (c2†):

$$\begin{aligned}
X_{[a,c]}X_{[a,b]} &\overset{(a2)}{\approx} X_{[a,b]}X_{[a,b]}X_{[a,c]}X_{[a,b]}\\
&\overset{(c2)}{\approx} X_{[a,b]}X_{[b,c]}X_{[a,b]}X_{[a,b]}\\
&\overset{(a2)}{\approx} X_{[a,b]}X_{[b,c]}
\end{aligned}$$

方程证明 (c4†):

$$\begin{aligned}
H_{[a,c]}X_{[a,b]} &\overset{(a2)}{\approx} X_{[a,b]}X_{[a,b]}H_{[a,c]}X_{[a,b]}\\
&\overset{(c4)}{\approx} X_{[a,b]}H_{[b,c]}X_{[a,b]}X_{[a,b]}\\
&\overset{(a2)}{\approx} X_{[a,b]}H_{[b,c]}
\end{aligned}$$

方程证明 (c5†):

$$\begin{aligned} H_{[a,b]}X_{[b,c]} &\overset{(a2)}{\approx} X_{[b,c]}X_{[b,c]}H_{[a,b]}X_{[b,c]} \\ &\overset{(c5)}{\approx} X_{[b,c]}H_{[a,c]}X_{[b,c]}X_{[b,c]} \\ &\overset{(a2)}{\approx} X_{[b,c]}H_{[a,c]} \end{aligned}$$

方程证明 (d2†):

$$\begin{aligned} H_{[a,b]}(-1)_{[b]} &\overset{(a3)(a2)}{\approx} H_{[a,b]}(-1)_{[b]}H_{[a,b]}X_{[a,b]}X_{[a,b]}H_{[a,b]} \\ &\overset{(d2)}{\approx} H_{[a,b]}(-1)_{[b]}(-1)_{[b]}H_{[a,b]}X_{[a,b]}H_{[a,b]} \\ &\overset{(a1)(a3)}{\approx} X_{[a,b]}H_{[a,b]} \end{aligned}$$

方程证明 (b2): [10]

$$\begin{aligned} (-1)_{[c]}X_{[a,b]} &\overset{(a2)}{\approx} X_{[a,c]}X_{[a,c]}(-1)_{[c]}X_{[a,b]} \\ &\overset{(c1)}{\approx} X_{[a,c]}(-1)_{[a]}X_{[a,c]}X_{[a,b]} \\ &\overset{(c2^{\dagger})}{\approx} X_{[a,c]}(-1)_{[a]}X_{[a,b]}X_{[b,c]} \\ &\overset{(c1)}{\approx} X_{[a,c]}X_{[a,b]}(-1)_{[b]}X_{[b,c]} \\ &\overset{(c1)}{\approx} X_{[a,c]}X_{[a,b]}X_{[b,c]}(-1)_{[c]} \\ &\overset{(c2^{\dagger})}{\approx} X_{[a,c]}X_{[a,c]}X_{[a,b]}(-1)_{[c]} \\ &\overset{(a2)}{\approx} X_{[a,b]}(-1)_{[c]} \end{aligned}$$

方程证明 (b5):

$$\begin{aligned} H_{[c,d]}X_{[a,b]} &\overset{(a2)}{\approx} X_{[a,c]}X_{[a,c]}H_{[c,d]}X_{[a,b]} \\ &\overset{(c4^{\dagger})}{\approx} X_{[a,c]}H_{[a,d]}X_{[a,c]}X_{[a,b]} \\ &\overset{(c2^{\dagger})}{\approx} X_{[a,c]}H_{[a,d]}X_{[a,b]}X_{[b,c]} \\ &\overset{(c4^{\dagger})}{\approx} X_{[a,c]}X_{[a,b]}H_{[b,d]}X_{[b,c]} \\ &\overset{(c4^{\dagger})}{\approx} X_{[a,c]}X_{[a,b]}X_{[b,c]}H_{[c,d]} \\ &\overset{(c2^{\dagger})}{\approx} X_{[a,c]}X_{[a,c]}X_{[a,b]}H_{[c,d]} \\ &\overset{(a2)}{\approx} X_{[a,b]}H_{[c,d]} \end{aligned}$$

方程证明 (b3): [11]

$$\begin{aligned} X_{[c,d]}X_{[a,b]} &\overset{(a2)}{\approx} X_{[a,c]}X_{[a,c]}X_{[c,d]}X_{[a,b]} \\ &\overset{(c2^{\dagger})}{\approx} X_{[a,c]}X_{[a,d]}X_{[a,c]}X_{[a,b]} \\ &\overset{(c2^{\dagger})}{\approx} X_{[a,c]}X_{[a,d]}X_{[a,b]}X_{[b,c]} \end{aligned}$$

[10]我们重新命名了指标，以强调其与方程（b5）和（b3）证明的相似之处。 [11]请注意，该证明与方程（b5）的证明相同，只需将 H 替换为 X，并将方程（c4†）替换为方程（c2†）。

$$\begin{aligned}
&\overset{(c2^\dagger)}{\approx} && X_{[a,c]}X_{[a,b]}X_{[b,d]}X_{[b,c]}\\
&\overset{(c2^\dagger)}{\approx} && X_{[a,c]}X_{[a,b]}X_{[b,c]}X_{[c,d]}\\
&\overset{(c2^\dagger)}{\approx} && X_{[a,c]}X_{[a,c]}X_{[a,b]}X_{[c,d]}\\
&\overset{(a2)}{\approx} && X_{[a,b]}X_{[c,d]}
\end{aligned}$$

方程证明 (b1)：

- 如果 $\{a,\ b\}=\{0,\ 1\}$，那么方程（b1）就是方程（b1*）。
- 如果 $a=0$ 且 $b\neq 0,\ 1$：

$$\begin{aligned}
(-1)_{[0]}(-1)_{[b]} &\overset{(a2)}{\approx} && X_{[1,b]}X_{[1,b]}(-1)_{[0]}(-1)_{[b]}\\
&\overset{(b2)}{\approx} && X_{[1,b]}(-1)_{[0]}X_{[1,b]}(-1)_{[b]}\\
&\overset{(c1)}{\approx} && X_{[1,b]}(-1)_{[0]}(-1)_{[1]}X_{[1,b]}\\
&\overset{(b1^*)}{\approx} && X_{[1,b]}(-1)_{[1]}(-1)_{[0]}X_{[1,b]}\\
&\overset{(b2)}{\approx} && X_{[1,b]}(-1)_{[1]}X_{[1,b]}(-1)_{[0]}\\
&\overset{(c1)}{\approx} && X_{[1,b]}X_{[1,b]}(-1)_{[b]}(-1)_{[0]}\\
&\overset{(a2)}{\approx} && (-1)_{[b]}(-1)_{[0]}
\end{aligned}$$

- 如果 $b=0$ 且 $a\neq 0,\ 1$，或者如果 $a=1$ 且 $b\neq 0,\ 1$，或者如果 $b=1$ 且 $a\neq 0,\ 1$，那么证明过程完全相同，只需将 a 替换为 b，并且/或者将 0 替换为 1。
- 如果 $\{a,\ b\}\cap\{0,\ 1\}=\emptyset$：

$$\begin{aligned}
(-1)_{[a]}(-1)_{[b]} &\overset{(a2)}{\approx} && X_{[0,a]}X_{[0,a]}(-1)_{[a]}(-1)_{[b]}\\
&\overset{(a2)}{\approx} && X_{[0,a]}X_{[1,b]}X_{[1,b]}X_{[0,a]}(-1)_{[a]}(-1)_{[b]}\\
&\overset{(c1)}{\approx} && X_{[0,a]}X_{[1,b]}X_{[1,b]}(-1)_{[0]}X_{[0,a]}(-1)_{[b]}\\
&\overset{(b2)}{\approx} && X_{[0,a]}X_{[1,b]}X_{[1,b]}(-1)_{[0]}(-1)_{[b]}X_{[0,a]}\\
&\overset{(b2)}{\approx} && X_{[0,a]}X_{[1,b]}(-1)_{[0]}X_{[1,b]}(-1)_{[b]}X_{[0,a]}\\
&\overset{(c1)}{\approx} && X_{[0,a]}X_{[1,b]}(-1)_{[0]}(-1)_{[1]}X_{[1,b]}X_{[0,a]}\\
&\overset{(b1^*)}{\approx} && X_{[0,a]}X_{[1,b]}(-1)_{[1]}(-1)_{[0]}X_{[1,b]}X_{[0,a]}\\
&\overset{(b2)}{\approx} && X_{[0,a]}X_{[1,b]}(-1)_{[1]}X_{[1,b]}(-1)_{[0]}X_{[0,a]}\\
&\overset{(c1)}{\approx} && X_{[0,a]}X_{[1,b]}(-1)_{[1]}X_{[1,b]}X_{[0,a]}(-1)_{[a]}\\
&\overset{(c1)}{\approx} && X_{[0,a]}X_{[1,b]}X_{[1,b]}(-1)_{[b]}X_{[0,a]}(-1)_{[a]}\\
&\overset{(b2)}{\approx} && X_{[0,a]}X_{[1,b]}X_{[1,b]}X_{[0,a]}(-1)_{[b]}(-1)_{[a]}\\
&\overset{(a2)}{\approx} && X_{[0,a]}X_{[0,a]}(-1)_{[b]}(-1)_{[a]}\\
&\overset{(a2)}{\approx} && (-1)_{[b]}(-1)_{[a]}
\end{aligned}$$

方程 (b4) 和 (b6) 的证明遵循与方程 (b1) 的证明相同的原理：利用方程 (a2)，再结合方程 (c1)、(b2)、(c4)、(c5) 和 (b5)（也可能还要用到 (e1)），我们可以任意重命名指标，但这要通过某些生成元进行共轭，X 因此可以利用方程 (b4*)（分别地，方程 (b6*)）得出结论。

方程证明 (d1)：

$$
\begin{aligned}
(-1)_{[a]}(-1)_{[b]}H_{[a,b]} &\overset{(d2)}{\approx} (-1)_{[a]}H_{[a,b]}X_{[a,b]} \\
&\overset{(e1)}{\approx} (-1)_{[a]}H_{[a,b]}X_{[b,a]} \\
&\overset{(e2^*)}{\approx} (-1)_{[a]}X_{[b,a]}H_{[b,a]} \\
&\overset{(a3)}{\approx} (-1)_{[a]}H_{[b,a]}H_{[b,a]}X_{[b,a]}H_{[b,a]} \\
&\overset{(d2)}{\approx} H_{[b,a]}X_{[b,a]}H_{[b,a]}X_{[b,a]}H_{[b,a]} \\
&\overset{(d2)}{\approx} H_{[b,a]}X_{[b,a]}(-1)_{[a]}H_{[b,a]}H_{[b,a]} \\
&\overset{(a3)}{\approx} H_{[b,a]}X_{[b,a]}(-1)_{[a]} \\
&\overset{(e1)}{\approx} H_{[b,a]}X_{[a,b]}(-1)_{[a]} \\
&\overset{(e2^*)}{\approx} X_{[a,b]}H_{[a,b]}(-1)_{[a]} \\
&\overset{(a3)}{\approx} H_{[a,b]}H_{[a,b]}X_{[a,b]}H_{[a,b]}(-1)_{[a]} \\
&\overset{(d2)}{\approx} H_{[a,b]}(-1)_{[b]}H_{[a,b]}H_{[a,b]}(-1)_{[a]} \\
&\overset{(a3)}{\approx} H_{[a,b]}(-1)_{[b]}(-1)_{[a]} \\
&\overset{(b1)}{\approx} H_{[a,b]}(-1)_{[a]}(-1)_{[b]}
\end{aligned}
$$

□

方程(d3)的证明：按照方程 (b1) 至 (b6) 的证明进行类似推导，我们可以任意重命名指标，因此只需证明以下方程：

$$(H_{[2,3]}H_{[0,2]}H_{[1,3]})^4 \approx H_{[0,1]}H_{[2,3]}$$

具体如下：

$$
\begin{aligned}
(H_{[2,3]}H_{[0,2]}H_{[1,3]})^4 =\ & H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]} \text{(a1)(b1)} \\
\approx\ & H_{[2,3]}(-1)^{[2]}(-1)^{[3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]} \text{(} \\
\text{b4)(d2)(b5)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}X_{[0,2]}X_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]} \text{(c5}^{\dagger}\text{)} \\
\text{(c4}^{\dagger}\text{)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}X_{[0,2]}X_{[1,3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]} \text{(b5)(d2}^{\dagger}\text{)} \\
\text{(b4)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(-1)^{[2]}(-1)_{[3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]} \text{(d1)} \\
\approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]} \text{(} \\
\text{b4)(d2)(b5)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}X_{[0,2]}X_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]} \text{(c5}^{\dagger}\text{)} \\
\text{(c4}^{\dagger}\text{)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}X_{[0,2]}X_{[1,3]}H_{[0,2]}H_{[1,3]} \text{(b5)(d2}^{\dagger}\text{)} \\
\text{(b4)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(-1)^{[2]}(-1)^{[3]} \text{(a1)(b1)} \\
\approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)^{[0]}(-1)^{[1]}(-1)^{[2]}(-1)^{[3]}(-1)^{[2]}(-1)^{[3]}(-1)^{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(-1)^{[2]}(-1)^{[3]} \\
\text{(b1)(b4)(d1)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)^{[0]}(-1)^{[1]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}(-1)^{[2]}(-1)^{[3]}(-1)^{[0]}(-1)_{[1]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(-1)^{[2]}(\\
-1)^{[3]}\text{(b4)(d2)(b5)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)^{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]}X_{[0,2]}X_{[1,3]}H_{[2,3]}H_{[0,2]}H_{[1,3]}(-1)^{[2]}(-1)^{[3]}(-1)^{[0]}(-1)_{[1]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(-1) \\
^{[2]}(-1)^{[3]}\text{(c5}^{\dagger}\text{)(c4}^{\dagger}\text{)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)^{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]}H_{[0,1]}X_{[0,2]}X_{[1,3]}H_{[0,2]}H_{[1,3]}(-1)^{[2]}(-1)^{[3]}(-1)^{[0]}(-1)_{[1]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(-1)^{[2]} \\
(-1)^{[3]}\text{(b5)(d2}^{\dagger}\text{)(b4)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)^{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(-1)^{[2]}(-1)^{[3]}(-1)^{[2]}(-1)^{[3]}(-1)^{[0]}(-1)_{[1]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(\\
-1)^{[2]}(-1)^{[3]}\text{(b1)(a1)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)^{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(-1)^{[0]}(-1)_{[1]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(\\
-1)^{[2]}(-1)^{[3]}\text{(d3*)} \approx\ & H_{[2,3]}(-1)^{[2]}(-1)_{[3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)^{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]}H_{[0,2]}H_{[1,3]}(-1)^{[0]}(-1)_{[1]}H_{[0,1]}H_{[0,2]}H_{[1,3]}(-1) \\
^{[2]}(-1)^{[3]}20
\end{aligned}
$$

$$\overset{(b1)(b6)(a3)(a1)}{\approx} H_{[2,3]}(-1)_{[2]}(-1)_{[3]}H_{[0,1]}(-1)_{[2]}(-1)_{[3]}$$
$$\overset{(b4)(b6)(b1)(a1)}{\approx} H_{[0,1]}H_{[2,3]}$$

方程证明 (d4)：与方程（b1）到（b6）的证明类似，我们可以任意重命名指标，因此只需证明下列方程：

$$(H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]})^3 \approx H_{[4,2]}H_{[5,3]}H_{[2,3]}H_{[4,2]}H_{[5,3]}X_{[4,2]}X_{[5,3]}$$

我们如下进行：

$$\begin{aligned}
&= (H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]})^3 \\
&= H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(b5)(c5)} \\
&\approx H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}X_{[4,2]}X_{[5,3]}X_{[4,2]}X_{[5,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(b3)(a2)} \\
&\approx H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(a1)(b1)} \approx H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}(-1)_{[4]}(-1)_{[5]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(d1)(b4)(b1)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}H_{[0,4]}H_{[1,5]}(-1)_{[4]}(-1)_{[5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(b4)(d2}^\dagger\text{)(b5)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}X_{[0,4]}X_{[1,5]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(a3)(b6)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}X_{[0,4]}X_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(d4*)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}X_{[0,4]}X_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(b6)(a3)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}X_{[0,4]}X_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(b6)(a3)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}X_{[0,4]}X_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(d1)(a3)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}X_{[0,4]}X_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(c4)(c5)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}H_{[4,2]}H_{[5,3]}H_{[4,5]}H_{[4,2]}H_{[5,3]}X_{[0,4]}X_{[1,5]}H_{[0,4]}H_{[1,5]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(b5)(d2}^\dagger\text{)(b4)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}H_{[4,2]}H_{[5,3]}H_{[4,5]}H_{[4,2]}H_{[5,3]}H_{[0,4]}H_{[1,5]}(-1)_{[4]}(-1)_{[5]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(b1)(b4)(d1)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}H_{[4,2]}H_{[5,3]}H_{[4,5]}H_{[4,2]}H_{[5,3]}(-1)_{[4]}(-1)_{[5]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,4]}H_{[1,5]}X_{[4,2]}X_{[5,3]} \text{(b6)(a3)} \approx (-1)_{[0]}(-1)_{[1]}(-1)_{[4]}(-1)_{[5]}H_{[4,2]}H_{[5,3]}H_{[4,5]}H_{[4,2]}H_{[5,3]}(-1)_{[4]}(-1)_{[5]}(-1)_{[0]}(-1)_{[1]}X_{[4,2]}X_{[5,3]} \text{(b1)(b4)(a1)} \approx (-1)_{[4]}(-1)_{[5]}(-1)_{[0]}(-1)_{[1]}H_{[4,2]}H_{[5,3]}H_{[4,5]}H_{[4,2]}H_{[5,3]}(-1)_{[4]}(-1)_{[5]}X_{[4,2]}X_{[5,3]} \text{(a1)(b1)} \approx (-1)_{[4]}(-1)_{[5]}(-1)_{[2]}(-1)_{[3]}(-1)_{[2]}(-1)_{[3]}H_{[4,2]}H_{[5,3]}H_{[4,5]}H_{[4,2]}H_{[5,3]}(-1)_{[4]}(-1)_{[5]}X_{[4,2]}X_{[5,3]} \text{(b4)(d2)(b5)} \approx (-1)_{[4]}(-1)_{[5]}(-1)_{[2]}(-1)_{[3]}H_{[4,2]}H_{[5,3]}X_{[4,2]}X_{[5,3]}H_{[4,5]}H_{[4,2]}H_{[5,3]}(-1)_{[4]}(-1)_{[5]}X_{[4,2]}X_{[5,3]} \text{(c4)(c5)} \approx (-1)_{[4]}(-1)_{[5]}(-1)_{[2]}(-1)_{[3]}H_{[4,2]}H_{[5,3]}H_{[2,3]}X_{[4,2]}X_{[5,3]}H_{[4,2]}H_{[5,3]}(-1)_{[4]}(-1)_{[5]}X_{[4,2]}X_{[5,3]} \text{(b5)(d2}^\dagger\text{)(b4)} \approx (-1)_{[4]}(-1)_{[5]}(-1)_{[2]}(-1)_{[3]} \\
&\overset{}{\approx} H_{[4,2]}H_{[5,3]}H_{[2,3]}H_{[4,2]}H_{[5,3]}(-1)_{[2]}(-1)_{[3]}(-1)_{[4]}(-1)_{[5]}X_{[4,2]}X_{[5,3]} \text{(b1)(b4)(d1)(a1)} \\
&\approx H_{[4,2]}H_{[5,3]}H_{[2,3]}H_{[4,2]}H_{[5,3]}X_{[4,2]}X_{[5,3]}
\end{aligned}$$

A.3 应用 Reidemeister-Schreier 定理

A.3.1 幺半群的 *Reidemeister-Schreier* 定理中的元素。我们用 $U_{偶N}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 表示 $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 的子幺半群（或子群），它由具有偶数 H 和 ZX 奇偶性的矩阵组成。

为了应用 [6] (第 4.2 节)中所述的幺半群的 Reidemeister-Schreier 定理，只需给出以下元素：

- 集合 C，由 $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 中作为子群的 $U_{偶N}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 的四个陪集各自的一个代表元组成，其中 $U_{偶N}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ 本身的代表元必定是单位元 I
- 一个函数 $f: \mathrm{P}_N \to \mathrm{G}_N^*$（其中 G_N^* 表示由 G_N 生成的自由幺半群），它保持语义 • 一个函数 $h: C \times \mathrm{G}_N \to \mathrm{P}_N^* \times C$，使得对于任意 (c, g)，如果 $(p, c') = h(c, g)$，那么 $[\![cg]\!] = [\![pc']\!]$。

然后，令 $h^{**}: C \times \mathrm{G}_N^* \to \mathrm{P}_N^* \times C$ 为由 $h^{**}(c_0, x_1 \ldots x_k) = (w_1 \cdot \ldots \cdot w_k, c_k)$ 定义的函数，其中对所有 $i = 1, \ldots, k$，有 $h(c_{i-1}, x_i) = (w_i, c_i)$。[6] 中所述的幺半群的 Reidemeister-Schreier 定理告诉我们，由以下方程构成的等式理论是完备的：

（a）对每个 $x \in \mathrm{P}_N$，有方程 $x \approx v$，其中 v满足 $h^{**}(I, f(x)) = (v, c)$（注意，在此情形下，语义保持蕴含 $c = I$）（b）对图 7 中每个形如 $w \approx w'$ 的方程以及每个 $c \in C$，有方程 $v \approx v'$，其中 v、v'满足 $h^{**}(c, w) = (v, c')$ 且 $h^{**}(c, w') = (v', c'')$（注意，在此情形下，语义保持蕴含 $c' = c''$）。

集合 C和函数 f和 h定义于下文的定义 A.2 中（根据 f和 h的输出进行分类讨论）。按上述方式构建的等式理论见附录 A.3.2。

定义 A.2（幺半群的 Reidemeister-Schreier 定理的元素 [6]）。

$$C = \{\epsilon, (-1)_{[1]}, H_{[0,1]}, H_{[0,1]}(-1)_{[1]}\}$$

$$\begin{aligned}
f\colon \quad ((-1)_{[a]}(-1)_{[b]}) &\mapsto (-1)_{[a]}(-1)_{[b]}((\\
-1)_{[a]}X_{[c,d]}) &\mapsto (-1)_{[a]}X_{[c,d]}\\
(X_{[a,b]}X_{[c,d]}) &\mapsto X_{[a,b]}X_{[c,d]}\\
(H_{[a,b]}H_{[c,d]}) &\mapsto H_{[a,b]}H_{[c,d]}
\end{aligned}$$

$$\begin{aligned}
h\colon (\epsilon, (-1)_{[a]}) &\mapsto \left(((-1)_{[1]}(-1)_{[a]}), (-1)_{[1]}\right)\\
(\epsilon, X_{[a,b]}) &\mapsto \begin{cases} \left(((-1)_{[ab]}X_{[a,b]}), (-1)_{[1]}\right) & \text{if } a = 1 \text{ or } b = 1\\ \left(((-1)_{[1]}X_{[a,b]}), (-1)_{[1]}\right) & \text{if } a, b \neq 1 \end{cases}\\
(\epsilon, H_{[a,b]}) &\mapsto \left((H_{[a,b]}H_{[0,1]}), H_{[0,1]}\right)\\
((-1)_{[1]}, (-1)_{[a]}) &\mapsto \left(((-1)_{[1]}(-1)_{[a]}), \ \epsilon\right)\\
((-1)_{[1]}, X_{[a,b]}) &\mapsto \left(((-1)_{[1]}X_{[a,b]}), \ \epsilon\right)\\
((-1)_{[1]}, H_{[a,b]}) &\mapsto \begin{cases} \left((-1)_{[b]}X_{[a,b]}\right)(H_{[a,b]}H_{[0,1]}), \ H_{[0,1]}(-1)_{[1]}\right) & \text{如果 } a = 1 \text{ 或 } b = 1\\ \left((H_{[a,b]}H_{[0,1]}), H_{[0,1]}(-1)_{[1]}\right) & \text{如果 } a, b \neq 1 \end{cases}\\
(H_{[0,1]}, (-1)_{[a]}) &\mapsto \begin{cases} \left(((-1)_{[1]}(-1)_{[a]}), H_{[0,1]}(-1)_{[1]}\right) & \text{如果 } a \in \{0,1\}\\ \left((-1)_{[a]}X_{[0,1]}\right), \ H_{[0,1]}(-1)_{[1]}\right) & \text{如果 } a \notin \{0,1\} \end{cases}\\
(H_{[0,1]}, X_{[a,b]}) &\mapsto \begin{cases} \left((-1)_{[1]}X_{[0,1]}\right), \ H_{[0,1]}(-1)_{[1]}\right) & \text{若 } \{a, \ b\} = \{0, \ 1\}\\ \left(\left(X_{[0,1]}X_{[a,b]}\right)(H_{[a+b,1]}H_{[0,1]}), H_{[0,1]}(-1)_{[1]}\right) & \text{若 } \{a, \ b\} \cap \{0, \ 1\} = \{0\}\\ \left((-1)_{[ab]}X_{[a,b]}\right)(H_{[0,ab]}H_{[0,1]}), \ H_{[0,1]}(-1)_{[1]}\right) & \text{若 } \{a, \ b\} \cap \{0, \ 1\} = \{1\}\\ \left(\left(X_{[a,b]}X_{[0,1]}\right), H_{[0,1]}(-1)_{[1]}\right) & \text{如果 } \{a, \ b\} \cap \{0, \ 1\} = \emptyset \end{cases}\\
(H_{[0,1]}, \ H_{[a,b]}) &\mapsto \left((H_{[0,1]}H_{[a,b]}), \epsilon\right)\\
(H_{[0,1]}(-1)_{[1]}, (-1)_{[a]}) &\mapsto \begin{cases} \left(((-1)_{[1]}(-1)_{[a]}), \ H_{[0,1]}\right) & \text{如果 } a \in \{0,1\}\\ \left(((-1)_{[a]}X_{[0,1]}), H_{[0,1]}\right) & \text{如果 } a \notin \{0,1\} \end{cases}
\end{aligned}$$

$$\left(H_{[0,1]}(-1)_{[1]}, X_{[a,b]}\right) \quad \mapsto \quad \begin{cases} \left(\left((-1)_{[0]}X_{[0,1]}\right), H_{[0,1]}\right) & \text{if } \{a,b\} = \{0,1\} \\ \left(\left(X_{[0,1]}X_{[a,b]}\right)\left(H_{[a+b,1]}H_{[0,1]}\right), H_{[0,1]}\right) & \text{if } \{a,b\} \cap \{0,1\} = \{0\} \\ \left(\left(X_{[0,1]}X_{[a,b]}\right)\left(H_{[0,ab]}H_{[0,1]}\right), H_{[0,1]}\right) & \text{if } \{a,b\} \cap \{0,1\} = \{1\} \\ \left(\left(X_{[a,b]}X_{[0,1]}\right), H_{[0,1]}\right) & \text{if } \{a,b\} \cap \{0,1\} = \emptyset \end{cases}$$

$$\left(H_{[0,1]}(-1)_{[1]}, H_{[a,b]}\right) \quad \mapsto \quad \begin{cases} \left(\left(H_{[0,1]}H_{[a,b]}\right)\left((-1)_{[a]}X_{[a,b]}\right), (-1)_{[1]}\right) & \text{if } a = 1 \text{ or } b = 1 \\ \left(\left(H_{[0,1]}H_{[a,b]}\right), (-1)_{[1]}\right) & \text{if } a, b \neq 1 \end{cases}$$

A.3.2 Reidemeister-Schreier 定理的原始输出。 我们对这些方程采用以下命名约定：

- 由条目 *(a)* 得出的方程称为 (DE-**) 或 (DE-**-*k*)，其中 ** 根据 x 是 $\left((-1)_{[a]}(-1)_{[b]}\right)$、$\left((-1)_{[a]}X_{[c,d]}\right)$、$\left(X_{[a,b]}X_{[c,d]}\right)$ 还是 $\left(H_{[a,b]}H_{[c,d]}\right)$ 而分别称为 ZZ、ZX、XX 或 HH。
- 由条目 *(b)* 得出的方程称为 (**-††) 或 (**-††-*k*)，其中 ** 根据 ϵ 是 c，ϵ、$(-1)_{[1]}$、$H_{[0,1]}$ 还是 $H_{[0,1]}(-1)_{[1]}$ 而分别称为 ††，†† 是图 7 中原始方程的标签。

在这两种情形中，当需要根据参数的取值划分情形时，会使用额外的索引 k。

等式理论如下：

$$\begin{aligned}
\left((-1)_{[a]}(-1)_{[b]}\right) &\approx \left((-1)_{[1]}(-1)_{[a]}\right)\left((-1)_{[1]}(-1)_{[b]}\right) && && \text{(DE-ZZ)}\\
\left((-1)_{[a]}X_{[c,d]}\right) &\approx \left((-1)_{[1]}(-1)_{[a]}\right)\left((-1)_{[1]}X_{[c,d]}\right) && && \text{(DE-ZX)}\\
\left(X_{[a,b]}X_{[c,d]}\right) &\approx \left((-1)_{[ab]}X_{[a,b]}\right)\left((-1)_{[1]}X_{[c,d]}\right) && (a = 1 \text{ 或 } b = 1) && \text{(DE-XX-1)}\\
\left(X_{[a,b]}X_{[c,d]}\right) &\approx \left((-1)_{[1]}X_{[a,b]}\right)\left((-1)_{[1]}X_{[c,d]}\right) && (a,\ b \neq 1) && \text{(DE-XX-2)}\\
\left(H_{[a,b]}H_{[c,d]}\right) &\approx \left(H_{[a,b]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[c,d]}\right) && && \text{(DE-HH)}
\end{aligned}$$

$$\begin{aligned}
\left((-1)_{[1]}(-1)_{[0]}\right)^2 &\approx \epsilon && && (\epsilon\text{-a1})\\
\left((-1)_{[1]}(-1)_{[0]}\right)^2 &\approx \epsilon && && \text{(Z-a1)}\\
\left((-1)_{[1]}(-1)_{[0]}\right)^2 &\approx \epsilon && && \text{(H-a1)}\\
\left((-1)_{[1]}(-1)_{[0]}\right)^2 &\approx \epsilon && && \text{(HZ-a1)}
\end{aligned}$$

$$\begin{aligned}
\left(H_{[j,k]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[j,k]}\right) &\approx \epsilon && && (\epsilon\text{-a3})\\
\left((-1)_{[k]}X_{[j,k]}\right)\left(H_{[j,k]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[j,k]}\right)\left((-1)_{[j]}X_{[j,k]}\right) &\approx \epsilon && j = 1 \text{ 或 } k = 1 && \text{(Z-a3-1)}\\
\left(H_{[j,k]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[j,k]}\right) &\approx \epsilon && j,\ k \neq 1 && \text{(Z-a3-2)}\\
\left(H_{[0,1]}H_{[j,k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) &\approx \epsilon && && \text{(H-a3)}\\
\left(H_{[0,1]}H_{[j,k]}\right)\left((-1)_{[j]}X_{[j,k]}\right)\left((-1)_{[k]}X_{[j,k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) &\approx \epsilon && j = 1 \text{ 或 } k = 1 && \text{(HZ-a3-1)}\\
\left(H_{[0,1]}H_{[j,k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) &\approx \epsilon && j, k \neq 1 && \text{(HZ-a3-2)}
\end{aligned}$$

$$\begin{aligned}
\left((-1)_{[jk]}X_{[j,k]}\right)\left((-1)_{[1]}X_{[j,k]}\right) &\approx \epsilon && j = 1 \text{ 或 } k = 1 && (\epsilon\text{-a2-1})\\
\left((-1)_{[1]}X_{[j,k]}\right)\left((-1)_{[1]}X_{[j,k]}\right) &\approx \epsilon && j,\ k \neq 1 && (\epsilon\text{-a2-2})\\
\left((-1)_{[1]}X_{[j,k]}\right)\left((-1)_{[jk]}X_{[j,k]}\right) &\approx \epsilon && j = 1 \text{ or } k = 1 && \text{(Z-a2-1)}\\
\left((-1)_{[1]}X_{[j,k]}\right)\left((-1)_{[1]}X_{[j,k]}\right) &\approx \epsilon && j, k \neq 1 && \text{(Z-a2-2)}\\
\left((-1)_{[1]}X_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right) &\approx \epsilon && \{j,k\} = \{0,1\} && \text{(H⌜⌝-a2-1)}\\
\left(X_{[0,1]}X_{[j,k]}\right)\left(H_{[j+k,1]}H_{[0,1]}\right)\left(X_{[0,1]}X_{[j,k]}\right)\left(H_{[j+k,1]}H_{[0,1]}\right) &\approx \epsilon && \{j,k\} \cap \{0,1\} = \{0\} && \text{(H⌜⌝-a2-2)}\\
\left((-1)_{[jk]}X_{[j,k]}\right)\left(H_{[0,jk]}H_{[0,1]}\right)\left(X_{[0,1]}X_{[j,k]}\right)\left(H_{[0,jk]}H_{[0,1]}\right) &\approx \epsilon && \{j,k\} \cap \{0,1\} = \{1\} && \text{(H⌜⌝-a2-3)}\\
\left(X_{[j,k]}X_{[0,1]}\right)\left(X_{[j,k]}X_{[0,1]}\right) &\approx \epsilon && \{j,k\} \cap \{0,1\} = \emptyset && \text{(H⌜⌝-a2-4)}
\end{aligned}$$

$$((-1)_{[0]}X_{[0,1]})\,((-1)_{[1]}X_{[0,1]}) \approx \epsilon\{j,k\} = \{0,1\} \text{ (HZ-a2-1)}$$
$$(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]})\,(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]}) \approx \epsilon\{j,k\} \cap \{0,1\} = \{0\} \text{ (HZ-a2-2)}$$
$$(X_{[0,1]}X_{[j,k]})\,(H_{[0,jk]}H_{[0,1]})\,((-1)_{[jk]}X_{[j,k]})\,(H_{[0,jk]}H_{[0,1]}) \approx \epsilon\{j,k\} \cap \{0,1\} = \{1\} \text{ (HZ-a2-3)}$$
$$(X_{[j,k]}X_{[0,1]})\,(X_{[j,k]}X_{[0,1]}) \approx \epsilon\{j,k\} \cap \{0,1\} = \emptyset \text{ (HZ-a2-4)}$$

$$((-1)_{[1]}(-1)_{[0]})\,((-1)_{[1]}(-1)_{[1]}) \approx ((-1)_{[1]}(-1)_{[1]})\,((-1)_{[1]}(-1)_{[0]})\,(\epsilon\text{-b1*})((-1)_{[1]}(-1)_{[0]})\,((-1)_{[1]}(-1)_{[1]}) \approx ((-1)_{[1]}(-1)_{[1]})\,((-1)_{[1]}(-1)_{[0]})\,(\text{Z-b1*})((-1)_{[1]}(-1)_{[0]})\,((-1)_{[1]}(-1)_{[1]}) \approx ((-1)_{[1]}(-1)_{[1]})\,((-1)_{[1]}(-1)_{[0]})\,(\text{H 门-b1*})((-1)_{[1]}(-1)_{[0]})\,((-1)_{[1]}(-1)_{[1]}) \approx ((-1)_{[1]}(-1)_{[1]})\,((-1)_{[1]}(-1)_{[0]})\,(\text{HZ-b1*})$$

$$((-1)_{[1]}(-1)_{[1]})\,(H_{[0,2]}H_{[0,1]}) \approx (H_{[0,2]}H_{[0,1]})\,((-1)_{[1]}(-1)_{[1]})\,(\epsilon\text{-b4*})((-1)_{[1]}(-1)_{[1]})\,(H_{[0,2]}H_{[0,1]}) \approx (H_{[0,2]}H_{[0,1]})\,((-1)_{[1]}(-1)_{[1]})\,(\text{Z-b4*})((-1)_{[1]}(-1)_{[1]})\,(H_{[0,1]}H_{[0,2]}) \approx (H_{[0,1]}H_{[0,2]})\,((-1)_{[1]}(-1)_{[1]})\,(\text{H 门-b4*})((-1)_{[1]}(-1)_{[1]})\,(H_{[0,1]}H_{[0,2]}) \approx (H_{[0,1]}H_{[0,2]})\,((-1)_{[1]}(-1)_{[1]})\,(\text{HZ-b4*})$$

$$(H_{[0,1]}H_{[0,1]})\,(H_{[0,1]}H_{[2,3]}) \approx (H_{[2,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,(\epsilon\text{-b6*})((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,(H_{[0,1]}H_{[2,3]}) \approx (H_{[2,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,(\text{Z-b6*})(H_{[0,1]}H_{[0,1]})\,(H_{[2,3]}H_{[0,1]}) \approx (H_{[0,1]}H_{[2,3]})\,(H_{[0,1]}H_{[0,1]})\,(\text{H 门-b6*})(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,(H_{[2,3]}H_{[0,1]}) \approx (H_{[0,1]}H_{[2,3]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,(\text{HZ-b6*})$$

$$\begin{aligned}
((-1)_{[jk]}X_{[j,k]})\,((-1)_{[1]}(-1)_{[k]}) &\approx ((-1)_{[1]}(-1)_{[j]})\,((-1)_{[1]}X_{[j,k]}) && (j=1 \text{ 或 } k=1) && (\epsilon\text{-c1-1})\\
((-1)_{[1]}X_{[j,k]})\,((-1)_{[1]}(-1)_{[k]}) &\approx ((-1)_{[1]}(-1)_{[j]})\,((-1)_{[1]}X_{[j,k]}) && j,k\neq 1 && (\epsilon\text{-c1-2})\\
((-1)_{[1]}X_{[j,k]})\,((-1)_{[1]}(-1)_{[k]}) &\approx ((-1)_{[1]}(-1)_{[j]})\,((-1)_{[jk]}X_{[j,k]}) && (j=1 \text{ 或 } k=1) && (\text{Z-c1-1})\\
((-1)_{[1]}X_{[j,k]})\,((-1)_{[1]}(-1)_{[k]}) &\approx ((-1)_{[1]}(-1)_{[j]})\,((-1)_{[1]}X_{[j,k]}) && j,k\neq 1 && (\text{Z-c1-2})\\
((-1)_{[1]}X_{[0,1]})\,((-1)_{[1]}(-1)_{[k]}) &\approx ((-1)_{[1]}(-1)_{[j]})\,((-1)_{[0]}X_{[0,1]}) && \{j,k\}=\{0,1\} && (\text{H 门-c1-1})\\
(X_{[0,1]}X_{[0,k]})\,(H_{[k,1]}H_{[0,1]})\,((-1)_{[k]}X_{[0,1]}) &\approx ((-1)_{[1]}(-1)_{[0]})\,(X_{[0,1]}X_{[0,k]})\,(H_{[k,1]}H_{[0,1]}) && j=0,k\notin\{0,1\} && (\text{H 门-c1-2})\\
((-1)_{[k]}X_{[1,k]})\,(H_{[0,k]}H_{[0,1]})\,((-1)_{[k]}X_{[0,1]}) &\approx ((-1)_{[1]}(-1)_{[1]})\,(X_{[0,1]}X_{[1,k]})\,(H_{[0,k]}H_{[0,1]}) && j=1,k\notin\{0,1\} && (\text{H 门-c1-3})\\
(X_{[0,1]}X_{[j,0]})\,(H_{[j,1]}H_{[0,1]})\,((-1)_{[1]}(-1)_{[0]}) &\approx ((-1)_{[j]}X_{[0,1]})\,(X_{[0,1]}X_{[j,0]})\,(H_{[j,1]}H_{[0,1]}) && k=0,j\notin\{0,1\} && (\text{H 门-c1-4})\\
((-1)_{[j]}X_{[j,1]})\,(H_{[0,j]}H_{[0,1]})\,((-1)_{[1]}(-1)_{[1]}) &\approx ((-1)_{[j]}X_{[0,1]})\,(X_{[0,1]}X_{[j,1]})\,(H_{[0,j]}H_{[0,1]}) && k=1,j\notin\{0,1\} && (\text{H-c1-5})\\
(X_{[j,k]}X_{[0,1]})\,((-1)_{[k]}X_{[0,1]}) &\approx ((-1)_{[j]}X_{[0,1]})\,(X_{[j,k]}X_{[0,1]}) && \{j,k\}\cap\{0,1\}=\emptyset && (\text{H-c1-6})\\
((-1)_{[0]}X_{[0,1]})\,((-1)_{[1]}(-1)_{[k]}) &\approx ((-1)_{[1]}(-1)_{[j]})\,((-1)_{[1]}X_{[0,1]}) && \{j,k\}=\{0,1\} && (\text{HZ-c1-1})\\
(X_{[0,1]}X_{[0,k]})\,(H_{[k,1]}H_{[0,1]})\,((-1)_{[k]}X_{[0,1]}) &\approx ((-1)_{[1]}(-1)_{[0]})\,(X_{[0,1]}X_{[0,k]})\,(H_{[k,1]}H_{[0,1]}) && j=0,k\notin\{0,1\} && (\text{HZ-c1-2})\\
(X_{[0,1]}X_{[1,k]})\,(H_{[0,k]}H_{[0,1]})\,((-1)_{[k]}X_{[0,1]}) &\approx ((-1)_{[1]}(-1)_{[1]})\,((-1)_{[k]}X_{[1,k]})\,(H_{[0,k]}H_{[0,1]}) && j=1,k\notin\{0,1\} && (\text{HZ-c1-3})\\
(X_{[0,1]}X_{[j,0]})\,(H_{[j,1]}H_{[0,1]})\,((-1)_{[1]}(-1)_{[0]}) &\approx ((-1)_{[j]}X_{[0,1]})\,(X_{[0,1]}X_{[j,0]})\,(H_{[j,1]}H_{[0,1]}) && k=0,j\notin\{0,1\} && (\text{H 门Z-c1-4})\\
(X_{[0,1]}X_{[j,1]})\,(H_{[0,j]}H_{[0,1]})\,((-1)_{[1]}(-1)_{[1]}) &\approx ((-1)_{[j]}X_{[0,1]})\,((-1)_{[j]}X_{[j,1]})\,(H_{[0,j]}H_{[0,1]}) && k=1,j\notin\{0,1\} && (\text{HZ-c1-5})\\
(X_{[j,k]}X_{[0,1]})\,((-1)_{[k]}X_{[0,1]}) &\approx ((-1)_{[j]}X_{[0,1]})\,(X_{[j,k]}X_{[0,1]}) && \{j,k\}\cap\{0,1\}=\emptyset && (\text{HZ-c1-6})
\end{aligned}$$

$$\begin{aligned}
((-1)_{[1]}X_{[j,k]})\,((-1)_{[j]}X_{[1,j]})\,(H_{[1,j]}H_{[0,1]}) &\approx (H_{[1,k]}H_{[0,1]})\,(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]}) && l=1,(j=0 \text{ 或 } k=0)\,(\epsilon\text{-c5-1})((-1)_{[1]}X_{[j,k]})\,((-1)_{[j]}X_{[1,j]})\,(H_{[1,j]}H_{[0,1]}) \approx (H_{[1,k]}H_{[0,1]})\,(X_{[j,k]}X_{[0,1]}) && l=1,\ j,k\notin\{0,1\}\,(\epsilon\text{-c5-2})((-1)_{[0]}X_{[1,0]})\,((-1)_{[1]}X_{[l,1]})\,(H_{[l,1]}H_{[0,1]}) \approx (H_{[l,0]}H_{[0,1]})\,((-1)_{[1]}X_{[0,1]}) && j=1,k=0\,(\epsilon\text{-c5-3})((-1)_{[k]}X_{[1,k]})\,((-1)_{[1]}X_{[l,1]})\,(H_{[l,1]}H_{[0,1]}) \approx (H_{[l,k]}H_{[0,1]})\,((-1)_{[k]}X_{[1,k]})\,(H_{[0,k]}H_{[0,1]}) && j=1,k\notin\{0,1\}\,(\epsilon\text{-c5-4})\ 24
\end{aligned}$$

$$((-1)_{[0]}X_{[0,1]})\,(H_{[l,0]}H_{[0,1]}) \approx (H_{[l,1]}H_{[0,1]})\,((-1)_{[1]}X_{[0,1]}) \quad k=1, j=0\ (\epsilon\text{-c5-5})((-1)$$

$$_{[j]}X_{[j,1]})\,(H_{[l,j]}H_{[0,1]}) \approx (H_{[l,1]}H_{[0,1]})\,((-1)_{[j]}X_{[j,1]})\,(H_{[0,j]}H_{[0,1]}) \quad k=1, j\notin\{0,1\}\ (\epsilon\text{-c5-6})((-1)$$

$$_{[1]}X_{[j,k]})\,(H_{[l,j]}H_{[0,1]}) \approx (H_{[l,k]}H_{[0,1]})\,(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]}) \quad l\neq 1, \{j,k\}\cap\{0,1\}=\{0\}\ (\epsilon\text{-c5-7})((-1)$$

$$_{[1]}X_{[j,k]})\,(H_{[l,j]}H_{[0,1]}) \approx (H_{[l,k]}H_{[0,1]})\,(X_{[j,k]}X_{[0,1]}) \quad l\neq 1, \{j,k\}\cap\{0,1\}=\emptyset\ (\epsilon\text{-c5-8})((-1)$$

$$_{[1]}X_{[j,k]})\,(H_{[1,j]}H_{[0,1]}) \approx ((-1)_{[k]}X_{[1,k]})\,(H_{[1,k]}H_{[0,1]})\,(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]}) \quad l=1, (\ j=0\text{或}\ k=0)\ (\text{Z-c5-1})((-1)$$

$$_{[1]}X_{[j,k]})\,(H_{[1,j]}H_{[0,1]}) \approx ((-1)_{[k]}X_{[1,k]})\,(H_{[1,k]}H_{[0,1]})\,(X_{[j,k]}X_{[0,1]}) \quad l=1,\ j,k\notin\{0,1\}\ (\text{Z-c5-2})((-1)_{[1]}X_{[0,1]})\,(H_{[l,0]}H_{[0,1]}) \approx ((-1)_{[1]}X_{[l,1]})\,(H_{[l,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]}) \quad k=1, j=0\ (\text{Z-c5-3})((-1)_{[1]}X_{[j,1]})\,(H_{[l,j]}H_{[0,1]}) \approx ((-1)$$

$$_{[1]}X_{[l,1]})\,(H_{[l,1]}H_{[0,1]})\,(X_{[0,1]}X_{[j,1]})\,(H_{[0,j]}H_{[0,1]}) \quad k=1, j\notin\{0,1\}\ (\text{Z-c5-4})((-1)_{[1]}X_{[1,0]})\,(H_{[l,1]}H_{[0,1]}) \approx (H_{[l,0]}H_{[0,1]})\,((-1)$$

$$_{[0]}X_{[0,1]}) \quad j=1, k=0\ (\text{Z-c5-5})((-1)_{[1]}X_{[1,k]})\,(H_{[l,1]}H_{[0,1]}) \approx (H_{[l,k]}H_{[0,1]})\,(X_{[0,1]}X_{[1,k]})\,(H_{[0,k]}H_{[0,1]}) \quad j=1,$$

$$k\notin\{0,1\}\ (\text{Z-c5-6})((-1)_{[1]}X_{[j,k]})\,(H_{[l,j]}H_{[0,1]}) \approx (H_{[l,k]}H_{[0,1]})\,(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]}) \quad l\neq 1, \{j,k\}\cap\{0,1\}=\{0\}$$

$$(\text{Z-c5-7})((-1)_{[1]}X_{[j,k]})\,(H_{[l,j]}H_{[0,1]}) \approx (H_{[l,k]}H_{[0,1]})\,(X_{[j,k]}X_{[0,1]}) \quad l\neq 1, \{j,k\}\cap\{0,1\}=\emptyset\ (\text{Z-c5-8})$$

$$(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]})\,(H_{[0,1]}H_{[1,j]})\,((-1)_{[1]}X_{[1,j]}) \approx (H_{[0,1]}H_{[1,k]})\,((-1)_{[1]}X_{[j,k]}) \quad l=1, (\ j=0\text{或}\ k=0)\ (\text{H-c5-1})$$

$$(X_{[j,k]}X_{[0,1]})\,(H_{[0,1]}H_{[1,j]})\,((-1)_{[1]}X_{[1,j]}) \approx (H_{[0,1]}H_{[1,k]})\,((-1)_{[1]}X_{[j,k]}) \quad l=1,\ j,k\notin\{0,1\}\ (\text{H-c5-2})((-1)$$

$$_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[l,1]})\,((-1)_{[l]}X_{[l,1]}) \approx (H_{[0,1]}H_{[l,0]})\,((-1)_{[0]}X_{[1,0]}) \quad j=1, k=0\ (\text{H-c5-3})((-1)$$

$$_{[k]}X_{[1,k]})\,(H_{[0,k]}H_{[0,1]})\,(H_{[0,1]}H_{[l,1]})\,((-1)_{[l]}X_{[l,1]}) \approx (H_{[0,1]}H_{[l,k]})\,((-1)_{[k]}X_{[1,k]}) \quad j=1, k\notin\{0,1\}\ (\text{H-c5-4})((-1)$$

$$_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[l,0]}) \approx (H_{[0,1]}H_{[l,1]})\,((-1)_{[0]}X_{[0,1]}) \quad k=1, j=0\ (\text{H-c5-5})((-1)$$

$$_{[j]}X_{[j,1]})\,(H_{[0,j]}H_{[0,1]})\,(H_{[0,1]}H_{[l,j]}) \approx (H_{[0,1]}H_{[l,1]})\,((-1)_{[j]}X_{[j,1]}) \quad k=1, j\notin\{0,1\}\ (\text{H-c5-6})$$

$$(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]})\,(H_{[0,1]}H_{[l,j]}) \approx (H_{[0,1]}H_{[l,k]})\,((-1)_{[1]}X_{[j,k]}) \quad l\neq 1, \{j,k\}\cap\{0,1\}=\{0\}\ (\text{H-c5-7})$$

$$(X_{[j,k]}X_{[0,1]})\,(H_{[0,1]}H_{[l,j]}) \approx (H_{[0,1]}H_{[l,k]})\,((-1)_{[1]}X_{[j,k]}) \quad l\neq 1, \{j,k\}\cap\{0,1\}=\emptyset\ (\text{H-c5-8})$$

$$(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]})\,(H_{[0,1]}H_{[l,j]})\,((-1)_{[1]}X_{[1,k]})\,((-1)_{[1]}X_{[j,k]}) \quad l=1, (\ j=0\text{或}\ k=0)\ (\text{HZ-c5-1})$$

$$(X_{[j,k]}X_{[0,1]})\,(H_{[0,1]}H_{[1,j]}) \approx (H_{[0,1]}H_{[1,k]})\,((-1)_{[1]}X_{[1,k]})\,((-1)_{[1]}X_{[j,k]}) \quad l=1,\ j,k\notin\{0,1\}\ (\text{HZ-c5-2})((-1)$$

$$_{[0]}X_{[0,1]})\,(H_{[0,1]}H_{[l,0]}) \approx (H_{[0,1]}H_{[l,1]})\,((-1)_{[l]}X_{[l,1]})\,((-1)_{[1]}X_{[0,1]}) \quad k=1, j=0\ (\text{HZ-c5-3})$$

$$(X_{[0,1]}X_{[j,1]})\,(H_{[0,j]}H_{[0,1]})\,(H_{[0,1]}H_{[l,j]}) \approx (H_{[0,1]}H_{[l,1]})\,((-1)_{[l]}X_{[l,1]})\,((-1)_{[1]}X_{[j,1]}) \quad k=1, j\notin\{0,1\}\ (\text{HZ-c5-4})((-1)$$

$$_{[0]}X_{[0,1]})\,(H_{[0,1]}H_{[l,1]}) \approx (H_{[0,1]}H_{[l,0]})\,((-1)_{[1]}X_{[1,0]}) \quad j=1, k=0\ (\text{HZ-c5-5})$$

$$(X_{[0,1]}X_{[1,k]})\,(H_{[0,k]}H_{[0,1]})\,(H_{[0,1]}H_{[l,1]}) \approx (H_{[0,1]}H_{[l,k]})\,((-1)_{[1]}X_{[1,k]}) \quad j=1, k\notin\{0,1\}\ (\text{HZ-c5-6})$$

$$(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]})\,(H_{[0,1]}H_{[l,j]}) \approx (H_{[0,1]}H_{[l,k]})\,((-1)_{[1]}X_{[j,k]}) \quad l\neq 1, \{j,k\}\cap\{0,1\}=\{0\}\ (\text{HZ-c5-7})$$

$$(X_{[j,k]}X_{[0,1]})\,(H_{[0,1]}H_{[l,j]}) \approx (H_{[0,1]}H_{[l,k]})\,((-1)_{[1]}X_{[j,k]}) \quad l\neq 1, \{j,k\}\cap\{0,1\}=\emptyset\ (\text{HZ-c5-8})$$

$$((-1)_{[0]}X_{[j,k]})\,((-1)_{[k]}X_{[j,k]})\,(H_{[j,k]}H_{[0,1]}) \approx (H_{[k,j]}H_{[0,1]})\,((-1)_{[1]}X_{[0,1]}) \quad \{j,k\}=\{0,1\}\ (\epsilon\text{-e2*-1})$$

$$((-1)_{[jk]}X_{[j,k]})\,((-1)_{[k]}X_{[j,k]})\,(H_{[j,k]}H_{[0,1]}) \approx (H_{[k,j]}H_{[0,1]})\,((-1)_{[jk]}X_{[j,k]})\,(H_{[0,jk]}H_{[0,1]}) \quad \{j,k\}\cap\{0,1\}=\{1\}\ (\epsilon\text{-e2*-2})$$

$$((-1)_{[1]}X_{[j,k]})\,(H_{[j,k]}H_{[0,1]}) \approx (H_{[k,j]}H_{[0,1]})\,(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]}) \quad \{j,k\}\cap\{0,1\}=\{0\}\ (\epsilon\text{-e2*-3})$$

$$((-1)_{[1]}X_{[j,k]})\,(H_{[j,k]}H_{[0,1]}) \approx (H_{[k,j]}H_{[0,1]})\,(X_{[j,k]}X_{[0,1]}) \quad \{j,k\}\cap\{0,1\}=\emptyset\ (\epsilon\text{-e2*-4})$$

$$((-1)_{[1]}X_{[j,k]})\,(H_{[j,k]}H_{[0,1]}) \approx ((-1)_{[j]}X_{[k,j]})\,(H_{[k,j]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]}) \quad \{j,k\}=\{0,1\}\ (\text{Z-e2*-1})$$

$$((-1)_{[1]}X_{[j,k]})\,(H_{[j,k]}H_{[0,1]}) \approx ((-1)_{[j]}X_{[k,j]})\,(H_{[k,j]}H_{[0,1]})\,(X_{[0,1]}X_{[j,k]})\,(H_{[0,jk]}H_{[0,1]}) \quad \{j,\ k\}\cap\{0,\ 1\}=\{1\}\ (\text{Z-e2*-2})$$

$$((-1)_{[1]}X_{[j,k]})\,(H_{[j,k]}H_{[0,1]}) \approx (H_{[k,j]}H_{[0,1]})\,(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]}) \quad \{j,k\}\cap\{0,1\}=\{0\}\ (\text{Z-e2*-3})$$

$$((-1)_{[1]}X_{[j,k]})\,(H_{[j,k]}H_{[0,1]}) \approx (H_{[k,j]}H_{[0,1]})\,(X_{[j,k]}X_{[0,1]}) \quad \{j,k\}\cap\{0,1\}=\emptyset\ (\text{Z-e2*-4})$$

$$((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[j,k]})\,((-1)_{[j]}X_{[j,k]}) \approx (H_{[0,1]}H_{[k,j]})\,((-1)_{[0]}X_{[j,k]}) \quad \{j,k\}=\{0,1\}\ (\text{H}\lceil\rceil\text{-e2*-1})$$

$$((-1)_{[jk]}X_{[j,k]})\,(H_{[0,jk]}H_{[0,1]})\,(H_{[0,1]}H_{[j,k]})\,((-1)_{[j]}X_{[j,k]}) \approx (H_{[0,1]}H_{[k,j]})\,((-1)_{[jk]}X_{[j,k]}) \quad \{j,k\}\cap\{0,1\}=\{1\}\ (\text{H-e2*-2})$$

$$(X_{[0,1]}X_{[j,k]})\,(H_{[j+k,1]}H_{[0,1]})\,(H_{[0,1]}H_{[j,k]}) \approx (H_{[0,1]}H_{[k,j]})\,((-1)_{[1]}X_{[j,k]}) \quad \{j,k\}\cap\{0,1\}=\{0\}\ (\text{H-e2*-3})$$

$$(X_{[j,k]}X_{[0,1]})\,(H_{[0,1]}H_{[j,k]}) \approx (H_{[0,1]}H_{[k,j]})\,((-1)_{[1]}X_{[j,k]}) \quad \{j,k\}\cap\{0,1\}=\emptyset\ (\text{H}\lceil\rceil\text{-e2*-4})$$

$$((-1)_{[0]}X_{[0,1]})\,(H_{[0,1]}H_{[j,k]}) \approx (H_{[0,1]}H_{[k,j]})\,((-1)_{[k]}X_{[k,j]})\,((-1)_{[1]}X_{[j,k]}) \quad \{j,k\}=\{0,1\}\ (\text{H}\lceil\rceil\ \text{Z-e2*-1})$$

$$\begin{aligned}
\left(X_{[0,1]}X_{[j,k]}\right)\left(H_{[0,jk]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[j,k]}\right) &\approx \left(H_{[0,1]}H_{[k,j]}\right)\left((-1)_{[k]}X_{[k,j]}\right)\left((-1)_{[1]}X_{[j,k]}\right) && \{j,k\}\cap\{0,1\}=\{1\} && \text{(HZ-e2*-2)}\\
\left(X_{[0,1]}X_{[j,k]}\right)\left(H_{[j+k,1]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[j,k]}\right) &\approx \left(H_{[0,1]}H_{[k,j]}\right)\left((-1)_{[1]}X_{[j,k]}\right) && \{j,k\}\cap\{0,1\}=\{0\} && \text{(HZ-e2*-3)}\\
\left(X_{[j,k]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[j,k]}\right) &\approx \left(H_{[0,1]}H_{[k,j]}\right)\left((-1)_{[1]}X_{[j,k]}\right) && \{j,k\}\cap\{0,\ 1\}=\emptyset && \text{(HZ-e2*-4)}
\end{aligned}$$

$$\begin{aligned}
\left(H_{[j,k]}H_{[0,1]}\right)\left((-1)_{[1]}X_{[0,1]}\right) &\approx \left((-1)^{[1]}(-1)_{[k]}\right)\left((-1)_{[k]}X_{[j,k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) && \{j,k\}=\{0,1\} && (\epsilon\text{-d2-1})\\
\left(H_{[j,k]}H_{[0,1]}\right)\left((-1)_{[jk]}X_{[j,k]}\right)\left(H_{[0,jk]}H_{[0,1]}\right) &\approx \left((-1)^{[1]}(-1)_{[k]}\right)\left((-1)_{[k]}X_{[j,k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) && \{j,\ k\}\cap\{0,\ 1\}=\{1\} && (\epsilon\text{-d2-2})\\
\left(H_{[j,k]}H_{[0,1]}\right)\left(X_{[0,1]}X_{[j,k]}\right)\left(H_{[j+k,1]}H_{[0,1]}\right) &\approx \left((-1)^{[1]}(-1)_{[k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) && \{j,k\}\cap\{0,1\}=\{0\} && (\epsilon\text{-d2-3})\\
\left(H_{[j,k]}H_{[0,1]}\right)\left(X_{[j,k]}X_{[0,1]}\right) &\approx \left((-1)^{[1]}(-1)_{[k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) && \{j,k\}\cap\{0,1\}=\emptyset && (\epsilon\text{-d2-4})\\
\left((-1)_{[k]}X_{[j,k]}\right)\left(H_{[j,k]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right) &\approx \left((-1)^{[1]}(-1)_{[k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) && \{j,k\}=\{0,1\} && \text{(Z-d2-1)}\\
\left((-1)_{[k]}X_{[j,k]}\right)\left(H_{[j,k]}H_{[0,1]}\right)\left(X_{[0,1]}X_{[j,k]}\right)\left(H_{[0,jk]}H_{[0,1]}\right) &\approx \left((-1)^{[1]}(-1)_{[k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) && \{j,k\}\cap\{0,1\}=\{1\} && \text{(Z-d2-2)}\\
\left(H_{[j,k]}H_{[0,1]}\right)\left(X_{[0,1]}X_{[j,k]}\right)\left(H_{[j+k,1]}H_{[0,1]}\right) &\approx \left((-1)^{[1]}(-1)_{[k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) && \{j,k\}\cap\{0,1\}=\{0\} && \text{(Z-d2-3)}\\
\left(H_{[j,k]}H_{[0,1]}\right)\left(X_{[j,k]}X_{[0,1]}\right) &\approx \left((-1)^{[1]}(-1)_{[k]}\right)\left(H_{[j,k]}H_{[0,1]}\right) && \{j,k\}\cap\{0,\ 1\}=\emptyset && \text{(Z-d2-4)}\\
\left(H_{[0,1]}H_{[j,1]}\right)\left((-1)_{[j]}X_{[j,1]}\right) &\approx \left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,1]}H_{[j,1]}\right)\left((-1)_{[j]}X_{[j,1]}\right) && k=1 && \text{(H }\lceil\rceil\text{-d2-1)}\\
\left(H_{[0,1]}H_{[1,0]}\right)\left((-1)_{[0]}X_{[1,0]}\right) &\approx \left((-1)^{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[1,0]}\right)\left((-1)_{[1]}X_{[1,0]}\right) && j=1,k=0 && \text{(H }\lceil\rceil\text{-d2-2)}\\
\left(H_{[0,1]}H_{[1,k]}\right)\left((-1)_{[k]}X_{[1,k]}\right) &\approx \left((-1)_{[k]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[1,k]}\right)\left((-1)_{[1]}X_{[1,k]}\right) && j=1,k\notin\{0,1\} && \text{(H }\lceil\rceil\text{-d2-3)}\\
\left(H_{[0,1]}H_{[j,0]}\right)\left((-1)_{[1]}X_{[j,0]}\right) &\approx \left((-1)^{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[j,0]}\right) && j\neq 1,k=0 && \text{(H }\lceil\rceil\text{-d2-4)}\\
\left(H_{[0,1]}H_{[j,k]}\right)\left((-1)_{[1]}X_{[j,k]}\right) &\approx \left((-1)_{[k]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[j,k]}\right) && j\neq 1,k\notin\{0,1\} && \text{(H-d2-5)}\\
\left(H_{[0,1]}H_{[j,1]}\right)\left((-1)_{[j]}X_{[j,1]}\right)\left((-1)_{[1]}X_{[j,1]}\right) &\approx \left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,1]}H_{[j,1]}\right) && k=1 && \text{(HZ-d2-1)}\\
\left(H_{[0,1]}H_{[1,0]}\right)\left((-1)_{[1]}X_{[1,0]}\right)\left((-1)_{[1]}X_{[1,0]}\right) &\approx \left((-1)^{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[1,0]}\right) && j=1,k=0 && \text{(HZ-d2-2)}\\
\left(H_{[0,1]}H_{[1,k]}\right)\left((-1)_{[1]}X_{[1,k]}\right)\left((-1)_{[1]}X_{[1,k]}\right) &\approx \left((-1)_{[k]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[1,k]}\right) && j=1,k\notin\{0,1\} && \text{(HZ-d2-3)}\\
\left(H_{[0,1]}H_{[j,0]}\right)\left((-1)_{[1]}X_{[j,0]}\right) &\approx \left((-1)^{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[j,0]}\right) && j\neq 1,k=0 && \text{(HZ-d2-4)}\\
\left(H_{[0,1]}H_{[j,k]}\right)\left((-1)_{[1]}X_{[j,k]}\right) &\approx \left((-1)_{[k]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[j,k]}\right) && j\neq 1,k\notin\{0,1\} && \text{(HZ-d2-5)}
\end{aligned}$$

$$\begin{aligned}
&\left(H_{[0,1]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\\
&\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\\
&\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\\
&\left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)
\end{aligned}
\approx \quad (\epsilon\text{-d3*})$$

$$\begin{aligned}
&\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\\
&\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\\
&\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\\
&\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)
\end{aligned}
\approx \quad (\text{Z-d3*})$$

$$\begin{aligned}
&\left(H_{[0,1]}H_{[0,1]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\\
&\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\\
&\left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\\
&\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left(H_{[0,1]}H_{[0,1]}\right)
\end{aligned}
\approx \quad \begin{matrix}\text{(H }\lceil\rceil\text{-}\\ \text{d3*)}\end{matrix}$$

$$\begin{aligned}
&\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\\
&\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\\
&\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\\
&\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)
\end{aligned}
\approx \quad (\text{HZ-d3*})$$

$$
\begin{aligned}
&\left(H_{[0,1]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,4]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,5]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right) \approx_{(\epsilon\text{-d4*})}\\
&\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left(H_{[0,4]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,5]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\\
&\left(H_{[0,1]}H_{[0,4]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,4]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right) \approx_{(\text{Z-d4*})}\\
&\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left(H_{[0,4]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,5]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left(H_{[0,4]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\\
&\left(H_{[0,1]}H_{[0,1]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left(H_{[0,4]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,5]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right) \approx_{(\text{H}^{\urcorner}\text{-d4*})}\\
&\left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\\
&\left(H_{[0,4]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,5]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right) \approx_{(\text{HZ-d4*})}\\
&\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left((-1)^{[1]}(-1)_{[1]}\right)\left(H_{[0,4]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)
\end{aligned}
$$

A.4 简化 Reidemeister-Schreier 定理的输出

A.4.1 方程（(36) 和 (37)的细节。 方程（36）和（37）的右端分别定义如下：

$$
\begin{aligned}
\mathcal{W}_1 \coloneqq\ & \left(\prod_{j=m+1}^{m+\ell} E_{n-j-2,j}(\supset\!\!\times)\right)\circ\left(\prod_{j=0}^{m-1} E_{n-j-2,j}(\supset\!\!\times)\circ E_{n-j-3,j+1}(\supset\!\!\times)\right)\circ E_{n-2,0}(\supset\!\!\times)\circ\\
&\left(\prod_{j=k+\ell}^{n-3} \mathcal{E}^{1-z_j}_{j,n-j-2}(-\oplus-)\right)\circ\left(\prod_{j=k}^{k+\ell-1} \mathcal{E}^{1-y_j}_{j,n-j-2}(-\oplus-)\right)\circ\left(\prod_{j=0}^{k-1} \mathcal{E}^{1-x_j}_{j,n-j-2}(-\oplus-)\right)\circ\\
&\left(H_{[0,1]}H_{[3,2]}\right)\circ\\
&\left(\prod_{j=0}^{k-1} \mathcal{E}^{1-x_j}_{j,n-j-2}(-\oplus-)\right)\circ\left(\prod_{j=k}^{k+\ell-1} \mathcal{E}^{1-y_j}_{j,n-j-2}(-\oplus-)\right)\circ\left(\prod_{j=k+\ell}^{n-3} \mathcal{E}^{1-z_j}_{j,n-j-2}(-\oplus-)\right)\circ\\
&E_{n-2,0}(\supset\!\!\times)\circ\left(\prod_{j=0}^{m-1} E_{n-j-3,j+1}(\supset\!\!\times)\circ E_{n-j-2,j}(\supset\!\!\times)\right)\circ\left(\prod_{j=m+1}^{m+\ell} E_{n-j-2,j}(\supset\!\!\times)\right)
\end{aligned}
$$

and

$$
\mathcal{W}_2 \coloneqq \left(\prod_{j=m+1}^{m+\ell} E_{n-j-2,j}(\supset\!\!\times)\right)\circ\left(\prod_{j=0}^{m-1} E_{n-j-2,j}(\supset\!\!\times)\circ E_{n-j-3,j+1}(\supset\!\!\times)\right)\circ
$$

$$\left(\overleftarrow{\prod_{j=k+\ell}^{n-3}} \mathcal{E}^{1-z_j}_{j,n-j-2}(-\!\oplus\!-)\right)\circ\left(\overleftarrow{\prod_{j=k}^{k+\ell-1}} \mathcal{E}^{1-y_j}_{j,n-j-2}(-\!\oplus\!-)\right)\circ\left(\overleftarrow{\prod_{j=0}^{k-1}} \mathcal{E}^{1-x_j}_{j,n-j-2}(-\!\oplus\!-)\right)\circ$$

$$\left(H_{[0,1]}H_{[3,2]}\right)\circ$$

$$\left(\overrightarrow{\prod_{j=0}^{k-1}} \mathcal{E}^{1-x_j}_{j,n-j-2}(-\!\oplus\!-)\right)\circ\left(\overrightarrow{\prod_{j=k}^{k+\ell-1}} \mathcal{E}^{1-y_j}_{j,n-j-2}(-\!\oplus\!-)\right)\circ\left(\overrightarrow{\prod_{j=k+\ell}^{n-3}} \mathcal{E}^{1-z_j}_{j,n-j-2}(-\!\oplus\!-)\right)\circ$$

$$\left(\overrightarrow{\prod_{j=0}^{m-1}} E_{n-j-3,j+1}(\supset\!\subset)\circ E_{n-j-2,j}(\supset\!\subset)\right)\circ\left(\overrightarrow{\prod_{j=m+1}^{m+\ell}} E_{n-j-2,j}(\supset\!\subset)\right)$$

其中记号 $\overleftarrow{\prod}$ 和 $\overrightarrow{\prod}$ 在定义 8.3中引入，而 $\mathrm{E}^{1-x}_{k\,\ell}(\,)$ 是一个简写，其定义如下（乘积的顺序未作规定）：

$$\mathcal{E}^{1-x}_{k,\ell}(-\!\oplus\!-) \coloneqq \begin{cases} \epsilon & \text{if } x=1 \\ E_{k,\ell}(-\!\bullet\!-)\circ \prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^\ell}} \left((-1)_{[G_n^{-1}(x1y)]}X_{[G_n^{-1}(x0y),G_n^{-1}(x1y)]}\right) & \text{if } x=0. \end{cases}$$

A.4.2 证明 $\approx$ 对于 $\mathcal{P}^*_N$的完备性。本附录旨在证明定理 4.10 的完备性部分（如下文推论 A.12 所述）。为此，我们将证明一系列逐步增强的部分完备性结果，并给出一些辅助方程，从而最终能够以最小的工作量推导出附录 A.3.2 中的方程。

引理 A.3。 图 *9* 中的方程是图 *8*中方程的推论。

证明。 [12]

方程证明*(47)*: ( )

$$\begin{aligned} \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) &\overset{(20)(22)(21)}{\approx} \left((-1)_{[a]}(-1)_{[a+1]}\right)^2\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\ &\overset{(23)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)^4\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\ &\overset{(29)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)^4 \\ &\overset{(23)(21)(22)(20)}{\approx} \epsilon \end{aligned}$$

方程证明 (48):

$$\begin{aligned} \left((-1)_{[a+1]}X_{[a,a+1]}\right) &\overset{(20)(22)(21)}{\approx} \left((-1)_{[a]}(-1)_{[a+1]}\right)^2\left((-1)_{[a+1]}X_{[a,a+1]}\right) \\ &\overset{(23)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)^4\left((-1)_{[a+1]}X_{[a,a+1]}\right) \\ &\overset{(29)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)^3 \end{aligned}$$

方程证明 (49)： 若 $c-a$ 为奇数，则方程 (49) 就是方程 (25)，因此我们只需考虑 $c-a$ 为偶数的情况。我们对 $c-a$使用归纳法。若 $c-a=2$，则有

$$\begin{aligned} \left((-1)_{[a]}X_{[a,a+2]}\right) &\overset{(27)}{\approx} \left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right) \\ &\overset{(48)}{\approx} \left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)^3 \\ &\overset{(24)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \end{aligned}$$

[12]请注意，本文中凡是我们给出推导来证明附带参数条件的方程时，都默认这些方程的条件成立。

$$\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \approx \epsilon \tag{47}$$

$$\left((-1)_{[a+1]}X_{[a,a+1]}\right) \approx \left((-1)_{[a]}X_{[a,a+1]}\right)^3 \tag{48}$$

$$\left((-1)_{[a]}X_{[a,c]}\right) \approx \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \quad a+1<c \tag{49}$$

$$\left((-1)_{[c]}X_{[a,c]}\right) \approx \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \quad a+1<c \tag{50}$$

$$\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}X_{[a,b]}\right) \approx \epsilon \tag{51}$$

$$\left((-1)_{[a]}(-1)_{[b]}\right) \approx \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \quad a\neq b \tag{52}$$

$$\left((-1)_{[c]}X_{[a,b]}\right) \approx \left((-1)_{[c]}(-1)_{[a]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \tag{53}$$

$$\left((-1)_{[a]}X_{[a,c]}\right) \approx \left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \quad a+1<c \tag{54}$$

$$\left((-1)_{[c]}(-1)_{[d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \approx \left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}(-1)_{[d]}\right) \quad \{a,a+1\}\cap\{c,d\}=\emptyset \tag{55}$$

$$\left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \approx \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}(-1)_{[b]}\right) \tag{56}$$

$$\left((-1)_{[b]}(-1)_{[a]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \approx \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}(-1)_{[a]}\right) \tag{57}$$

$$\left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \approx \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right) \quad c\neq a,b \tag{58}$$

$$\left((-1)_{[c]}(-1)_{[a]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \approx \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}(-1)_{[b]}\right) \quad c\neq a,b \tag{59}$$

$$\left((-1)_{[b]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \approx \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}(-1)_{[c]}\right) \quad c\neq a,b \tag{60}$$

$$\left((-1)_{[c]}(-1)_{[b]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \approx \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}(-1)_{[a]}\right) \quad c\neq a,b \tag{61}$$

$$\left((-1)_{[c]}(-1)_{[d]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \approx \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}(-1)_{[d]}\right) \quad \{a,b\}\cap\{c,d\}=\emptyset \tag{62}$$

$$\left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[c]}(-1)_{[d]}\right) \approx \left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[b]}(-1)_{[d]}\right) \tag{63}$$

$$\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}X_{[c,d]}\right) \approx \left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \quad \{a,b\}\cap\{c,d\}=\emptyset \tag{64}$$

图 9：有用的辅助方程。

$$\overset{(48)}{\approx} \quad \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)$$

并且若 $c-a\geq 4$，则我们有

$$\begin{aligned}
&\left((-1)_{[a]}X_{[a,c]}\right)\\
\overset{(27)}{\approx}\ &\left((-1)_{[c-1]}X_{[c-1,c]}\right)\left((-1)_{[a]}X_{[a,c-1]}\right)\left((-1)_{[c]}X_{[c-1,c]}\right)\\
\overset{(25)}{\approx}\ &\left((-1)_{[c-1]}X_{[c-1,c]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,c-1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c-1,c]}\right)\\
\overset{\text{induction hypothesis}}{\approx}\ &\left((-1)_{[c-1]}X_{[c-1,c]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,c-1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c-1,c]}\right)\\
\overset{(48)(32)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[c-1]}X_{[c-1,c]}\right)\left((-1)_{[a+2]}X_{[a+2,c-1]}\right)\left((-1)_{[c]}X_{[c-1,c]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(27)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,c]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(25)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)
\end{aligned}$$

方程证明（50）：若 $c-a$ 为奇数，则方程（50）即为方程（26），因此我们只需考虑 $c-a$ 为偶数的情形。我们对 $c-a$ 使用归纳法。若 $c-a=2$，则有

$$\begin{aligned}
\left((-1)_{[a+2]}X_{[a,a+2]}\right) &\overset{(28)}{\approx} \left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\\
&\overset{(47)(29)}{\approx} \left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\\
&\quad\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\quad\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(49)}{\approx} \left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\\
&\quad\left((-1)_{[a]}X_{[a,a+2]}\right)
\end{aligned}$$

$$
\begin{aligned}
& \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(27)}{\approx}\ & \left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right) \\
& \left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right) \\
& \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(47)(29)}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)
\end{aligned}
$$

而若 $c-a\geq 4$，则有

$$
\begin{aligned}
& \left((-1)_{[c]}X_{[a,c]}\right) \\
\overset{(28)}{\approx}\ & \left((-1)_{[c-1]}X_{[c-1,c]}\right)\left((-1)_{[c-1]}X_{[a,c-1]}\right)\left((-1)_{[c]}X_{[c-1,c]}\right) \\
\overset{(26)}{\approx}\ & \left((-1)_{[c-1]}X_{[c-1,c]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[c-1]}X_{[a+1,c-1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c-1,c]}\right) \\
\overset{\text{induction hypothesis}}{\approx}\ & \left((-1)_{[c-1]}X_{[c-1,c]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[c-1]}X_{[a+2,c-1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c-1,c]}\right) \\
\overset{(48)(32)}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[c-1]}X_{[c-1,c]}\right)\left((-1)_{[c-1]}X_{[a+2,c-1]}\right)\left((-1)_{[c]}X_{[c-1,c]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(28)}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[c]}X_{[a+2,c]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(26)}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)
\end{aligned}
$$

方程的证明 (51) 和 (52)：首先，我们在 $a<b$ 的情形下，对 a 进行有限递降归纳法，证明这两个方程。若 $a=b-1$，则方程 (51) 是方程 (29) 的一个特例。假设方程 (51) 对 $a+1$ 成立，我们如下证明它对 a 也成立：

$$
\begin{aligned}
& \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}X_{[a,b]}\right) \\
\overset{(49)(50)}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[b]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(29)}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[b]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{\text{induction hypothesis}}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(20)(22)(21)}{\approx}\ & \left((-1)_{[a]}(-1)_{[a+1]}\right)^2\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(23)}{\approx}\ & \left((-1)_{[a]}X_{[a,a+1]}\right)^4\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(29)}{\approx}\ & \left((-1)_{[a]}X_{[a,a+1]}\right)^4 \\
\overset{(23)(21)(22)(20)}{\approx}\ & \epsilon
\end{aligned}
$$

如果 $a=b-1$，那么方程 (52) 是方程 (23) 的一个实例。假设方程 (52) 对 $a+1$成立，我们证明它对 a也成立，如下：

$$
\begin{aligned}
& \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \\
\overset{(49)}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(29)}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{\text{induction hypothesis}}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}(-1)_{[b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(31)}{\approx}\ & \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a]}(-1)_{[b]}\right) \\
\overset{(20)(22)(21)}{\approx}\ & \left((-1)_{[a]}(-1)_{[a+1]}\right)^2\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a]}(-1)_{[b]}\right) \\
\overset{(23)}{\approx}\ & \left((-1)_{[a]}X_{[a,a+1]}\right)^4\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a]}(-1)_{[b]}\right) \\
\overset{(29)}{\approx}\ & \left((-1)_{[a]}X_{[a,a+1]}\right)^4\left((-1)_{[a]}(-1)_{[b]}\right) \\
\overset{(23)(21)(22)(20)}{\approx}\ & \left((-1)_{[a]}(-1)_{[b]}\right)
\end{aligned}
$$

剩下需要证明的是，在 $b < a$的情况下，方程 (51) 和 (52)。根据方程 (33)，这等价于证明以下方程对$a < b$成立：

$$\left((-1)_{[b]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,b]}\right) \approx \epsilon$$
$$\left((-1)_{[b]}X_{[a,b]}\right)\left((-1)_{[b]}X_{[a,b]}\right) \approx \left((-1)_{[b]}(-1)_{[a]}\right)$$

第一个的证明如下：

$$\begin{aligned}
&\left((-1)_{[b]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
\overset{(20)(22)(21)}{\approx}\ &\left((-1)_{[a]}(-1)_{[b]}\right)^2\left((-1)_{[b]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
\overset{\text{case } a<b \text{ of } (52)}{\approx}\ &\left((-1)_{[a]}X_{[a,b]}\right)^4\left((-1)_{[b]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
\overset{\text{case } a<b \text{ of } (51)}{\approx}\ &\left((-1)_{[a]}X_{[a,b]}\right)^3\left((-1)_{[a]}X_{[a,b]}\right)\\
\overset{\text{case } a<b \text{ of } (52)}{\approx}\ &\left((-1)_{[a]}(-1)_{[b]}\right)^2\\
\overset{(21)(22)(20)}{\approx}\ &\epsilon
\end{aligned}$$

第二个的证明如下：

$$\begin{aligned}
&\left((-1)_{[b]}X_{[a,b]}\right)\left((-1)_{[b]}X_{[a,b]}\right)\\
\overset{(20)(22)}{\approx}\ &\left((-1)_{[b]}(-1)_{[a]}\right)\left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[b]}X_{[a,b]}\right)\left((-1)_{[b]}X_{[a,b]}\right)\\
\overset{\text{case } a<b \text{ of } (52)}{\approx}\ &\left((-1)_{[b]}(-1)_{[a]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}X_{[a,b]}\right)\left((-1)_{[b]}X_{[a,b]}\right)\\
\overset{\text{case } a<b \text{ of } (51)}{\approx}\ &\left((-1)_{[b]}(-1)_{[a]}\right)
\end{aligned}$$

方程 (53)的证明：若 $c \neq a,\ b$，则该方程就是方程 (30)。若 $c = a$，则结论由方程 (20) 得出。因此，只需处理 $c = b$ 的情况：

$$\begin{aligned}
&\left((-1)_{[b]}X_{[a,b]}\right)\\
\overset{(51)(33)}{\approx}\ &\left((-1)_{[b]}X_{[a,b]}\right)\left((-1)_{[b]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
\overset{(33)(52)}{\approx}\ &\left((-1)_{[b]}(-1)_{[a]}\right)\left((-1)_{[a]}X_{[a,b]}\right)
\end{aligned}$$

方程 (54)的证明：

$$\begin{aligned}
\left((-1)_{[a]}X_{[a,c]}\right) &\overset{(49)}{\approx} \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(53)}{\approx} \left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(21)}{\approx} \left((-1)_{[a]}(-1)_{[a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(23)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)
\end{aligned}$$

方程 (55)的证明：

$$\begin{aligned}
\left((-1)_{[c]}(-1)_{[d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) &\overset{(22)(21)}{\approx} \left((-1)_{[a+1]}(-1)_{[c]}\right)\left((-1)_{[a+1]}(-1)_{[d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(31)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a]}(-1)_{[d]}\right)\\
&\overset{(21)(22)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}(-1)_{[d]}\right)
\end{aligned}$$

方程证明 (56)：

$$\begin{aligned}
\left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[a]}X_{[a,b]}\right) &\overset{(52)}{\approx} \left((-1)_{[a]}(-1)_{[b]}\right)^3\\
&\overset{(52)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}(-1)_{[b]}\right)
\end{aligned}$$

方程证明 (57):

$$\begin{aligned}
\left((-1)_{[b]}(-1)_{[a]}\right)\left((-1)_{[a]}X_{[a,b]}\right) &\overset{(21)}{\approx} \left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
&\overset{(56)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}(-1)_{[b]}\right)\\
&\overset{(21)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}(-1)_{[a]}\right)
\end{aligned}$$

方程证明 (58): 首先，我们证明方程 (58) 在 $a<b$ 且 $c\notin[a,b]$ (即 $c<a<b$ 或 $a<b<c$) 的情况下，采用关于 a 的有限递降归纳法。

若 $a=b-1$，则有

$$\begin{aligned}
\left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) &\overset{(22)}{\approx} \left((-1)_{[a]}(-1)_{[a+1]}\right)\left((-1)_{[a+1]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(31)}{\approx} \left((-1)_{[a]}(-1)_{[a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a]}(-1)_{[c]}\right)\\
&\overset{(23)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a]}(-1)_{[c]}\right)\\
&\overset{(23)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a]}(-1)_{[a+1]}\right)\left((-1)_{[a]}(-1)_{[c]}\right)\\
&\overset{(21)(22)}{\approx} \left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}(-1)_{[c]}\right)
\end{aligned}$$

假设 $c\notin[a,b]$ 且方程 (58) 对 $a+1$成立，我们证明方程 (58) 对 a成立，如下:

$$\begin{aligned}
&\left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
\overset{(49)}{\approx}\ &\left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(51)(33)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(31)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(29)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}(-1)_{[c]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{\text{induction hypothesis}}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(55)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\\
\overset{(49)}{\approx}\ &\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)
\end{aligned}$$

接着，我们在 $a<c<b$ 的情形下证明方程 (58)，同样对 a 使用有限递降归纳法。若 $a=c-1$，则由于 $b\neq c$，必然有 $b>a+1$。我们有

$$\begin{aligned}
&\left((-1)_{[a]}(-1)_{[a+1]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
\overset{(49)}{\approx}\ &\left((-1)_{[a]}(-1)_{[a+1]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(21)(52)(33)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(33)(52)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{\text{previous case}}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[b]}(-1)_{[a]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(21)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{\text{previous case}}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}(-1)_{[b]}\right)\\
\overset{(49)}{\approx}\ &\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a+1]}(-1)_{[b]}\right)\\
\overset{(21)}{\approx}\ &\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}(-1)_{[a+1]}\right)
\end{aligned}$$

假设 $a+1<c$ $<b$ 以及方程（58）对于 $a+1$，我们以与前一种情况相同的方式证明方程（58）对于 a:

$$\begin{aligned}
&\left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
\overset{(49)}{\approx}\ &\left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)
\end{aligned}$$

$$
\begin{aligned}
&\overset{(51)(33)}{\approx} && \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(31)}{\approx} && \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(29)}{\approx} && \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}(-1)_{[c]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{\text{induction hypothesis}}{\approx} && \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(55)}{\approx} && \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\\
&\overset{(49)}{\approx} && \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)
\end{aligned}
$$

最后，还需证明在 $b<a$的情况下，方程（58）：

$$
\begin{aligned}
& && \left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
&\overset{(33)}{\approx} && \left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[b,a]}\right)\\
&\overset{(53)}{\approx} && \left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[b]}X_{[b,a]}\right)\\
&\overset{(21)(22)}{\approx} && \left((-1)_{[b]}(-1)_{[c]}\right)\left((-1)_{[b]}X_{[b,a]}\right)\\
&\overset{\text{previous cases}}{\approx} && \left((-1)_{[b]}X_{[b,a]}\right)\left((-1)_{[a]}(-1)_{[c]}\right)\\
&\overset{(22)}{\approx} && \left((-1)_{[b]}X_{[b,a]}\right)\left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\\
&\overset{(52)}{\approx} && \left((-1)_{[b]}X_{[b,a]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\\
&\overset{(33)(51)}{\approx} && \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)
\end{aligned}
$$

方程证明 (59):

$$
\begin{aligned}
\left((-1)_{[c]}(-1)_{[a]}\right)\left((-1)_{[a]}X_{[a,b]}\right) &\overset{(21)}{\approx} \left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
&\overset{(58)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\\
&\overset{(21)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}(-1)_{[b]}\right)
\end{aligned}
$$

方程证明 (60):

$$
\begin{aligned}
\left((-1)_{[b]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,b]}\right) &\overset{(22)}{\approx} \left((-1)_{[b]}(-1)_{[a]}\right)\left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
&\overset{(58)(57)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}(-1)_{[a]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\\
&\overset{(21)(22)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}(-1)_{[c]}\right)
\end{aligned}
$$

方程证明 (61):

$$
\begin{aligned}
\left((-1)_{[c]}(-1)_{[b]}\right)\left((-1)_{[a]}X_{[a,b]}\right) &\overset{(21)}{\approx} \left((-1)_{[b]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
&\overset{(60)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}(-1)_{[c]}\right)\\
&\overset{(21)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}(-1)_{[a]}\right)
\end{aligned}
$$

方程证明 (62):

$$
\begin{aligned}
\left((-1)_{[c]}(-1)_{[d]}\right)\left((-1)_{[a]}X_{[a,b]}\right) &\overset{(22)}{\approx} \left((-1)_{[c]}(-1)_{[a]}\right)\left((-1)_{[a]}(-1)_{[d]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
&\overset{(58)(59)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}(-1)_{[b]}\right)\left((-1)_{[b]}(-1)_{[d]}\right)\\
&\overset{(22)}{\approx} \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}(-1)_{[d]}\right)
\end{aligned}
$$

方程证明 (63):

$$
\begin{aligned}
\left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[c]}(-1)_{[d]}\right) &\overset{(20)}{\approx} \left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[b]}(-1)_{[b]}\right)\left((-1)_{[c]}(-1)_{[d]}\right)\\
&\overset{(22)}{\approx} \left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\left((-1)_{[c]}(-1)_{[b]}\right)\left((-1)_{[c]}(-1)_{[d]}\right)
\end{aligned}
$$

$$\overset{(21)}{\approx} \quad \left((-1)_{[a]}(-1)_{[b]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\left((-1)_{[b]}(-1)_{[c]}\right)\left((-1)_{[c]}(-1)_{[d]}\right)$$
$$\overset{(22)}{\approx} \quad \left((-1)_{[a]}(-1)_{[c]}\right)\left((-1)_{[b]}(-1)_{[d]}\right)$$

方程证明 (64)：首先，考虑 $a<b<c<d$或 $c<d<a<b$的情形。我们对 $b-a$进行归纳。若 $b-a=1$，则对 $d-c$进行归纳。若 $d-c=1$，则方程 (64) 只是方程 (32) 的一个实例。若 $d-c>1$，则有

$$\begin{aligned}
&\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\\
\overset{(54)}{\approx}\quad &\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)^3\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\\
\overset{\text{induction hypothesis}}{\approx}\quad &\left((-1)_{[c]}X_{[c,c+1]}\right)^3\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(54)}{\approx}\quad &\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)
\end{aligned}$$

现在，如果 $b-a>1$，我们有

$$\begin{aligned}
&\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\\
\overset{(54)}{\approx}\quad &\left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\\
\overset{\text{induction hypothesis}}{\approx}\quad &\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(54)}{\approx}\quad &\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,b]}\right)
\end{aligned}$$

然后我们考虑 $c<a<b<d$ 的情况。同样，我们对 $b-a$ 使用归纳法。如果 $b-a=1$，则我们对 $a-c$ 使用归纳法。如果 $a-c=1$，则我们有

$$\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\overset{(49)}{\approx}\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c+1]}X_{[c,c+1]}\right)\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\overset{(49)}{\approx}\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c+1]}X_{[c,c+1]}\right)\left((-1)_{[c+2]}X_{[c+1,c+2]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\overset{(53)}{\approx}\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)^{[c+1]}(-1)_{[c]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)^{[c+2]}(-1)_{[c+1]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\overset{(59)}{\approx}\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)^{[c+1]}(-1)_{[c]}\right)\left((-1)^{[c+2]}(-1)_{[c]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\overset{(60)(58)}{\approx}\left((-1)^{[c+2]}(-1)_{[c]}\right)\left((-1)^{[c+1]}(-1)_{[c]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\overset{(24)}{\approx}\left((-1)^{[c+2]}(-1)_{[c]}\right)\left((-1)^{[c+1]}(-1)_{[c]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\overset{(53)}{\approx}\left((-1)^{[c+2]}(-1)_{[c]}\right)\left((-1)_{[c+1]}X_{[c,c+1]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\overset{(33)(61)}{\approx}\left((-1)_{[c+1]}X_{[c,c+1]}\right)\left((-1)^{[c+2]}(-1)_{[c+1]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\overset{(53)}{\approx}\left((-1)_{[c+1]}X_{[c,c+1]}\right)\left((-1)_{[c+2]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\text{前一种情况}\approx\left((-1)_{[c+1]}X_{[c,c+1]}\right)\left((-1)_{[c+2]}X_{[c+1,c+2]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\overset{(24)}{\approx}\left((-1)_{[c+1]}X_{[c,c+1]}\right)\left((-1)_{[c+2]}X_{[c+1,c+2]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[c+2]}X_{[c+1,c+2]}\right)\left((-1)_{[c+2]}X_{[c+2,d]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\overset{(49)}{\approx}\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[c+1]}X_{[c+1,c+2]}\right)$$

并且如果 $a-c>1$，我们有

$$\begin{aligned}
&\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\\
\overset{(54)}{\approx}\quad &\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)^3\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\\
\overset{(32)}{\approx}\quad &\left((-1)_{[c]}X_{[c,c+1]}\right)^3\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\\
\overset{\text{induction hypothesis}}{\approx}\quad &\left((-1)_{[c]}X_{[c,c+1]}\right)^3\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\\
\overset{(32)}{\approx}\quad &\left((-1)_{[c]}X_{[c,c+1]}\right)^3\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
\overset{(54)}{\approx}\quad &\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)
\end{aligned}$$

现在，如果 $b-a>1$，我们有

$$\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}X_{[c,d]}\right)$$

$$\begin{aligned}
&\overset{(54)}{\approx} && \left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\\
&\overset{\text{induction hypothesis}}{\approx} && \left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(54)}{\approx} && \left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,b]}\right)
\end{aligned}$$

接下来，我们考虑 $a<c<b<d$ 的情况。我们对 $b-c$ 使用归纳法。如果 $b-c=1$，则对 $c-a$ 使用归纳法。如果$c-a=1$，则我们有

$$\left((-1)_{[a]}X_{[a,a+2]}\right)\left((-1)_{[a+1]}X_{[a+1,d]}\right)(49)\approx \left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)(53)\approx \left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)(24)\approx \left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)(29)\approx \left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)$第一种情况$\approx \left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)(29)\approx \left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)(53)\approx \left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}(-1)_{[a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)(24)\approx \left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}(-1)_{[a+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)(22)(21)(53)\approx \left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}(-1)_{[a]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)(58)(62)(60)\approx \left((-1)_{[a+1]}(-1)_{[a]}\right)\left((-1)_{[a+2]}(-1)_{[a]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)(21)(22)\approx \left((-1)_{[a+2]}(-1)_{[a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)(53)\approx \left((-1)_{[a+2]}X_{[a+1,a+2]}\right)\left((-1)_{[a+2]}X_{[a+2,d]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)(49)\approx \left((-1)_{[a+1]}X_{[a+1,d]}\right)\left((-1)_{[a]}X_{[a,a+2]}\right)$$

并且，如果 $c-a>1$，我们有

$$\begin{aligned}
&&& \left((-1)_{[a]}X_{[a,c+1]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\\
&\overset{(54)}{\approx} && \left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,c+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\\
&\overset{\text{first case}}{\approx} && \left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,c+1]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{\text{induction hypothesis}}{\approx} && \left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a+1]}X_{[a+1,c+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{\text{first case}}{\approx} && \left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)^3\left((-1)_{[a+1]}X_{[a+1,c+1]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(54)}{\approx} && \left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,c+1]}\right)
\end{aligned}$$

现在，如果 $b-c>1$，我们有

$$\begin{aligned}
&&& \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\\
&\overset{(54)}{\approx} && \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)^3\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\\
&\overset{\text{previous case}}{\approx} && \left((-1)_{[c]}X_{[c,c+1]}\right)^3\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\\
&\overset{\text{induction hypothesis}}{\approx} && \left((-1)_{[c]}X_{[c,c+1]}\right)^3\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\\
&\overset{\text{previous case}}{\approx} && \left((-1)_{[c]}X_{[c,c+1]}\right)^3\left((-1)_{[c+1]}X_{[c+1,d]}\right)\left((-1)_{[c]}X_{[c,c+1]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\\
&\overset{(54)}{\approx} && \left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,b]}\right)
\end{aligned}$$

由对称性可知，情形 $a<c<d<b$ 与情形 $c<a<b<d$ 类似，情形 $c<a<d<b$ 与情形 $a<c<b<d$ 类似。因此，我们已经处理了所有满足 $a<b$ 和 $c<d$ 的情形。

最后，如果 $b<a$ 且 $c<d$，则有

$$\begin{aligned}
&&& \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\\
&\overset{(51)}{\approx} && \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[b]}X_{[b,a]}\right)\left((-1)_{[a]}X_{[b,a]}\right)
\end{aligned}$$

$$\begin{aligned}
&\overset{\text{previous cases}}{\approx} && \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}X_{[b,a]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[b,a]}\right)\\
&\overset{(33)(51)}{\approx} && \left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,b]}\right)
\end{aligned}$$

由对称性可得 $a<b$ 且 $d<c$ 的情形。最后， $b<a$ 且 $d<c$ 的情形可通过完全相同的推导得出：

$$\begin{aligned}
& && \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\\
&\overset{(51)}{\approx} && \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[b]}X_{[b,a]}\right)\left((-1)_{[a]}X_{[b,a]}\right)\\
&\overset{\text{previous cases}}{\approx} && \left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[b]}X_{[b,a]}\right)\left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[b,a]}\right)\\
&\overset{(33)(51)}{\approx} && \left((-1)_{[c]}X_{[c,d]}\right)\left((-1)_{[a]}X_{[a,b]}\right)
\end{aligned}$$

□

引理 A.4. 由$\mathcal{P}_N$的生成元构成且不含形如 $\left(H_{[a,b]}H_{[c,d]}\right)$ 的生成元的任意字，都与唯一一个字 $\approx$-等价，称为其标准形，其形式为

$$\left((-1)_{[a_1]}(-1)_{[b_1]}\right)\cdots\left((-1)_{[a_k]}(-1)_{[b_k]}\right)\overrightarrow{\prod_{i=1}^{N-1}}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}\left((-1)_{[j]}X_{[j,j+1]}\right)\right) \tag{B}$$

其中 $k\geq 0$； $a_1<b_1<\cdots<a_k<b_k$；且对于每个 $i\in\{1,\dots,N\}$， $d_i\in\{0,\dots,N-i\}$ （空乘积为单位元）。此外，语义相同的两个字具有相同的标准形。

注 6. 下文中，当我们讨论形如 (B) 的字，或讨论将其化为 (B)的形式时，我们也默认要求它们满足引理 k,a_i,b_i,d_i 中给出的参数条件 *A.4*。

引理 A.4 的证明。

由语义确定唯一性： 给定一个形如 (B) 的字，其语义是一个置换矩阵与一个对角元素全为 ±1 的对角矩阵的乘积。容易看出，置换 d_i由该置换唯一确定，因为乘积 $\overrightarrow{\prod}_{i=1}^{N-1}\left(\overrightarrow{\prod}_{j=d_i}^{N-i-1}X_{[j,j+1]}\right)$对应于置换分解为对换之积的一种众所周知的规范分解。于是，在已知 d_i的情况下， k连同 a_i和 b_i都由对角矩阵的元素唯一确定。

存在性：首先，P_N 的所有生成元中，除形式为 $\left(H_{[a,b]}H_{[c,d]}\right)$ 的生成元外，其余均可利用图 8 中的方程写成形式为 $\left((-1)_{[j]}X_{[j,j+1]}\right)$ 的生成元之积。具体而言：首先，根据方程（34）和（53），这些生成元中的任意一个都可写成形式为 $\left((-1)_{[a]}(-1)_{[b]}\right)$ 和 $\left((-1)_{[a]}X_{[a,b]}\right)$ 的生成元之积；接着，根据方程（33）、（53）、（20）和（21），可以确保所有形式为 $\left((-1)_{[a]}(-1)_{[b]}\right)$ 和 $\left((-1)_{[a]}X_{[a,b]}\right)$ 的生成元都满足 $a<b$；然后，根据方程（52），可以将 $\left((-1)_{[a]}(-1)_{[b]}\right)$ 写成两个 $\left((-1)_{[a]}X_{[a,b]}\right)$ 的乘积；最后，当 $a<b$ 时，方程（54）允许我们通过对 $b-a$ 直接使用归纳法，将 $\left((-1)_{[a]}X_{[a,b]}\right)$ 写成形式为 $\left((-1)_{[j]}X_{[j,j+1]}\right)$ 的生成元之积。

因此，只需证明任意 $\left((-1)_{[j]}X_{[j,j+1]}\right)$的乘积都可以写成 (B) 的形式。我们用归纳法证明：单位元具有 (B) 的形式，即 $k=0$，且 $d_i=N-i$ 对所有 i都成立。接下来，只需证明，对于任意具有 (B) 形式的字 P以及任意 $a\in\{0,\dots,N-2\}$，字 $P\left((-1)_{[a]}X_{[a,a+1]}\right)$ 都可以写成 (B) 的形式：

$$\begin{aligned}
& && \left((-1)_{[a_1]}(-1)_{[b_1]}\right)\cdots\left((-1)_{[a_k]}(-1)_{[b_k]}\right)\overrightarrow{\prod_{i=1}^{N-1}}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}\left((-1)_{[j]}X_{[j,j+1]}\right)\right)\circ\left((-1)_{[a]}X_{[a,a+1]}\right)\\
&\overset{(64)}{\approx} && \left((-1)_{[a_1]}(-1)_{[b_1]}\right)\cdots\left((-1)_{[a_k]}(-1)_{[b_k]}\right)\overrightarrow{\prod_{i=1}^{N-a}}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}\left((-1)_{[j]}X_{[j,j+1]}\right)\right)\circ\left((-1)_{[a]}X_{[a,a+1]}\right)\circ\overrightarrow{\prod_{i=N-a+1}^{N-1}}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}\left((-1)_{[j]}X_{[j,j+1]}\right)\right)\\
&= && \left((-1)_{[a_1]}(-1)_{[b_1]}\right)\cdots\left((-1)_{[a_k]}(-1)_{[b_k]}\right)\overrightarrow{\prod_{i=1}^{N-a-2}}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}\left((-1)_{[j]}X_{[j,j+1]}\right)\right)\circ\overrightarrow{\prod_{j=d_{N-a-1}}^{a}}\left((-1)_{[j]}X_{[j,j+1]}\right)\circ\overrightarrow{\prod_{j=d_{N-a}}^{a-1}}\left((-1)_{[j]}X_{[j,j+1]}\right)\circ\left((-1)_{[a]}X_{[a,a+1]}\right)\circ\overrightarrow{\prod_{i=N-a+1}^{N-1}}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}\left((-1)_{[j]}X_{[j,j+1]}\right)\right)
\end{aligned}$$

- 如果 $d_{N-a-1} = d_{N-a} + 1$，那么根据方程（64），可将其改写为$((-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)_{[a_k]}(-1)_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ \overrightarrow{\prod_{j=d_{N-a-1}}^{a}} ((-1)_{[j]} X_{[j,j+1]}) ((-1)_{[j-1]} X_{[j-1,j]}) \circ (($
$-1)_{[a]} X_{[a,a+1]}) \circ \overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) (24) \approx ((-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)_{[a_k]}(-1)_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ ((-1)_{[d_{N-a-1}-1]} X_{[d_{N-a-1}-1, d_{N-a-1}]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}}^{a}} ((-1)_{[j]} X_{[j,j+1]}) ((-1)$
$_{[j-1]} X_{[j-1,j]}) \circ \overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) (64) \approx ((-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)_{[a_k]}(-1)_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ ((-1)_{[d_{N-a-1}-1]} X_{[d_{N-a-1}-1, d_{N-a-1}]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}}^{a}} ((-1)_{[j]} X_{[j,j+1]}) \circ$
$\overrightarrow{\prod_{j=d_{N-a-1}-1}^{a-1}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) = ((-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)_{[a_k]}(-1)_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ \overrightarrow{\prod_{j=d_{N-a-1}-1}^{a}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}-1}^{a-1}} ((-1)_{[j]} X_{[j,j+1]}) \circ$
$\overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right)$

其形式为 (B)。

- 如果 $d_{N-a-1} > d_{N-a} + 1$，那么这等于$((-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)_{[a_k]}(-1)_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ \overrightarrow{\prod_{j=d_{N-a-1}}^{a}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{j=d_{N-a}}^{d_{N-a-1}-2}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}}^{a-1}} ((-1)_{[j]} X_{[j,j+1]}) \circ ((-1)_{[a]} X_{[a,a+1]}) \circ \overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) ($
$64) \approx ((-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)_{[a_k]}(-1)_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ \overrightarrow{\prod_{j=d_{N-a}}^{d_{N-a-1}-2}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}}^{a}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}-1}^{a-1}} ((-1)_{[j]} X_{[j,j+1]}) \circ ((-1)_{[a]} X_{[a,a+1]}) \circ \overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right)$
$(64) \approx ((-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)_{[a_k]}(-1)_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ \overrightarrow{\prod_{j=d_{N-a}}^{d_{N-a-1}-2}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}}^{a}} ((-1)_{[j]} X_{[j,j+1]}) ((-1)_{[j-1]} X_{[j-1,j]}) \circ ((-1)_{[a]} X_{[a,a+1]}) \circ \overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) (24) \approx ($
$-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)_{[a_k]}(-1)_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ \overrightarrow{\prod_{j=d_{N-a}}^{d_{N-a-1}-2}} ((-1)_{[j]} X_{[j,j+1]}) \circ ((-1)_{[d_{N-a-1}-1]} X_{[d_{N-a-1}-1, d_{N-a-1}]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}}^{a}} ((-1)_{[j]} X_{[j,j+1]}) ((-1)_{[j-1]} X_{[j-1,j]}) \circ \overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right)$
$= ((-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)_{[a_k]}(-1)_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ \overrightarrow{\prod_{j=d_{N-a}}^{d_{N-a-1}-1}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{j=d_{N-a}}^{a}} ((-1)_{[j]} X_{[j,j+1]}) ((-1)_{[j-1]} X_{[j-1,j]}) \circ \overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) (64) \approx ((-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)$
$_{[a_k]}(-1)_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ \overrightarrow{\prod_{j=d_{N-a}}^{d_{N-a-1}-1}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}}^{a}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}-1}^{a-1}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) = ((-1)_{[a_1]}(-1)_{[b_1]}) \cdots ((-1)_{[a_k]}(-1)$
$_{[b_k]}) \overrightarrow{\prod_{i=1}^{N-a-2}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right) \circ \overrightarrow{\prod_{j=d_{N-a}}^{a}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{j=d_{N-a-1}-1}^{a-1}} ((-1)_{[j]} X_{[j,j+1]}) \circ \overrightarrow{\prod_{i=N-a+1}^{N-1}} \left(\overrightarrow{\prod_{j=d_i}^{N-i-1}} ((-1)_{[j]} X_{[j,j+1]}) \right)$

其形式为 (B)。

- 并且如果 $d_{N-a-1} < d_{N-a+1}-1$，那么这就等于

$$((-1)_{[a_1]}(-1)_{[b_1]})\cdots((-1)_{[a_k]}(-1)_{[b_k]})\prod_{i=1}^{N-2}\left(\overrightarrow{\prod_{j=d_i}^{d_{N-a}}}((-1)_{[j]}X_{[j,j+1]})\right)\circ\overrightarrow{\prod_{j=d_{N-a-1}}^{d_{N-a}}}((-1)_{[j]}X_{[j,j+1]})\circ\overrightarrow{\prod_{j=d_{N-a}+1}^{a}}((-1)_{[j]}X_{[j,j+1]})\circ\overrightarrow{\prod_{j=d_{N-a}}^{a-1}}((-1)_{[j]}X_{[j,j+1]})\circ((-1)_{[a]}X_{[a,a+1]})\circ\prod_{i=N-a+1}^{N-1}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\tag{64}\approx$$

$$((-1)_{[a_1]}(-1)_{[b_1]})\cdots((-1)_{[a_k]}(-1)_{[b_k]})\prod_{i=1}^{N-a-2}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\circ\overrightarrow{\prod_{j=d_{N-a-1}}^{d_{N-a}}}((-1)_{[j]}X_{[j,j+1]})\circ\overrightarrow{\prod_{j=d_{N-a}+1}^{a}}((-1)_{[j]}X_{[j,j+1]})((-1)_{[j-1]}X_{[j-1,j]})\circ((-1)_{[a]}X_{[a,a+1]})\circ\prod_{i=N-a+1}^{N-1}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\tag{24}\approx$$

$$((-1)_{[a_1]}(-1)_{[b_1]})\cdots((-1)_{[a_k]}(-1)_{[b_k]})\prod_{i=1}^{N-a-2}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\circ\overrightarrow{\prod_{j=d_{N-a-1}}^{d_{N-a}}}((-1)_{[j]}X_{[j,j+1]})\circ((-1)_{[d_{N-a}]}X_{[d_{N-a},d_{N-a}+1]})\circ\overrightarrow{\prod_{j=d_{N-a}+1}^{a}}((-1)_{[j]}X_{[j,j+1]})((-1)_{[j-1]}X_{[j-1,j]})\circ\prod_{i=N-a+1}^{N-1}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\tag{23}\approx$$

$$((-1)_{[a_1]}(-1)_{[b_1]})\cdots((-1)_{[a_k]}(-1)_{[b_k]})\prod_{i=1}^{N-a-2}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\circ\overrightarrow{\prod_{j=d_{N-a-1}}^{d_{N-a}-1}}((-1)_{[j]}X_{[j,j+1]})\circ((-1)_{[d_{N-a}]}(-1)_{[d_{N-a}+1]})\circ\overrightarrow{\prod_{j=d_{N-a}+1}^{a}}((-1)_{[j]}X_{[j,j+1]})((-1)_{[j-1]}X_{[j-1,j]})\circ\prod_{i=N-a+1}^{N-1}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\tag{56到62}=$$

$$((-1)_{[a_1]}(-1)_{[b_1]})\cdots((-1)_{[a_k]}(-1)_{[b_k]})((-1)_{[\alpha]}(-1)_{[\beta]})\prod_{i=1}^{N-a-2}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\circ\overrightarrow{\prod_{j=d_{N-a-1}}^{d_{N-a}-1}}((-1)_{[j]}X_{[j,j+1]})\circ\overrightarrow{\prod_{j=d_{N-a}+1}^{a}}((-1)_{[j]}X_{[j,j+1]})((-1)_{[j-1]}X_{[j-1,j]})\circ\prod_{i=N-a+1}^{N-1}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\text{对于某些 }\alpha,\beta\in\{0,\dots,N-1\}\ (64)\approx$$

$$((-1)_{[a_1]}(-1)_{[b_1]})\cdots((-1)_{[a_k]}(-1)_{[b_k]})((-1)_{[\alpha]}(-1)_{[\beta]})\prod_{i=1}^{N-a-2}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\circ\overrightarrow{\prod_{j=d_{N-a-1}}^{d_{N-a}-1}}((-1)_{[j]}X_{[j,j+1]})\circ\overrightarrow{\prod_{j=d_{N-a}+1}^{a}}((-1)_{[j]}X_{[j,j+1]})\circ\overrightarrow{\prod_{j=d_{N-a}}^{a-1}}((-1)_{[j]}X_{[j,j+1]})\circ\prod_{i=N-a+1}^{N-1}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\tag{64}\approx$$

$$((-1)_{[a_1]}(-1)_{[b_1]})\cdots((-1)_{[a_k]}(-1)_{[b_k]})((-1)_{[\alpha]}(-1)_{[\beta]})\prod_{i=1}^{N-a-2}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}\left(\left(\overrightarrow{\prod_{j=d_{N-a}+1}^{a}}((-1)_{[j]}X_{[j,j+1]})\right)\circ\overrightarrow{\prod_{j=d_{N-a-1}}^{d_{N-a}-1}}((-1)_{[j]}X_{[j,j+1]})\circ\overrightarrow{\prod_{j=d_{N-a}}^{a-1}}((-1)_{[j]}X_{[j,j+1]})\circ\prod_{i=N-a+1}^{N-1}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\right)=$$

$$((-1)_{[a_1]}(-1)_{[b_1]})\cdots((-1)_{[a_k]}(-1)_{[b_k]})((-1)_{[\alpha]}(-1)_{[\beta]})\prod_{i=1}^{N-a-2}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\circ\overrightarrow{\prod_{j=d_{N-a}+1}^{a}}\left(\overrightarrow{\prod_{j=d_{N-a-1}}^{a-1}}((-1)_{[j]}X_{[j,j+1]})\circ\prod_{i=N-a+1}^{N-1}\left(\overrightarrow{\prod_{j=d_i}^{N-i-1}}((-1)_{[j]}X_{[j,j+1]})\right)\right)$$

最后，要将其写成（B）的形式，只需将由 (-1) 构成的左侧部分整理成适当的形式，这可以利用方程（20）至（22）以及（63）来完成。
□

推论 A.5. 给定 $\mathcal{P}_N$ 的生成元上的任意两个字 w, w'，且其中不含形如 $\left(H_{[a,b]}H_{[c,d]}\right)$ 的生成元，若 $[\![w]\!]=[\![w']\!]$，则 $w\approx w'$。

证明. 由于 w和 w' 在语义上等价，根据引理 A.4，它们都与同一个标准形（形式为（B））$\approx$-等价，因此可得它们彼此 $\approx$-等价。□

引理 A.6. 对于 $\mathcal{P}_N$ 的生成元上的任意字 w，若其中不含形如 $\left(H_{[a,b]}H_{[c,d]}\right)$ 的生成元，且 $[\![w\left(H_{[0,1]}H_{[3,2]}\right)]\!]=[\![\left(H_{[0,1]}H_{[3,2]}\right)w]\!]$，则 w 与一个如下形式的字 $\approx$-等价

$$\left((-1)_{[0]}(-1)_{[1]}\right)^{\alpha}\left((-1)_{[3]}(-1)_{[2]}\right)^{\beta}\left(X_{[0,3]}X_{[1,2]}\right)^{\gamma}Q$$

其中 Q是形如 $(-1)_{[a]}X_{[a,a+1]}$ 的生成元乘积，其中 $a\geq 4$，且 α、β、$\gamma\in\{0,\ 1\}$.
证明。 通过分析 $[\![w\left(H_{[0,1]}H_{[3,2]}\right)]\!]$ 和 $[\![\left(H_{[0,1]}H_{[3,2]}\right)w]\!]$ 对 $\mathbb{C}^N$典范基的向量的作用，特别注意到 $[\![w]\!]$ 除其元素的符号外只是一个置换矩阵，可以证明 w 在语义上必定等价于一个具有所示形式的字。由此根据推论 A.5即可得出结论。□

推论 A.7。 对于生成元 A、A'、B、B'构成的任意字，若其中不含形如 $\left(H_{[a,b]}H_{[c,d]}\right)$的生成元，且 $[\![AA']\!]=[\![BB']\!]=I$和 $[\![A\left(H_{[0,1]}H_{[3,2]}\right)A']\!]=[\![B\left(H_{[0,1]}H_{[3,2]}\right)B']\!]$，则 $A\left(H_{[0,1]}H_{[3,2]}\right)A'\approx B\left(H_{[0,1]}H_{[3,2]}\right)B'$。
证明。可得

$$\begin{aligned}[\![B'A\left(H_{[0,1]}H_{[3,2]}\right)]\!] &= [\![B'A\left(H_{[0,1]}H_{[3,2]}\right)A'A]\!]\\ &= [\![B'B\left(H_{[0,1]}H_{[3,2]}\right)B'A]\!]\\ &= [\![\left(H_{[0,1]}H_{[3,2]}\right)B'A]\!].\end{aligned}$$

因此，根据引理 A.6， $B'A$ 与 $\approx$-等价于以下形式的一个字

$$\left((-1)_{[0]}(-1)_{[1]}\right)^{\alpha}\left((-1)_{[3]}(-1)_{[2]}\right)^{\beta}\left(X_{[0,3]}X_{[1,2]}\right)^{\gamma}Q$$

其中 Q是由形如 $(-1)_{[a]}X_{[a,a+1]}$ 的生成元构成的乘积，其中 $a\geq 4$，且 α，β，$\gamma\in\{0,\ 1\}$。于是有

$$\begin{aligned}A\left(H_{[0,1]}H_{[3,2]}\right)A' &\overset{\text{Corollary A.5}}{\approx} BB'A\left(H_{[0,1]}H_{[3,2]}\right)A'\\ &\approx B\left((-1)_{[0]}(-1)_{[1]}\right)^{\alpha}\left((-1)_{[3]}(-1)_{[2]}\right)^{\beta}\left(X_{[0,3]}X_{[1,2]}\right)^{\gamma}Q\left(H_{[0,1]}H_{[3,2]}\right)A'\\ &\overset{(38)}{\approx} B\left((-1)_{[0]}(-1)_{[1]}\right)^{\alpha}\left((-1)_{[3]}(-1)_{[2]}\right)^{\beta}\left(X_{[0,3]}X_{[1,2]}\right)^{\gamma}\left(H_{[0,1]}H_{[3,2]}\right)QA'\end{aligned}$$

$$
\begin{aligned}
&\left(H_{[a,b]}H_{[c,d]}\right) \approx \Sigma_{a,\ b,\ c,\ d} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{a,\ b,\ c,\ d}\{a,\ b\} \cap \{c,\ d\} = \emptyset (65) \left(H_{[a,b]}H_{[c,d]}\right) \approx \left(H_{[c,d]}H_{[a,b]}\right)\{a,\ b\} \cap \{c,\ d\} = \emptyset (66) \left(H_{[b,a]}H_{[c,d]}\right) \approx \left(H_{[a,b]}H_{[c,d]}\right) \left((-1)_{[b]}X_{[a,b]}\right)\{a,\ b\} \cap \{c,\ d\} = \emptyset (67) \left((-1)_{[a]}X_{[a,a+1]}\right) \left(H_{[a,b]}H_{[c,d]}\right) \approx \left(H_{[a+1,b]}H_{[c,d]}\right) \left((-1)_{[a]}X_{[a,a+1]}\right) \quad |\{a,\ a+1,\ b,\ c,\ d\}| = 5 (68) \left((-1)_{[a]}X_{[a,a+1]}\right) \left(H_{[a+1,b]}H_{[c,d]}\right) \approx \left(H_{[a,b]}H_{[c,d]}\right) \left((-1)_{[a]}X_{[a,b]}\right) \left((-1)_{[a]}X_{[a,a+1]}\right) \quad |\{a,\ a+1,\ b,\ c,\ d\}| = 5 (69) \\
&\left(H_{[a,b]}H_{[a,b]}\right) \approx \epsilon (70) \left(H_{[a,b]}H_{[c,d]}\right) \left(H_{[c,d]}H_{[e,f]}\right) \approx \left(H_{[a,b]}H_{[e,f]}\right) (71) \left(H_{[a,b]}H_{[b,a]}\right) \approx \left((-1)_{[b]}X_{[a,b]}\right) (72) \\
&\left(H_{[a,b]}H_{[c,d]}\right) \left(H_{[e,f]}H_{[g,h]}\right) \approx \left(H_{[a,b]}H_{[e,f]}\right) \left(H_{[c,d]}H_{[g,h]}\right)\{c,\ d\} \cap \{e,\ f\} = \emptyset (73) \left((-1)_{[a]}X_{[a,b]}\right) \left(H_{[c,d]}H_{[e,f]}\right) \approx \left(H_{[c,d]}H_{[e,f]}\right) \left((-1)_{[a]}X_{[a,b]}\right)\{a,\ b\} \cap \{c,\ d,\ e,\ f\} = \emptyset (74) \left((-1)_{[a]}X_{[a,b]}\right) \left(H_{[a,b]}H_{[c,d]}\right) \approx \left(H_{[a,b]}H_{[c,d]}\right) \left((-1)_{[b]}X_{[a,b]}\right)\{a,\ b\} \cap \{c,\ d\} = \emptyset (75) \left((-1)_{[a]}X_{[a,e]}\right) \left(H_{[a,b]}H_{[c,d]}\right) \approx \left(H_{[e,b]}H_{[c,d]}\right) \left((-1)_{[a]}X_{[a,e]}\right) \quad |\{a,\ e,\ b,\ c,\ d\}| = 5 \left((-1)_{[a]}X_{[a,e]}\right) \left(H_{[e,b]}H_{[c,d]}\right) \approx \left(H_{[a,b]}H_{[c,d]}\right) \left((-1)_{[a]}X_{[a,b]}\right) \left((-1)_{[a]}X_{[a,e]}\right) \quad |\{a,\ e,\ b,\ c,\ d\}| = 5 (77)
\end{aligned}
\tag{76}
$$

图 10：更多实用的辅助方程。方程（65）与方程（35）相同，但不再对元组$(G_n(a)\ G_n(b)\ G_n(c)\ G_n(d))$施加限制。

$$
\begin{aligned}
&\overset{\text{Corollary A.5}}{\approx} && B\left((-1)_{[0]}(-1)_{[1]}\right)^{\alpha}\left(X_{[0,3]}X_{[1,2]}\right)^{\gamma}\left((-1)_{[0]}(-1)_{[1]}\right)^{\beta}\left(H_{[0,1]}H_{[3,2]}\right)QA' \\
&\overset{(39)}{\approx} && B\left((-1)_{[0]}(-1)_{[1]}\right)^{\alpha}\left(X_{[0,3]}X_{[1,2]}\right)^{\gamma}\left(H_{[0,1]}H_{[3,2]}\right)\left((-1)_{[0]}(-1)_{[1]}\right)^{\beta}QA' \\
&\overset{(44)}{\approx} && B\left((-1)_{[0]}(-1)_{[1]}\right)^{\alpha}\left(H_{[0,1]}H_{[3,2]}\right)\left(X_{[0,3]}X_{[1,2]}\right)^{\gamma}\left((-1)_{[0]}(-1)_{[1]}\right)^{\beta}QA' \\
&\overset{(39)}{\approx} && B\left(H_{[0,1]}H_{[3,2]}\right)\left((-1)_{[0]}(-1)_{[1]}\right)^{\alpha}\left(X_{[0,3]}X_{[1,2]}\right)^{\gamma}\left((-1)_{[0]}(-1)_{[1]}\right)^{\beta}QA' \\
&\overset{\text{Corollary A.5}}{\approx} && B\left(H_{[0,1]}H_{[3,2]}\right)\left((-1)_{[0]}(-1)_{[1]}\right)^{\alpha}\left((-1)_{[3]}(-1)_{[2]}\right)^{\beta}\left(X_{[0,3]}X_{[1,2]}\right)^{\gamma}QA' \\
&\approx && B\left(H_{[0,1]}H_{[3,2]}\right)B'AA' \\
&\overset{\text{Corollary A.5}}{\approx} && B\left(H_{[0,1]}H_{[3,2]}\right)B'.
\end{aligned}
$$

□

推论 A.8。图 *10* 中的方程可由图 *8*中的方程推出。 证明。

方程证明 (65)： 已知方程（35）、（36）和（37）及其可靠性，并且方程（65）对 a、 b、 c、 d 的所有取值均可靠，结论可直接由推论 A.7得出。

方程证明 (66)：

$$
\begin{aligned}
\left(H_{[a,b]}H_{[c,d]}\right) &\overset{(65)}{\approx} \Sigma_{a,b,c,d} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{a,b,c,d} \\
&\overset{\text{Corollary A.7}}{\approx} \Sigma_{c,d,a,b} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{c,d,a,b} \\
&\overset{(65)}{\approx} \left(H_{[c,d]}H_{[a,b]}\right)
\end{aligned}
$$

方程证明 (67)：

$$
\begin{aligned}
\left(H_{[b,a]}H_{[c,d]}\right) &\overset{(65)}{\approx} \Sigma_{b,a,c,d} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{b,a,c,d} \\
&\overset{\text{Corollary A.7}}{\approx} \Sigma_{c,d,a,b} \circ \left((-1)_{[3]}(-1)_{[4]}\right)\left(H_{[0,1]}H_{[3,2]}\right)\left((-1)_{[2]}(-1)_{[4]}\right) \circ \Sigma'_{c,d,a,b} \\
&\overset{(40)}{\approx} \Sigma_{c,d,a,b} \circ \left(H_{[0,1]}H_{[3,2]}\right)\left((-1)_{[3]}(-1)_{[4]}\right)\left((-1)_{[2]}X_{[2,3]}\right)\left((-1)_{[2]}(-1)_{[4]}\right) \circ \Sigma'_{c,d,a,b} \\
&\overset{\text{Corollary A.5}}{\approx} \Sigma_{c,d,a,b} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{c,d,a,b} \circ \left((-1)_{[b]}X_{[a,b]}\right)
\end{aligned}
$$

$$\begin{aligned}
&\overset{\text{Corollary A.7}}{\approx} && \Sigma_{a,b,c,d} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{a,b,c,d} \circ \left((-1)_{[b]} X_{[a,b]}\right) \\
&\overset{(65)}{\approx} && \left(H_{[a,b]} H_{[c,d]}\right) \left((-1)_{[b]} X_{[a,b]}\right)
\end{aligned}$$

方程证明 (68):

$$\begin{aligned}
& && \left((-1)_{[a]} X_{[a,a+1]}\right) \left(H_{[a,b]} H_{[c,d]}\right) \\
&\overset{\text{Corollary A.5}}{\approx} && \left((-1)_{[a]} X_{[a,a+1]}\right) \left(H_{[a,b]} H_{[c,d]}\right) \left((-1)_{[a+1]} X_{[a,a+1]}\right) \left((-1)_{[a]} X_{[a,a+1]}\right) \\
&\overset{(65)}{\approx} && \left((-1)_{[a]} X_{[a,a+1]}\right) \circ \Sigma_{a,b,c,d} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{a,b,c,d} \circ \left((-1)_{[a+1]} X_{[a,a+1]}\right) \left((-1)_{[a]} X_{[a,a+1]}\right) \\
&\overset{\text{Corollary A.7}}{\approx} && \Sigma_{a+1,b,c,d} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{a+1,b,c,d} \circ \left((-1)_{[a]} X_{[a,a+1]}\right) \\
&\overset{(65)}{\approx} && \left(H_{[a+1,b]} H_{[c,d]}\right) \left((-1)_{[a]} X_{[a,a+1]}\right)
\end{aligned}$$

方程证明 (69):

$$\begin{aligned}
& && \left((-1)_{[a]} X_{[a,a+1]}\right) \left(H_{[a+1,b]} H_{[c,d]}\right) \\
&\overset{\text{Corollary A.5}}{\approx} && \left((-1)_{[a]} X_{[a,a+1]}\right) \left(H_{[a+1,b]} H_{[c,d]}\right) \left((-1)_{[a+1]} X_{[a,a+1]}\right) \left((-1)_{[a]} X_{[a,a+1]}\right) \\
&\overset{(65)}{\approx} && \left((-1)_{[a]} X_{[a,a+1]}\right) \circ \Sigma_{a+1,b,c,d} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{a+1,b,c,d} \circ \left((-1)_{[a+1]} X_{[a,a+1]}\right) \left((-1)_{[a]} X_{[a,a+1]}\right) \\
&\overset{\text{Corollary A.7}}{\approx} && \Sigma_{c,d,a,b} \circ \left((-1)_{[3]} (-1)_{[4]}\right) \left(H_{[0,1]} H_{[3,2]}\right) \left((-1)_{[3]} (-1)_{[4]}\right) \circ \Sigma'_{c,d,a,b} \circ \left((-1)_{[a]} X_{[a,a+1]}\right) \\
&\overset{(40)}{\approx} && \Sigma_{c,d,a,b} \circ \left(H_{[0,1]} H_{[3,2]}\right) \left((-1)_{[3]} (-1)_{[4]}\right) \left((-1)_{[2]} X_{[2,3]}\right) \left((-1)_{[3]} (-1)_{[4]}\right) \circ \Sigma'_{c,d,a,b} \circ \left((-1)_{[a]} X_{[a,a+1]}\right) \\
&\overset{\text{Corollary A.5}}{\approx} && \Sigma_{c,d,a,b} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{c,d,a,b} \circ \left((-1)_{[a]} X_{[a,b]}\right) \circ \left((-1)_{[a]} X_{[a,a+1]}\right) \\
&\overset{\text{Corollary A.7}}{\approx} && \Sigma_{a,b,c,d} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{a,b,c,d} \circ \left((-1)_{[a]} X_{[a,b]}\right) \circ \left((-1)_{[a]} X_{[a,a+1]}\right) \\
&\overset{(65)}{\approx} && \left(H_{[a,b]} H_{[c,d]}\right) \left((-1)_{[a]} X_{[a,b]}\right) \circ \left((-1)_{[a]} X_{[a,a+1]}\right)
\end{aligned}$$

方程证明 (70):

$$\begin{aligned}
\left(H_{[a,b]} H_{[a,b]}\right) &\overset{(42)}{\approx} && \left(H_{[a,b]} H_{[e,f]}\right) \left(H_{[e,f]} H_{[a,b]}\right) \\
&\overset{(66)}{\approx} && \left(H_{[a,b]} H_{[e,f]}\right) \left(H_{[a,b]} H_{[e,f]}\right) \\
&\overset{(65)}{\approx} && \Sigma_{a,b,e,f} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{a,b,e,f} \circ \Sigma_{a,b,e,f} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{a,b,e,f} \\
&\overset{\text{Corollary A.5}}{\approx} && \Sigma_{a,b,e,f} \circ \left(H_{[0,1]} H_{[3,2]}\right) \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{a,b,e,f} \\
&\overset{(41)}{\approx} && \Sigma_{a,b,e,f} \circ \Sigma'_{a,b,e,f} \\
&\overset{\text{Corollary A.5}}{\approx} && \epsilon
\end{aligned}$$

其中 e, f在图 8中定义。

方程（71）的证明：首先，考虑 a, b, c, d, e, f 互不相同的情形。设 $\mathrm{T}_{a,b,c,d,e,f}$ 和 $\mathrm{T}'_{a,b,c,d,e,f}$ 是由 P_N 的生成元构成的字，且不包含形如 $(H_{[g,h]} H_{[i,j]})$ 的生成元，使得 $\left[\!\left[\mathrm{T}'_{a,b,c,d,e,f}\right]\!\right] = \left[\!\left[\mathrm{T}_{a,b,c,d,e,f}\right]\!\right]^{-1}$，并且 $\left[\!\left[\mathrm{T}_{a,b,c,d,e,f}\right]\!\right] = \tau \circ \left[\!\left[(-1)_{[\nu]}\right]\!\right]$，其中 $\nu \notin \{0, 1, 3, 2, 4, 5\}$，而 τ 是一个置换矩阵，分别将 $|0\rangle$ $|1\rangle$ $|3\rangle$ $|2\rangle$ $|4\rangle$ $|5\rangle$ 映射到 $|a\rangle$ $|b\rangle$ $|c\rangle$ $|d\rangle$ $|e\rangle$ $|f\rangle$。[13] 我们有

$$\begin{aligned}
& && \left(H_{[a,b]} H_{[c,d]}\right) \left(H_{[c,d]} H_{[e,f]}\right) \\
&\overset{(65)}{\approx} && \Sigma_{a,b,c,d} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{a,b,c,d} \circ \Sigma_{c,d,e,f} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{c,d,e,f} \\
&\overset{\text{Corollary A.7}}{\approx} && \mathcal{T}_{a,b,c,d,e,f} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \mathcal{T}'_{a,b,c,d,e,f} \circ \mathcal{T}_{a,b,c,d,e,f} \circ \Sigma_{3,2,4,5} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \Sigma'_{3,2,4,5} \circ \mathcal{T}'_{a,b,c,d,e,f} \\
&\overset{(65)}{\approx} && \mathcal{T}_{a,b,c,d,e,f} \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ \mathcal{T}'_{a,b,c,d,e,f} \circ \mathcal{T}_{a,b,c,d,e,f} \circ \left(H_{[3,2]} H_{[4,5]}\right) \circ \mathcal{T}'_{a,b,c,d,e,f}
\end{aligned}$$

[13] $\mathrm{T}_{a,b,c,d,e}$以及 $\mathrm{T}'_{a,b,c,d,e,f}$（以及 $\Xi^{(a,b,e,f)}{}_{i,j|c,d}$和 $\Xi^{(a,b,e,f)\prime}{}_{i,j|c,d}$如下）都可以用与 $\Sigma_{a,b,c,d}$和 $\Sigma_{a,b,c,d}$类似的方式构造（见附录 E.1）。

$$
\begin{aligned}
&\overset{\text{Corollary A.5}}{\approx} && \mathcal{T}_{a,b,c,d,e,f} \circ \left(H_{[0,1]}H_{[3,2]}\right)\left(H_{[3,2]}H_{[4,5]}\right) \circ \mathcal{T}'_{a,b,c,d,e,f} \\
&\overset{(43)}{\approx} && \mathcal{T}_{a,b,c,d,e,f} \circ \left(X_{[0,3]}X_{[1,2]}\right)\left(H_{[3,2]}H_{[4,5]}\right)\left(X_{[0,3]}X_{[1,2]}\right) \circ \mathcal{T}'_{a,b,c,d,e,f} \\
&\overset{(65)}{\approx} && \mathcal{T}_{a,b,c,d,e,f} \circ \left(X_{[0,3]}X_{[1,2]}\right) \circ \Sigma_{3,2,4,5} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{3,2,4,5} \circ \left(X_{[0,3]}X_{[1,2]}\right) \circ \mathcal{T}'_{a,b,c,d,e,f} \\
&\overset{\text{Corollary A.7}}{\approx} && \Sigma_{a,b,e,f} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{a,b,e,f} \\
&\overset{(65)}{\approx} && \left(H_{[a,b]}H_{[e,f]}\right)
\end{aligned}
$$

接下来，我们考虑 $|\{a、\ b、\ e、\ f\}| \le 3$和 $\{c、\ d\} \cap \{a、\ b、\ e、\ f\} = \emptyset$的情形。令 $i、\ j$为 $i < j$下 $\{0, ..., N-1\} \setminus \{a、\ b、\ e、\ f\}$ 中最小的两个元素。令 $\Xi^{(a,b,e,f)}_{i,\ j\,|\,c、\ d}$和 $\Xi^{(a,b,e,f)\prime}_{i、\ j\,|\,c、\ d}$为 P_N的生成元上的字，其中不含形如 $\left(H_{[g,h]}H_{[k,\ell]}\right)$的生成元，并满足 $\left[\!\left[\Xi^{(a,b,e,f)\prime}_{i\ j\,|\,c}\right]\!\right]_{、\ 、\ d} = \left[\!\left[\Xi^{(a,b,e,f)}_{i\ j\,|\,c}\right]\!\right]_{、\ 、\ d}$，且满足 $\left[\!\left[\Xi^{(a,b,e,f)}_{i\ j\,|\,c}\right]\!\right]_{、\ 、\ d} = \xi$或 $\left[\!\left[\Xi^{(a,b,e,f)}_{i\ j\,|\,c}\right]\!\right]_{、\ 、\ d} = \xi \circ \left[\!\left[(-1)_{[\rho]}\right]\!\right]$，其中[14] $\rho \notin \{a、\ b、\ c、\ d、\ e、\ f、\ i、\ j\}$，并且 ξ 是一个置换矩阵，分别将 $|a\ \ |b\ \ |e\ \ |f\ \ |i\ \ |j$ 映射到 $|a\ \ |b\ \ |e\ \ |f\ \ |c\ \ |d$。我们有

$$
\begin{aligned}
& && \left(H_{[a,b]}H_{[c,d]}\right)\left(H_{[c,d]}H_{[e,f]}\right) \\
&\overset{(65)}{\approx} && \Sigma_{a,b,c,d} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{a,b,c,d} \circ \Sigma_{c,d,e,f} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{c,d,e,f} \\
&\overset{\text{Corollary A.7}}{\approx} && \Xi^{(a,b,e,f)}_{i,j\,|\,c,d} \circ \Sigma_{a,b,i,j} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{a,b,i,j} \circ \Xi^{(a,b,e,f)\prime}_{i,j\,|\,c,d} \circ \Xi^{(a,b,e,f)}_{i,j\,|\,c,d} \circ \Sigma_{i,j,e,f} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{i,j,e,f} \circ \Xi^{(a,b,e,f)\prime}_{i,j\,|\,c,d} \\
&\overset{(65)}{\approx} && \Xi^{(a,b,e,f)}_{i,j\,|\,c,d} \circ \left(H_{[a,b]}H_{[i,j]}\right) \circ \Xi^{(a,b,e,f)\prime}_{i,j\,|\,c,d} \circ \Xi^{(a,b,e,f)}_{i,j\,|\,c,d} \circ \left(H_{[i,j]}H_{[e,f]}\right) \circ \Xi^{(a,b,e,f)\prime}_{i,j\,|\,c,d} \\
&\overset{\text{Corollary A.5}}{\approx} && \Xi^{(a,b,e,f)}_{i,j\,|\,c,d} \circ \left(H_{[a,b]}H_{[i,j]}\right)\left(H_{[i,j]}H_{[e,f]}\right) \circ \Xi^{(a,b,e,f)\prime}_{i,j\,|\,c,d} \\
&\overset{(42)}{\approx} && \Xi^{(a,b,e,f)}_{i,j\,|\,c,d} \circ \left(H_{[a,b]}H_{[e,f]}\right) \circ \Xi^{(a,b,e,f)\prime}_{i,j\,|\,c,d} \\
&\overset{(65)}{\approx} && \Xi^{(a,b,e,f)}_{i,j\,|\,c,d} \circ \Sigma_{a,b,e,f} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{a,b,e,f} \circ \Xi^{(a,b,e,f)\prime}_{i,j\,|\,c,d} \\
&\overset{\text{Corollary A.7}}{\approx} && \Sigma_{a,b,e,f} \circ \left(H_{[0,1]}H_{[3,2]}\right) \circ \Sigma'_{a,b,e,f} \\
&\overset{(65)}{\approx} && \left(H_{[a,b]}H_{[e,f]}\right)
\end{aligned}
$$

我们已经处理了所有满足 $\{c,d\} \cap \{a,b,e,f\} = \emptyset$ 的情形，因此还需处理满足 $\{c,d\} \cap \{a,b,e,f\} \neq \emptyset$ 的情形。在这种情形下，令 i,j 为 $\{0,...,N-1\} \setminus \{a,b,c,d,e,f\}$ 中两个最小的元素，其中 $i<j$。我们有

$$
\begin{aligned}
& && \left(H_{[a,b]}H_{[c,d]}\right)\left(H_{[c,d]}H_{[e,f]}\right) \\
&\overset{\text{previous cases}}{\approx} && \left(H_{[a,b]}H_{[i,j]}\right)\left(H_{[i,j]}H_{[c,d]}\right)\left(H_{[c,d]}H_{[i,j]}\right)\left(H_{[i,j]}H_{[e,f]}\right) \\
&\overset{\text{previous cases}}{\approx} && \left(H_{[a,b]}H_{[i,j]}\right)\left(H_{[i,j]}H_{[i,j]}\right)\left(H_{[i,j]}H_{[e,f]}\right) \\
&\overset{(70)}{\approx} && \left(H_{[a,b]}H_{[i,j]}\right)\left(H_{[i,j]}H_{[e,f]}\right) \\
&\overset{\text{previous cases}}{\approx} && \left(H_{[a,b]}H_{[e,f]}\right)
\end{aligned}
$$

方程证明 (72)：令 c，d满足 $c \neq d$且 $\{a,\ b\} \cap \{c,\ d\} = \emptyset$。这些指标存在，因为 $N \ge 4$。我们有

$$
\begin{aligned}
\left(H_{[a,b]}H_{[b,a]}\right) &\overset{(71)}{\approx} \left(H_{[a,b]}H_{[c,d]}\right)\left(H_{[c,d]}H_{[b,a]}\right) \\
&\overset{(66)}{\approx} \left(H_{[a,b]}H_{[c,d]}\right)\left(H_{[b,a]}H_{[c,d]}\right) \\
&\overset{(67)}{\approx} \left(H_{[a,b]}H_{[c,d]}\right)\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[b]}X_{[a,b]}\right) \\
&\overset{(66)}{\approx} \left(H_{[a,b]}H_{[c,d]}\right)\left(H_{[c,d]}H_{[a,b]}\right)\left((-1)_{[b]}X_{[a,b]}\right) \\
&\overset{(71)}{\approx} \left(H_{[a,b]}H_{[a,b]}\right)\left((-1)_{[b]}X_{[a,b]}\right) \\
&\overset{(70)}{\approx} \left((-1)_{[b]}X_{[a,b]}\right)
\end{aligned}
$$

[14] ρ存在，因为 $N \ge 8$，且 $|\{a,b,e,f\}| \le 3$意味着 $|\{a,b,c,d,e,f,i,j\}| < 8$。

方程证明 (73):

$$\begin{aligned}
\left(H_{[a,b]}H_{[c,d]}\right)\left(H_{[e,f]}H_{[g,h]}\right) &\overset{(70)}{\approx} \left(H_{[a,b]}H_{[c,d]}\right)\left(H_{[c,d]}H_{[c,d]}\right)\left(H_{[e,f]}H_{[g,h]}\right)\\
&\overset{(71)}{\approx} \left(H_{[a,b]}H_{[c,d]}\right)\left(H_{[c,d]}H_{[e,f]}\right)\left(H_{[e,f]}H_{[c,d]}\right)\left(H_{[e,f]}H_{[g,h]}\right)\\
&\overset{(66)}{\approx} \left(H_{[a,b]}H_{[c,d]}\right)\left(H_{[c,d]}H_{[e,f]}\right)\left(H_{[c,d]}H_{[e,f]}\right)\left(H_{[e,f]}H_{[g,h]}\right)\\
&\overset{(71)}{\approx} \left(H_{[a,b]}H_{[e,f]}\right)\left(H_{[c,d]}H_{[g,h]}\right)
\end{aligned}$$

方程证明 (74):

$$\begin{aligned}
\left((-1)_{[a]}X_{[a,b]}\right)\left(H_{[c,d]}H_{[e,f]}\right) &\overset{(33)}{\approx} \left((-1)_{[a]}X_{[b,a]}\right)\left(H_{[c,d]}H_{[e,f]}\right)\\
&\overset{(72)}{\approx} \left(H_{[b,a]}H_{[a,b]}\right)\left(H_{[c,d]}H_{[e,f]}\right)\\
&\overset{(73)}{\approx} \left(H_{[b,a]}H_{[c,d]}\right)\left(H_{[a,b]}H_{[e,f]}\right)\\
&\overset{(66)}{\approx} \left(H_{[c,d]}H_{[b,a]}\right)\left(H_{[e,f]}H_{[a,b]}\right)\\
&\overset{(73)}{\approx} \left(H_{[c,d]}H_{[e,f]}\right)\left(H_{[b,a]}H_{[a,b]}\right)\\
&\overset{(72)}{\approx} \left(H_{[c,d]}H_{[e,f]}\right)\left((-1)_{[a]}X_{[b,a]}\right)\\
&\overset{(33)}{\approx} \left(H_{[c,d]}H_{[e,f]}\right)\left((-1)_{[a]}X_{[a,b]}\right)
\end{aligned}$$

方程证明 (75):

$$\begin{aligned}
\left((-1)_{[a]}X_{[a,b]}\right)\left(H_{[a,b]}H_{[c,d]}\right) &\overset{(33)(72)}{\approx} \left(H_{[b,a]}H_{[a,b]}\right)\left(H_{[a,b]}H_{[c,d]}\right)\\
&\overset{(71)}{\approx} \left(H_{[b,a]}H_{[c,d]}\right)\\
&\overset{(67)}{\approx} \left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[b]}X_{[a,b]}\right)
\end{aligned}$$

方程的证明 (76)和 (77) :

- 如果 $e-a=1$，那么方程（76）和（77）分别只是方程（68）和（69）的特例。
- 如果 $a-e=1$，那么我们按如下方式进行。[15] 方程（76）：

$$\begin{aligned}
&\left((-1)_{[a]}X_{[a,a-1]}\right)\left(H_{[a,b]}H_{[c,d]}\right)\\
\overset{\text{Corollary A.5}}{\approx}\ &\left((-1)_{[a-1]}X_{[a-1,a]}\right)^3\left(H_{[a,b]}H_{[c,d]}\right)\\
\overset{(69)}{\approx}\ &\left((-1)_{[a-1]}X_{[a-1,a]}\right)^2\left(H_{[a-1,b]}H_{[c,d]}\right)\left((-1)_{[a-1]}X_{[a-1,b]}\right)\left((-1)_{[a-1]}X_{[a-1,a]}\right)\\
\overset{(68)}{\approx}\ &\left((-1)_{[a-1]}X_{[a-1,a]}\right)\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[a-1]}X_{[a-1,a]}\right)\left((-1)_{[a-1]}X_{[a-1,b]}\right)\left((-1)_{[a-1]}X_{[a-1,a]}\right)\\
\overset{(69)}{\approx}\ &\left(H_{[a-1,b]}H_{[c,d]}\right)\left((-1)_{[a-1]}X_{[a-1,b]}\right)\left((-1)_{[a-1]}X_{[a-1,a]}\right)\left((-1)_{[a-1]}X_{[a-1,a]}\right)\left((-1)_{[a-1]}X_{[a-1,b]}\right)\left((-1)_{[a-1]}X_{[a-1,a]}\right)\\
\overset{\text{Corollary A.5}}{\approx}\ &\left(H_{[a-1,b]}H_{[c,d]}\right)\left((-1)_{[a]}X_{[a,a-1]}\right)
\end{aligned}$$

以及对于方程（77）：

$$\begin{aligned}
&\left((-1)_{[a]}X_{[a,a-1]}\right)\left(H_{[a-1,b]}H_{[c,d]}\right)\\
\overset{\text{Corollary A.5}}{\approx}\ &\left((-1)_{[a-1]}X_{[a-1,a]}\right)^3\left(H_{[a-1,b]}H_{[c,d]}\right)\\
\overset{(68)}{\approx}\ &\left((-1)_{[a-1]}X_{[a-1,a]}\right)^2\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[a-1]}X_{[a-1,a]}\right)\\
\overset{(69)}{\approx}\ &\left((-1)_{[a-1]}X_{[a-1,a]}\right)\left(H_{[a-1,b]}H_{[c,d]}\right)\left((-1)_{[a-1]}X_{[a-1,b]}\right)\left((-1)_{[a-1]}X_{[a-1,a]}\right)^2\\
\overset{(68)}{\approx}\ &\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[a-1]}X_{[a-1,a]}\right)\left((-1)_{[a-1]}X_{[a-1,b]}\right)\left((-1)_{[a-1]}X_{[a-1,a]}\right)^2\\
\overset{\text{Corollary A.5}}{\approx}\ &\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,a-1]}\right)
\end{aligned}$$

[15]注意，这些推导与下述情形完全相同： $e<a$且 $\{a,\dots,e\}\cap\{b,c,d\}=\emptyset$

- 若 $a < e$ 且 $\{a,\ \ldots\ldots,\ e\} \cap \{b,\ c,\ d\} = \emptyset$，则对 $e - a$进行有限归纳。基本情形已经处理。方程（76）的归纳步骤如下：

$$\begin{aligned}
&\left((-1)_{[a]}X_{[a,e]}\right)\left(H_{[a,b]}H_{[c,d]}\right) \\
\overset{(49)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,e]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left(H_{[a,b]}H_{[c,d]}\right) \\
\overset{\text{induction hypothesis}}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,e]}\right)\left(H_{[a+1,b]}H_{[c,d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{\text{induction hypothesis}}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left(H_{[e,b]}H_{[c,d]}\right)\left((-1)_{[a+1]}X_{[a+1,e]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(74)}{\approx}\ &\left(H_{[e,b]}H_{[c,d]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,e]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(49)}{\approx}\ &\left(H_{[e,b]}H_{[c,d]}\right)\left((-1)_{[a]}X_{[a,e]}\right)
\end{aligned}$$

方程（77）的归纳步骤如下：

$$\begin{aligned}
&\left((-1)_{[a]}X_{[a,e]}\right)\left(H_{[e,b]}H_{[c,d]}\right) \\
\overset{(49)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,e]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left(H_{[e,b]}H_{[c,d]}\right) \\
\overset{(74)}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,e]}\right)\left(H_{[e,b]}H_{[c,d]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{\text{induction hypothesis}}{\approx}\ &\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left(H_{[a+1,b]}H_{[c,d]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a+1]}X_{[a+1,e]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{\text{case } a-e=1 \text{ for (76)}}{\approx}\ &\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a+1]}X_{[a+1,e]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(51)}{\approx}\ &\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,b]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,e]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right) \\
\overset{(49)}{\approx}\ &\left(H_{[e,b]}H_{[c,d]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,e]}\right)
\end{aligned}$$

- 若 $e < a$ 且 $\{e,\ \ldots\ldots,\ a\} \cap \{b,\ c,\ d\} = \emptyset$，则可由前一种情况推出结果，如下所示。对于方程（76）：

$$\begin{aligned}
&\left((-1)_{[a]}X_{[a,e]}\right)\left(H_{[a,b]}H_{[c,d]}\right) \\
\overset{\text{Corollary A.5}}{\approx}\ &\left((-1)_{[e]}X_{[e,a]}\right)^3\left(H_{[a,b]}H_{[c,d]}\right) \\
\overset{\text{case } a<e \text{ of (77)}}{\approx}\ &\left((-1)_{[e]}X_{[e,a]}\right)^2\left(H_{[e,b]}H_{[c,d]}\right)\left((-1)_{[e]}X_{[e,b]}\right)\left((-1)_{[e]}X_{[e,a]}\right) \\
\overset{\text{case } a<e \text{ of (76)}}{\approx}\ &\left((-1)_{[e]}X_{[e,a]}\right)\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[e]}X_{[e,a]}\right)\left((-1)_{[e]}X_{[e,b]}\right)\left((-1)_{[e]}X_{[e,a]}\right) \\
\overset{\text{case } a<e \text{ of (77)}}{\approx}\ &\left(H_{[e,b]}H_{[c,d]}\right)\left((-1)_{[e]}X_{[e,b]}\right)\left((-1)_{[e]}X_{[e,a]}\right)\left((-1)_{[e]}X_{[e,a]}\right)\left((-1)_{[e]}X_{[e,b]}\right)\left((-1)_{[e]}X_{[e,a]}\right) \\
\overset{\text{Corollary A.5}}{\approx}\ &\left(H_{[e,b]}H_{[c,d]}\right)\left((-1)_{[a]}X_{[a,e]}\right)
\end{aligned}$$

对于方程（77）：

$$\begin{aligned}
&\left((-1)_{[a]}X_{[a,e]}\right)\left(H_{[e,b]}H_{[c,d]}\right) \\
\overset{\text{Corollary A.5}}{\approx}\ &\left((-1)_{[e]}X_{[e,a]}\right)^3\left(H_{[e,b]}H_{[c,d]}\right) \\
\overset{\text{case } a<e \text{ of (76)}}{\approx}\ &\left((-1)_{[e]}X_{[e,a]}\right)^2\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[e]}X_{[e,a]}\right) \\
\overset{\text{case } a<e \text{ of (77)}}{\approx}\ &\left((-1)_{[e]}X_{[e,a]}\right)\left(H_{[e,b]}H_{[c,d]}\right)\left((-1)_{[e]}X_{[e,b]}\right)\left((-1)_{[e]}X_{[e,a]}\right)^2 \\
\overset{\text{case } a<e \text{ of (76)}}{\approx}\ &\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[e]}X_{[e,a]}\right)\left((-1)_{[e]}X_{[e,b]}\right)\left((-1)_{[e]}X_{[e,a]}\right)^2 \\
\overset{\text{Corollary A.5}}{\approx}\ &\left(H_{[a,b]}H_{[c,d]}\right)\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,e]}\right)
\end{aligned}$$

- 为处理一般情形，证明以下辅助方程将很有帮助：

$$\left((-1)_{[a]}X_{[a,c]}\right)\left(H_{[a,b]}H_{[c,d]}\right) \approx \left(H_{[c,b]}H_{[a,d]}\right)\left((-1)_{[a]}X_{[a,d]}\right)\left((-1)_{[a]}X_{[a,c]}\right) \qquad |\{a,b,c,d\}| = 4,\ [a,c] \cap \{b,d\} = \emptyset,\ |a-c| \le N-4 \tag{78}$$

其中，$[a,c]$ 表示区间 $\{a,\ \ldots c\}$（若 $a < c$），或 $\{c,\ \ldots a\}$ 如果 $c < a$.

为证明方程 (78)，令 $f_b, g_b, f_d, g_d \in \{0, ..., N-1\} \setminus [a,c]$ 满足 $f_b \neq g_b$, $f_d \neq g_d$, $f_b, g_b \neq d$ 且 $f_d, g_d \neq b$。这些指标的存在性得益于条件 $|a-c| \leq N-4$。可得以下推导（其中对方程 (76) 和 (77) 的引用均指其在上文证明的受限版本）：

$$
\begin{aligned}
&\left((-1)_{[a]}X_{[a,c]}\right)\left(H_{[a,b]}H_{[c,d]}\right)\\
\overset{(71)}{\approx}\ &\left((-1)_{[a]}X_{[a,c]}\right)\left(H_{[a,b]}H_{[f_d,g_d]}\right)\left(H_{[f_d,g_d]}H_{[f_b,g_b]}\right)\left(H_{[f_b,g_b]}H_{[c,d]}\right)\\
\overset{(66)}{\approx}\ &\left((-1)_{[a]}X_{[a,c]}\right)\left(H_{[a,b]}H_{[f_d,g_d]}\right)\left(H_{[f_d,g_d]}H_{[f_b,g_b]}\right)\left(H_{[c,d]}H_{[f_b,g_b]}\right)\\
\overset{(76)}{\approx}\ &\left(H_{[c,b]}H_{[f_d,g_d]}\right)\left((-1)_{[a]}X_{[a,c]}\right)\left(H_{[f_d,g_d]}H_{[f_b,g_b]}\right)\left(H_{[c,d]}H_{[f_b,g_b]}\right)\\
\overset{(74)}{\approx}\ &\left(H_{[c,b]}H_{[f_d,g_d]}\right)\left(H_{[f_d,g_d]}H_{[f_b,g_b]}\right)\left((-1)_{[a]}X_{[a,c]}\right)\left(H_{[c,d]}H_{[f_b,g_b]}\right)\\
\overset{(77)}{\approx}\ &\left(H_{[c,b]}H_{[f_d,g_d]}\right)\left(H_{[f_d,g_d]}H_{[f_b,g_b]}\right)\left(H_{[a,d]}H_{[f_b,g_b]}\right)\left((-1)_{[a]}X_{[a,d]}\right)\left((-1)_{[a]}X_{[a,c]}\right)\\
\overset{(66)}{\approx}\ &\left(H_{[c,b]}H_{[f_d,g_d]}\right)\left(H_{[f_d,g_d]}H_{[f_b,g_b]}\right)\left(H_{[f_b,g_b]}H_{[a,d]}\right)\left((-1)_{[a]}X_{[a,d]}\right)\left((-1)_{[a]}X_{[a,c]}\right)\\
\overset{(71)}{\approx}\ &\left(H_{[c,b]}H_{[a,d]}\right)\left((-1)_{[a]}X_{[a,d]}\right)\left((-1)_{[a]}X_{[a,c]}\right)
\end{aligned}
$$

现在，为了在一般情形下证明方程（76）和（77），令 $i_0 < \cdots < i_k$ 满足 $1 \leq k \leq 4$，$\{i_0, \ldots, i_k\} \cap [a,e] = \{a, e\}$，$\{i_1, \ldots, i_{k-1}\} \cap [b,c,d] = \emptyset$，$i_0 = a$，$i_k = e$，$\{i_1, \ldots, i_{k-1}\} \subset \{b, c, d\}$（也就是说，$i_0$ 是 a，i_k 是 e，$i_1, \ldots, i_{k-1}$ 中介于 a 和 e 之间的指标）。由推论 A.5可得

$$\left((-1)_{[a]}X_{[a,e]}\right) \approx \left((-1)_{[i_1]}X_{[i_0,i_1]}\right)\cdots\left((-1)_{[i_{k-1}]}X_{[i_{k-2},i_{k-1}]}\right) \circ \left((-1)_{[i_{k-1}]}X_{[i_{k-1},i_k]}\right) \circ \left((-1)_{[i_{k-2}]}X_{[i_{k-2},i_{k-1}]}\right)\cdots\left((-1)_{[i_0]}X_{[i_0,i_1]}\right), \quad \text{(C)}$$

且对每个 $j \in \{0, \ldots, k-2\}$，

$$\left((-1)_{[i_{j+1}]}X_{[i_j,i_{j+1}]}\right) \approx \left((-1)_{[i_j]}X_{[i_j,i_{j+1}]}\right)^3 \quad \text{(D)}$$

每一对指标 i_j, i_{j+1} 都满足其余三个指标均位于区间 $[i_j, i_{j+1}]$ 之外，这也意味着 $|i_j - i_{j+1}| \leq N-4$。因此，从 $\left((-1)_{[a]}X_{[a,e]}\right)\left(H_{[a,b]}H_{[c,d]}\right)$（分别从 $\left((-1)_{[a]}X_{[a,e]}\right)\left(H_{[e,b]}H_{[c,d]}\right)$）开始，并按照方程（C）和方程（D）分解 $\left((-1)_{[a]}X_{[a,e]}\right)$ 后，我们可以结合方程（78）和方程（75），利用方程（76）和方程（77）中已经证明的情形（这四个方程都可能与方程（66）和方程（67）结合使用），将所有 $\left((-1)_{[i_j]}X_{[i_j,i_{j+1}]}\right)$ 推至右侧。可以验证，所得结果为 $\left(H_{[e,b]}H_{[c,d]}\right)$（分别为 $\left(H_{[a,b]}H_{[c,d]}\right)$），其右侧乘有一个由形如 $\left((-1)_{[f]}X_{[f,g]}\right)$ 和 $\left((-1)_{[g]}X_{[f,g]}\right)$ 的生成元构成的乘积。根据推论 A.5，我们可以将该乘积改写为 $\left((-1)_{[a]}X_{[a,e]}\right)$（分别改写为 $\left((-1)_{[a]}X_{[a,b]}\right)\left((-1)_{[a]}X_{[a,e]}\right)$），由此完成证明。 □

推论 A.9。由 $\mathcal{P}_N$ 的生成元构成且至多包含一个形如 $\left(H_{[a,b]}H_{[c,d]}\right)$ 的生成元的任意字，都与唯一一个字 $\approx$ 等价；这个字称为其标准形，其形式为

$$P \qquad or \qquad \left(H_{[a,b]}H_{[c,d]}\right)P$$

其中 $a < b$；$c < d$；$\{a, b\} \neq \{c, d\}$；若 $\{a, b\} \cap \{c, d\} = \emptyset$ 则 $a < c$；且 P 形如 (B)。此外，语义相同的两个字具有相同的标准形。

证明。

由语义可知唯一性：通过分析 $[\![P]\!]$ 和 $\left[\!\left[\left(H_{[a,b]}H_{[c,d]}\right)P\right]\!\right]$ 对 $\mathbb{C}^N$ 的典范基的作用，并注意到 $[\![P]\!]$ 除其元素的符号外是一个置换矩阵。

存在性：如果字中不包含任何 $\left(H_{[a,b]}H_{[c,d]}\right)$，那么结论可直接由引理 A.4 推得。

如果字中只包含一个 $\left(H_{[a,b]}H_{[c,d]}\right)$，那么它具有如下形式：$w = p_1\left(H_{[a,b]}H_{[c,d]}\right)p_2$ 其中 p_1，p_2 是两个不包含形如 $\left(H_{[e,f]}H_{[g,h]}\right)$ 的生成元的字。正如我们在引理 A.4 的证明中所示，字 p_1 可以写成形如 $\left((-1)_{[j]}X_{[j,j+1]}\right)$ 的生成元之积，因此只需证明 $p_1 = \left((-1)_{[j]}X_{[j,j+1]}\right)$ 的结论。为便于实际处理，我们将证明一个稍微更一般的情形，即 $p_1 = \left((-1)_{[j]}X_{[j,k]}\right)$。

设 $e, f \in \{0, ..., N-1\}$，使得 $e \neq f$ 且 $e, f \notin \{a, b, c, d, j, k\}$。这样的指标存在，因为 $N \geq 8$。我们 has

$$\left((-1)_{[j]}X_{[j,k]}\right)\left(H_{[a,b]}H_{[c,d]}\right) \overset{(71)}{\approx} \left((-1)_{[j]}X_{[j,k]}\right)\left(H_{[a,b]}H_{[e,f]}\right)\left(H_{[e,f]}H_{[c,d]}\right)$$

$$\overset{(66)}{\approx} \left((-1)_{[j]}X_{[j,k]}\right)\left(H_{[a,b]}H_{[e,f]}\right)\left(H_{[c,d]}H_{[e,f]}\right)$$

我们首先考虑 $\left((-1)_{[j]}X_{[j,k]}\right)\left(H_{[a,b]}H_{[e,f]}\right)$。共有七种情形：

- 如果 $a = j$ 并且 $b = k$，那么$\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[a,b]} H_{[e,f]}\right)$ (75) $\approx \left(H_{[a,b]} H_{[e,f]}\right)\left(\left(-1\right)_{[k]} X_{[j,k]}\right)$ (33) $\approx \left(H_{[a,b]} H_{[e,f]}\right)\left(\left(-1\right)_{[k]} X_{[k,j]}\right)$

- 如果 $a = k$ 且 $b = j$，则$\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[a,b]} H_{[e,f]}\right) = \left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[k,j]} H_{[e,f]}\right)(67)\approx \left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[j,k]} H_{[e,f]}\right)\left(\left(-1\right)_{[k]} X_{[j,k]}\right)(75)\approx \left(H_{[j,k]} H_{[e,f]}\right)\left(\left(-1\right)_{[k]} X_{[j,k]}\right)\left(\left(-1\right)_{[k]} X_{[j,k]}\right)$(53)(21) $\approx \left(H_{[j,k]} H_{[e,f]}\right)\left(\left(-1\right)^{[j]} \left(-1\right)_{[k]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(\left(-1\right)^{[k]} \left(-1\right)_{[j]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)(56)\approx \left(H_{[j,k]} H_{[e,f]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(\left(-1\right)^{[j]} \left(-1\right)_{[k]}\right)\left(\left(-1\right)^{[k]} \left(-1\right)_{[j]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)$(22)(20)$\approx \left(H_{[j,k]} H_{[e,f]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)^2$

- 若 $a = j$ 且 $b \neq k$，则$\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[a,b]} H_{[e,f]}\right) = \left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[j,b]} H_{[e,f]}\right)$(76) $\approx \left(H_{[k,b]} H_{[e,f]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)$

- 若 $a = k$ 且 $b \neq j$，则$\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[a,b]} H_{[e,f]}\right) = \left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[k,b]} H_{[e,f]}\right)$(77) $\approx \left(H_{[j,b]} H_{[e,f]}\right)\left(\left(-1\right)_{[j]} X_{[j,b]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)$

- 若 $b = j$ 且 $a \neq k$，则$\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[a,b]} H_{[e,f]}\right) = \left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[a,j]} H_{[e,f]}\right)(67)\approx \left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(H_{[j,a]} H_{[e,f]}\right)\left(\left(-1\right)_{[a]} X_{[j,a]}\right)(76)\approx \left(H_{[k,a]} H_{[e,f]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(\left(-1\right)_{[a]} X_{[j,a]}\right)$(67) $\approx \left(H_{[a,k]} H_{[e,f]}\right)\left(\left(-1\right)_{[k]} X_{[a,k]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(\left(-1\right)_{[a]} X_{[j,a]}\right)(33)\approx \left(H_{[a,k]} H_{[e,f]}\right)\left(\left(-1\right)_{[k]} X_{[k,a]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(\left(-1\right)_{[a]} X_{[j,a]}\right)(51)\approx \left(H_{[a,k]} H_{[e,f]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(\left(-1\right)_{[k]} X_{[j,k]}\right)\left(\left(-1\right)_{[k]} X_{[k,a]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(\left(-1\right)_{[a]} X$

$_{[j,a]}\right)$

推论 A.$\approx$ 5 $\left(H_{[a,k]} H_{[e,f]}\right)\left(\left(-1\right)_{[j]} X_{[j,k]}\right)\left(\left(-1\right)_{[j]} X_{[j,a]}\right)\left(\left(-1\right)_{[a]} X_{[j,a]}\right)$45

$$\overset{(51)}{\approx} \quad \left(H_{[a,k]}H_{[e,f]}\right)\left((-1)_{[j]}X_{[j,k]}\right)$$

- 若 $b=k$ 且 $a\neq j$，则

$$\begin{aligned}
&\left((-1)_{[j]}X_{[j,k]}\right)\left(H_{[a,b]}H_{[e,f]}\right)\\
=\;&\left((-1)_{[j]}X_{[j,k]}\right)\left(H_{[a,k]}H_{[e,f]}\right)\\
\overset{(67)}{\approx}\;&\left((-1)_{[j]}X_{[j,k]}\right)\left(H_{[k,a]}H_{[e,f]}\right)\left((-1)_{[a]}X_{[k,a]}\right)\\
\overset{(77)}{\approx}\;&\left(H_{[j,a]}H_{[e,f]}\right)\left((-1)_{[j]}X_{[j,a]}\right)\left((-1)_{[j]}X_{[j,k]}\right)\left((-1)_{[a]}X_{[k,a]}\right)\\
\overset{(33)}{\approx}\;&\left(H_{[j,a]}H_{[e,f]}\right)\left((-1)_{[j]}X_{[j,a]}\right)\left((-1)_{[j]}X_{[j,k]}\right)\left((-1)_{[a]}X_{[a,k]}\right)
\end{aligned}$$

- 如果 $\{a,b\}\cap\{j,k\}=\emptyset$，那么

$$\left((-1)_{[j]}X_{[j,k]}\right)\left(H_{[a,b]}H_{[e,f]}\right)\overset{(74)}{\approx}\left(H_{[a,b]}H_{[e,f]}\right)\left((-1)_{[j]}X_{[j,k]}\right)$$

在所有七种情形中，我们都将 $\left((-1)_{[j]}X_{[j,k]}\right)\left(H_{[a,b]}H_{[e,f]}\right)$ 变换为某个 $\left(H_{[a',b']}H_{[e,f]}\right)q$，其中 $\{a',b'\}\cap\{e,f\}=\emptyset$，且 q 是由一个到三个形如 $\left((-1)_{[j']}X_{[j',k']}\right)$ 的生成元相乘得到的，这些生成元满足 j',k' 与 e,f 互不相同。然后，我们可以用同样的推理将 $q\left(H_{[c,d]}H_{[e,f]}\right)$ 变换为某个 $\left(H_{[c',d']}H_{[e,f]}\right)p$，其中 $\{c',d'\}\cap\{e,f\}=\emptyset$，且 p 是由一个到九个形如 $\left((-1)_{[j']}X_{[j',k']}\right)$ 的生成元相乘得到的。

这表明字 $w=p_1\left(H_{[a,b]}H_{[c,d]}\right)p_2$ 可以写成 $\left(H_{[a',b']}H_{[e,f]}\right)\left(H_{[c',d']}H_{[e,f]}\right)p_3$ 的形式，其中 p_3 是形如 $\left((-1)_{[j']}X_{[j',k']}\right)$ 的生成元之积。下一步是确保指标 a',b,c',d' 满足所需条件。如果 $a'<b'$

，那么我们按如下方式继续

$$\left(H_{[a',b']}H_{[e,f]}\right)\left(H_{[c',d']}H_{[e,f]}\right)p_3\overset{(67)}{\approx}\left(H_{[b',a']}H_{[e,f]}\right)\left((-1)_{[a']}X_{[b',a']}\right)\left(H_{[c',d']}H_{[e,f]}\right)p_3$$

$$\overset{(33)}{\approx}\left(H_{[b',a']}H_{[e,f]}\right)\left((-1)_{[a']}X_{[a',b']}\right)\left(H_{[c',d']}H_{[e,f]}\right)p_3$$

并采用与上文相同的推理，得到 $\left(H_{[b',a']}H_{[e,f]}\right)\left(H_{[c'',d'']}H_{[e,f]}\right)p_3'$，其中 p_3' 是形如 $\left((-1)_{[j']}X_{[j',k']}\right)$ 的生成元之积。因此，我们得到 $\left(H_{[a'',b'']}H_{[e,f]}\right)\left(H_{[c'',d'']}H_{[e,f]}\right)p_3'$，其中 p_3' 是形如 $\left((-1)_{[j']}X_{[j',k']}\right)$ 的生成元之积，且 $a''<b''$。然后，若 $c''<d''$，我们再应用一次方程 (67) 和 (33)，得到 $\left(H_{[a'',b'']}H_{[e,f]}\right)\left(H_{[d'',c'']}H_{[e,f]}\right)p_3''$，其中 p_3'' 仍是形如 $\left((-1)_{[j']}X_{[j',k']}\right)$ 的生成元之积。因此，我们得到 $\left(H_{[a'',b'']}H_{[e,f]}\right)\left(H_{[c''',d''']}H_{[e,f]}\right)p_3''$，其中 p_3'' 是形如 $\left((-1)_{[j']}X_{[j',k']}\right)$ 的生成元之积，且 $a''<b''$ 和 $c'''<d'''$。

最后，我们得到

$$\left(H_{[a'',b'']}H_{[e,f]}\right)\left(H_{[c''',d''']}H_{[e,f]}\right)p_3''\overset{(66)}{\approx}\left(H_{[a'',b'']}H_{[e,f]}\right)\left(H_{[e,f]}H_{[c''',d''']}\right)p_3''$$

$$\overset{(71)}{\approx}\left(H_{[a'',b'']}H_{[c''',d''']}\right)p_3''$$

在以下情形中应用方程 (70)：$\{a'',b''\}=\{c''',d'''\}$；或者在以下情形中应用方程 (66)：$\{a'',b''\}\cap\{c''',d'''\}=\emptyset$ 并且 $a''>c'''$，再对 p_3'' 应用引理 A.4，即可得到所需形式。□

推论 A.10. 给定生成元 $\mathcal{P}_N$ 上的任意两个字 w,w'，其中一个至多包含一个形如 $\left(H_{[a,b]}H_{[c,d]}\right)$ 的生成元，另一个至多包含两个这种形式的生成元。若 $[\![w]\!]=[\![w']\!]$，则 $w\approx w'$。

证明。通过反复应用推论 A.9，次数等于形如 $\left(H_{[a,b]}H_{[c,d]}\right)$ 的生成元的个数，我们可以将 w（分别地，w'）变换为一个字 $\tilde{w}$（分别地，$\tilde{w}'$），其中这类生成元的个数至多与 w（分别地，w'）中的个数相同，且所有这类生成元都位于左侧。接着，分析 $[\![\tilde{w}]\!]$ 和 $[\![\tilde{w}']\!]$ 对 $\mathbb{C}^N$ 的典范基的作用可知，若 $\tilde{w}$ 或 $\tilde{w}'$ 含有两个形如 $\left(H_{[a,b]}H_{[c,d]}\right)$ 的生成元，则必然可以借助方程 (66)、(70)、(71) 和 (73) 将它们相消。最后，由标准形的唯一性，再次应用推论 A.9，即得结论。□

推论 A.11. 图 *11* 的方程是图 *8* 的方程的推论。证明。

$$(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]}) \approx_{(79)} (H_{[0,2]}H_{[1,3]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]}) \approx_{(80)} (H_{[0,2]}H_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})$$

图 11：更简单的版本 方程（45）和（46）的版本，虽然更难解码，但在推导中更容易使用 **s.**

证明 方程 (79):$(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})$推论 A.$\approx^{5}$ $((-1)_{[4]}X_{[2,3]})\,((-1)_{[4]}X_{[2,3]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})$推论 A.$\approx^{10}$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,1]}H_{[0,3]})\,((-1)_{[4]}X_{[2,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})$推论 A.$\approx^{10}$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[0,1]})\,((-1)_{[4]}X_{[2,3]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})$推论 A.$\approx^{5}$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)_{[4]}X_{[2,3]})\,(H_{[0,2]}H_{[1,3]})$推论 A.$\approx^{10}$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,3]}H_{[1,2]})\,((-1)_{[4]}X_{[2,3]})(70)\approx$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[0,1]})\,(H_{[7,6]}H_{[7,6]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,3]}H_{[1,2]})\,((-1)_{[4]}X_{[2,3]})(73)\approx$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[7,6]})\,(H_{[0,1]}H_{[7,6]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,3]}H_{[1,2]})\,((-1)_{[4]}X_{[2,3]})(66)\approx$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[7,6]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,3]}H_{[1,2]})\,((-1)_{[4]}X_{[2,3]})(73)\approx$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,3]}H_{[1,2]})\,((-1)_{[4]}X_{[2,3]})(21)\approx$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)^{[0]}(-1)_{[1]})\,(H_{[0,3]}H_{[1,2]})\,((-1)_{[4]}X_{[2,3]})(45)\approx$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[0]}(-1)_{[1]})\,(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)_{[4]}X_{[2,3]})(21)\approx$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)_{[4]}X_{[2,3]})(73)\approx$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[7,6]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)_{[4]}X_{[2,3]})(66)\approx$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[7,6]})\,(H_{[0,1]}H_{[7,6]})\,((-1)_{[4]}X_{[2,3]})(73)\approx$ $((-1)_{[4]}X_{[2,3]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[0,1]})\,(H_{[7,6]}H_{[7,6]})\,((-1)_{[4]}X_{[2,3]})$47

$$\overset{(70)}{\approx} \left((-1)_{[4]}X_{[2,3]}\right)\left(H_{[0,3]}H_{[1,2]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[0,3]}\right)\left(H_{[1,2]}H_{[0,1]}\right)\left((-1)_{[4]}X_{[2,3]}\right)$$

推论 A.$\approx$ $\left(H_{[0,2]}H_{[1,3]}\right)\left((-1)^{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right)$

方程证明(80):

$$(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\text{推论 A.}\approx^{5}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\text{推论 A.}\approx^{10}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,((-1)_{[2]}X_{[0,3]})\,((-1)_{[6]}X_{[2,3]})\,(H_{[1,3]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\text{推论 A.}\approx^{10}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[3,4]})\,(X_{[1,2]}X_{[0,3]})\,((-1)_{[6]}X_{[2,3]})\,(H_{[1,5]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\text{推论 A.}\approx^{10}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[3,4]})\,(H_{[2,5]}H_{[3,2]})\,(X_{[1,2]}X_{[0,3]})\,((-1)_{[6]}X_{[2,3]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\text{推论 A.}\approx^{5}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[3,4]})\,(H_{[2,5]}H_{[3,2]})\,((-1)^{[2]}(-1)_{[3]})\,(X_{[1,2]}X_{[0,3]})\,((-1)_{[6]}X_{[2,3]})\,(H_{[0,4]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\text{推论 A.}\approx^{10}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[3,4]})\,(H_{[2,5]}H_{[3,2]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,4]}H_{[2,5]})\,(X_{[1,2]}X_{[0,3]})\,((-1)_{[6]}X_{[2,3]})\,(H_{[0,2]}H_{[1,3]})\text{推论 A.}\approx^{10}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[3,4]})\,(H_{[2,5]}H_{[3,2]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(70)(73)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[3,4]})\,(H_{[2,5]}H_{[3,2]})\,(H_{[7,6]}H_{[4,5]})\,(H_{[7,6]}H_{[4,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(73)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[3,4]})\,(H_{[2,5]}H_{[7,6]})\,(H_{[3,2]}H_{[4,5]})\,(H_{[7,6]}H_{[4,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(66)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[3,4]})\,(H_{[7,6]}H_{[2,5]})\,(H_{[3,2]}H_{[4,5]})\,(H_{[7,6]}H_{[4,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(73)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[1,2]}H_{[7,6]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[3,2]}H_{[4,5]})\,(H_{[7,6]}H_{[4,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(66)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[0,3]})\,(H_{[7,6]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[3,2]}H_{[4,5]})\,(H_{[7,6]}H_{[4,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(73)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[3,2]}H_{[4,5]})\,(H_{[7,6]}H_{[4,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(46)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[7,6]}H_{[4,5]})\,(H_{[3,2]}H_{[4,5]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(73)(70)(66)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,2]}H_{[7,6]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(73)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,2]}H_{[3,4]})\,(H_{[7,6]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(66)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,2]}H_{[3,4]})\,(H_{[2,5]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(73)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,2]}H_{[3,4]})\,(H_{[2,5]}H_{[0,3]})\,(H_{[7,6]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(66)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,2]}H_{[3,4]})\,(H_{[2,5]}H_{[0,3]})\,(H_{[1,2]}H_{[7,6]})\,(H_{[7,6]}H_{[0,1]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})$$

$$(71)\approx((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,2]}H_{[3,4]})\,(H_{[2,5]}H_{[0,3]})\,(H_{[1,2]}H_{[0,1]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})\text{推论 A.}\approx^{10}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,2]}H_{[3,4]})\,(H_{[2,5]}H_{[0,3]})\,(H_{[3,4]}X_{[1,2]})\,((-1)_{[6]}X_{[2,3]})\,(H_{[1,3]}H_{[0,1]})\text{推论 A.}\approx^{10}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[3,2]}H_{[3,4]})\,(X_{[1,2]}X_{[0,3]})\,((-1)_{[6]}X_{[2,3]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\text{推论 A.}\approx^{10}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)^{[2]}(-1)_{[3]})\,(X_{[1,2]}X_{[0,3]})\,((-1)_{[6]}X_{[2,3]})\,(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\text{推论 A.}\approx^{5}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,(X_{[1,2]}X_{[0,3]})\,((-1)_{[6]}X_{[2,3]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\text{推论 A.}\approx^{10}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,(X_{[1,2]}X_{[0,3]})\,((-1)_{[6]}X_{[2,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\text{推论 A.}\approx^{10}((-1)_{[6]}X_{[2,3]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)^{[2]}(-1)_{[3]})\,((-1)_{[6]}X_{[2,3]})\,(H_{[0,2]}H_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\text{推论 A.}\approx^{5}(H_{[0,2]}H_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})49$$

请注意，由于推论 A.10 取代了推论 A.5 以及方程 (66)、(70)、(71) 和 (73)，上述两次推导中的所有步骤本都可以由推论 A.10加以证明，45所示方程和方程 (46) 的使用除外。□

推论 A.12. 图 *8* 的等式理论是完备的，即对于任意两个由 w、w' 生成元构成的字，其中生成元来自 $\mathcal{P}_N$，若 $[\![w]\!] = [\![w']\!]$ 则 $w \approx w'$。

证明。 根据 Reidemeister-Schreier 定理，只需证明附录 A.3.2 中的所有方程都是图 8中方程的推论。注意，附录 A.3.2中的所有方程，除了方程（ϵ-b6*）至（HZ-b6*）以及（ϵ-d3*）至（HZ-d4*），其一侧至多包含一个形如 $(H_{[a,b]}H_{[c,d]})$ 的生成元，另一侧至多包含两个这样的生成元。因此，由于这些方程在语义上是可靠的，推论 A.10 表明它们都是图 8中方程的推论。因此，只需手动推导方程（ϵ-b6*）至（HZ-b6*）以及（ϵ-d3*）至（HZ-d4*）。

方程证明 (ϵ-b6*):

$$\begin{aligned}
(H_{[0,1]}H_{[0,1]})\,(H_{[0,1]}H_{[2,3]}) &\overset{(71)}{\approx} (H_{[0,1]}H_{[2,3]})\\
&\overset{(66)}{\approx} (H_{[2,3]}H_{[0,1]})\\
&\overset{(71)}{\approx} (H_{[2,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})
\end{aligned}$$

方程证明 (Z-b6*):

$$\begin{aligned}
((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,(H_{[0,1]}H_{[2,3]}) &\overset{(70)}{\approx} ((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[2,3]})\\
&\overset{\text{Corollary A.10}}{\approx} (H_{[0,1]}H_{[2,3]})\,((-1)_{[0]}X_{[0,1]})\\
&\overset{(66)}{\approx} (H_{[2,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\\
&\overset{(70)}{\approx} (H_{[2,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})
\end{aligned}$$

方程证明 (H-b6*):

$$\begin{aligned}
(H_{[0,1]}H_{[0,1]})\,(H_{[2,3]}H_{[0,1]}) &\overset{(70)}{\approx} (H_{[2,3]}H_{[0,1]})\\
&\overset{(66)}{\approx} (H_{[0,1]}H_{[2,3]})\\
&\overset{(70)}{\approx} (H_{[0,1]}H_{[2,3]})\,(H_{[0,1]}H_{[0,1]})
\end{aligned}$$

方程证明 (HZ-b6*):

$$\begin{aligned}
(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,(H_{[2,3]}H_{[0,1]}) &\overset{(70)}{\approx} ((-1)_{[0]}X_{[0,1]})\,(H_{[2,3]}H_{[0,1]})\\
&\overset{(66)}{\approx} ((-1)_{[0]}X_{[0,1]})\,(H_{[0,1]}H_{[2,3]})\\
&\overset{(75)}{\approx} (H_{[0,1]}H_{[2,3]})\,((-1)_{[1]}X_{[0,1]})\\
&\overset{(70)}{\approx} (H_{[0,1]}H_{[2,3]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})
\end{aligned}$$

方程证明 (ϵ-d3*):

$$\begin{aligned}
&(H_{[0,1]}H_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\\
&((-1)_{[1]}(-1)_{[0]})\,((-1)_{[1]}(-1)_{[1]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\\
\overset{(20)(71)}{\approx}\ &(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})\\
\overset{(79)}{\approx}\ &(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\\
\overset{(20)(70)(71)}{\approx}\ &(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[1]}(-1)_{[0]})\,((-1)_{[1]}(-1)_{[1]})\\
&(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})
\end{aligned}$$

方程证明 (Z-d3*):

$$\begin{aligned}
&((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\\
&((-1)_{[1]}(-1)_{[0]})\,((-1)_{[1]}(-1)_{[1]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})
\end{aligned}$$

$$(20)(71)\approx \quad ((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$$

推论 A.$\approx^{10}$ $((-1)^{[1]}(-1)_{[4]})\,((-1)_{[4]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$

推论 A.$\approx^{10}$ $((-1)^{[1]}(-1)_{[4]})\,(H_{[0,1]}H_{[0,2]})\,((-1)^{[4]}(-1)_{[1]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$

推论 A.$\approx^{10}$ $((-1)^{[1]}(-1)_{[4]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)^{[4]}(-1)_{[1]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$推论 A.$\approx^{10}$ $((-1)^{[1]}(-1)_{[4]})\,(H_{[0,2]}H_{[1,3]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[4]}(-1)_{[1]})(79)\approx$ $((-1)^{[1]}(-1)_{[4]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)^{[1]}(-1)_{[4]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[4]}(-1)_{[1]})$推论 A.$\approx^{10}$ $(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)^{[1]}(-1)_{[4]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[4]}(-1)_{[1]})$推论 A.$\approx^{10}$ $(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,((-1)^{[4]}(-1)_{[1]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[4]}(-1)_{[1]})$推论 A.$\approx^{10}$ $(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})$(20)(70)(71)$\approx$ $(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})$

方程证明（H ⁅ˆ⁆-d3*）：

$$(H_{[0,1]}H_{[0,1]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,(H_{[0,1]}H_{[0,1]})((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})$$(20)(70)(71)$\approx$ $(H_{[0,2]}H_{[1,3]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})(79)\approx$ $(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})$(20)(70)(71)$\approx$ $(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,(H_{[0,1]}H_{[0,1]})$

方程证明 (HZ-d3*):

$$
\begin{aligned}
&(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})(20)(70)(71)\approx\ (H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})(71)(66)\approx\ (H_{[0,1]}H_{[4,5]})\,(H_{[0,1]}H_{[4,5]})\,((-1)_{[0]}X_{[0,1]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\text{推论 A.}\approx\ {}^{10}(H_{[0,1]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[4,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})(73)(66)\approx\ (H_{[0,1]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[4,5]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\text{推论 A.}\approx\ {}^{10}(H_{[0,1]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[4,5]})\,(H_{[4,5]}H_{[0,2]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})(71)\approx\ (H_{[0,1]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[4,5]})\,(H_{[4,5]}H_{[0,2]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\text{推论 A.}\approx\ {}^{10}(H_{[0,1]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[4,5]})\,(H_{[4,5]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[4,5]}H_{[0,2]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})(71)\approx\ (H_{[0,1]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[4,5]}H_{[0,2]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\text{推论 A.}\approx\ {}^{10}(H_{[0,1]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[0,2]}H_{[4,5]})\,(H_{[1,3]}H_{[0,1]})(73)\approx\ (H_{[0,1]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[0,2]}H_{[1,3]})\,(H_{[4,5]}H_{[0,1]})\text{推论 A.}\approx\ {}^{10}(H_{[0,1]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})\,((-1)\\
&{}_{[1]}X_{[1,3]})\,(H_{[4,5]}H_{[0,1]})(20)(71)\approx\ (H_{[0,1]}H_{[4,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})((-1)^{[1]}(-1)_{[0]})\,((-1)\\
&{}^{[1]}(-1)_{[1]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[4,5]}H_{[0,1]})(\text{Z-d3*})\approx\ (H_{[0,1]}H_{[4,5]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)\\
&{}^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,(H_{[4,5]}H_{[0,1]})(20)(70)(71)\approx\ (H_{[0,1]}H_{[4,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)\\
&{}_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,(H_{[4,5]}H_{[0,1]})\text{推论 A.}\approx\ {}^{10}(H_{[0,1]}H_{[4,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((\\
&-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[4,5]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})(73)(66)\approx\ (H_{[0,1]}H_{[4,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)\\
&{}_{[0]})\,(H_{[4,5]}H_{[0,1]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\text{推论 A.}\approx\ {}^{10}(H_{[0,1]}H_{[4,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[4,5]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)\\
&{}_{[0]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\text{推论 A.}\approx\ {}^{10}(H_{[0,1]}H_{[4,5]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[0,2]}H_{[1,3]})\,(H_{[4,5]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})\,((-1)\\
&{}_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})(73)(66)\approx\ (H_{[0,1]}H_{[4,5]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[4,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\\
&\text{推论 A.}\approx\ {}^{10}(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})(20)(70)(71)\approx\ (H_{[0,1]}H_{[0,2]})\,((-1)\\
&{}_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})
\end{aligned}
$$

方程证明 (ϵ-d4*):

$$
\begin{aligned}
&(H_{[0,1]}H_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)\\
&{}_{[1]})\,(H_{[0,4]}H_{[0,1]})\,(H_{[0,1]}H_{[1,5]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})(20)(71)\\
&\approx\ (H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]})(80)\\
&\approx\ (H_{[0,2]}H_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)^{[1]}(-1)_{[0]})\,(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})(20)(70)(71)\\
&\approx\ (H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,(H_{[0,4]}H_{[0,1]})\,(H_{[0,1]}H_{[1,5]})\,(H_{[0,1]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})\\
&(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})52
\end{aligned}
$$

方程证明（Z-d4*）：

$$((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})$$
$$((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})\,(H_{[0,4]}H_{[0,1]})\,(H_{[0,1]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$$

$\overset{(20)(71)}{\approx}$
$$((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})$$
$$((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$((-1)^{[1]}(-1)_{[6]})\,((-1)_{[6]}X_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})$$
$$((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$((-1)^{[1]}(-1)_{[6]})\,(H_{[0,1]}H_{[0,2]})\,((-1)^{[6]}(-1)_{[1]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})$$
$$((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$((-1)^{[1]}(-1)_{[6]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,4]})\,((-1)^{[6]}(-1)_{[1]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})$$
$$((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$((-1)^{[1]}(-1)_{[6]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})\,((-1)^{[6]}(-1)_{[1]})$$
$$((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$((-1)^{[1]}(-1)_{[6]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})$$
$$((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,((-1)^{[6]}(-1)_{[1]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$((-1)^{[1]}(-1)_{[6]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})$$
$$((-1)^{[1]}(-1)_{[0]})\,(H_{[0,4]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)^{[6]}(-1)_{[1]})$$

$\overset{(80)}{\approx}$
$$((-1)^{[1]}(-1)_{[6]})\,(H_{[0,2]}H_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)^{[1]}(-1)_{[0]})$$
$$(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[6]}(-1)_{[1]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)^{[1]}(-1)_{[6]})\,(H_{[0,4]}H_{[1,5]})\,((-1)^{[1]}(-1)_{[0]})$$
$$(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[6]}(-1)_{[1]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)^{[1]}(-1)_{[6]})\,((-1)^{[1]}(-1)_{[0]})$$
$$(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[6]}(-1)_{[1]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})$$
$$(H_{[0,1]}H_{[0,4]})\,((-1)^{[1]}(-1)_{[6]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[6]}(-1)_{[1]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})$$
$$(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,2]})\,((-1)^{[1]}(-1)_{[6]})\,(H_{[1,3]}H_{[0,1]})\,((-1)^{[6]}(-1)_{[1]})$$

$\overset{\text{推论 A.10}}{\approx}$
$$(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})$$
$$(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})$$

$\overset{(20)(70)(71)}{\approx}$
$$(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[0,1]})\,(H_{[0,1]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})$$
$$(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})$$

方程证明 (H-d4*):

$$(H_{[0,1]}H_{[0,1]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,(H_{[0,4]}H_{[0,1]})\,(H_{[0,1]}H_{[1,5]})\,(H_{[0,1]}H_{[0,1]})$$
$$((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})\,(H_{[0,1]}H_{[0,4]})\,(H_{[1,5]}H_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[0,1]})$$

$$\overset{(20)(70)(71)}{\approx} \left(H_{[0,2]}H_{[1,3]}\right)\left(H_{[0,4]}H_{[1,5]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left(H_{[1,5]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\overset{(80)}{\approx} \left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,4]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[0,4]}H_{[1,5]}\right)\left(H_{[0,2]}H_{[1,3]}\right)\overset{(20)(70)(71)}{\approx} \left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left((-1)_{[1]}(-1)_{[1]}\right)\left(H_{[0,4]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,5]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left(H_{[0,1]}H_{[0,1]}\right)$$

P方程（H门Z-d4*）的证明：$\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\left(H_{[0,2]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left(H_{[0,4]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left((-1)_{[1]}(-1)_{[1]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\overset{(20)(71)}{\approx} \left(H_{[0,1]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\left(H_{[0,2]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left(H_{[0,4]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\overset{(71)(66)}{\approx} \left(H_{[0,1]}H_{[6,7]}\right)\left(H_{[0,1]}H_{[6,7]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\left(H_{[0,2]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left(H_{[0,4]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\overset{10}{\left((-1)_{[1]}X_{[0,1]}\right)}\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\overset{\text{推论 A.}}{\approx} \left(H_{[0,1]}H_{[6,7]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[6,7]}\right)\left(H_{[0,2]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left(H_{[0,4]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\overset{(73)(66)}{\approx} \left(H_{[0,1]}H_{[6,7]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left(H_{[1,3]}H_{[6,7]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left(H_{[0,4]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\overset{10}{\left((-1)_{[1]}X_{[0,1]}\right)}\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\overset{\text{推论 A.}}{\approx} \left(H_{[0,1]}H_{[6,7]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[6,7]}\right)\left(H_{[0,4]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\overset{(73)(66)}{\approx} \left(H_{[0,1]}H_{[6,7]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,4]}\right)\left(H_{[1,5]}H_{[6,7]}\right)\overset{10}{\left((-1)_{[1]}X_{[1,5]}\right)}\left((-1)_{[1]}X_{[0,1]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[0,1]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\overset{\text{推论 A.}}{\approx} \left(H_{[0,1]}H_{[6,7]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[6,7]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[6,7]}\right)\left(H_{[6,7]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,1]}\right)\overset{\text{推论 A.}}{\approx} \left(H_{[0,1]}H_{[6,7]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[0,4]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\left(H_{[6,7]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[6,7]}\right)\left(H_{[6,7]}H_{[0,1]}\right)\overset{\text{推论 A.}}{\approx} \left(H_{[0,1]}H_{[6,7]}\right)\left((-1)_{[1]}X_{[0,1]}\right)\left(H_{[0,1]}H_{[0,2]}\right)\left((-1)_{[3]}X_{[1,3]}\right)\left(H_{[1,3]}H_{[0,4]}\right)\left((-1)_{[5]}X_{[1,5]}\right)\left(H_{[1,5]}H_{[0,1]}\right)\left((-1)_{[0]}X_{[0,1]}\right)\left((-1)_{[1]}(-1)_{[0]}\right)\left(H_{[0,4]}H_{[1,5]}\right)\left((-1)_{[1]}X_{[1,5]}\right)\left(H_{[0,2]}H_{[1,3]}\right)\left((-1)_{[1]}X_{[1,3]}\right)\left(H_{[6,7]}H_{[0,1]}\right)54$$

$$(20)(70)(71)\approx \quad (H_{[0,1]}H_{[6,7]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})\,(H_{[0,4]}H_{[0,1]})\,(H_{[0,1]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[6,7]}H_{[0,1]})(\text{Z-d4*})$$

$$\approx \quad (H_{[0,1]}H_{[6,7]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[0,1]})\,(H_{[0,1]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)_{[1]})$$

$$(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,1]})\,(H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,(H_{[6,7]}H_{[0,1]})(20)(70)(71)$$

$$\approx \quad (H_{[0,1]}H_{[6,7]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,(H_{[6,7]}H_{[0,1]})\text{推论 A.}\approx \quad (H_{[0,1]}H_{[6,7]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[6,7]}H_{[0,1]})\,((-1)_{[1]}X_{[0,1]})\text{推论 A.}\approx \quad (H_{[0,1]}H_{[6,7]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,2]})\,(H_{[6,7]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})(73)(66)$$

$$\approx \quad (H_{[0,1]}H_{[6,7]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[6,7]}H_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\text{推论 A.}\approx \quad (H_{[0,1]}H_{[6,7]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,((-1)_{[1]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})(H_{[6,7]}H_{[0,1]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})(73)(66)$$

$$\approx \quad (H_{[0,1]}H_{[0,2]})\,(H_{[1,3]}H_{[6,7]})\,((-1)_{[1]}X_{[1,3]})\,(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[6,7]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\text{推论 A.}\approx \quad (H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[6,7]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[6,7]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})(H_{[0,4]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})(73)(66)$$

$$\approx \quad (H_{[0,1]}H_{[0,2]})\,((-1)_{[3]}X_{[1,3]})\,(H_{[1,3]}H_{[0,1]})\,(H_{[0,1]}H_{[0,4]})\,((-1)_{[5]}X_{[1,5]})\,(H_{[1,5]}H_{[0,1]})\,(H_{[0,1]}H_{[0,1]})\,((-1)_{[0]}X_{[0,1]})\,((-1)^{[1]}(-1)_{[0]})\,((-1)^{[1]}(-1)^{[1]}$$

$$(H_{[0,4]}H_{[0,1]})\,(H_{[0,1]}H_{[1,5]})\,((-1)_{[1]}X_{[1,5]})\,(H_{[0,2]}H_{[0,1]})\,(H_{[0,1]}H_{[1,3]})\,((-1)_{[1]}X_{[1,3]})\,((-1)_{[1]}X_{[0,1]})\,(H_{[0,1]}H_{[0,1]})$$

□

B 一些辅助方程及有用性质

B.1 电路的一些常用性质

定义 B.1. 电路 C的镜像版本，记作 $C^\dagger$，递归定义如下：

- $for\, g \in \left\{ \boxed{\ }, \text{—}, \times, -\boxed{H}-, \bullet\text{—}, \bullet\!\!\bullet, \bullet\!\!-\boxed{H} \right\},\ g^\dagger = g$
- $(C_1 \circ C_2)^\dagger = C_2^\dagger \circ C_1^\dagger$

- $(C_1 \otimes C_2)^\dagger = C_1^\dagger \otimes C_2^\dagger$.

注 7. 需要注意的是，严格来说，上述定义针对的是原始电路。要证明它对配备 *PROP* 公理的电路仍然成立，就必须证明：如果两个原始电路根据图 *1*的规则所生成的同余等价，那么它们的镜像版本也等价。这是因为图 *1* 中的所有规则都是对称的，方程 (f) 除外；其镜像版本可以推导得出（特别是利用方程 (g)）。

引理 B.2。 对于任意 n 量子比特电路 C，有 $\mathsf{QC} \vdash C^\dagger \circ C = C \circ C^\dagger = (\,)^{\otimes n}$。

证明。 由于 $(C^\dagger)^\dagger = C$，只需证明 $\mathsf{QC} \vdash C^\dagger \circ C = (\,)^{\otimes n}$。我们对 C 进行结构归纳[16]。对于 、 和 ，结论是拓扑规则的直接结果。对于 $\mathcal{H}$、 和 H，结论是方程（1）、（2）、（4）和（5）的直接结果。而对于归纳步骤，我们有

$$(C_1 \circ C_2)^\dagger \circ (C_1 \circ C_2) \;=\; C_2^\dagger \circ C_1^\dagger \circ C_1 \circ C_2 \overset{\text{induction hypothesis}}{=} C_2^\dagger \circ C_2 \overset{\text{induction hypothesis}}{=} (\text{———})^{\otimes n}$$

and

$$(C_1 \otimes C_2)^\dagger \circ (C_1 \otimes C_2) \;=\; (C_1^\dagger \circ C_1) \otimes (C_2^\dagger \circ C_2) \overset{\text{induction hypothesis}}{=} (\text{———})^{\otimes n}.$$

□

引理 B.3。 对于任意 n 量子比特电路 C_1、C_2，如果 $\mathsf{QC} \vdash C_1 = C_2$，则 $\mathsf{QC} \vdash C_1^\dagger = C_2^\dagger$。

证明。

$$C_1^\dagger \overset{\text{Lemma B.2}}{=} C_1^\dagger \circ C_2 \circ C_2^\dagger \overset{\text{hypothesis}}{=} C_1^\dagger \circ C_1 \circ C_2^\dagger \overset{\text{Lemma B.2}}{=} C_2^\dagger$$

□

引理 B.4。 对于任意 n 量子比特电路 C、C'，如果 $\mathsf{QC} \vdash C \circ C' = (\,)^{\otimes n}$，则 $\mathsf{QC} \vdash C' = C^\dagger$，且 $\mathsf{QC} \vdash C' \circ C = (\,)^{\otimes n}$。

证明。为了证明第一个断言，我们有

$$C' \overset{\text{Lemma B.2}}{=} C^\dagger \circ C \circ C' \overset{\text{hypothesis}}{=} C^\dagger$$

而第二个断言由引理 B.2 得出。 □

为了将分块电路纳入考虑，可以进一步推广引理 B.3 ，将每个分块的伴随替换为一个可证明与之等价的任意电路：

引理 B.5。 给定四组由 n 个量子比特电路组成的列表 $C_1, ..., C_k$, $D_1, ..., D_\ell$, $C'_1, ..., C'_k$ 和 $D'_1, ..., D'_\ell$，若对于每个 i，都有 $\mathsf{QC} \vdash C_i \circ C'_i = (\,)^{\otimes n}$，并且对于每个 j，都有 $\mathsf{QC} \vdash D_j \circ D'_j = (\,)^{\otimes n}$，那么

$$\mathsf{QC} \vdash C_1 \circ \cdots \circ C_k = D_1 \circ \cdots \circ D_\ell \qquad \textit{if and only if} \qquad \mathsf{QC} \vdash C'_k \circ \cdots \circ C'_1 = D'_\ell \circ \cdots \circ D'_1.$$

证明。 根据引理 B.4，我们也有 $\mathsf{QC} \vdash C'_i \circ C_i = (\,)^{\otimes n}$ 以及 $\mathsf{QC} \vdash D'_j \circ D_j = (\,)^{\otimes n}$，因此由对称性，只需证明“当且仅当”的一半。

如果 $\mathsf{QC} \vdash C_1 \circ \cdots \circ C_k = D_1 \circ \cdots \circ D_\ell$，则

$$C'_k \circ \cdots \circ C'_1 \overset{\text{hypothesis}}{=} C'_k \circ \cdots \circ C'_1 \circ D_1 \circ \cdots \circ D_\ell \circ D'_\ell \circ \cdots \circ D'_1 \overset{\text{assumption}}{=} C'_k \circ \cdots \circ C'_1 \circ C_1 \circ \cdots \circ C_k \circ D'_\ell \circ \cdots \circ D'_1 \overset{\text{Lemma B.4}}{=} D'_\ell \circ \cdots \circ D'_1.$$

□

引理 B.6. 给定任意三个 n 量子比特电路 C、D、D'，使得 $\mathsf{QC} \vdash D \circ D' = (\,)^{\otimes n}$，则有

$$\mathsf{QC} \vdash C \circ D = D \circ C \qquad \textit{if and only if} \qquad \mathsf{QC} \vdash C \circ D' = D' \circ C.$$

证明。 根据引理 B.4，我们也有 $\mathsf{QC} \vdash D' \circ D = (\,)^{\otimes n}$，因此由对称性，只需证明“当且仅当”的一半。如果 $\mathsf{QC} \vdash C \circ D = D \circ C$，则

$$C \circ D' \overset{\text{Lemma B.4}}{=} D' \circ D \circ C \circ D' \overset{\text{assumption}}{=} D' \circ C \circ D \circ D' \overset{\text{hypothesis}}{=} D' \circ C.$$

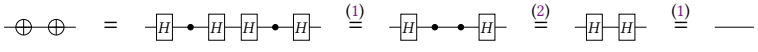
□

B.2 关于 1 量子比特和 2 量子比特的辅助方程

引理 B.7. 图 *12* 的方程是图 *4* 的方程的推论 .

证明。

方程证明 (81)：



[16]更确切地说，在任意底层原始电路上。

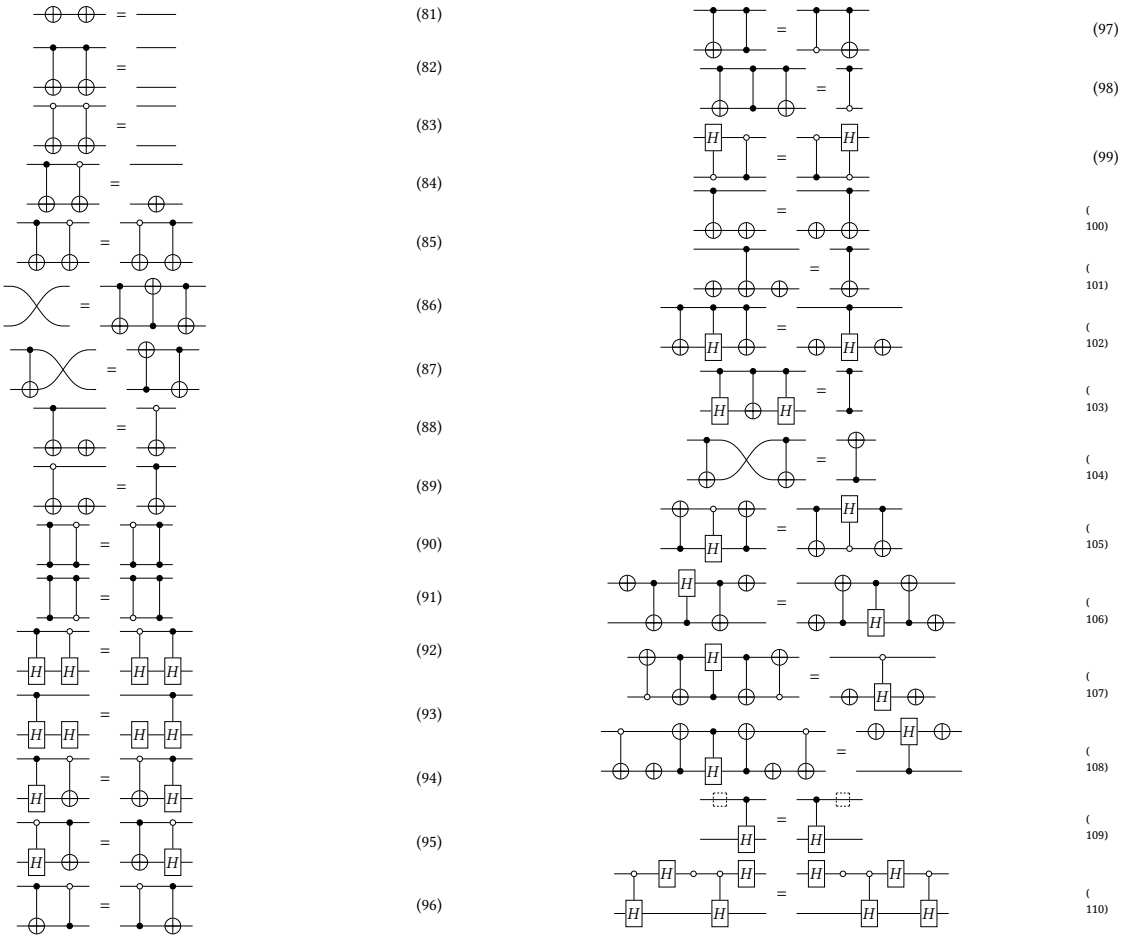
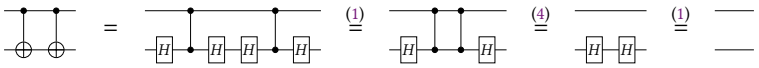
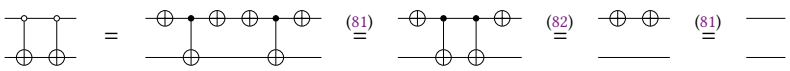


图 12：有用的辅助方程。

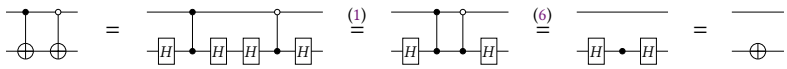
方程证明 (82)：



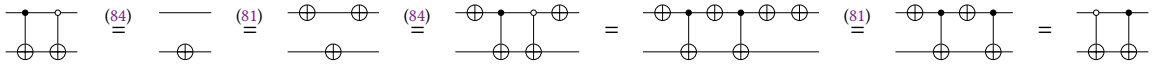
方程证明 (83)：



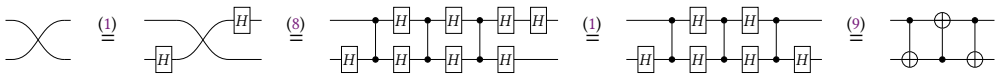
方程证明 (84)：



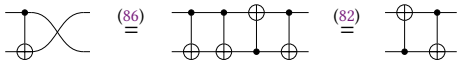
方程证明 (85)：



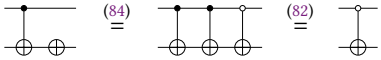
方程证明 (86)：



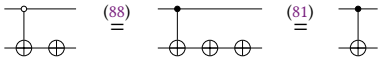
方程证明 (87):



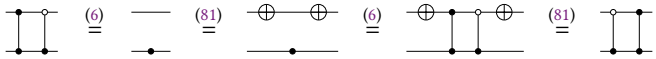
方程证明 (88):



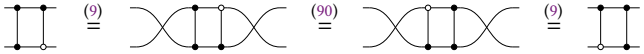
方程证明 (89):



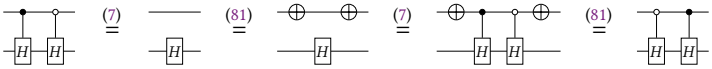
方程证明 (90):



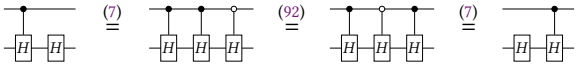
方程证明 (91):



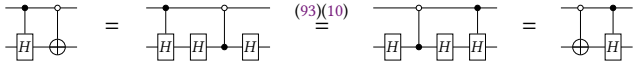
方程证明 (92):



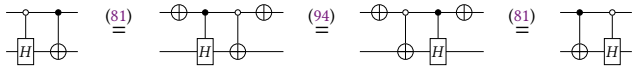
方程证明 (93):



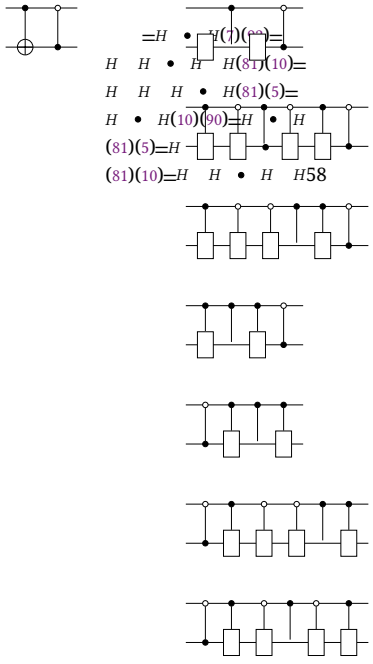
方程证明 (94):

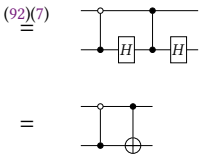


方程证明(95):

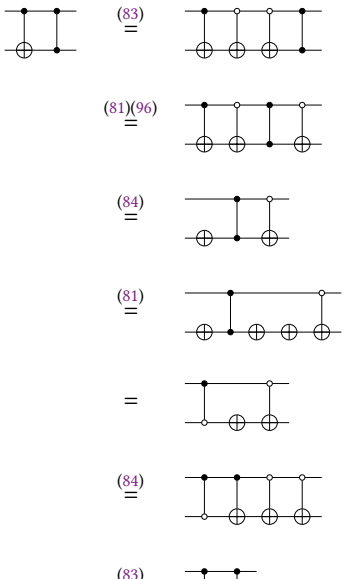


方程证明(96):

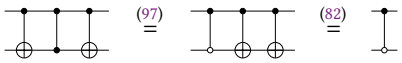




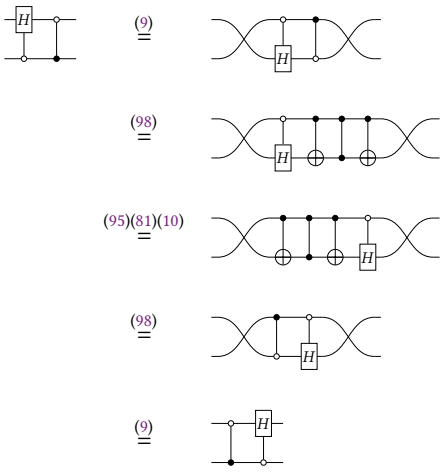
方程证明 (97):



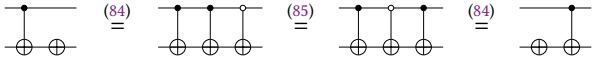
方程证明 (98):



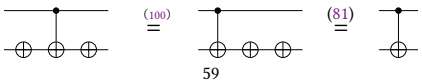
方程证明 (99):



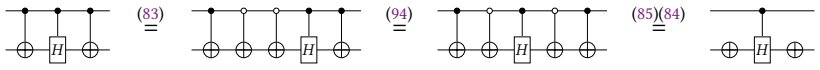
方程证明 (100):



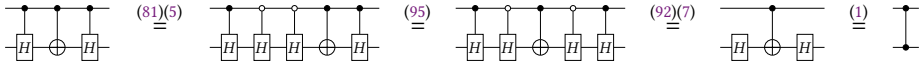
方程证明 (101):



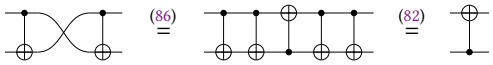
方程证明 (102):



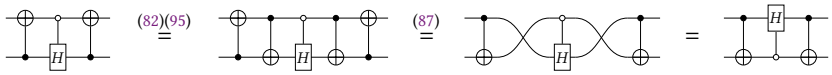
方程证明 (103):



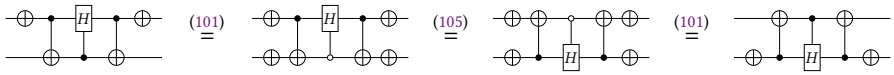
方程证明 (104): [17]



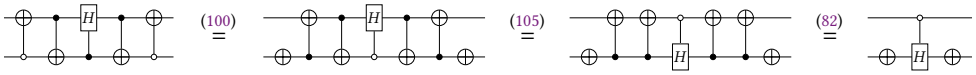
方程证明 (105):



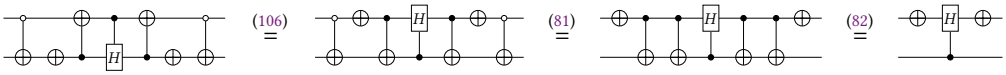
方程证明 (106):



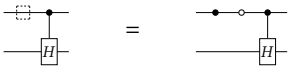
方程证明 (107):



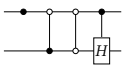
方程证明 (108):



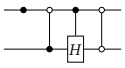
方程证明 (109):



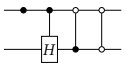
(6)(9)(81)



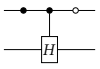
(81)(9)(99)



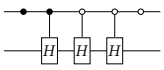
(10)



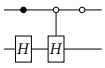
(81)(9)(6)



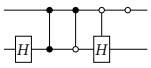
(81)(5)



(7)

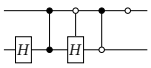


(6)(9)

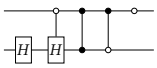


[17]注意，除去变形，方程 (104) 只是将左端和右端交换，并在左侧增加一个交换后的方程 (87)，因此我们也可以通过调用方程 (87) 一步证明它。

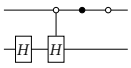
(9)(99) =



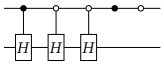
(81)(10) =



(9)(6) =



(7) =



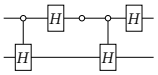
(81)(5) =



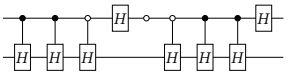
=



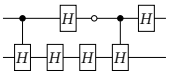
方程证明 (110):



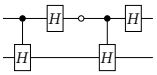
(5) =



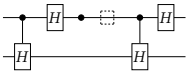
(92)(7) =



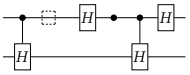
(1) =



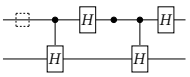
(2) =



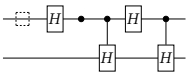
引理 7.1 =



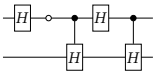
(109) =



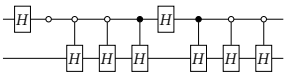
(11) =



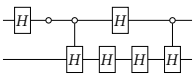
引理 7.1 =



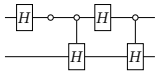
(81)(5) =



(92)(7) =



(1)
=



□

C 双量子比特完备性

C.1 引理证明7.4

我们将证明稍微强一些的结果：对于任意 n 比特电路 $C \in \mathbf{QC}$，任意满足 $|C'| = C$ 的 $C' \in \mathbf{QC}^{\mathbf{seq}}$，以及任意 k，ℓ 使得 $k+n+\ell = 2$，

$$\mathrm{QC} \vdash D(E_{k,\ell}(C')) = id_k \otimes C \otimes id_\ell.$$

更准确地说，我们将证明以下等价命题：对于任意满足 $|||C''||| = C$ 的 n 量子比特原始电路 C''，以及任意满足 $k+n+\ell = 2$ 的 k，ℓ，都有

$$\mathrm{QC} \vdash D(E_{k,\ell}(\|C''\|)) = id_k \otimes C \otimes id_\ell$$

其中，$\|C''\|$（分别地，$|||C''|||$）表示将 $\|C''\|$ 通过典范投影映射到 $\mathbf{QC}^{\mathbf{seq}}$（分别地，映射到 $\mathbf{QC}$）所得的像。为简单起见，在证明的其余部分，我们将省略典范投影 $\|\cdot\|$，这是对记号的滥用。我们对 C'' 使用结构归纳法。

对于任意两个满足 $k+n+\ell = 2$ 的 n 量子比特原始电路 C_1，C_2，都有

$$D(E_{k,\ell}(C_2 \circ C_1)) = D(E_{k,\ell}(C_2)) \circ D(E_{k,\ell}(C_1))$$

对于任意满足 $k+n+m+\ell = 2$ 的 n 量子比特原始电路 C_1 和 m 量子比特原始电路 C_3，

$$D(E_{k,\ell}(C_1 \otimes C_3)) = D(E_{k+n,\ell}(C_3)) \circ D(E_{k,\ell+m}(C_1)).$$

因此，剩下的就是基例：

$D(E_{0,0}($  $)) = D(X_{[1,2]}) =$  ,

$D(E_{k,\ell}($  $)) = D(\epsilon) =$  ,

$D(E_{k,\ell}($  $)) = D(\epsilon) =$  ,

$D(E_{1,0}($ $)) = D(H_{[0,1]}H_{[2,3]}) =$ $\overset{(7)}{=}$  ,

$D(E_{0,1}($  $)) = D(H_{[0,2]}H_{[1,3]}) =$  $\overset{(7)}{=}$  ,

$D(E_{1,0}($  $)) = D((-1)_{[1]}(-1)_{[3]}) =$  $\overset{(6)}{=}$  ,

$D(E_{0,1}($  $)) = D((-1)_{[2]}(-1)_{[3]}) =$  $\overset{(9)(6)}{=}$  ,

$D(E_{0,0}($  $)) = D((-1)_{[3]}) =$,

$D(E_{0,0}($  $)) = D(H_{[2,3]}) =$  .

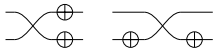
C.2 引理7.5 的证明

根据命题 4.8，只需证明对于图 7 中形如 $w_1 \approx w_2$ where $w_1, w_2 \in \mathrm{G}_4^*$ 的每条规则，以及任意两个字 $w_0, w_3 \in \mathrm{G}_4^*$，都有 $\mathrm{QC} \vdash D(w_0 w_1 w_3) = D(w_0 w_2 w_3)$。由于 D 是幺半群同态，只需证明 $\mathrm{QC} \vdash D(w_1) = D(w_2)$。注意，由于我们只在维度 4 中讨论，因此无需处理方程 (d4*)。

解码方程 (a1*)：

$D((-1)^2_{[0]})$ =  $\overset{(81)(4)}{=}$  = $D(\epsilon)$

解码方程 (a3)：有 $D(H^2_{[j,k]}) = D(H_{[j,k]})^2$，，并且可以验证，对于任意 j、k，电路 $D(H_{[j,k]})$ 都是对称的（左右对称）。根据方程 (1)、(2)、(4)、(5) 和 (g)，所有生成元都是自逆的，因此这意味着 $D(H_{[j,k]})^2$ 可以化简为单位元。

解码方程 (a2)：论证与方程 (a3) 相同，只需注意 = 。 

解码方程 (b1*)：

$D((-1)_{[0]}(-1)_{[1]})$ =  $\overset{(81)(91)}{=}$  = $D((-1)_{[1]}(-1)_{[0]})$

解码方程 (b4*):

$$D((-1)_{[1]}H_{[0,2]}) \quad = \quad \overset{(99)}{=} \quad = \quad D(H_{[0,2]}(-1)_{[1]})$$

解码方程 (b6*):

$$D(H_{[0,1]}H_{[2,3]}) \quad = \quad \overset{(92)}{=} \quad = \quad D(H_{[2,3]}H_{[0,1]})$$

解码方程 (c1)：如果 $(j,k)=(0,1)$、$(1,0)$、$(2,3)$ 和 $(3,2)$，则根据方程（97），结合方程（81）和引理 B.3，即可得出结果。情形 $(j,k)=(0,2)$、$(2,0)$、$(1,3)$ 和 $(3,1)$ 类似，但还需使用方程（9）。

情形 $(j,k)=(1,2)$ 和 $(2,1)$ 可由方程（9）（结合拓扑规则）推出，而情形 $(j,k)=(0,3)$ 和 $(3,0)$ 类似，但还需使用方程（81）。

解码方程 (c5) 和 (e2*)： 在每种情形下，我们都需要证明如下形式的一个方程

$$D(X_{[j,k]}) \circ D(H_{[l,m]}) = D(H_{[l',m']}) \circ D(X_{[j,k]})$$

其中或者是 $m=j$，或者是 $(l,\ m)=(j,\ k)$。

根据引理B.2，该方程等价于

$$D(X_{[j,k]}) \circ D(H_{[l,m]}) \circ D(X_{[j,k]})^{\dagger} = D(H_{[l',m']}).$$

此外，可以验证，对于任意 j，k、$D(X_{[j,k]})^{\dagger}=D(X_{[j,k]})$，因此该方程等价于 o

$$D(X_{[j,k]}) \circ D(H_{[l,m]}) \circ D(X_{[j,k]}) = D(H_{[l',m']}).$$

根据可靠性，为了推导出该方程，只需证明可以将左侧变换为某个 $D(H_{[l',m']})$。事实上，指标 l'，m' 由 $H_{[l',m']}$，的语义唯一确定，因此也由 $D(H_{[l',m']})$ 的语义唯一确定。

我们在表1中列出了为将 $D(X_{[j,k]})\circ D(H_{[l,m]})\circ D(X_{[j,k]})$ 变换为 $D(H_{[l',m']})$ 而需要应用的方程（空白单元格对应于我们不需要处理的情形，即不存在 $m=j$或 $(l,\ m)=(j,\ k)$ 的情形；交换 j 和 k 后亦然——注意，由于 $D(X_{[k,j]})=D(X_{[j,k]})$，我们在同一列中处理这两种情形）。为了使证明更容易检查，我们还描绘了所得的 $D(H_{[l',m']})$。

解码方程 (d2)：我们必须证明，对于每一个 j，k（其中 $j\neq k$），下列方程是图 4 中那些方程的推论：

$$D(H_{[j,k]}) \circ D(X_{[j,k]}) \ = \ D((-1)_{[k]}) \circ D(H_{[j,k]}).$$

根据引理 B.2（连同如下事实：$D(H_{[j,k]})^{\dagger}=D(H_{[j,k]})$），这等价于推导出下列方程：

$$D(H_{[j,k]}) \circ D(X_{[j,k]}) \circ D(H_{[j,k]}) \ = \ D((-1)_{[k]}).$$

对于 $(j,k)=(2,3)$、$(0,1)$、$(0,2)$ 和 $(1,3)$，容易验证它是方程 (103) 连同方程（81）的推论。情形 $(j,k)=(3,2)$、$(1,0)$、$(2,0)$ 和 $(3,1)$ 与此类似，但还需额外使用方程 (101)。

对于 $(j,k)=(2,1)$、$(1,2)$、$(0,3)$ 和 $(3,0)$，有如下推导：

$$D(H_{[2,1]}) \circ D(X_{[2,1]}) \circ D(H_{[2,1]}) \quad =$$

$$\overset{(104)}{=}$$

$$\overset{(103)}{=}$$

$$\overset{(9)(98)}{=} \quad = \quad D((-1)_{[1]})$$

$$D(H_{[1,2]}) \circ D(X_{[1,2]}) \circ D(H_{[1,2]}) \quad =$$

$$\overset{(104)}{=}$$

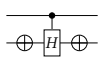
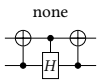
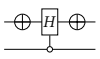
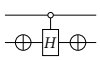
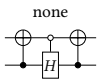
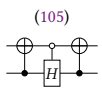
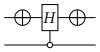
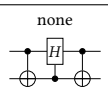
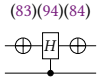
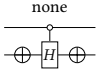
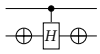
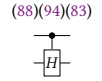
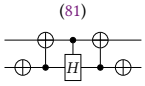
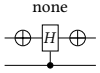
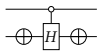
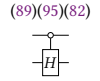
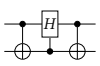
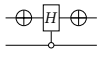
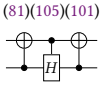
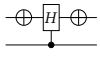
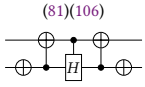
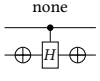
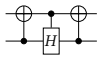
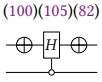
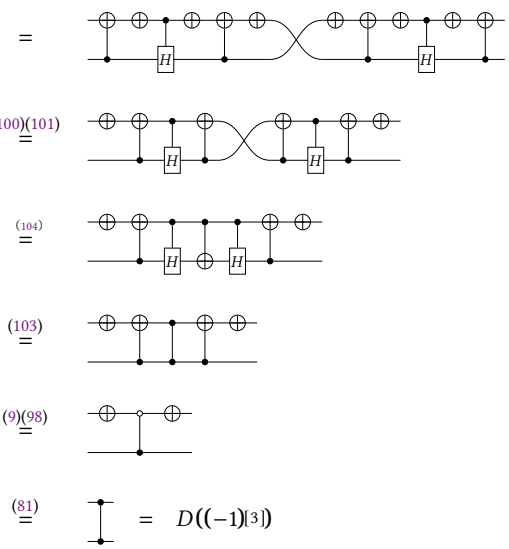
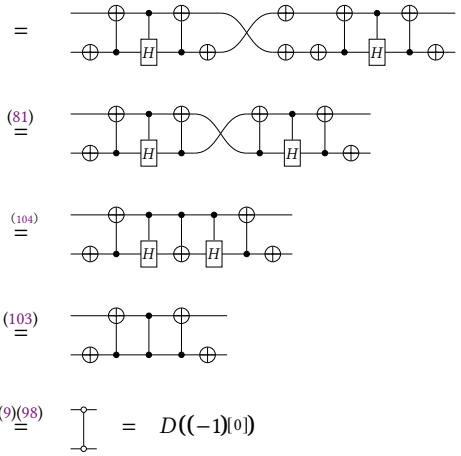
$D(H_{[l,m]})$ \ $D(X_{[j,k]})$	$D(X_{[2,3]})$ = 	$D(X_{[0,1]})$ = 	$D(X_{[0,2]})$ = 	$D(X_{[1,3]})$ = 	$D(X_{[1,2]})$ = 	$D(X_{[0,3]})$ = 
$D(H_{[2,3]})$ = 	(83)(94)(84) 			none 		none 
$D(H_{[0,1]})$ = 		(82)(95)(84) 		none 	none 	
$D(H_{[0,2]})$ = 	(105) 		(82)(95)(84) 		none 	
$D(H_{[1,3]})$ = 	none 			(83)(94)(84) 		none 
$D(H_{[3,2]})$ = 	(88)(94)(83) 		(81) 		none 	
$D(H_{[1,0]})$ = 		(89)(95)(82) 	(81)(105)(101) 			(81) 
$D(H_{[2,0]})$ = 		(81)(105)(101) 	(89)(95)(82) 			(81) 
$D(H_{[3,1]})$ = 		(81)(106) 		(88)(94)(83) 	none 	
$D(H_{[2,1]})$ = 		(100)(105)(82) 		(82)	none	
$D(H_{[0,3]})$ =	(105)(82)			(82)		(101)(106)
$D(H_{[1,2]})$ =	(82)		(107)		none	
$D(H_{[3,0]})$ =		(108)	(81)(82)			(81)(100)(105)

表 1：将 $D(X_{[j,k]})\circ D(H_{[l,m]})\circ D(X_{[j,k]})$ 转换为某个 $D(H_{[l',m']})$ 所需的方程，以及所得 $D(H_{[l',m']})$ 的图示。需要时，我们会隐式使用引理B.3（以及拓扑规则和快捷定义）。

$D(H_{[0,3]})\circ D(X_{[0,3]})\circ D(H_{[0,3]})$ =



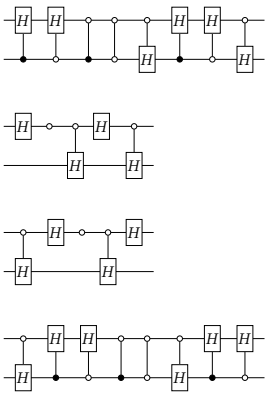
$D(H_{[3,0]}) \circ D(X_{[3,0]}) \circ D(H_{[3,0]})$ =



解码方程 (d3*):

$D(H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]})$

=



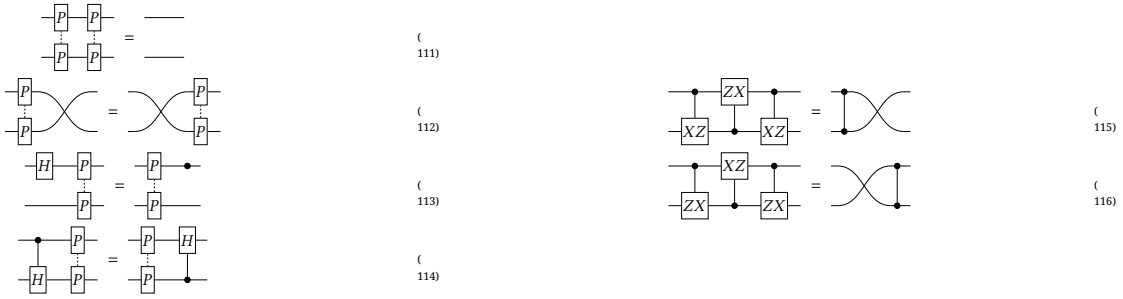


图 13：其他有用的 2个量子比特辅助方程。

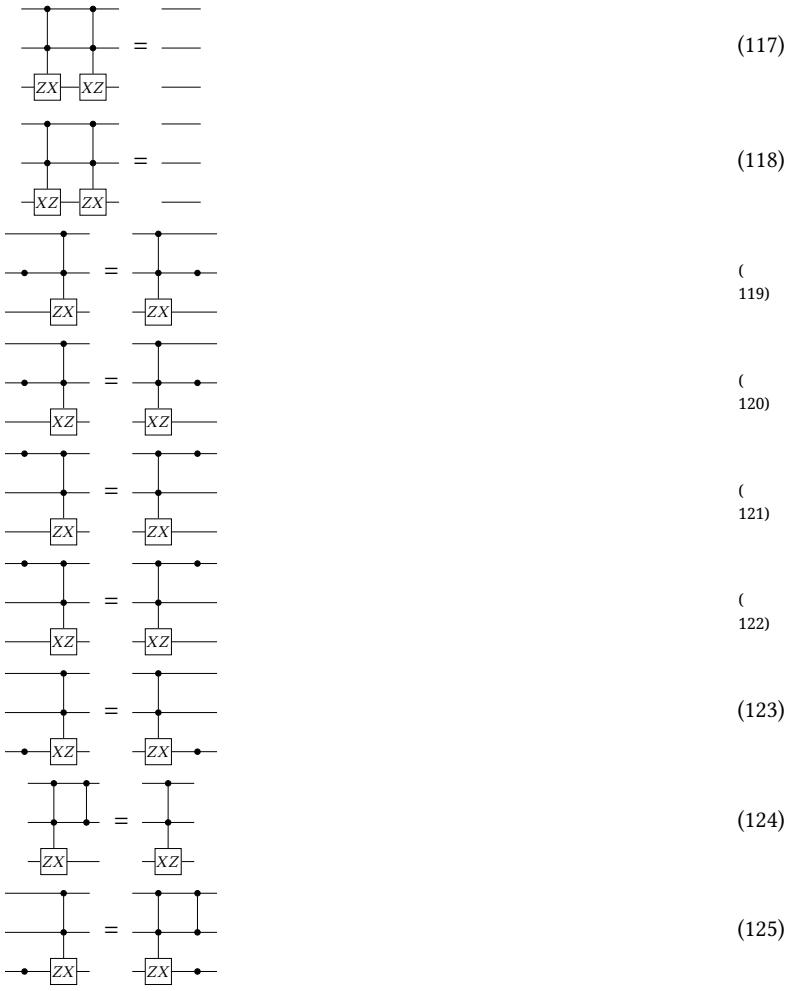
D 其他辅助方程及多重控制量子门的性质 D.1 2个量子比特的其他辅助方程

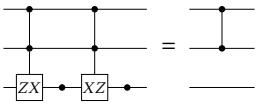
引理 D.1. 图 *13* 中的方程是图 *4*的推论。

证明。 这可直接由引理 7.6得出。 □

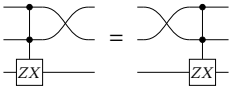
D.2 3个量子比特上的辅助方程

引理 D.2。 以下方程是图 *4*中的方程的推论：

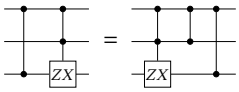




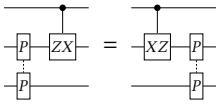
(126)



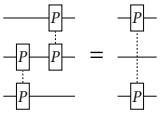
(127)



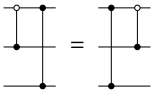
(128)

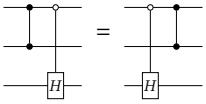


(129)

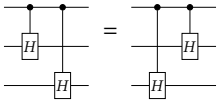


(130)

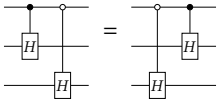

(131)



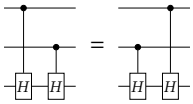
(132)



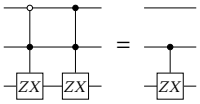
(133)



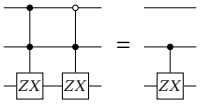
(134)



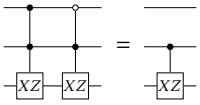
(135)



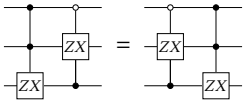
(136)



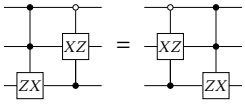
(137)



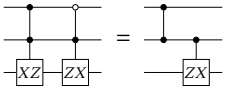
(138)



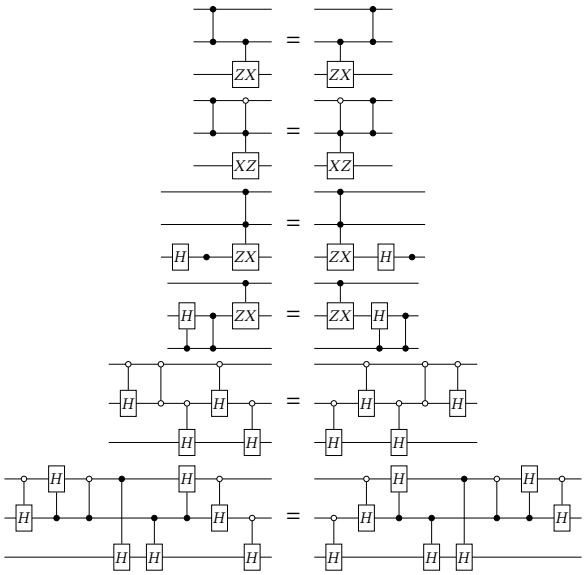
(139)



(140)



(141)



(142)

(143)

(144)

(145)

(146)

(147)

证明。

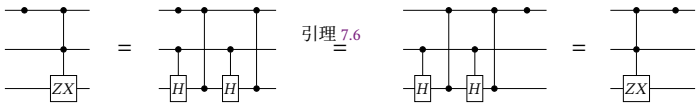
方程证明 (117)： 方程 (117) 直接由引理B.2得出。

方程证明 (118)： 方程 (118) 直接由引理B.2得出。

方程证明 (119)：

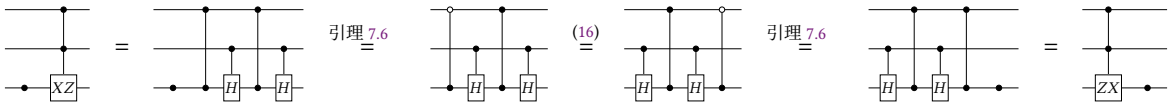


方程证明 (120)： 方程 (120) 由引理B.3应用于方程(119)可直接得出。方程证明 (121)：

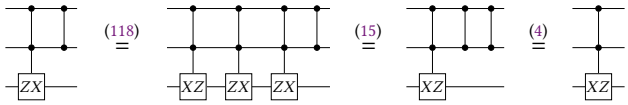


方程证明 (122)： 方程 (122) 由引理B.3应用于方程 (121) 可直接得出。

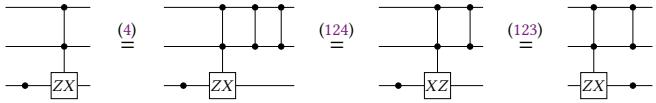
方程证明 (123)：



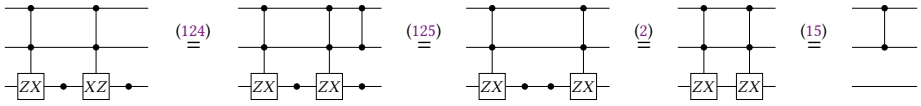
方程证明 (124)：



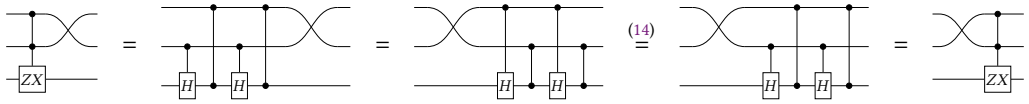
方程证明 (125)：



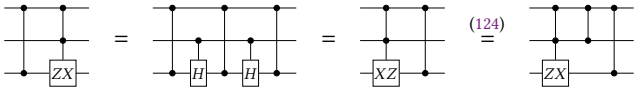
方程证明 (126)：



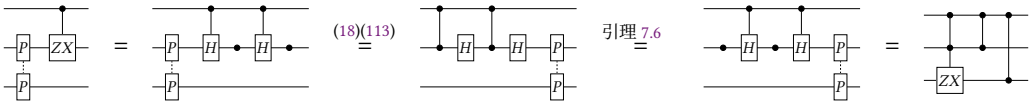
方程证明 (127):



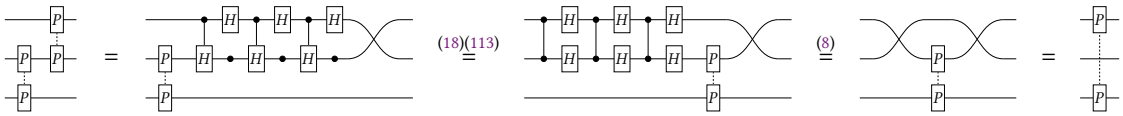
方程证明 (128):



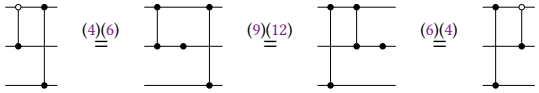
方程证明 (129):



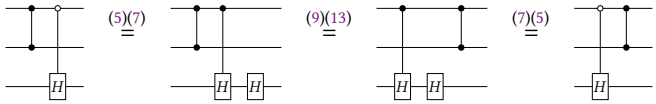
方程证明 (130):



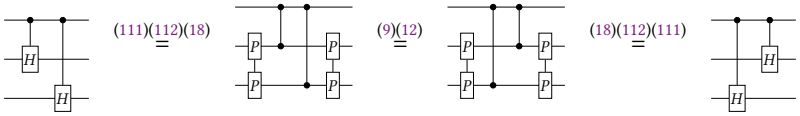
方程证明 (131):



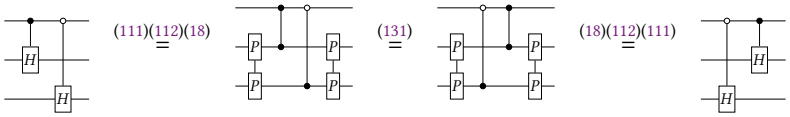
方程证明 (132):



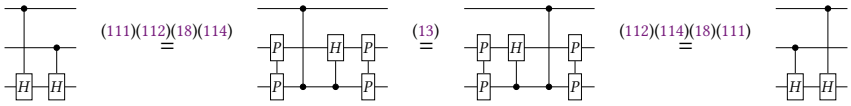
方程证明 (133):



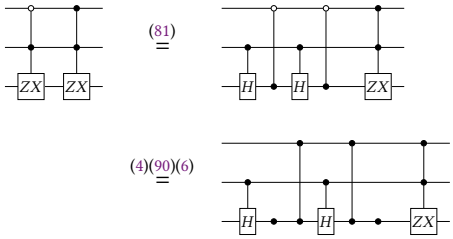
方程证明 (134):

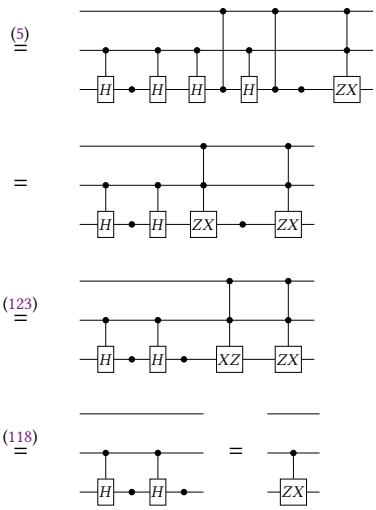


方程证明 (135):



方程证明 (136):

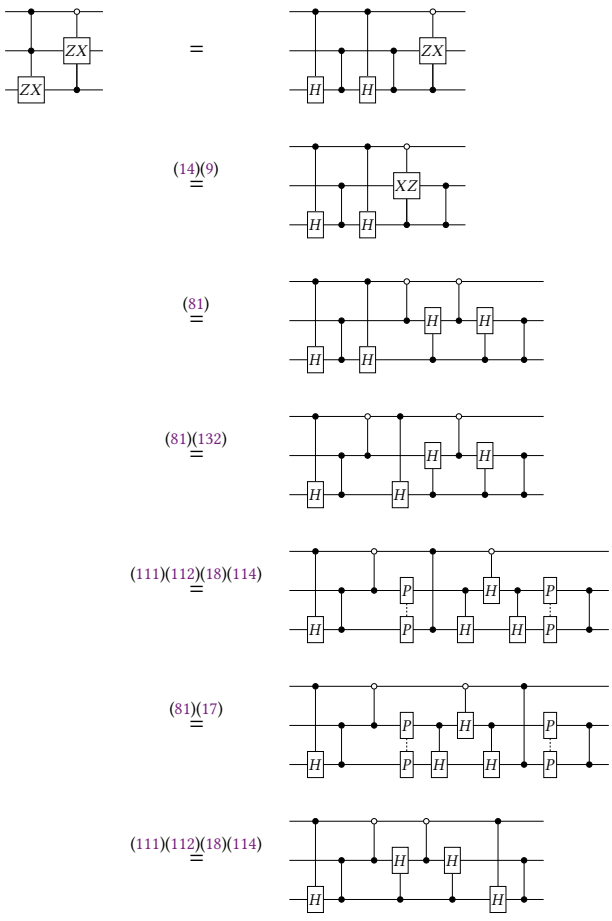




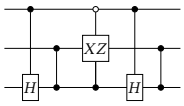
方程证明 (137)： 方程 (137) 由方程 (136) 以及方程 (8 1).

方程证明 (138)： 方程 (138) 可直接由引理B.3应用于方程 (136) 得出。

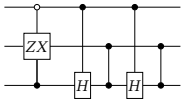
方程证明(139)：



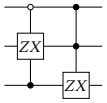
(81)=



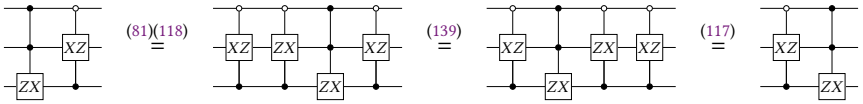
相似=



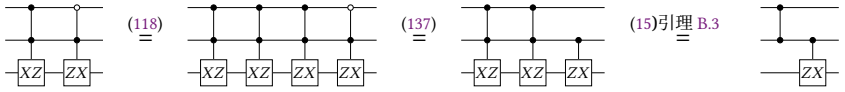
=



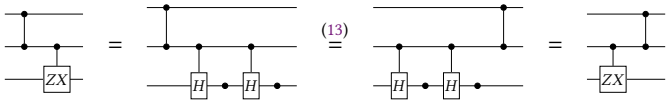
方程证明(140):



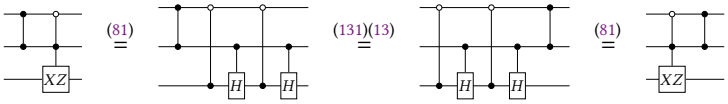
方程证明 (141):



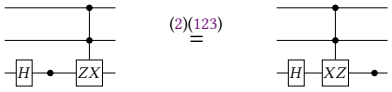
方程证明 (142):



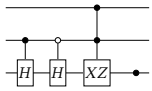
方程证明 (143):



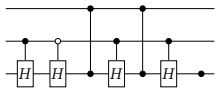
方程证明 (144):



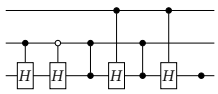
(7)=



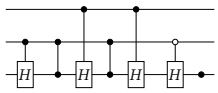
=



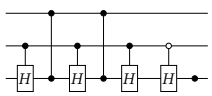
(14)引理 B.3=

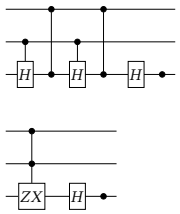


(81)(10)(135)=

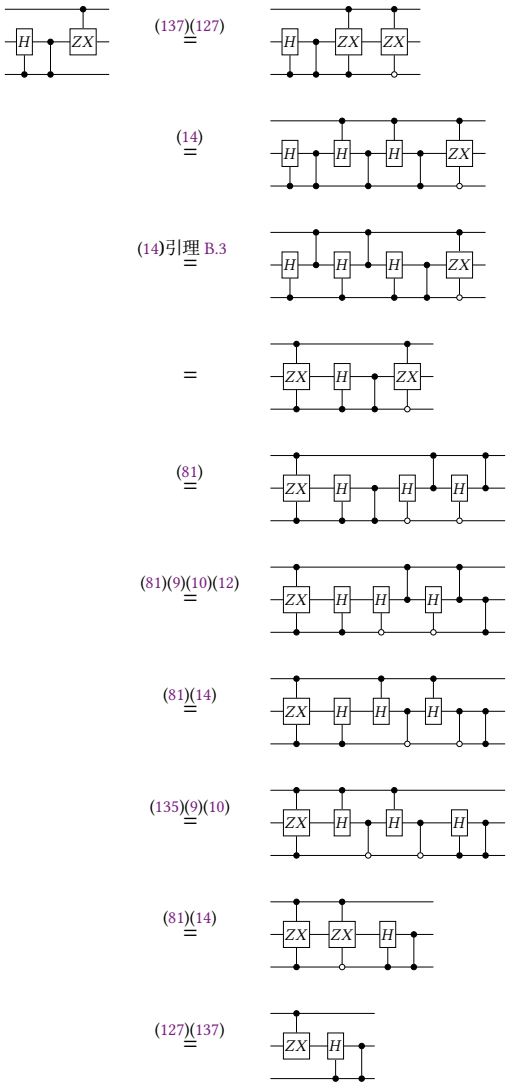


(14)引理 B.3=

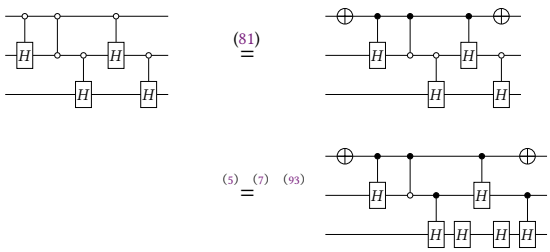




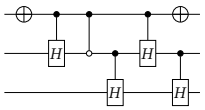
方程证明 (145):



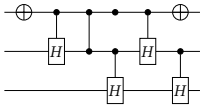
方程证明 (146):



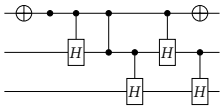
(1)
=



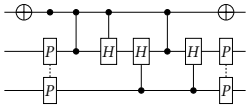
引理 7.6
=



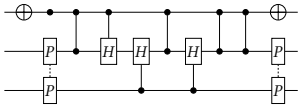
引理 7.6
=



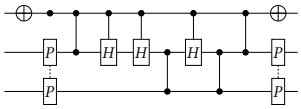
(111)(18)(114)
=



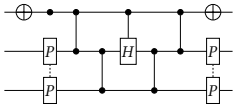
(4)
=



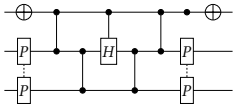
(14)
=



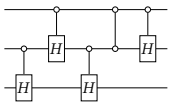
(5)
=



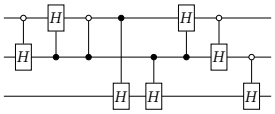
引理 7.6
=



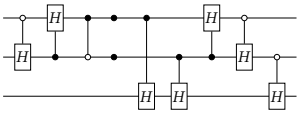
引理 B.3
连同
前面的步骤
=



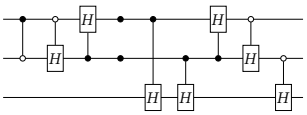
方程证明 (147):

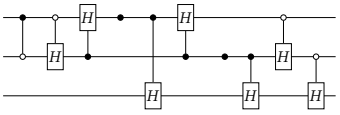


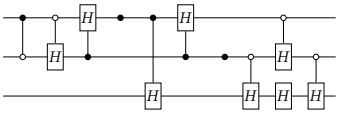
引理 7.6
=

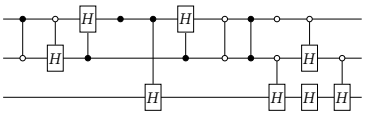


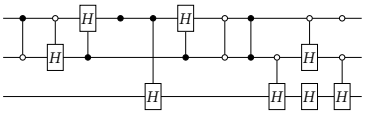
引理 7.6
=

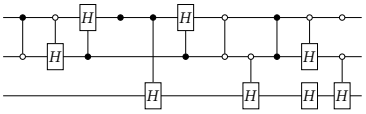


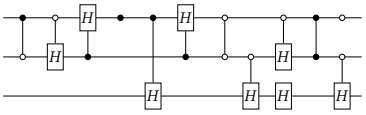
引理 7.6
=


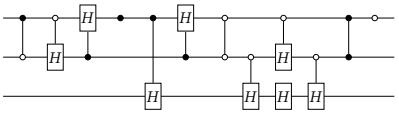
引理 7.6
=


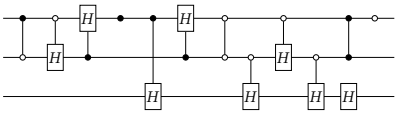
引理 7.6
=


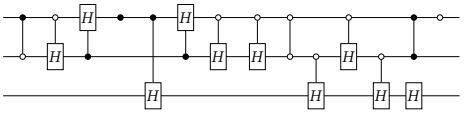
引理 7.6
=


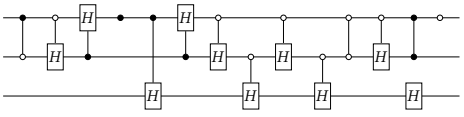
(9)(132)
=


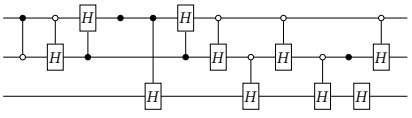
(81)(10)
=


(9)(132)
=


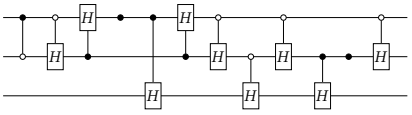
(93)
=


(81)(5)
=


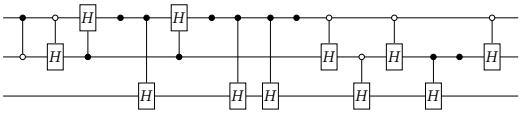
(146)
=


引理 7.6
=


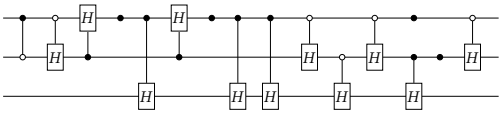
引理 7.6
=



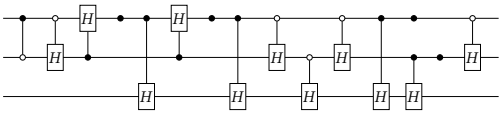
(2)(5)
=



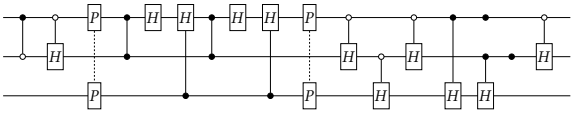
引理 7.6
=



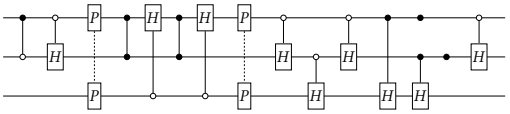
(134)(135)
=



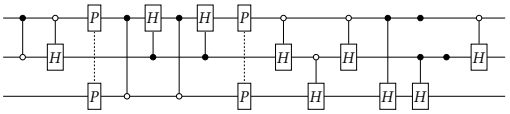
(111)(18)(9)(113)(114)
=



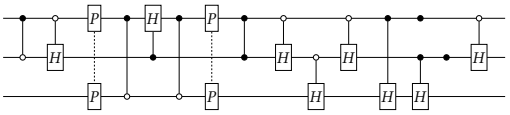
引理 7.6
=



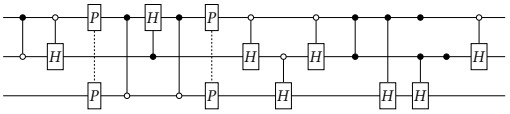
(81)(14)
=



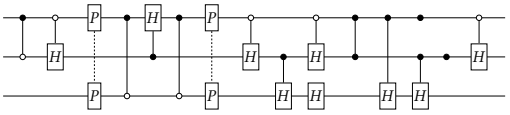
(111)(18)(9)
=



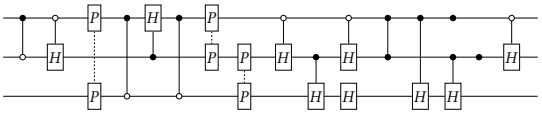
(81)(10)(9)(132)
=



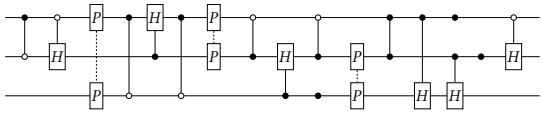
引理 7.6
=



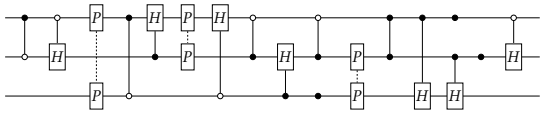
(112)(130)
=



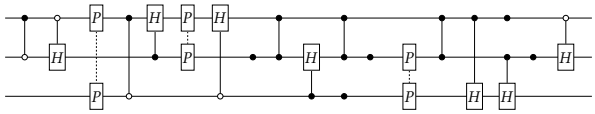
(18)(111)(112)(114)(113)
=



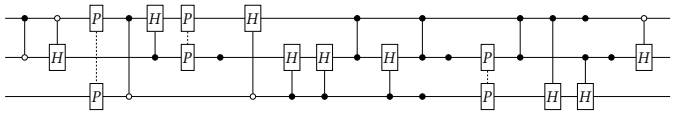
(18)
=



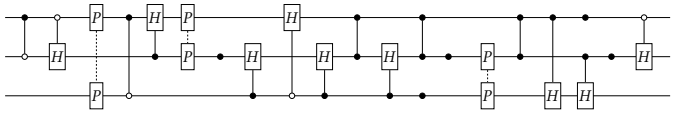
引理 7.6
=



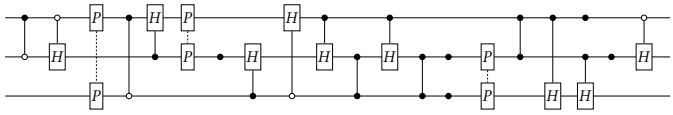
(5)
=



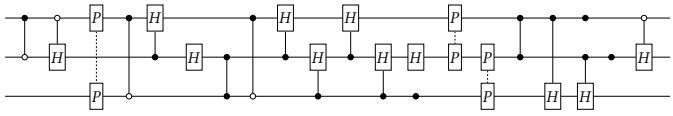
(134)
=



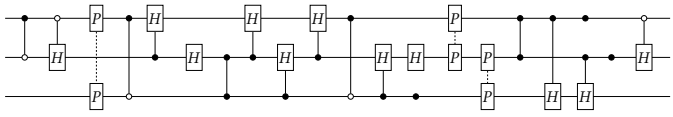
(14)
=



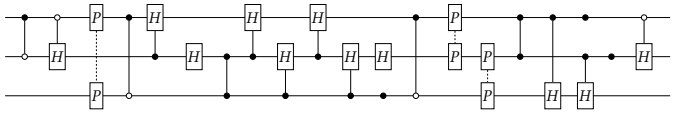
(112)(113)(18)(9)(114)(111)
=



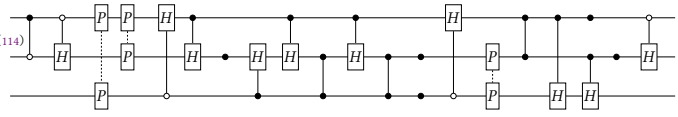
(9)(17)
=



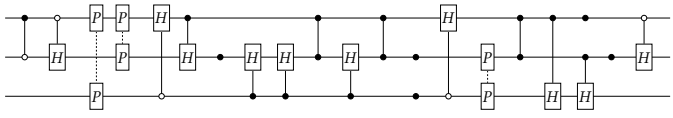
引理 7.6(132)
=



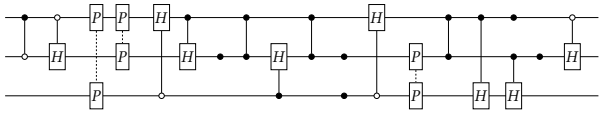
(111) (18) (112) (113) (9) (114)
=



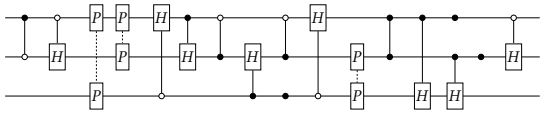
(14)
=



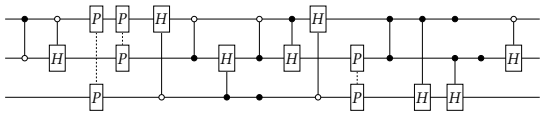
(5)
=



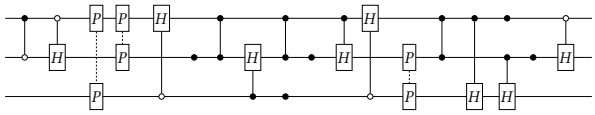
引理 7.6
=



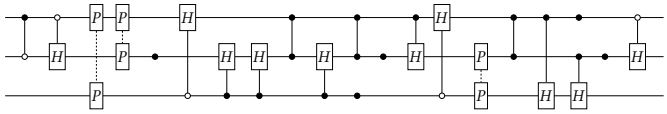
(10)(135)
=



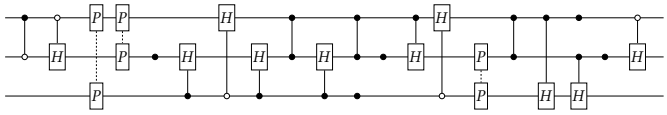
引理 7.6
=



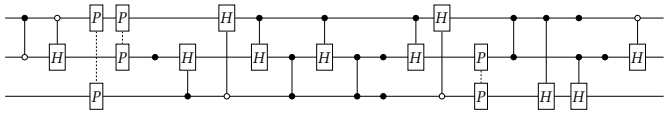
(5)
=



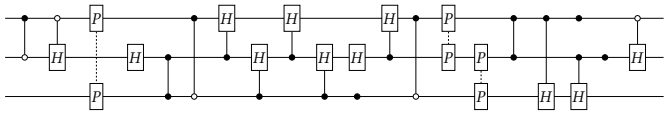
(134)
=



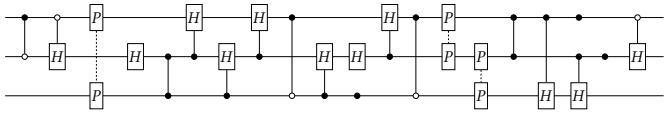
(14)
=



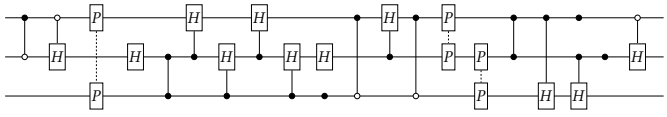
(112)(113)(18)(9)(114)(111)
=



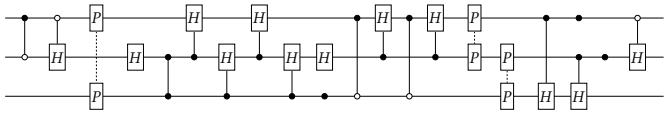
(9)(17)
=



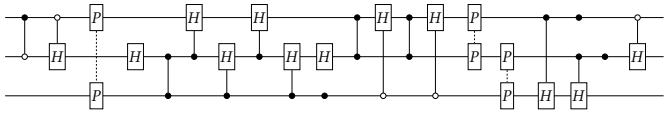
引理 7.6(132)
=



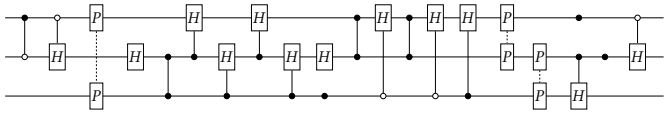
(111)(18)(114)
=



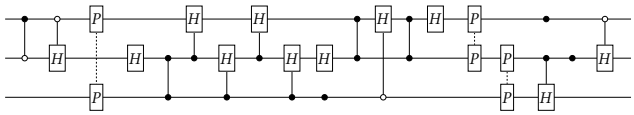
(81)(14)
=



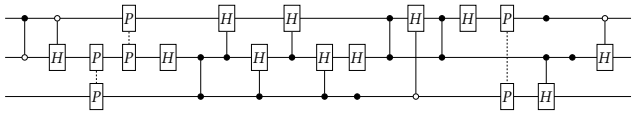
(112)(130)(114)
=



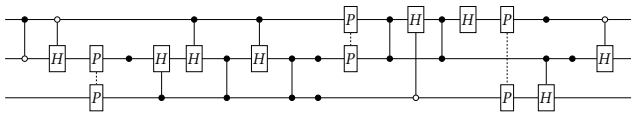
(92)(7)
=



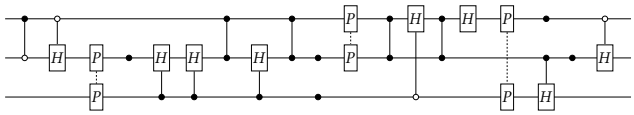
(112)(130)
=



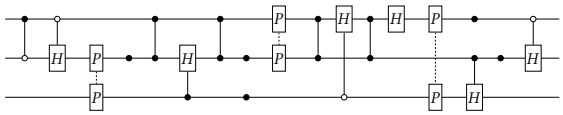
(112)(111)(113)(18)(9)(114)
=



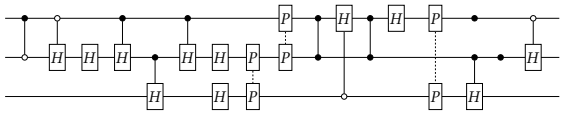
(14)
=



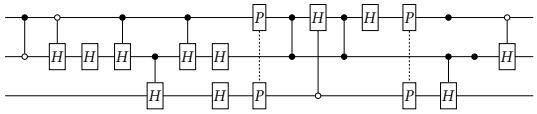
(5)
=



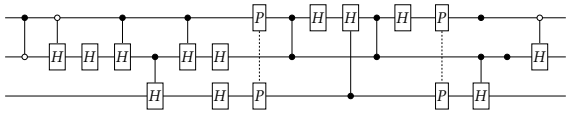
(113)(111)(18)(114)(112)
=



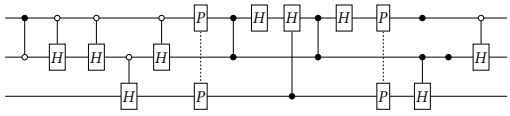
(130)
=



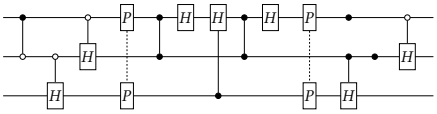
引理 7.6
=



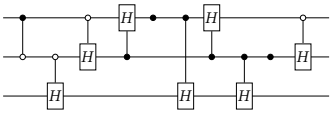
引理 7.6
=



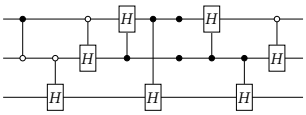
(81)(5)
=



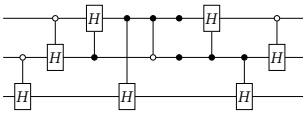
(9)(111)(18)(113)(114)
=



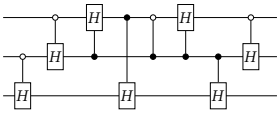
引理 7.6
=



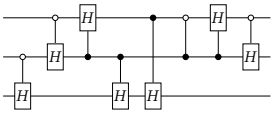
(81)(13)(9)(99)(10)
=



引理 7.6
=



(133)(13)(135)
=



□

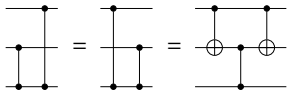
D.3 四量子比特上的辅助方程

在本节中，我们将使用引理 5.1 的四量子比特情形：

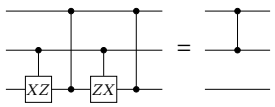
引理 D.3（条件式三量子比特完备性）。对于任意两个在 $\left\{ \square \text{上的三量子比特量子电路 } C_1、C_2, ,, \right\}$，若 $[\![C_1]\!] = [\![C_2]\!]$，则 $\mathrm{QC} \vdash (\otimes C_1) = (\otimes C_2)$ 且 $\mathrm{QC} \vdash (C_1 \otimes) = (C_2 \otimes)$。

特别是，为了使证明中使用这两个方程的地方更加清楚，我们将它们明确列出：

推论 D.4。在引理 *D.5* 的证明中，可以自由使用下列方程，仿佛我们已经证明了它们是图 *4* 中方程的推论：



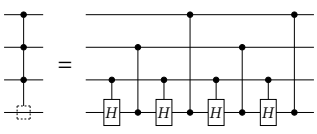
(148)



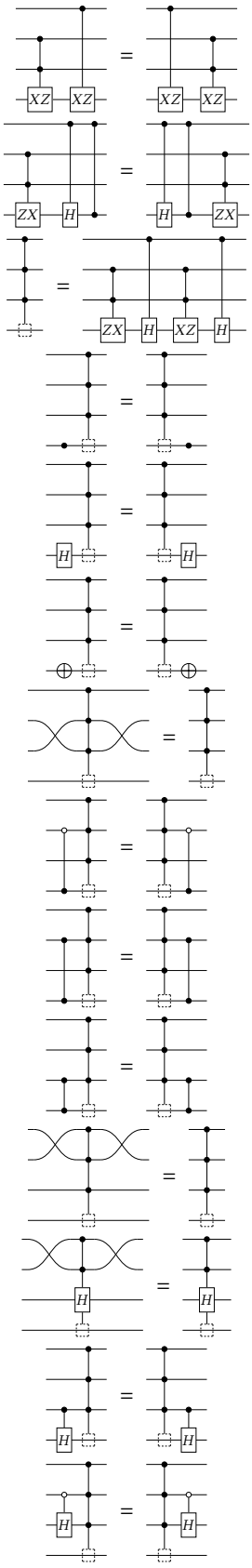
(149)

现在我们开始证明这些有用的四量子比特辅助方程：

引理 D.5. 以下方程是图 *4* 中方程的推论：



(150)



(151)

(152)

(153)

(154)

(155)

(156)

(157)

(158)

(159)

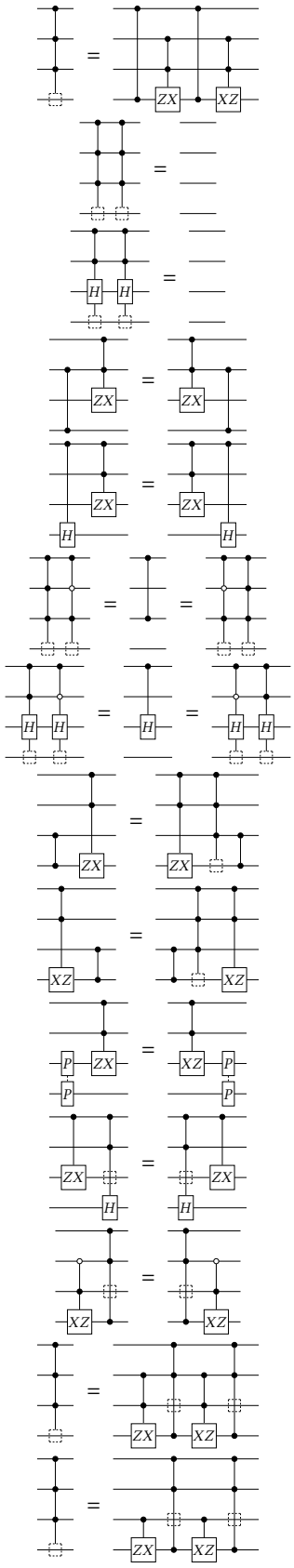
(160)

(161)

(162)

(163)

(164)



(165)

(166)

(167)

(168)

(169)

(170)

(171)

(172)

(173)

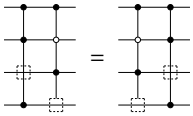
(174)

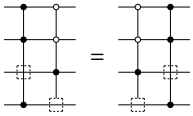
(175)

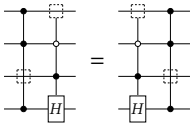
(176)

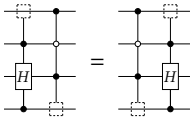
(177)

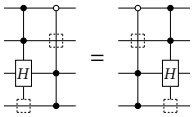
(178)

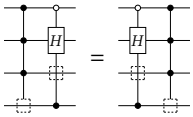

(179)

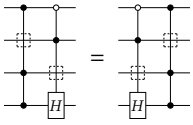

(180)

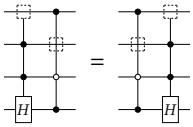

(181)

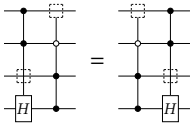

(182)

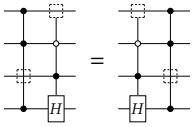

(183)

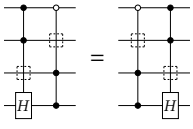

(184)

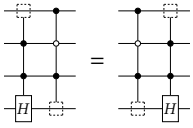

(185)

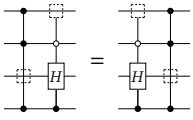

(186)

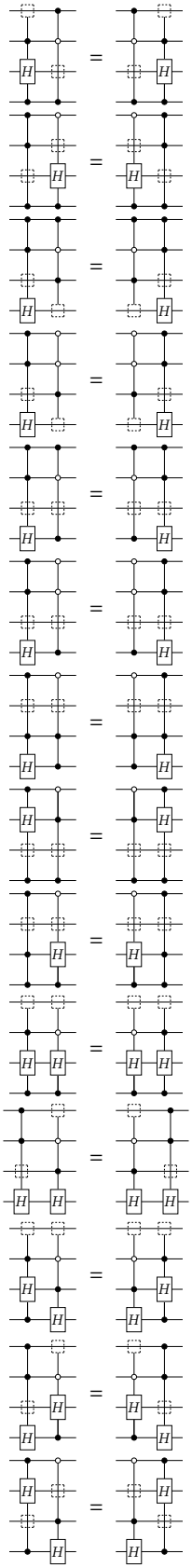

(187)


(188)


(189)


(190)


(191)



(192)

(193)

(194)

(195)

(196)

(197)

(198)

(199)

(200)

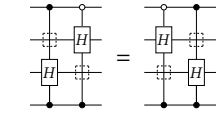
(201)

(202)

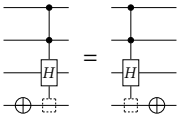
(203)

(204)

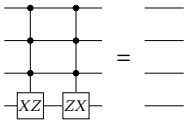
(205)



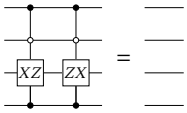
(206)



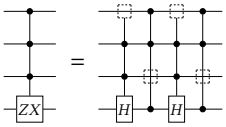
(207)



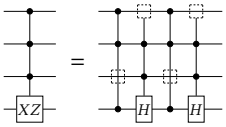
(208)



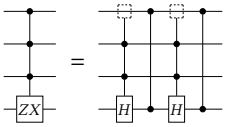
(209)



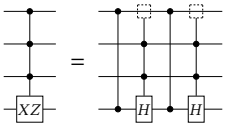
(210)



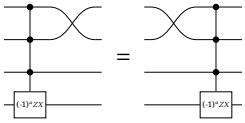
(211)



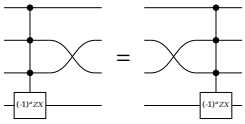
(212)



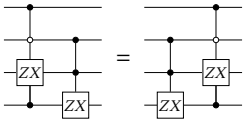
(213)



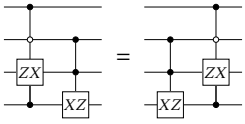
(214)



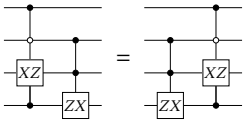
(215)



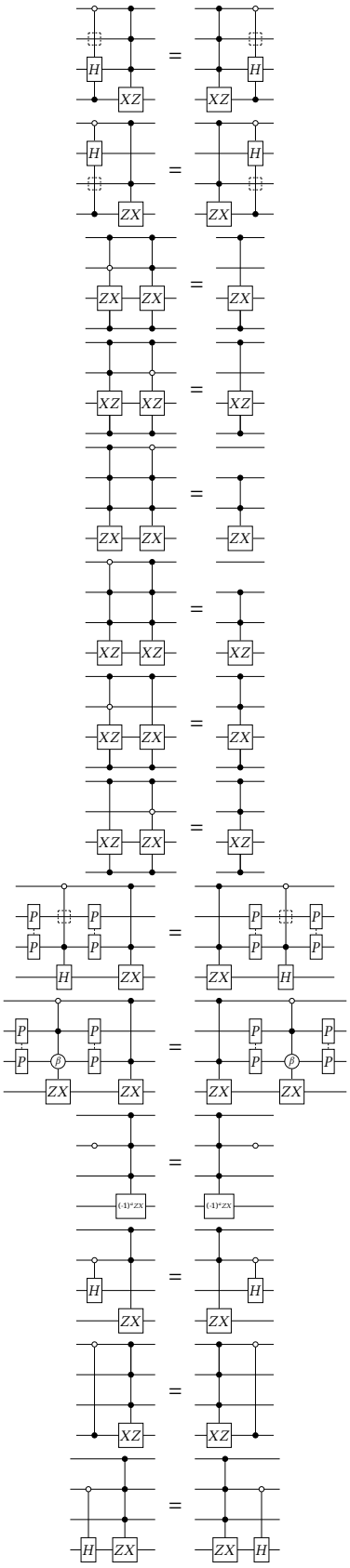
(216)



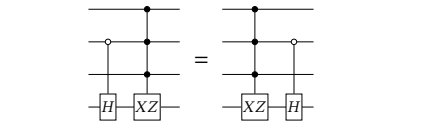
(217)



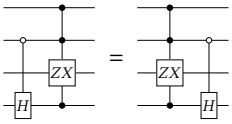
(218)



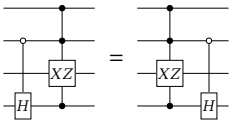
(219)
(220)
(221)
(222)
(223)
(224)
(225)
(226)
(227)
(228)
(229)
(230)
(231)
(232)



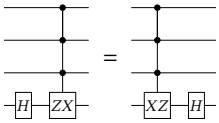
(233)



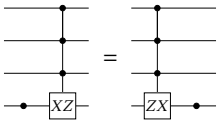
(234)



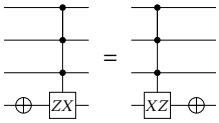
(235)



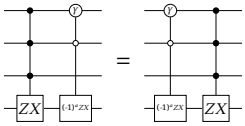
(236)



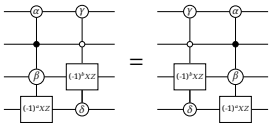
(237)



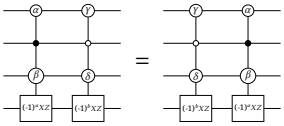
(238)



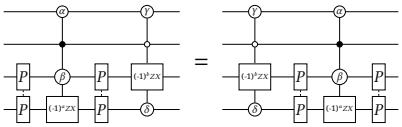
(239)



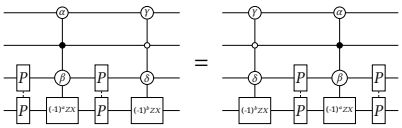
(240)



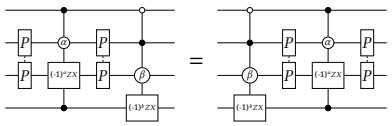
(241)



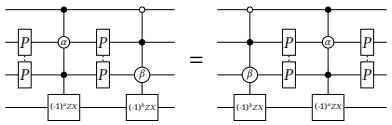
(242)



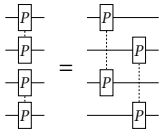
(243)



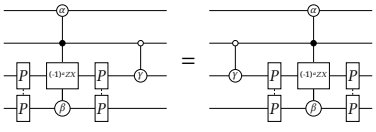
(244)



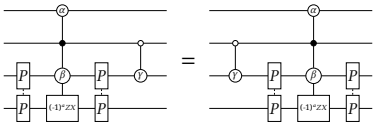
(245)



(246)



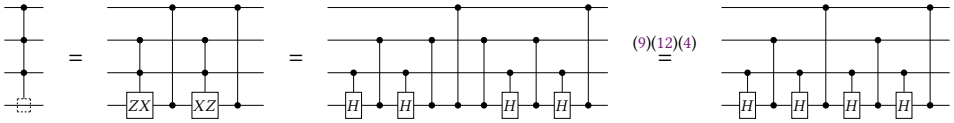
(247)



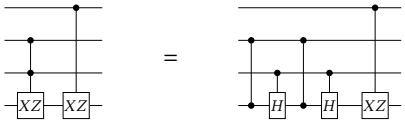
(248)

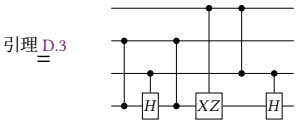
证明。

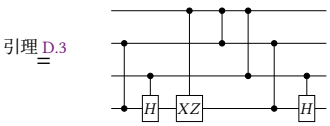
方程证明 (150)：

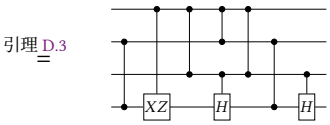


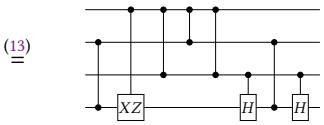
方程证明 (151)：

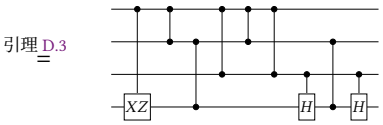


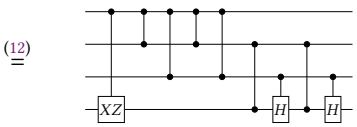




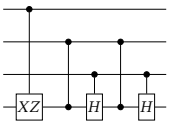




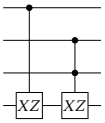




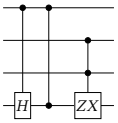
(9)(12)(4)
=



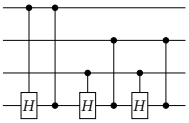
=



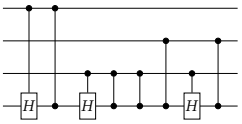
方程证明 (152):



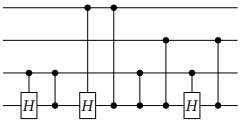
=



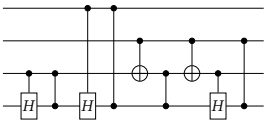
(4)
=



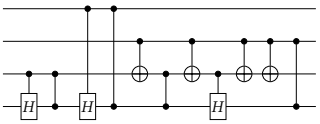
引理 D.3
=



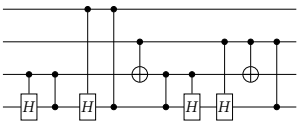
(148)
=



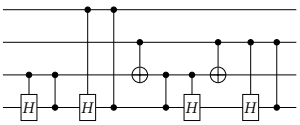
(82)
=



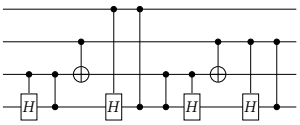
引理 D.3
=



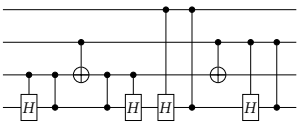
引理 D.3
=

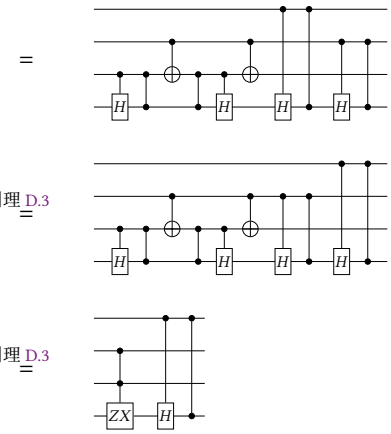


=

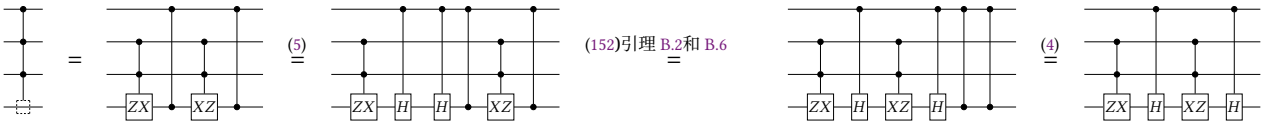


引理 D.3
=

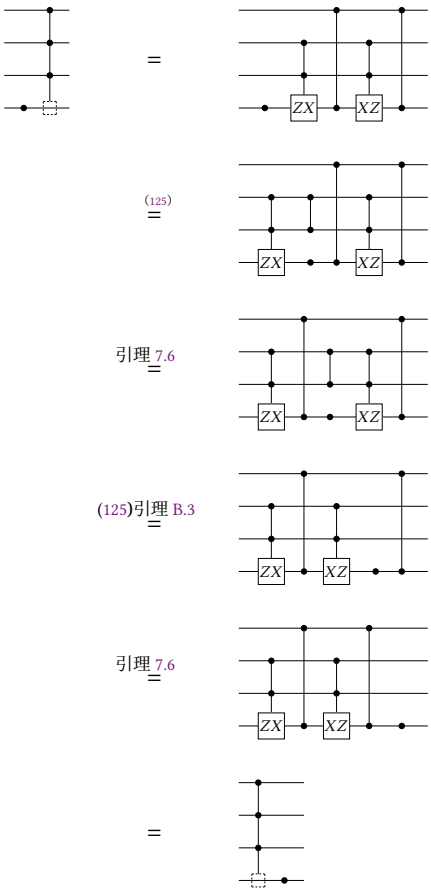




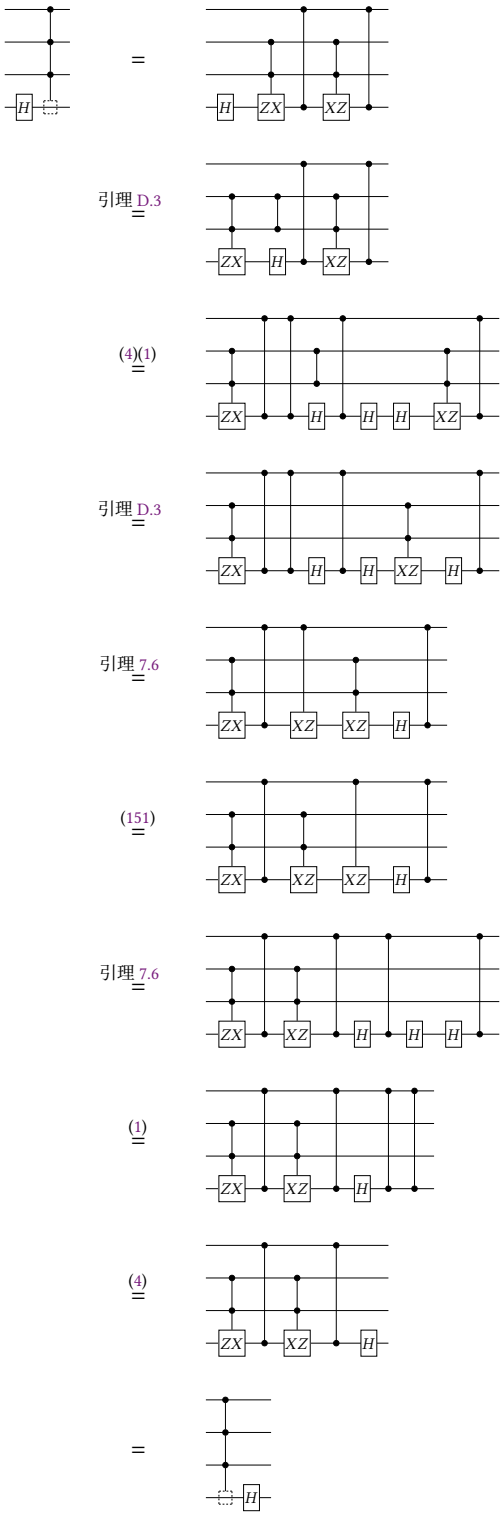
方程证明 (153):



方程证明 (154):

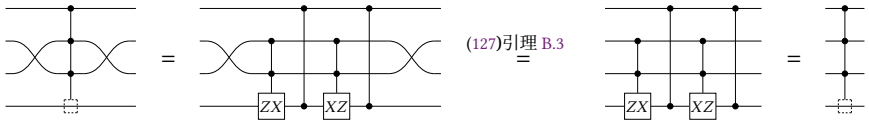


方程证明(155)：

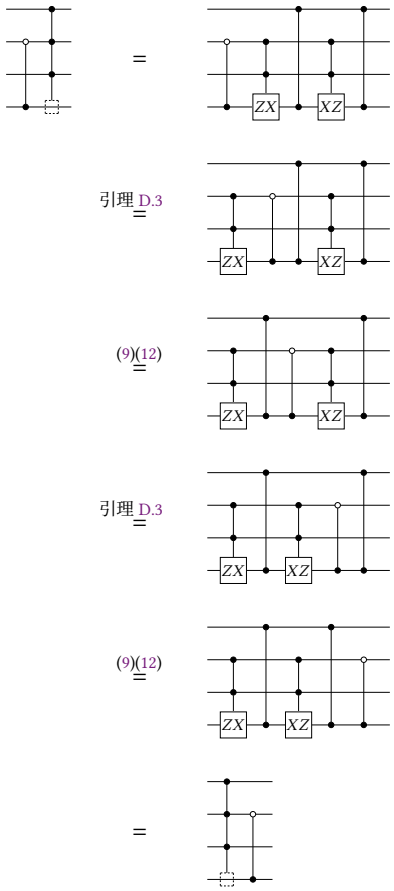


方程证明 (156)：方程 (156) 直接由方程 (154) 和 (155) 得出。90

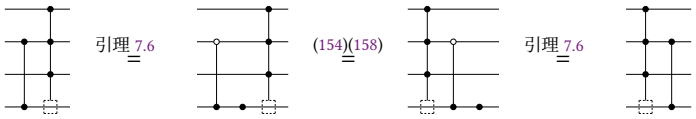
方程证明 (157)：



方程证明 (158)：

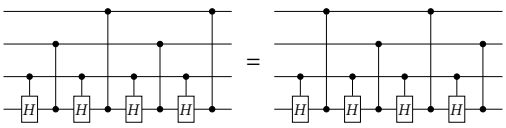


方程证明 (159)：

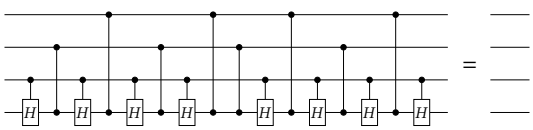


方程证明 (160)： 方程 (160) 可直接由方程 (157) 和 (159) 得出。

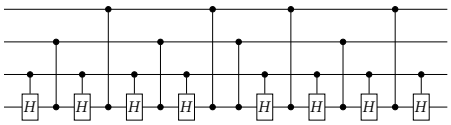
方程证明 (161)： 根据方程 (150)，我们只需证明以下方程：



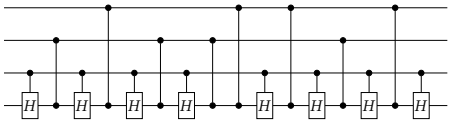
根据引理 B.4，为此只需证明以下方程：



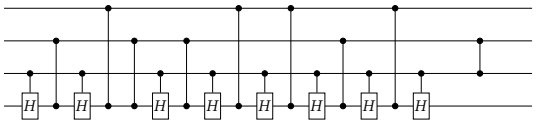
我们按如下方式进行：



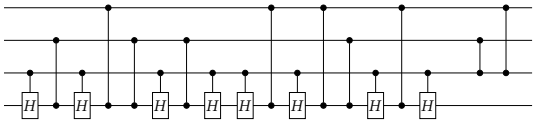
(9)(12)
=



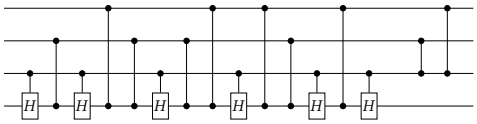
(4)(124)(13)(9)(12)
=



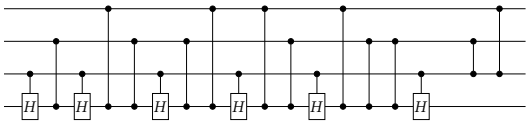
(124)(13)(9)(12)
=



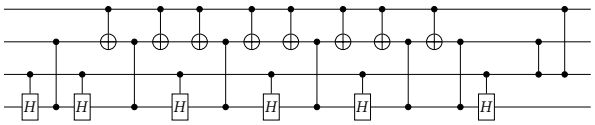
(5)
=



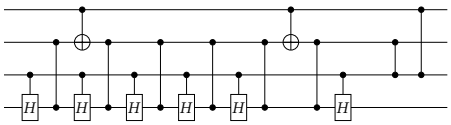
(4)
=



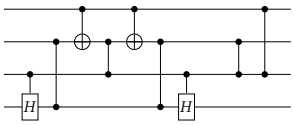
(148)
=



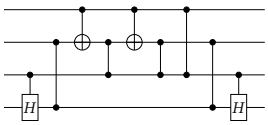
(82)
=

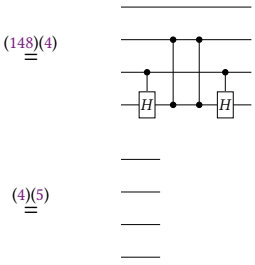


(15)
=

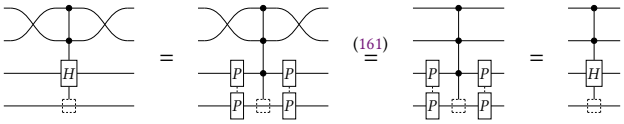


(13)(9)(12)
=

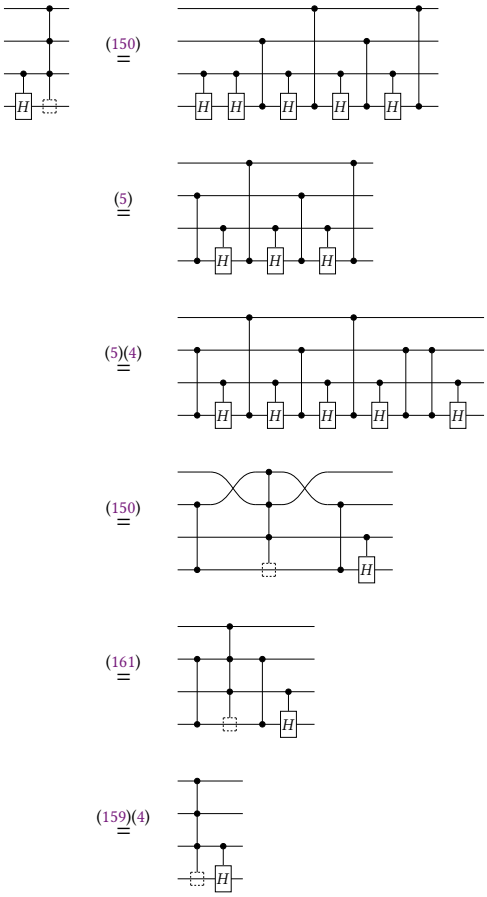




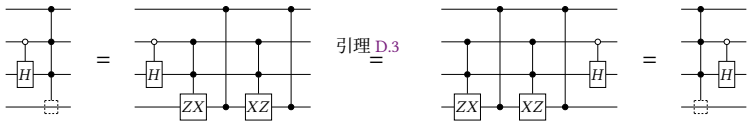
方程证明 (162)*:*



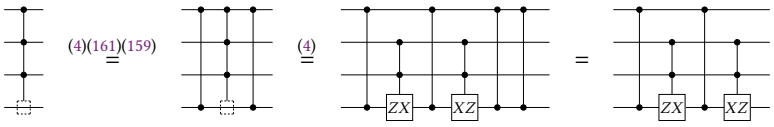
方程证明 (163)*:*



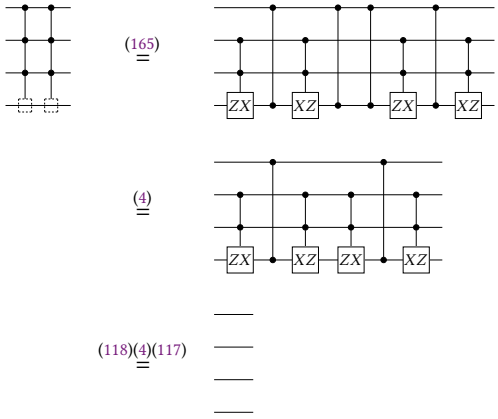
方程证明 (164):



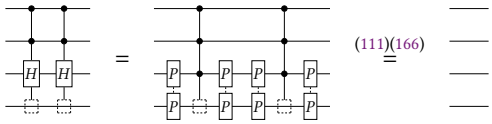
方程证明 (165):



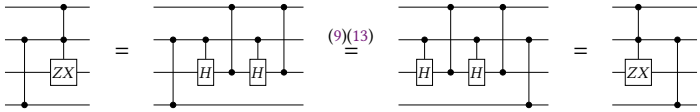
方程证明 (166):



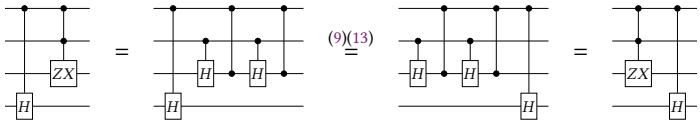
方程证明 (167):



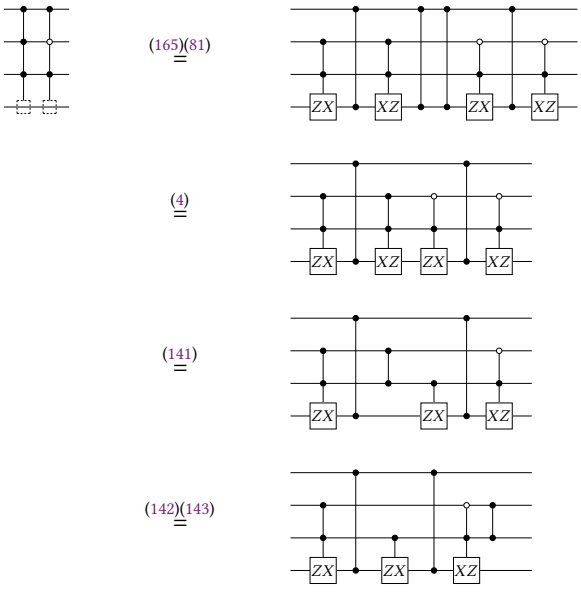
方程证明(168):

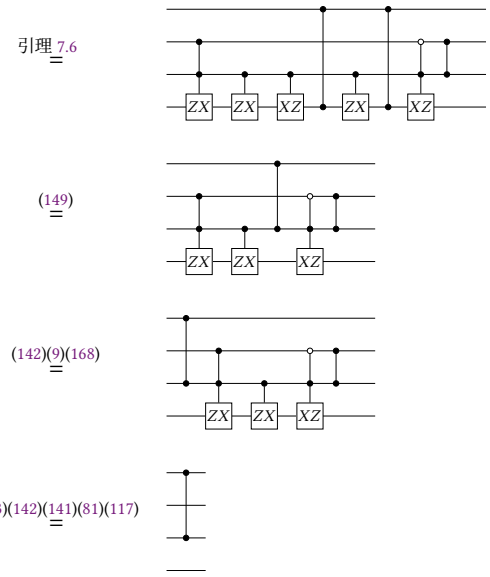


方程证明(169):

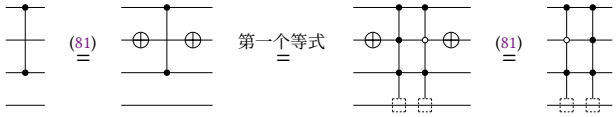


方程证明 (170): 为证明第一个等式，我们有

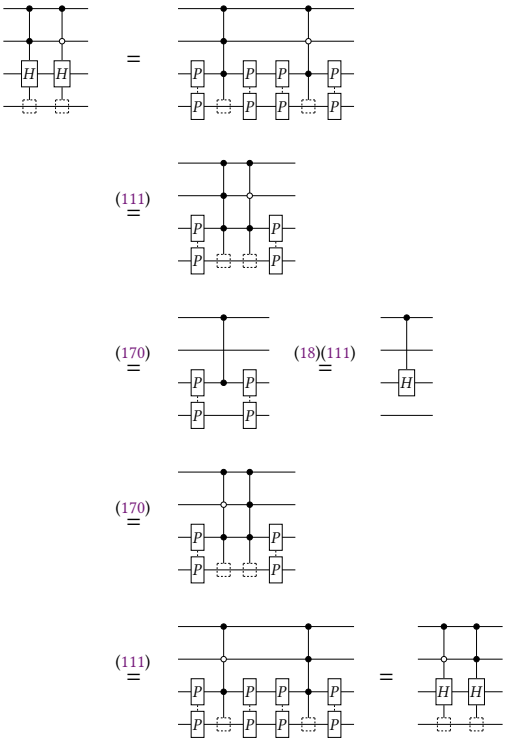




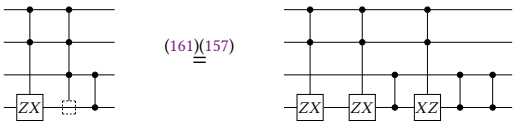
为证明第二个等式，我们有

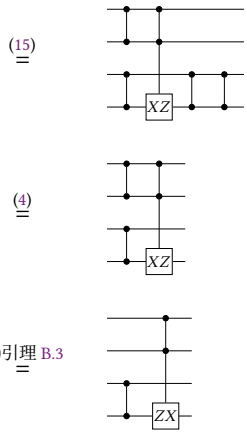


方程证明 (171)：



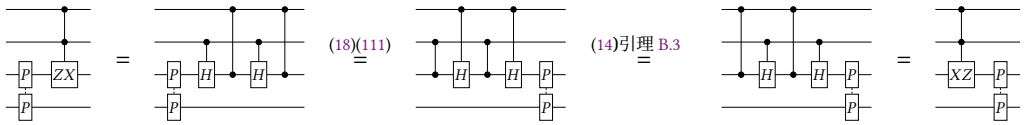
方程证明 (172)：



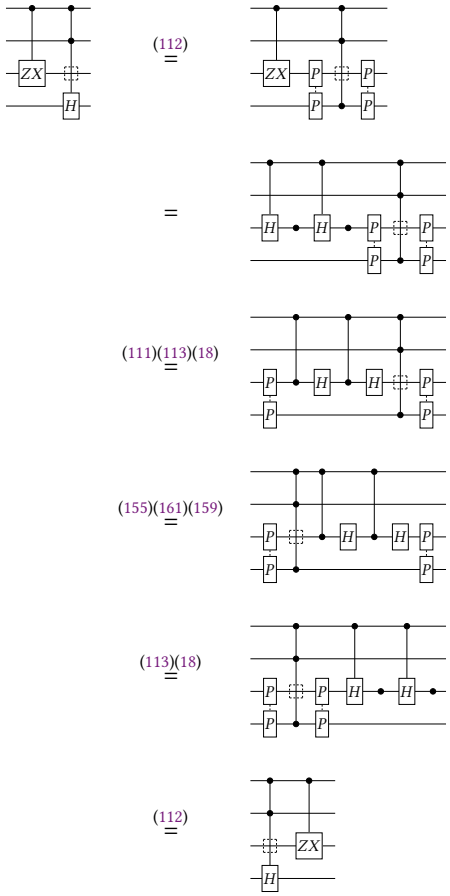


方程证明 (173)：给定方程 (172)，方程 (173) 由引理 B.5 与方程 (166) 得出。

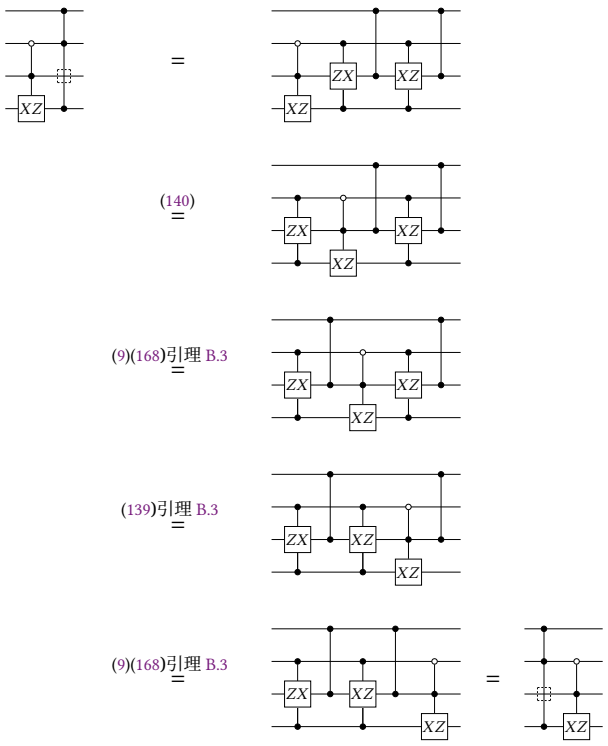
方程证明 (174)：



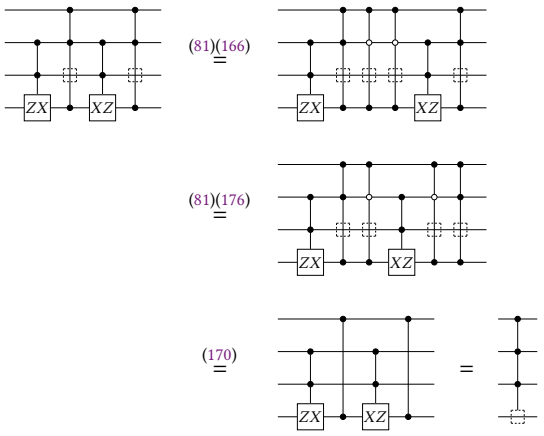
方程证明 (175)：



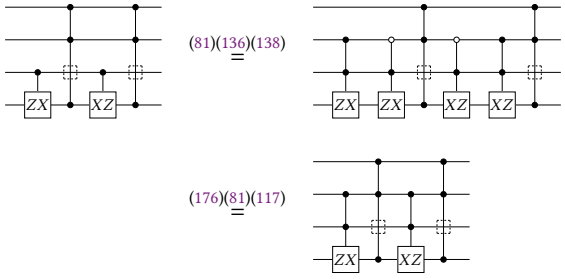
方程证明 (176):



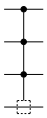
方程证明 (177):



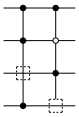
方程证明 (178):



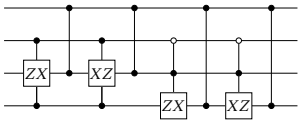
(177)
=



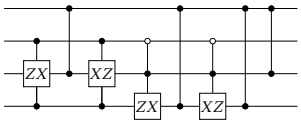
方程证明 (179):



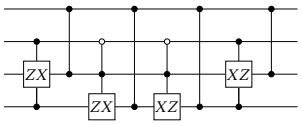
(81)
=



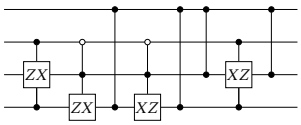
(9)(168)引理 B.3(12)
=



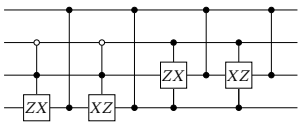
(139)(140)(9)(168)引理 B.3
=



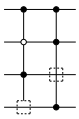
(9)(168)引理 B.3(12)
=



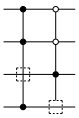
(139)(140)(9)(168)引理 B.3
=



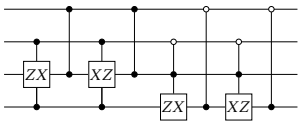
(81)
=



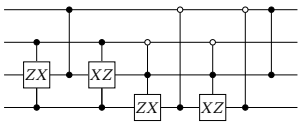
方程证明 (180):



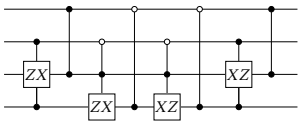
(81)
=



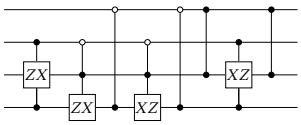
(9)(168)引理 B.3(131)
=



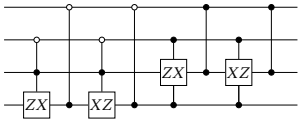
(139)(140)(9)(168)引理 B.3
=



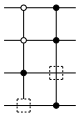
(9)(168)引理 B.3(131)
=



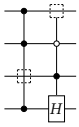
(139)(140)(9)(168)引理 B.3 =



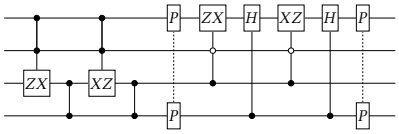
(81) =



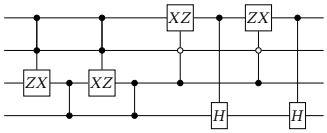
方程证明 (181):



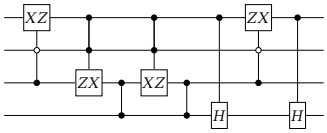
(112)(157)(161)(153)(81) =



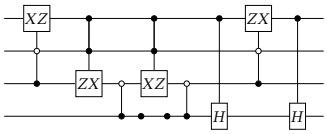
(174)(114)(111) =



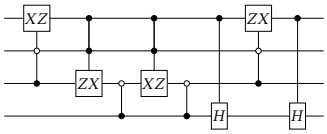
(168)(127)(139)引理 B.3(140) =



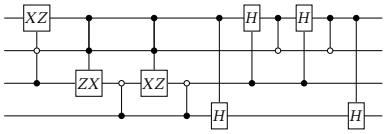
引理 7.6 =



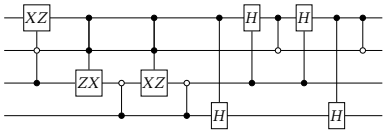
(2) =



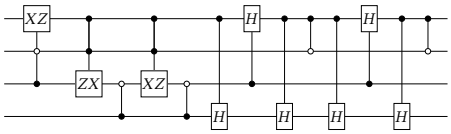
(81) =



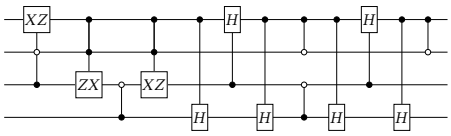
(9)(13) =



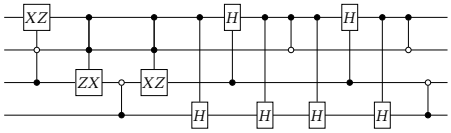
(5)(9)(13) =



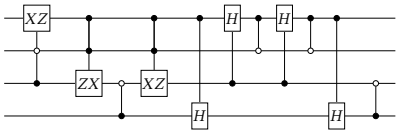
(17)
=



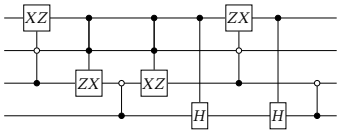
(17)
=



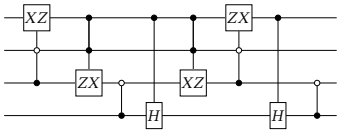
(9)(13)(5)
=



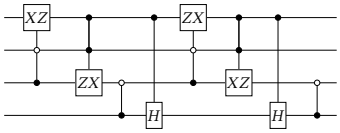
(81)
=



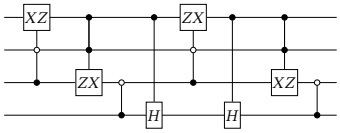
(169)引理 B.3
=



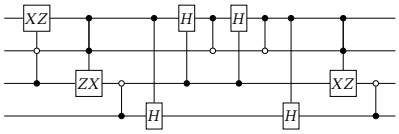
(127)引理 B.3(81)(140)
=



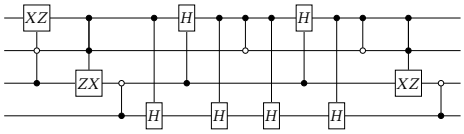
(169)引理 B.3
=



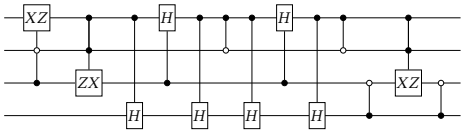
(81)
=



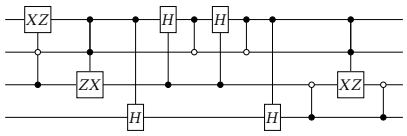
(5)(9)(13)
=



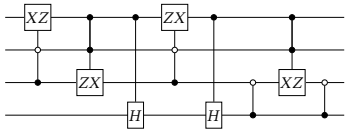
(17)
=



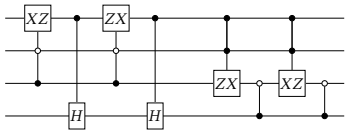
(9)(13)(5)
=



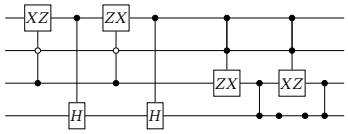
(81)
=



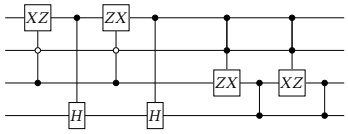
(169)(127)(139)
=



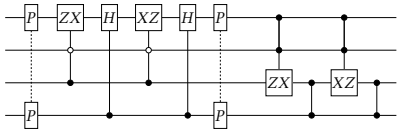
引理 7.6
=



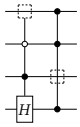
(2)
=



(111)(174)(114)
=

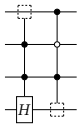


(81)(153)(161)(157)(112)
=

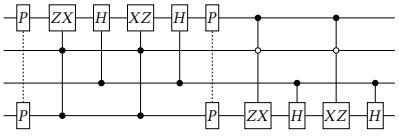


方程的证明 (182) 到 (189)： 方程 (182) 到 (189) 可由方程 (181) 以及方程 (81)、(157)、(161) 和 (162) 直接推出。

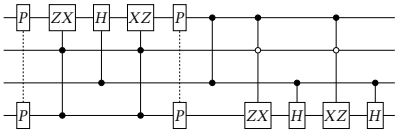
方程证明 (190)：



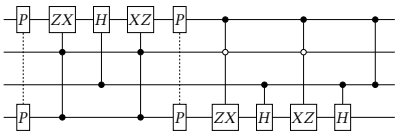
(112)(161)(157)(153)(81)
=



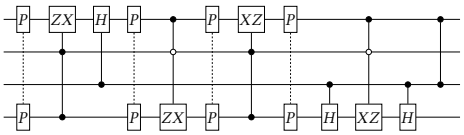
(111) (18) (9)
=



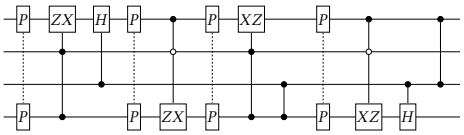
(127)(168)引理 B.3(13)
=



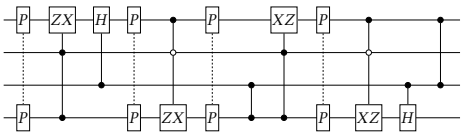
引理 D.3
=



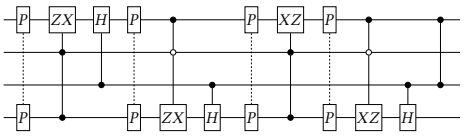
(112)(18)
=



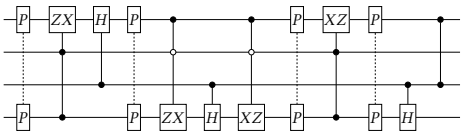
(9)(168)引理 B.3
=



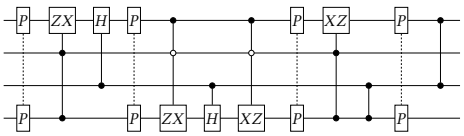
(112)(111)(18)
=



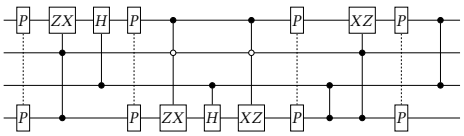
引理 D.3
=



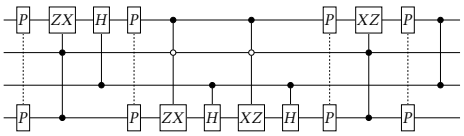
(112)(18)
=



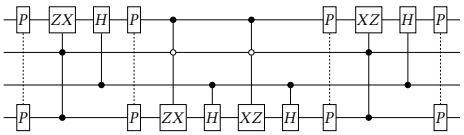
(9)(168)引理 B.3
=



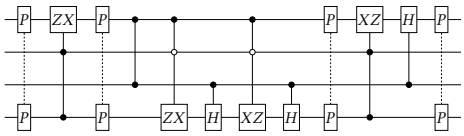
(112)(111)(18)
=



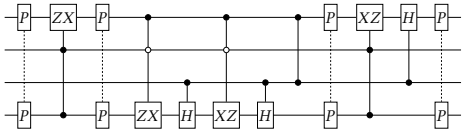
(9)(111)(18)
=



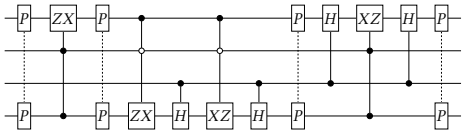
(111)（18）（9）
=



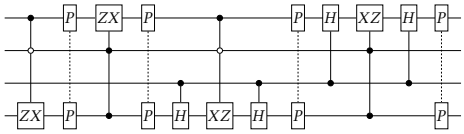
(127)(168)引理 B.3(13)
=



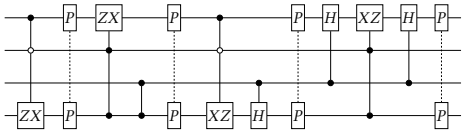
(9)(18)
=



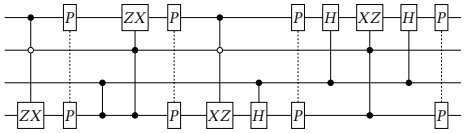
引理 D.3
=



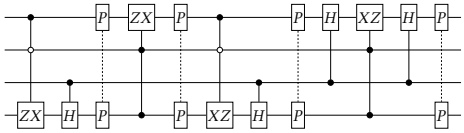
(112)(18)
=



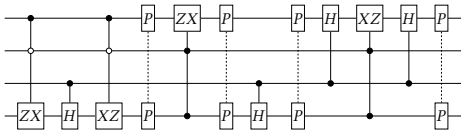
(9)(168)
=



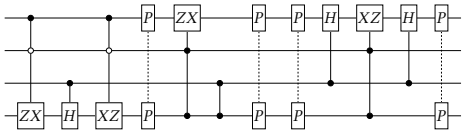
(112)(111)(18)
=



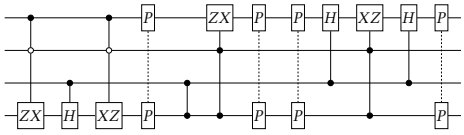
引理 D.3
=



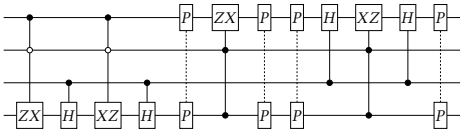
(112)(18)
=



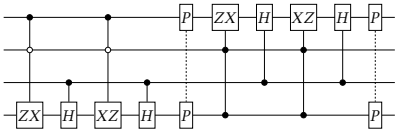
(9)(168)
=



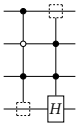
(112)(111)(18)
=



(111)
=

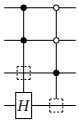


(81)(153)(161)(157)(112)
=

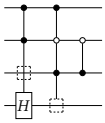


方程的证明 (191) 至 (194)： 方程 (191) 至 (194) 可由方程 (190) 与方程 (81)、(157)、(161) 和 (162) 直接推出。

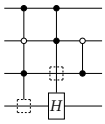
方程 (195)的证明：



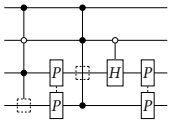
(81)(166)(161)(170)
=



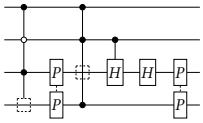
(194)
=



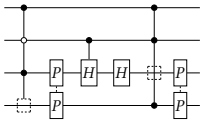
(112)(111)(18)
=



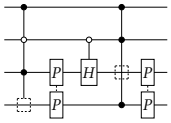
引理 7.6
=



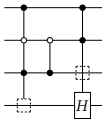
(157)(163)(155)
=



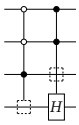
引理 7.6
=



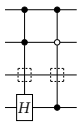
(18)(112)
=



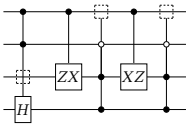
(170)(161)(81)(166)
=



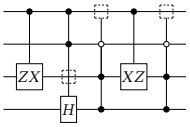
方程证明 (196):



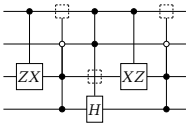
(161)(157)(178)(81)
=



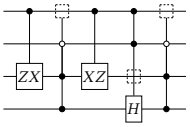
(175)
=



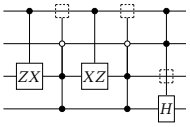
(162)(157)(183)
=



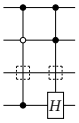
(175)引理 B.2和 B.6
=



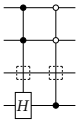
(162)(157)(183)
=



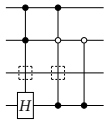
(81)(157)(178)(161)
=



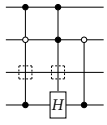
方程证明 (197):



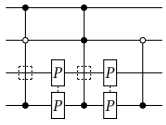
(81)(166)(161)(170)
=



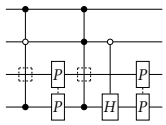
(196)
=



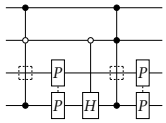
(112)
=



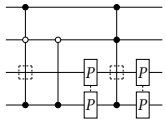
(112)(111)(18)
=



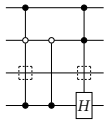
(164)
=



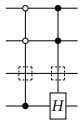
(112)(18)
=



(112)
=



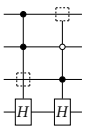
(170)(161)(81)(166)
=



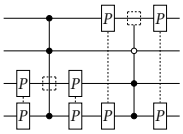
方程的证明 (198) 至 (200)： 方程 (198) 至 (200) 可由方程 (196) 以及方程 (81)、(157)、(161) 和 (162) 直接推出。

方程证明 (201)： 方程 (201) 可由方程 (162) 和 (171) 直接推出。

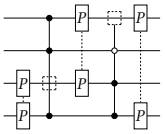
方程证明 (202)：



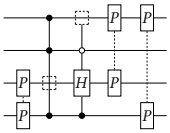
(112)
=



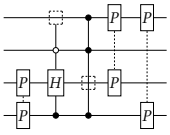
(112)(130)
=

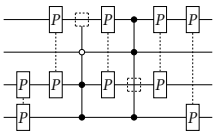


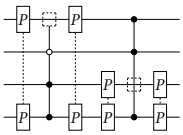
(157) (111) (112)
=

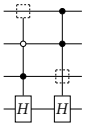


(191)
=

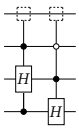


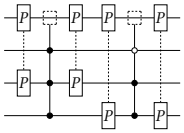
(112)(157)
=


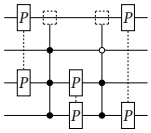
(130)(112)
=


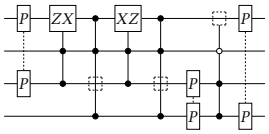
(112)
=


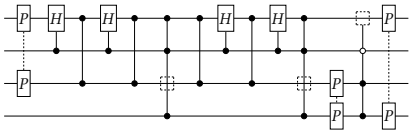
方程证明 (203):

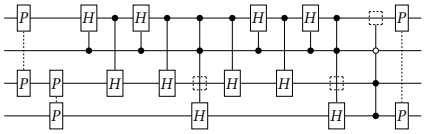


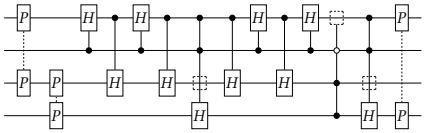
(112)(157)
=


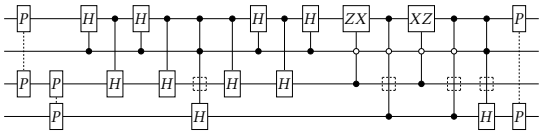
(112)(130)
=


(177)(157)(161)
=


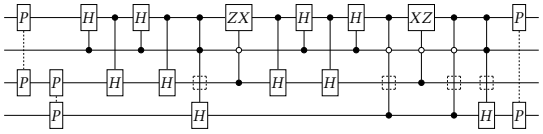
(9)
=


(111)(112)(18)
=


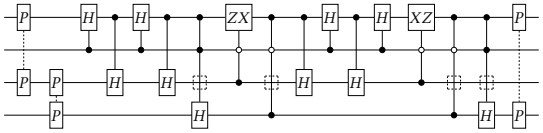
(187)
=


(177)(157)(161)(81)
=


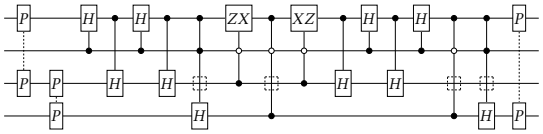
引理 D.3
=



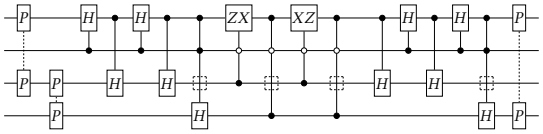
(161)(157)(81)(164)(163)
=



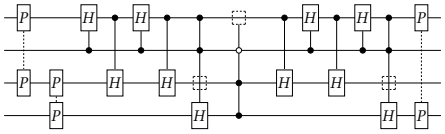
引理 D.3
=



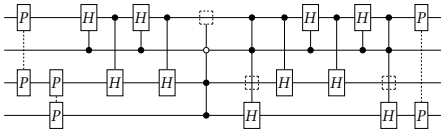
(161)(157)(81)(164)(163)
=



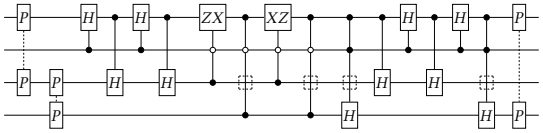
(81)(161)(157)(177)
=



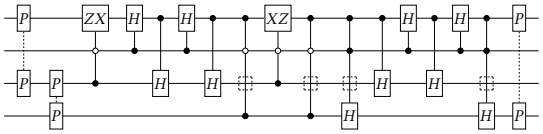
(187)
=



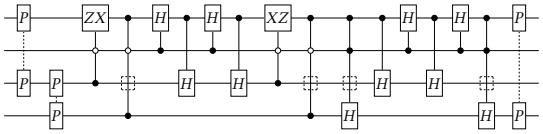
(177)(157)(161)(81)
=



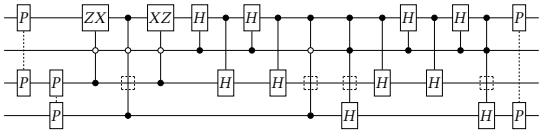
引理 D.3
=



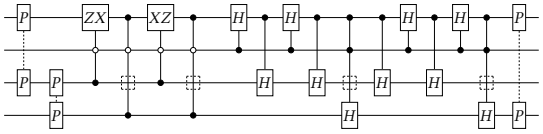
(161)(157)(163)(81)(164)
=



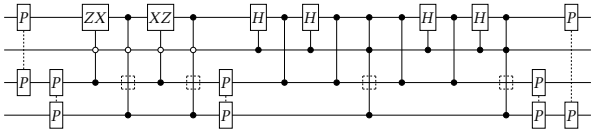
引理 D.3
=



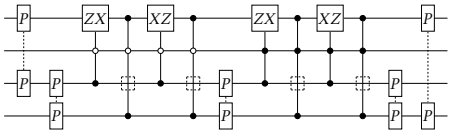
(161)(157)(163)(81)(164)
=



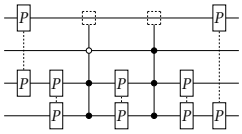
(111)(112)(18)
=



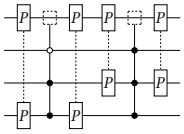
(9)
=



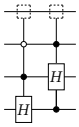
(81)(161)(157)(177)
=



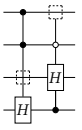
(112)(130)
=



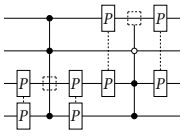
(112)(157)
=



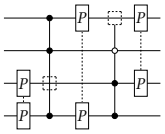
方程证明(204):



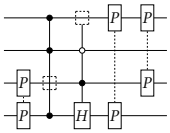
(112)(157)
=



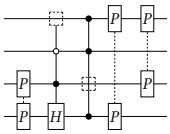
(130)
=



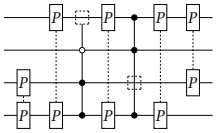
(111)(112)
=



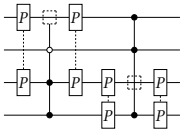
(188)
=



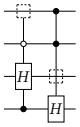
(112) =



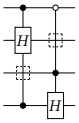
(112)(130) =



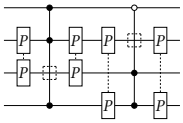
(112)(157) =



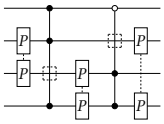
方程证明 (205)*:*



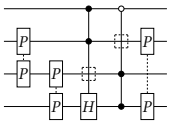
(112)(157) =



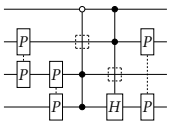
(112)(130) =



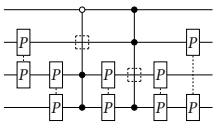
(111)(112) =



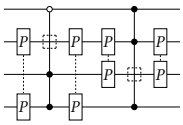
(189) =



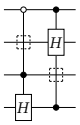
(112) =



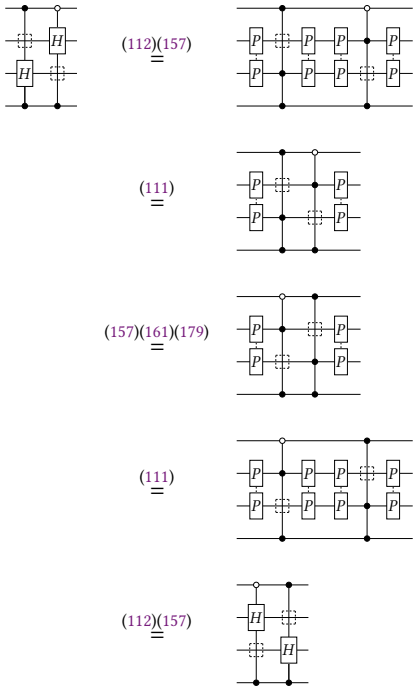
(112)(130) =



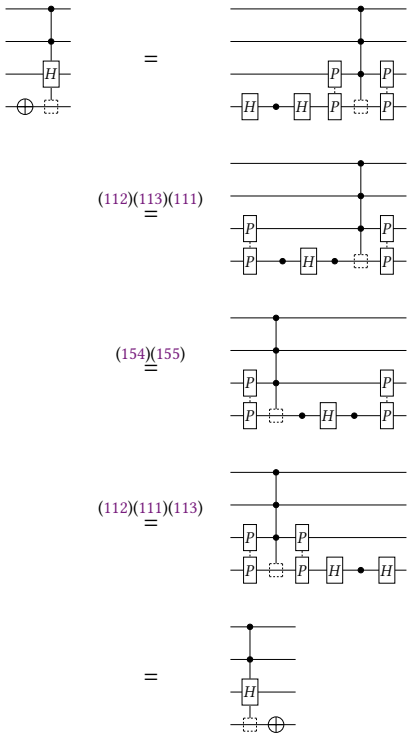
(112)(157) =



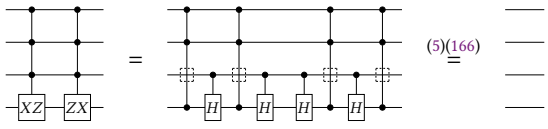
方程证明 (206)*:*



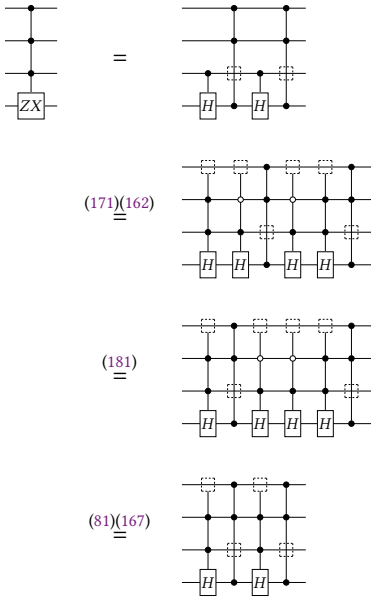
方程证明 (207)*:*



方程证明 (208)*:*

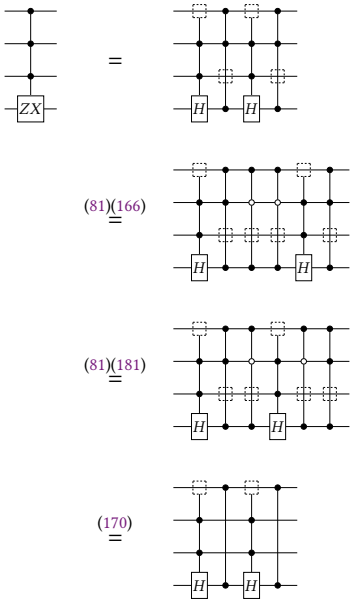


方程证明 (209): 方程 (209)followsfromEquations(81)and(208).方程证明
(210):



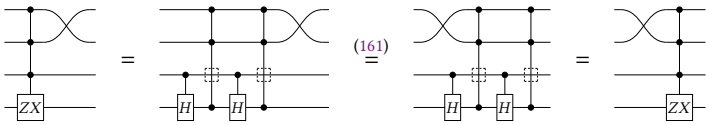
方程证明 (211)： 根据方程 (210)，方程 (211可由引理 B.5 结合方程 (81)、(166)、(167) 和 (208) 得出。

方程证明 (212):

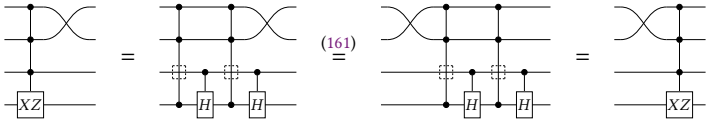


方程证明 (213)： 给定方程 (212)，方程 (213) 可由引理 B.5 结合方程 (4)、(81)、(167) 和 (208) 得出。

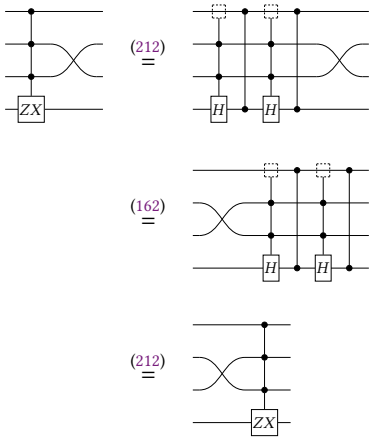
方程证明(214)：如果 $a = 0$，则我们有



并且如果 $a = 1$，则我们有

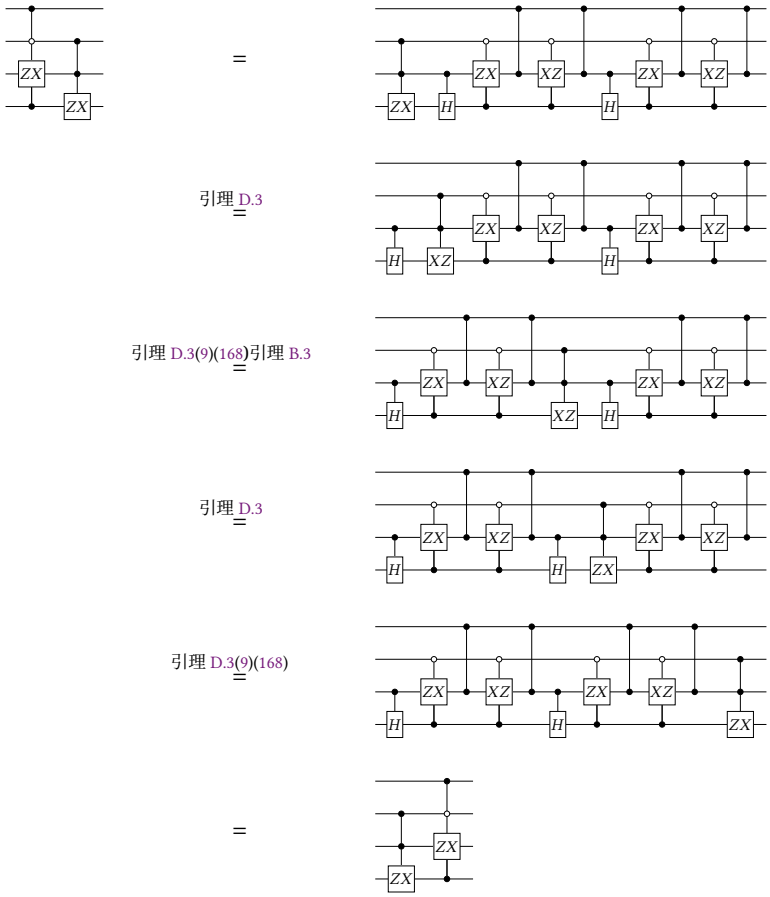


方程证明 (215)： 若 $a = 0$，则有



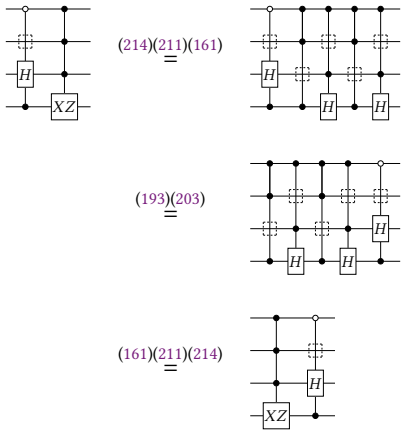
该情形 $a = 1$ 由引理 B.5 结合方程（208）得出。

方程证明 (216)：

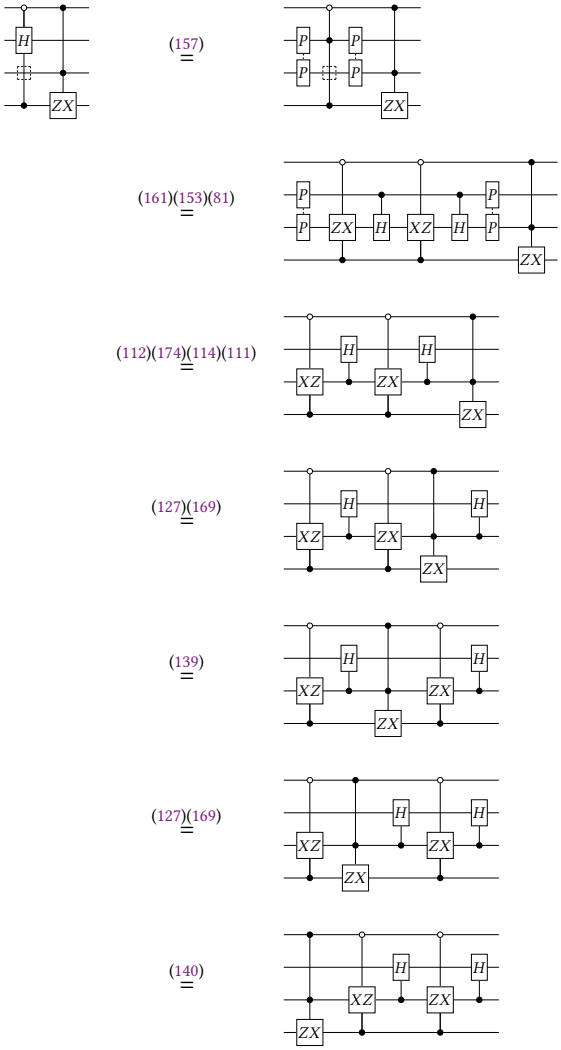


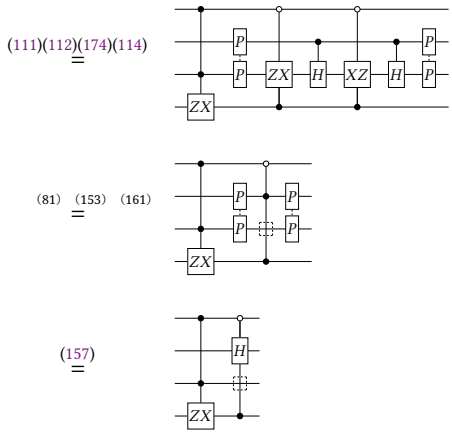
方程证明 （217）： 由方程（216），方程（217）可由引理B.6结合方程（118）得出。

方程证明 (218)： 由方程 (216)，结合引理 B.6 以及方程 (81) 和 (208)，即可得出方程 (218)。方程证明 (219)：

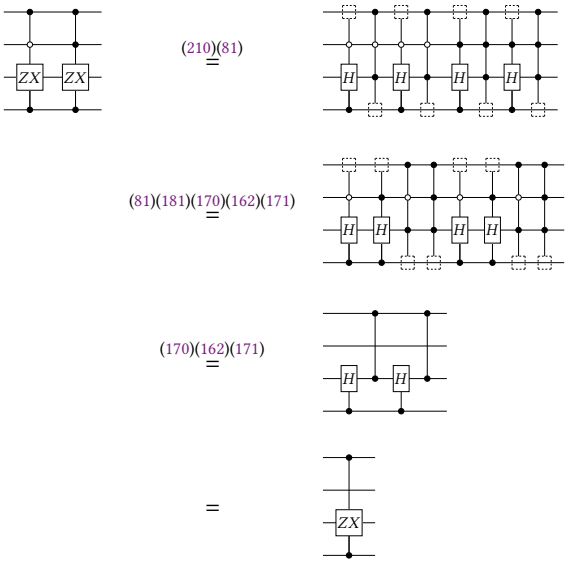


方程证明 (220)：



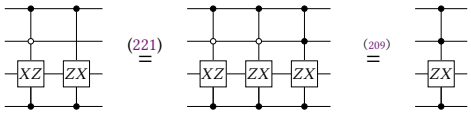


方程证明 (221):

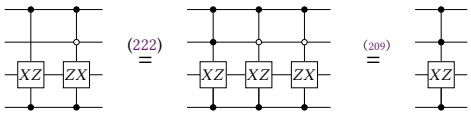


方程证明 (222): 由方程 (221)，方程 (222) 可由引理B.5 结合方程 (81)、(118) 和 (208) 得出 .

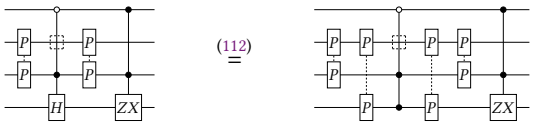
方程证明 (223): 方程 (223) 可直接由方程 (221) 结合方程 (81) 和 (214) 得出。方程证明 (224): 方程 (224) 可直接由方程 (222) 结合方程 (81) 和 (214) 得出。方程证明 (225):



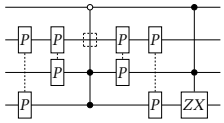
方程证明 (226):



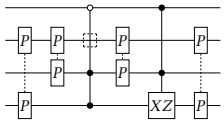
方程证明 (227):



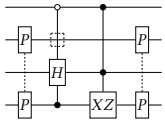
(112)(130)
=



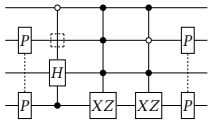
(112)(174)
=



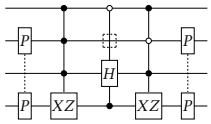
(157)(112)
=



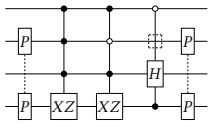
(222)
=



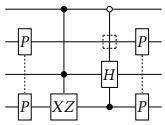
(219)
=



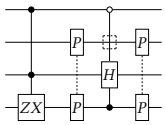
(207)(219)
=



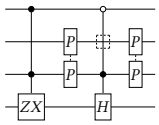
(222)
=



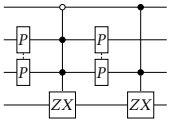
(112)(111)(174)
=



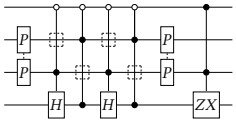
(112)(130)(157)
=



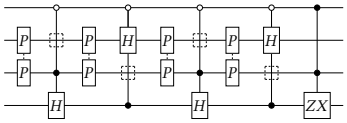
方程证明 (228)： 如果 $\beta = 1$, 则有



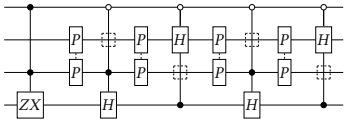
(214)(210)(161)(81)
=



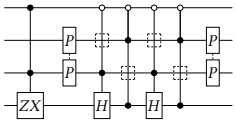
(111)(157)
=



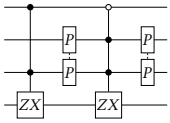
(220)(227)
=



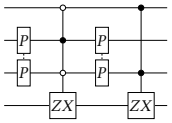
(111)(157)
=



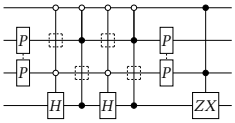
(81)(161)(210)(214)
=



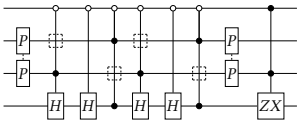
并且如果 $\beta = 0$, 我们有



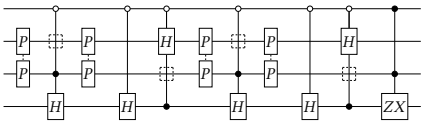
(214)(210)(161)(81)(156)
=



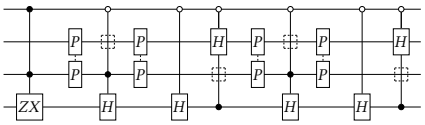
(81)(167)(171)
=



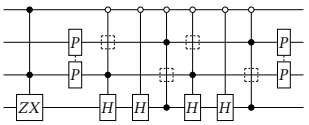
(111)(157)
=



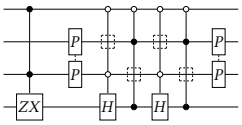
(220)引理 D.3(227)
=



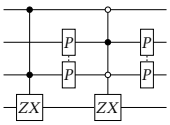
(111)(157)
=



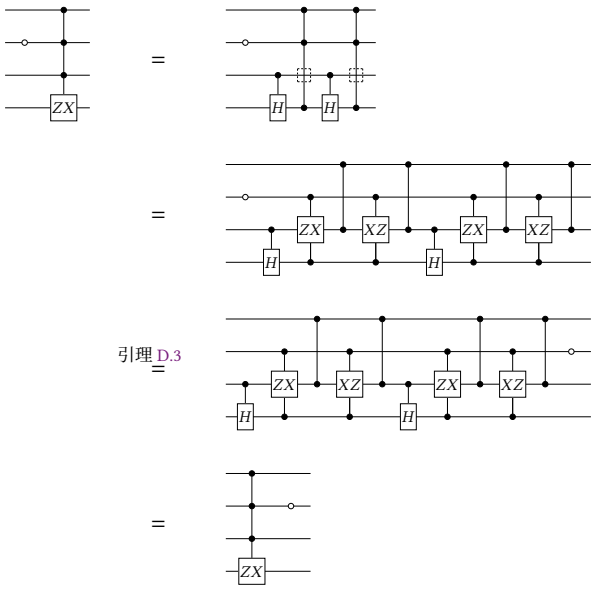
(171)(81)(167)
=



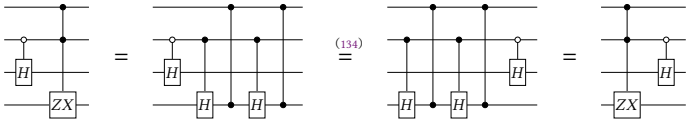
(156)(81)(161)(210)(214)
=



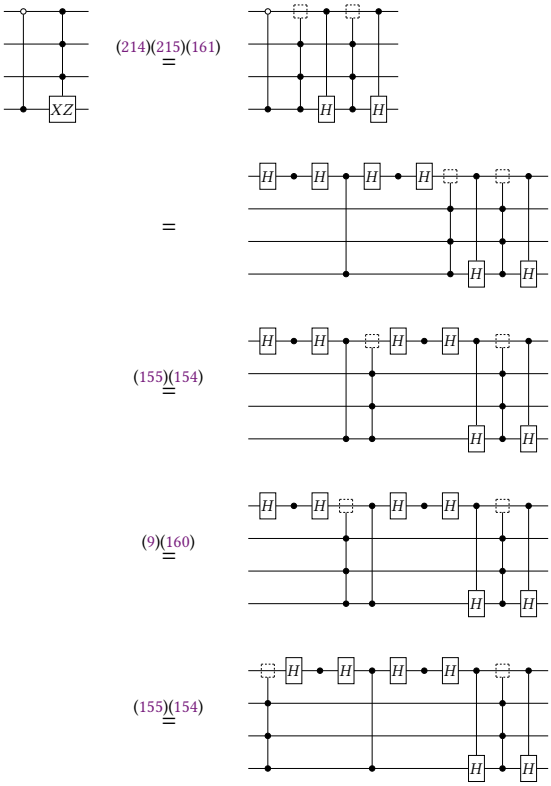
方程证明 (229)： 使用引理 B.6 （连同方程（81）和（208）），不失一般性地，我们可以假设 $a = 0$。我们有

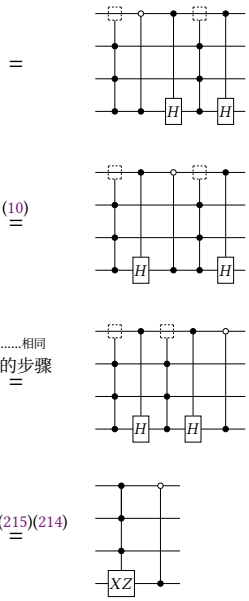


方程证明 (230)：

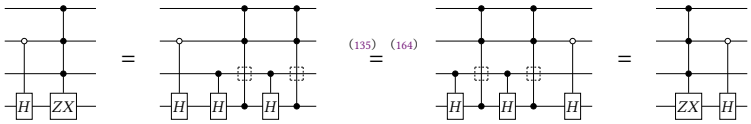


方程证明 (231)：

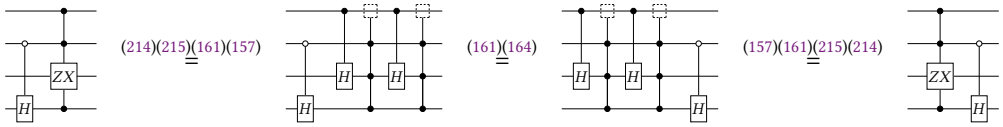




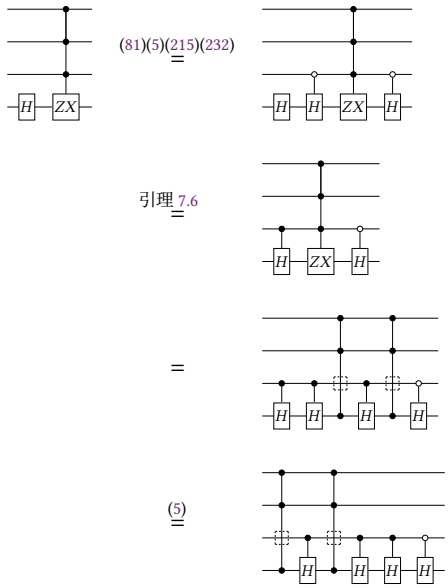
方程证明 (232):

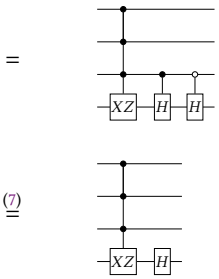


方程证明 (233): 由方程(232), 方程(233)可由引理B.5结合方程(5)、(81) 和 (208)得出。方程证明 (234):

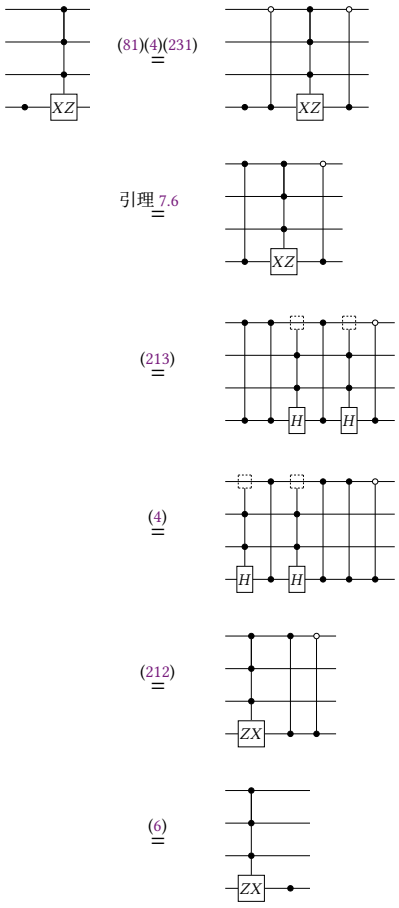


方程证明 (235): 根据方程 (234), 方程 (235) 可由引理 B.5 与方程 (5)、(81) 和 (208) 一起推出。方程证明 (236):

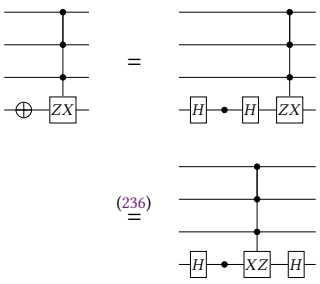




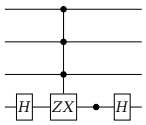
方程证明 (237):



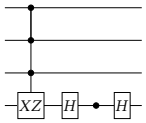
方程证明(238):



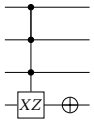
(237)
=



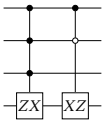
(236)
=



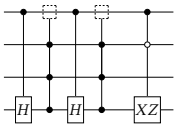
=



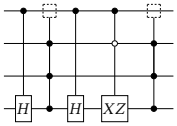
方程证明 (239)： 利用引理 B.6 (以及方程 (81) 和 (118))，我们可以不失一般性地假设 $a = 1$。若 $\gamma = 1$，则有



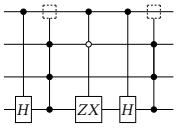
(214)(215)(161)
=



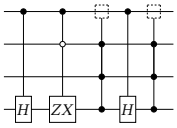
(127)引理 B.3(161)(176)
=



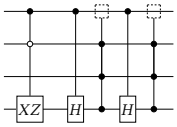
引理 D.3
=



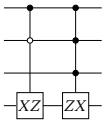
(127)(161)(176)引理B.2和 B.6
=



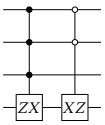
引理 D.3
=



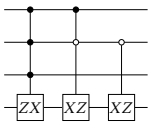
(161)(214)(215)
=



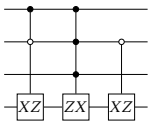
并且，如果 $\gamma = 0$，我们有



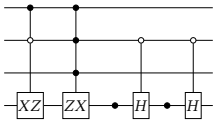
引理 D.3
=



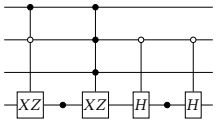
前一种情况 =



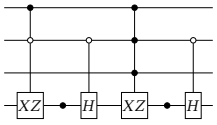
(81) =



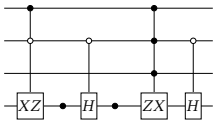
(237) =



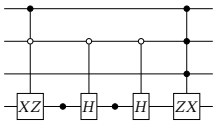
(233) =



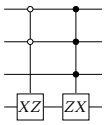
(2)(237) =



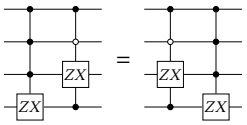
(232) =

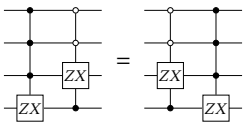


引理 D.3 =

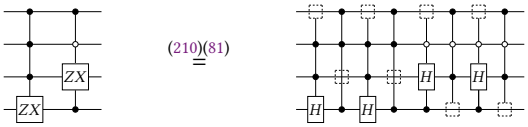


方程证明 (240)： 利用方程 (81)，不失一般性地假设 $\alpha = 1$。利用方程 (81) 和 (238)，不失一般性地假设 $\beta = 1$ 且 $\delta = 1$。再利用引理 B.6 (以及方程 (208))，不失一般性地假设 $a = 1$ 且 $b = 1$。也就是说，我们只需证明以下两个方程：

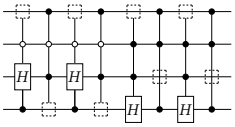




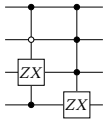
为了证明第一个，我们有



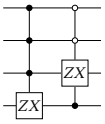
(191)(179)(203)(190)
=



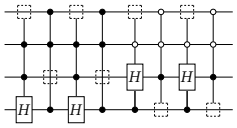
(81)(210)
=



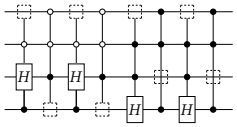
而为了证明第二个，我们有



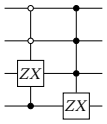
(210)(81)(207)
=



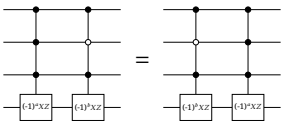
(191)(180)(203)(207)(190)
=



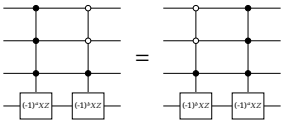
(207)(81)(210)
=



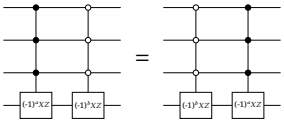
方程证明 (241)： 使用方程 (81后，不失一般性，我们可以假设 $\alpha = 1$ 且 $\beta = 1$。使用方程 (214) 和 (215后，我们可以不失一般性地假设 $\gamma \leq \delta$。也就是说，我们只需证明以下三个方程：



(241a)

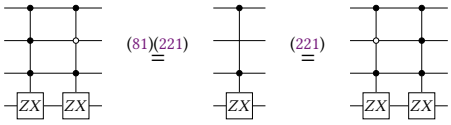


(241b)

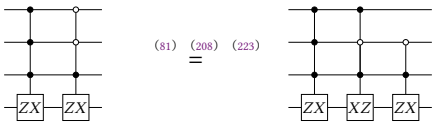


(241c)

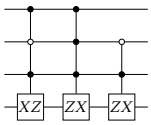
为证明方程 (241a)，在使用引理 B.6 （以及方程 (81) 和 (208)）的前提下，我们可以不失一般性地假设 $a = 1$ 且 $b = 1$。我们有



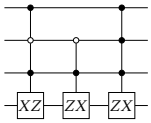
为证明方程 (241b)，同样在使用引理 B.6 (以及方程 (81) 和 (208)）的前提下，我们不失一般性地假设 $a = 1$ 和 $b = 1$。我们有



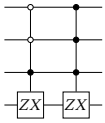
(241a)
=



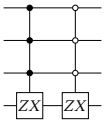
(14)(215)(214)(239)
=



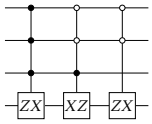
(223)(81)(208)
=



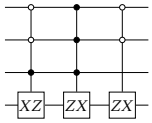
而为证明方程 (241c)，同样在使用引理 B.6 (以及方程 (81) 和 (208)) 的前提下，我们不失一般性地假设 $a = 1$ 和 $b = 1$。我们有



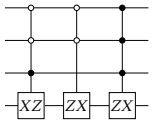
(81) (208) (223)
=



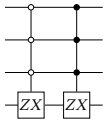
(241b)
=



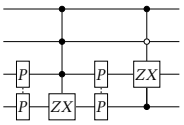
(239)
=



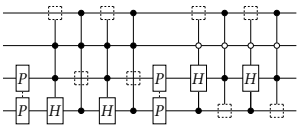
(223)(81)(208)
=



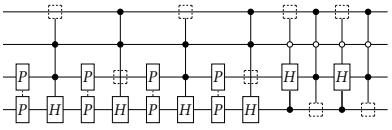
方程证明 (242)：利用方程 (81) 后，我们不失一般性地假设 $\alpha = 1$。首先，考虑 $\beta = \gamma = \delta = 1$ 的情况。利用引理 B.6 (以及方程 (81)、(111) 和 (208))，我们不失一般性地假设 $a = 0$ 且 $b = 0$。我们有



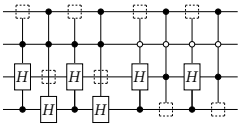
(210)(81)
=



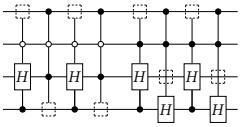
(111)(112)
=



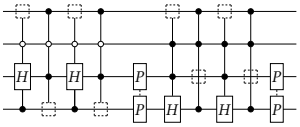
(112)(130)
=



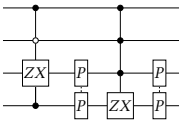
(204)(194)(201)(182)
=



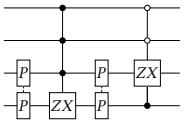
(112)(130)(111)
=



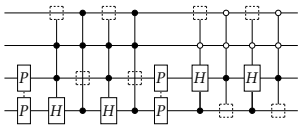
(81)(210)
=



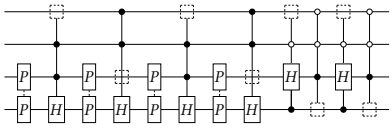
接下来，我们讨论 $\beta = \delta = 1$ 和 $\gamma = 0$ 的情况。同样，利用引理 B.6 （结合方程（81）、（111）和（208））， 不失一般性，我们可以假设 $a = 0$ 且 $b = 0$。我们有



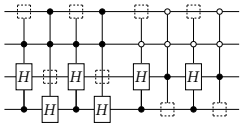
(210)(81)(207)
=



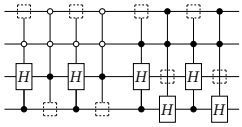
(111)(112)
=



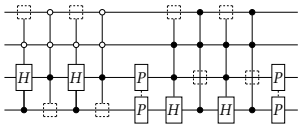
(112)(130)
=



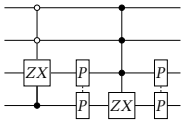
(204)(195)(201)(207)(182)
=



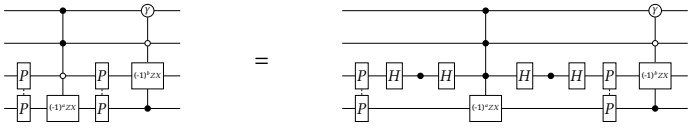
(112)(130)(111)
=



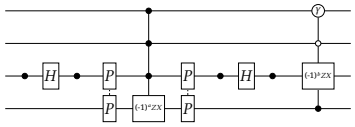
(207)(81)(210)
=



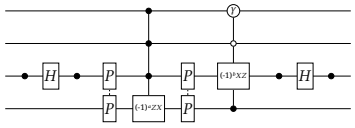
接下来，为了处理 $\beta = 0$ 和 $\delta = 1$的情形，我们有



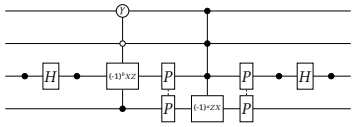
(111)(113)
=



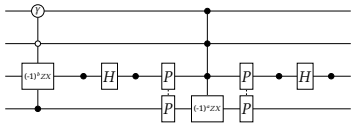
(2)(1)(237)(236)
=



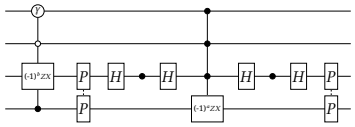
前述情形
=



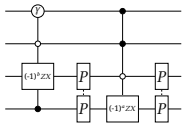
(2)(1)(237)(236)
=



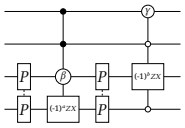
(111)(113)
=



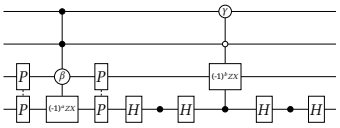
=



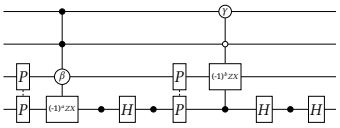
最后，对于 $\delta = 0$的情形，我们有



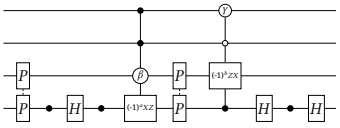
=



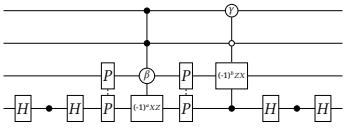
(112)(111)(113)
=



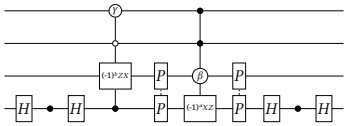
(2)(1)(237)(236)
=



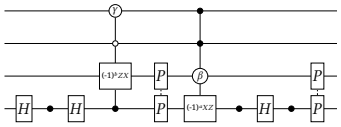
(112)(111)(113)
=



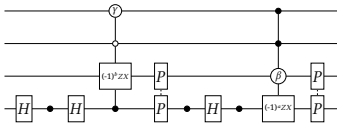
前述情形 =



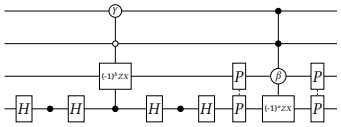
(112)(111)(113) =



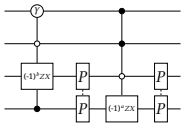
(2)(1)(237)(236) =



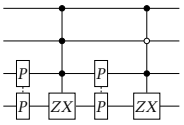
(112)(111)(113) =



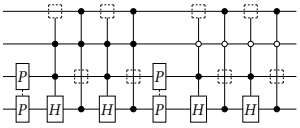
=



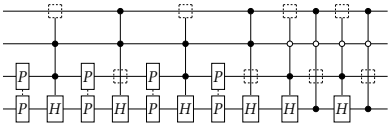
方程证明 (243)： 根据方程 (81)，不失一般性，我们可以假设 $\alpha = 1$。首先，我们讨论 $\beta = \gamma = \delta = 1$ 的情形。根据引理 B.6 (以及方程 (81)、(111) 和 (208))，不失一般性，我们可以假设 $a = 0$ 且 $b = 0$。我们有



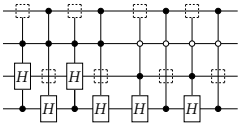
(210)(81) =



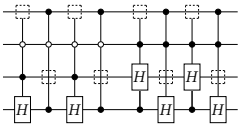
(111)(112) =



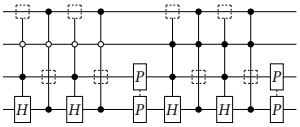
(112)(130) =



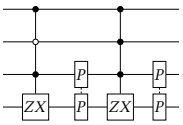
(202)(196)(203)(192) =



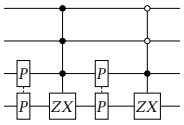
(112)(130)(111) =



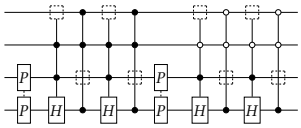
(81)(210)
=



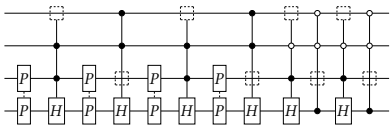
接下来，我们讨论 $\beta = \delta = 1$ 和 $\gamma = 0$的情形。同样，结合引理 B.6 （以及方程（81）、（111）和（208），不失一般性，我们可以假设 $a = 0$ 和 $b = 0$。我们有



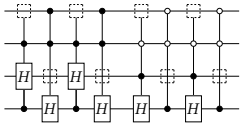
(210)(81)(207)
=



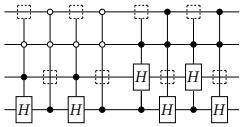
(111)(112)
=



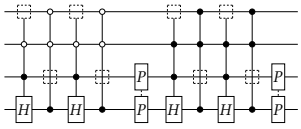
(112)(130)
=



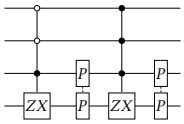
(202)(197)(203)(207)(192)
=



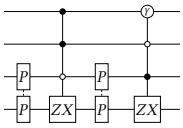
(112)(130)(111)
=



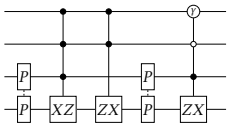
(207)(81)(210)
=



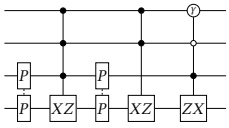
接下来，要处理 $\beta = 0$ 和 $\delta = 1$ 的情形，同样只需使用引理 B.6 （结合方程（81）、（111）和（208）），不失一般性，我们可以假设 $a = 0$ 和 $b = 0$。我们有



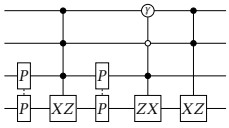
(208)(215)(81)(221)
=



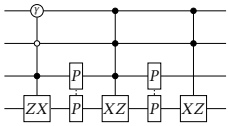
(112)(111)(174)
=



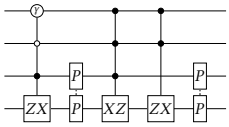
(81)(239)
=



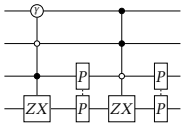
前述情形 =



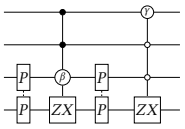
(112)(111)(174) =



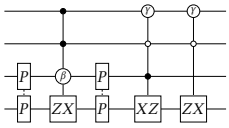
(81)(221)(215)(208) =



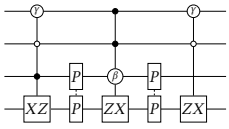
最后，对于 $\delta = 0$的情形，同样可以利用引理B.6 （结合方程 (81)、(111) 和 (208)），不失一般性地假设 $a = 0$ 且 $b = 0$。我们有



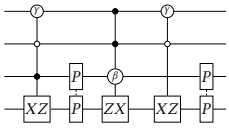
(81)(208)(215)(221) =



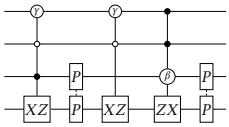
前述情形 =



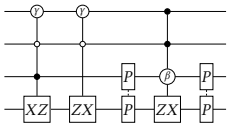
(112)(174) =



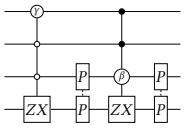
(239) =



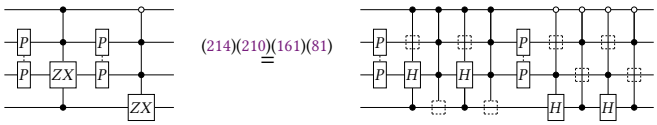
(112)(111)(174) =



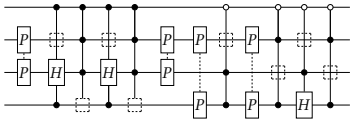
(81)(221)(215)(208) =



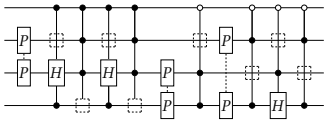
方程证明 (244)：如果 $\alpha = \beta = 1$，则在使用引理 B.6 （连同方程（81）、（111）和（208））的情况下，我们可以不失一般性地假设 $a = 0$ 且 $b = 0$。我们有



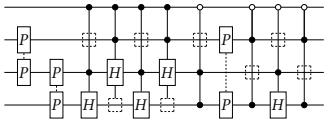
(112)
=



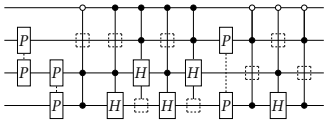
(112)(130)
=



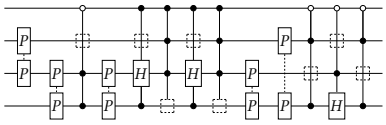
(111)(112)(130)
=



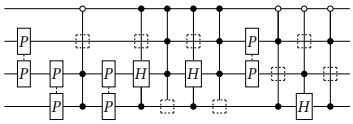
(183)(198)
=



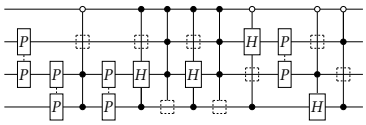
(111)(112)(130)
=



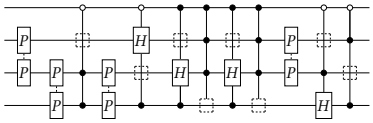
(112)(130)
=



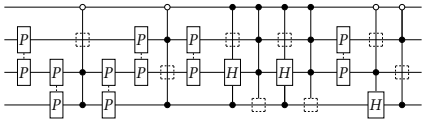
(157)(111)
=



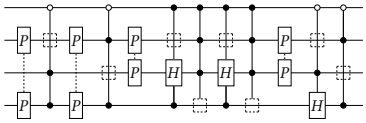
(184)(206)
=



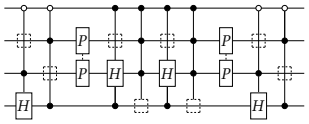
(157)
=



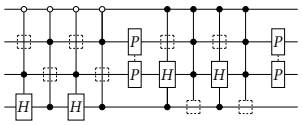
(112)(130)
=



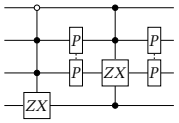
(112)
=



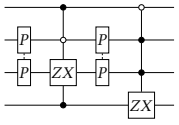
相同于
先前步骤
=



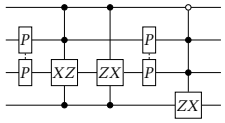
(81)(161)(210)(214)
=



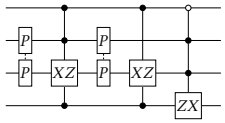
如果 $\beta = 1$ 且 $\alpha = 0$，则再次地，在使用引理 B.6 （连同方程（81）、（111）和（208））的前提下，我们可以不失一般性地假设 $a = 0$ 且 $b = 0$。我们有



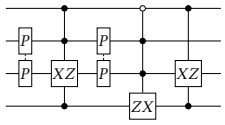
(208)(81)(221)
=



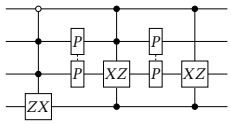
(112)(111)(174)
=



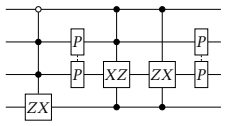
(214)(217)
=



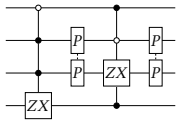
前述情形
=



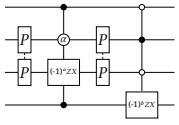
(112)(111)(174)
=



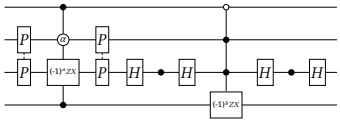
(81)(221)(208)
=



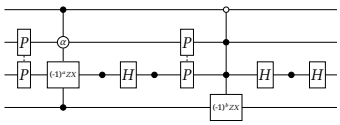
并且如果 $\beta = 0$，那么我们有



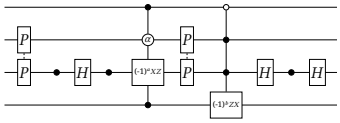
=



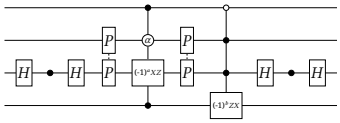
(112)(111)(113)
=



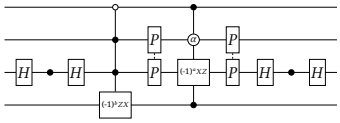
(2)(1)(237)(236)
=



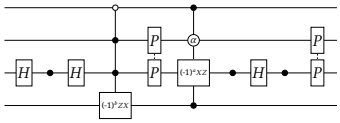
(112)(113)(111)
=



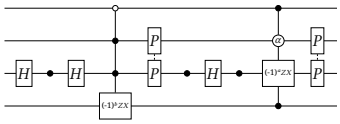
前述情形
=



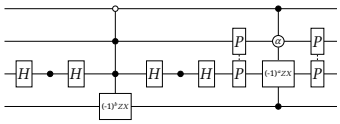
(112)(111)(113)
=



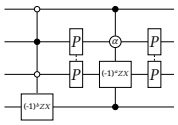
(2)(1)(237)(236)
=



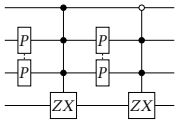
(112)(113)(111)
=



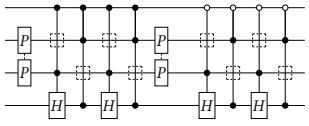
=



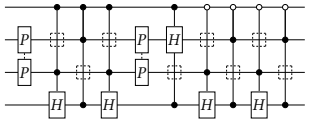
方程证明(245)：如果 $\alpha = \beta = 1$，则在使用引理B.6 （以及方程(81)、(111)和(208)）的前提下，我们可以不失一般性地假设 $a = 0$ 和 $b = 0$。我们有



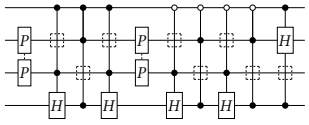
(214)(210)(161)(81)
=



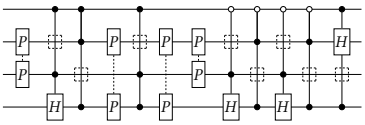
(157)(111)
=



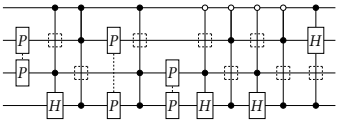
(205)(199)
=



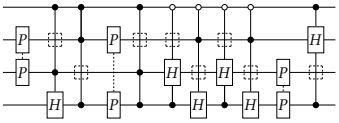
(112)
=



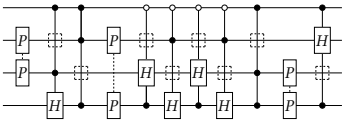
(112)(130)
=



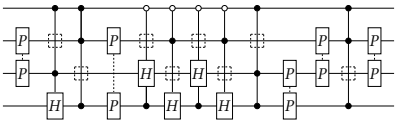
(111)(112)(130)(157)
=



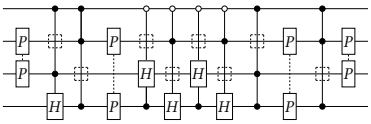
(200)(185)
=



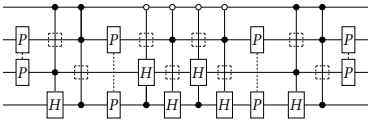
(157)
=



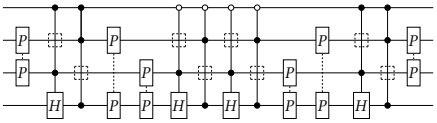
(130)
=



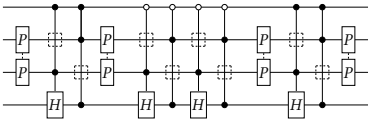
(111)(112)
=



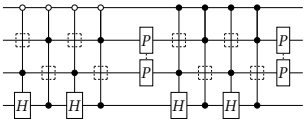
(111)(112)(130)(157)
=



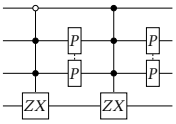
(112)(130)
=



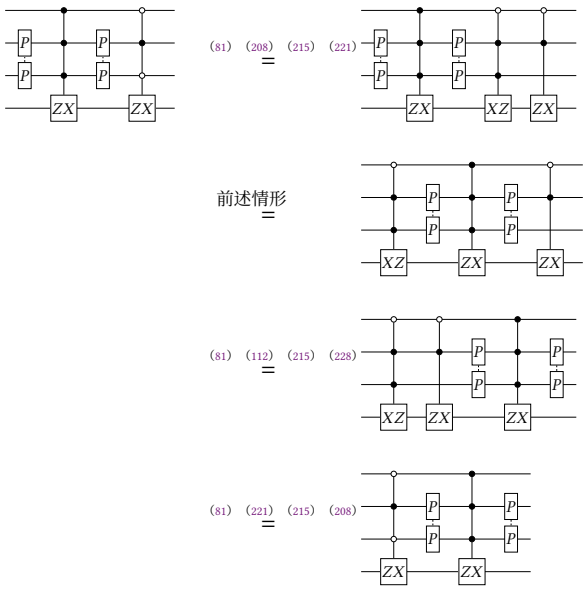
类似于
前面的步骤
=



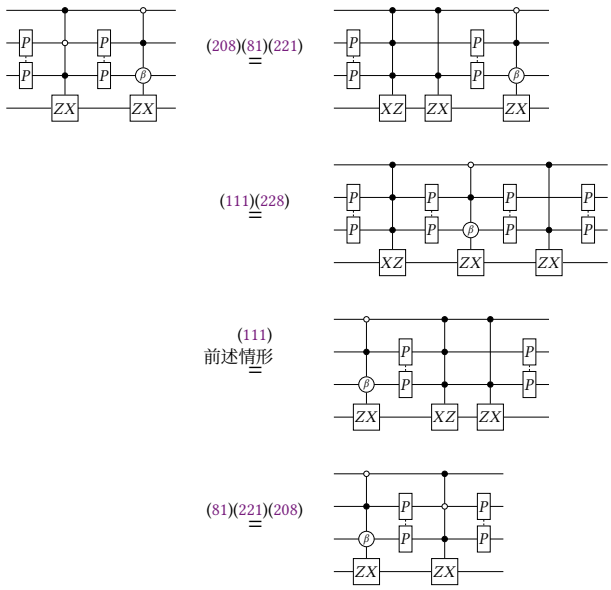
(81)(161)(210)(214)
=



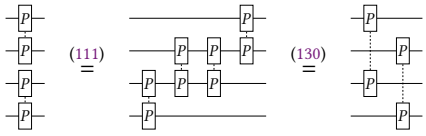
若 $\alpha = 1$ 且 $\beta = 0$，则再次利用引理B.6 （连同方程（81）、（111）和（208）），不失一般性地假设 $a = 0$ 且 $b = 0$。我们有



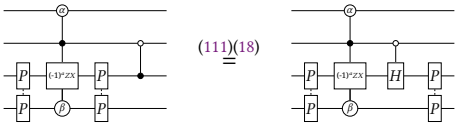
最后，如果 $\alpha = 0$，那么再次，向上 使用引理 B.6 (以及方程 (81)、(111) 和 (208))，不失一般性地假设一般性地， $a = 0$ 和 $b = 0$。我们 have

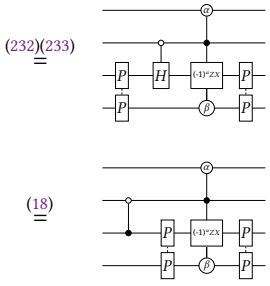


方程证明 (246)：

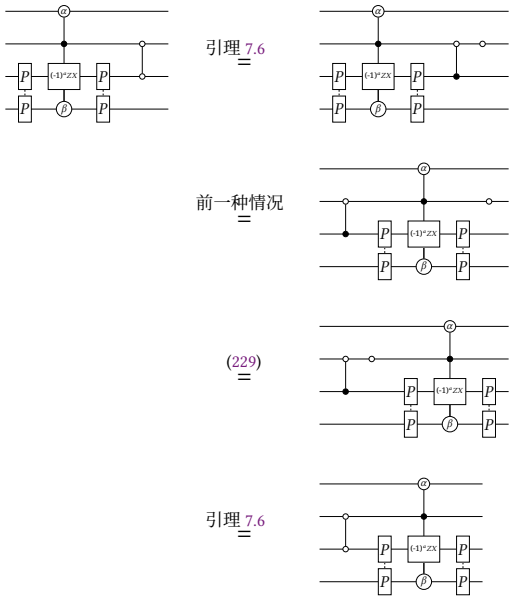


方程证明 (247)： 若 $\gamma = 1$，则有

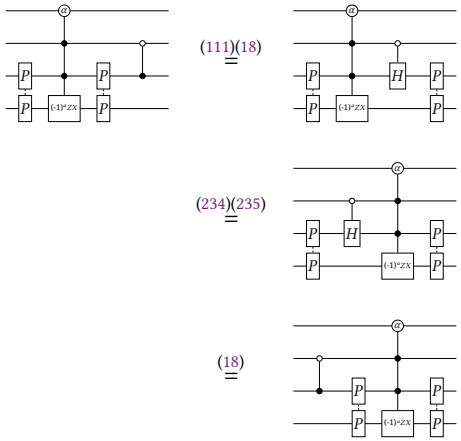




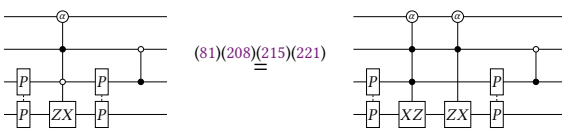
并且若 $\gamma = 0$，则有



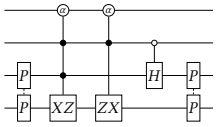
方程证明 (248)： 若 $\gamma = 1$ 且 $\beta = 1$，则有



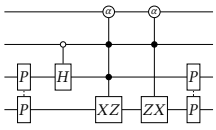
如果 $\gamma = 1$ 且 $\beta = 0$，则在使用引理 B.6 （连同方程（81）、（111）和（208））之后，我们可以不失一般性地假设 $a = 0$。我们有



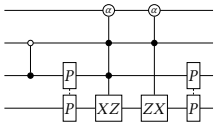
$\overset{(111)(18)}{=}$



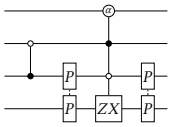
$\overset{(230)(235)}{=}$



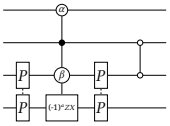
$\overset{(18)}{=}$



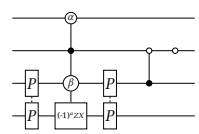
$\overset{(81)(221)(215)(208)}{=}$



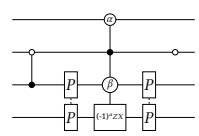
并且如果 $\gamma = 0$，则我们有



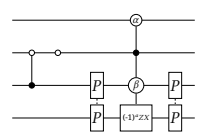
$\overset{\text{引理 7.6}}{=}$



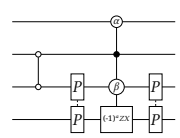
$\overset{\text{前述情形}}{=}$



$\overset{(229)}{=}$



$\overset{\text{引理 7.6}}{=}$



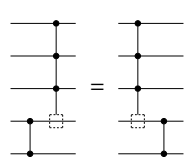
□

D.4 五量子比特辅助方程

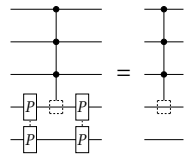
与附录 D.3类似，我们将使用引理 5.1 的四量子比特版本：

引理 D.6（条件四量子比特完备性）。对于任意定义在 $\left\{ \square \text{上的四量子比特量子电路 } C_1、C_2, \ , \ , \ \begin{array}{c} \bullet \\ \square \\ \bullet \end{array} \right\}$，若 $[\![C_1]\!] = [\![C_2]\!]$，则 $\mathrm{QC} \vdash \underline{(\otimes}\, C_1) = (\otimes\, \underline{C_2})$ 且 $\mathrm{QC} \vdash (C_1 \otimes) = \underline{(C_2 \otimes)}$。

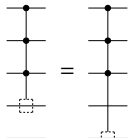
引理 D.7。以下方程是图 *4* 中方程的推论：



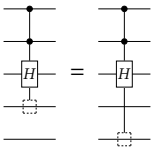
(249)



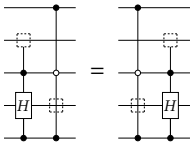
(250)



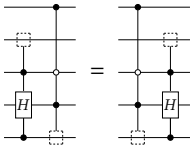
(251)



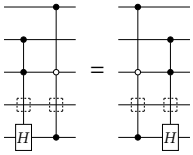
(252)



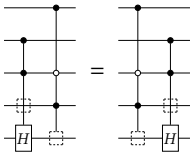
(253)



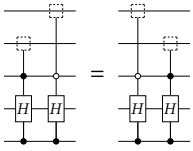
(254)



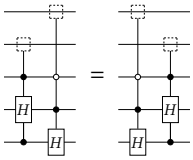
(255)



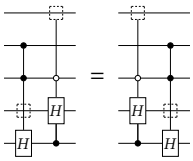
(256)



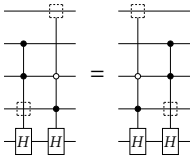
(257)



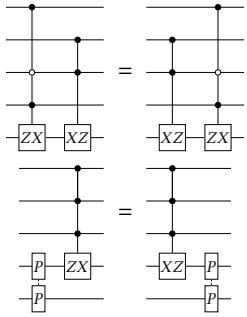
(258)



(259)

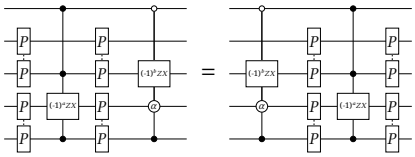


(260)

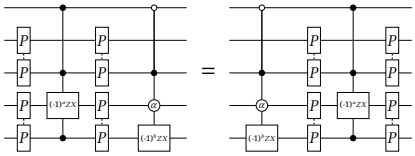


(261)

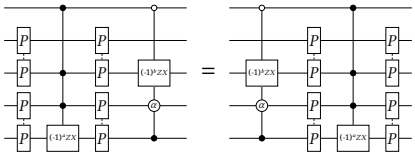
(262)



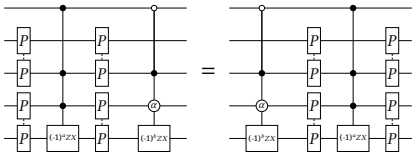
(263)



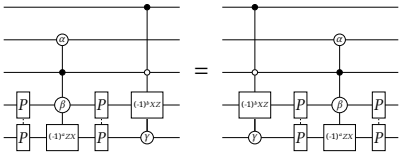
(264)



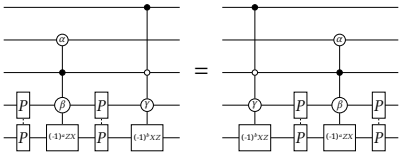
(265)



(266)



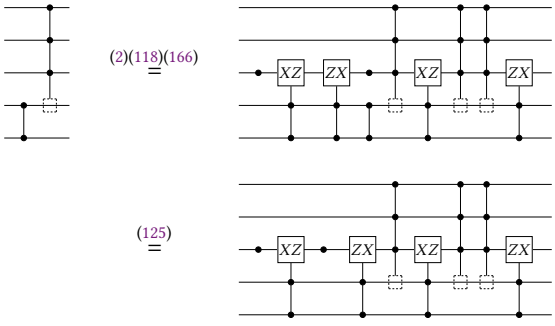
(267)



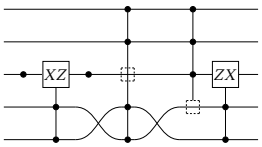
(268)

证明。

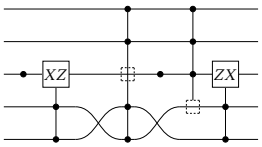
方程证明 (249)：



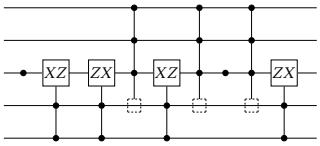
(127)引理 B.3 =



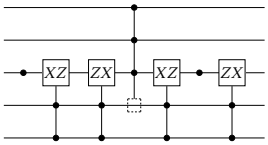
(19) =



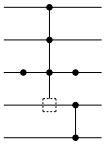
(127)引理 B.3 =



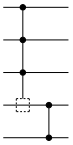
引理 D.6 =



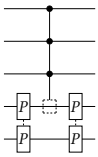
(125)(118) =



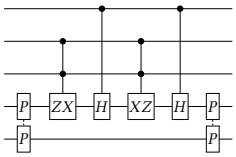
引理 D.6 =



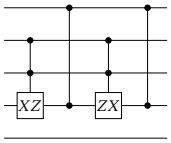
方程证明 (250):



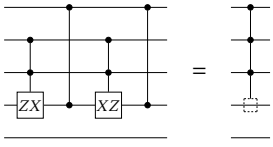
(153) =



(174)(18)(111) =

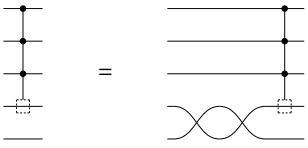


(124)引理 B.3(4) =

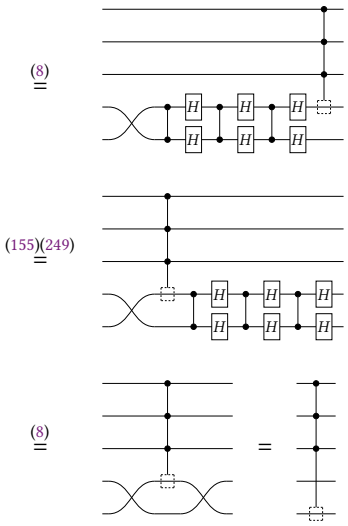


=

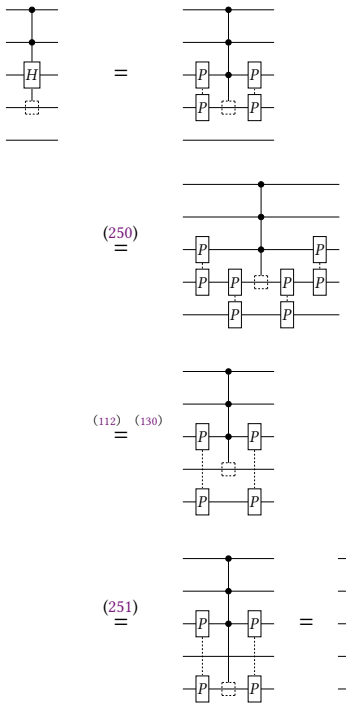
方程证明 (251):



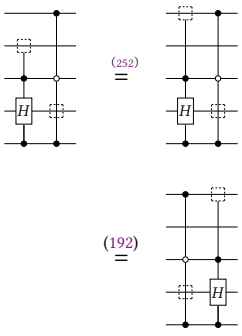
=

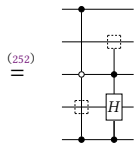


方程证明 (252)：

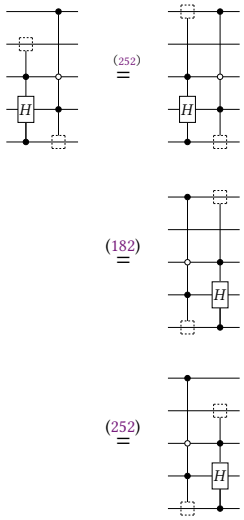


方程证明 (253)：

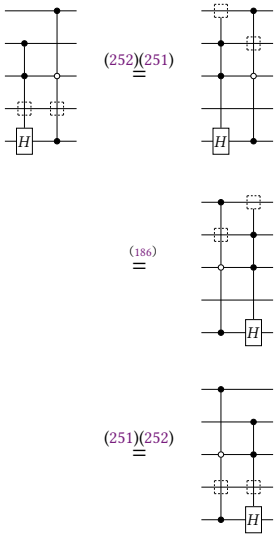




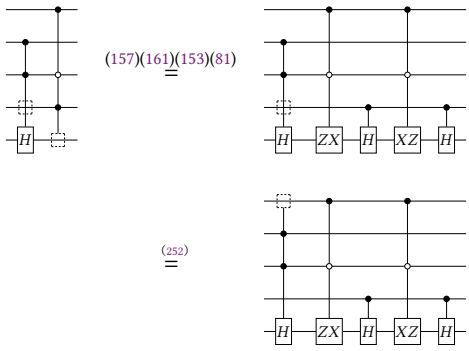
方程证明 (254):



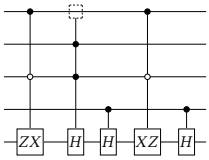
方程证明 (255):



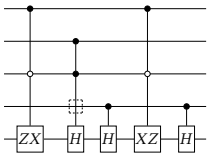
方程证明 (256):



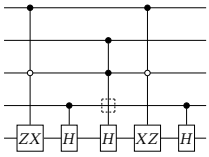
引理 D.6 =



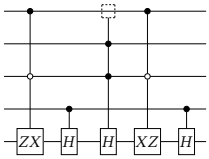
(252) =



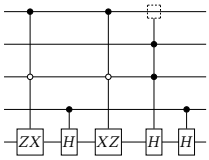
引理 D.6 =



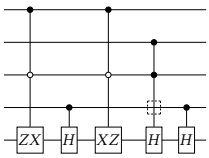
(252) =



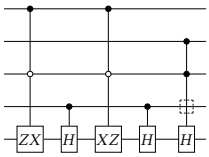
引理 D.6 =



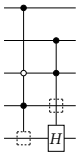
(252) =



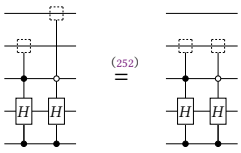
引理 D.6 =

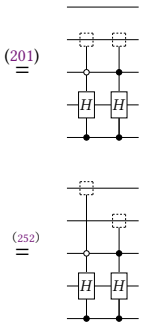


(81)(153)(157)(161) =

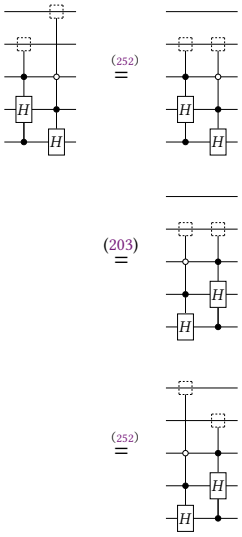


方程证明 (257):

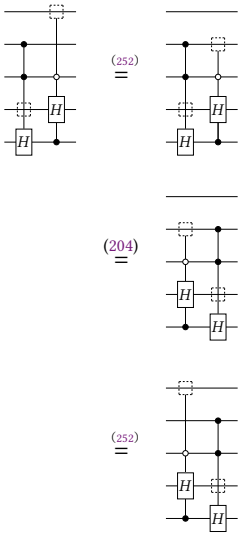




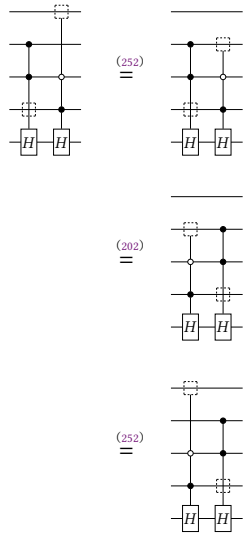
方程证明(258):



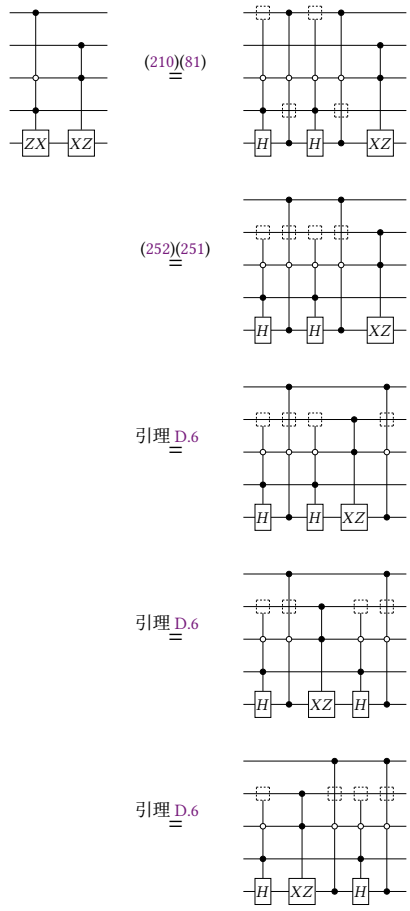
方程证明(259):



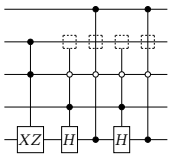
方程证明(260):



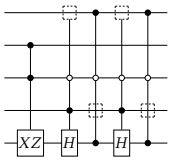
方程证明(261):



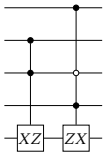
引理 D.6



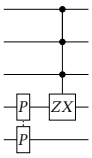
(252)(251)



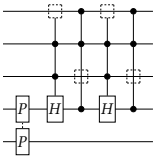
(81)(210)



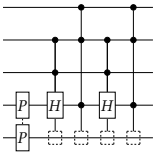
方程证明 (262)*:*



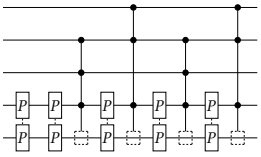
(210)



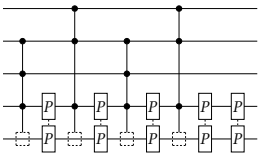
(252)(251)



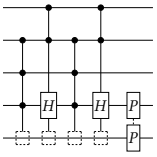
=



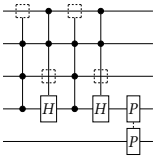
(111)



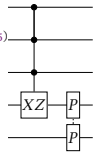
=



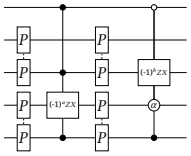
(251)(252)



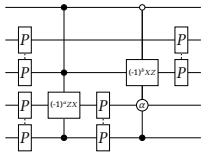
(161) (162) (211) (214) (215)
=



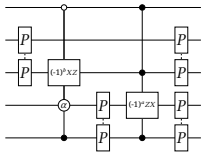
方程证明 （263）：



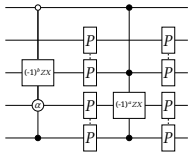
(112) (111) (262)
=



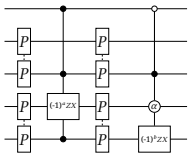
(215)(112)(244)
=



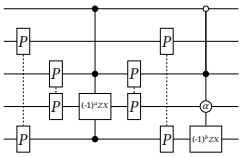
(112)(111)(262)
=



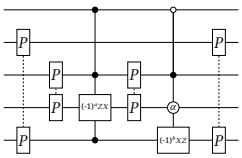
方程证明 (264):



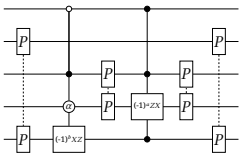
(112)(246)
=



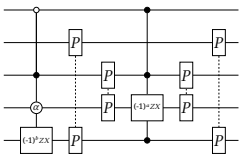
(112)(111)(262)
=



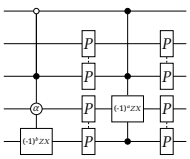
(244)
=



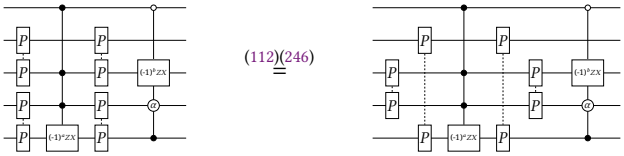
(112)(111)(262)
=

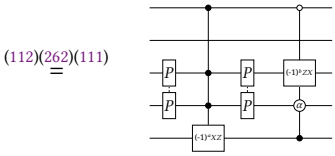


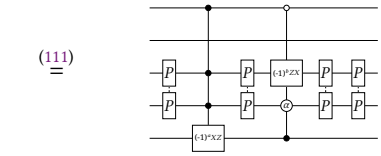
(246)(112)
=

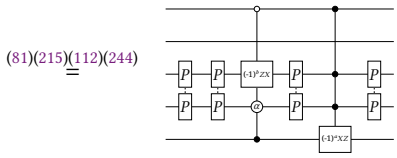


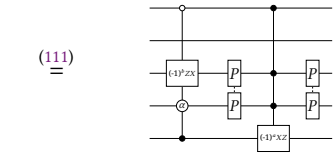
方程证明 (265)：

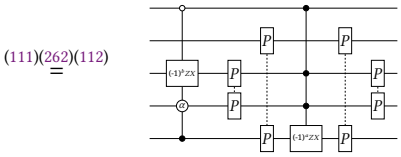


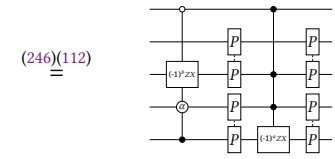




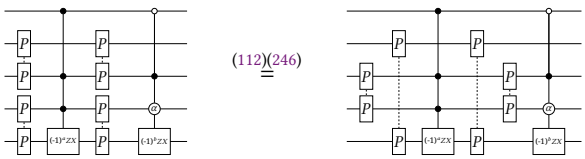




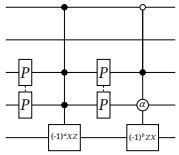




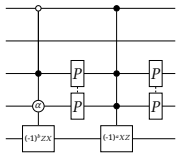
方程证明 (266)：



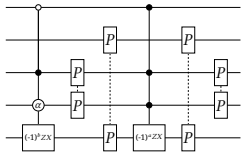
(112)(262)(111)
=



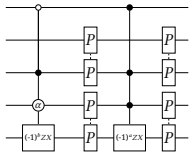
(245)
=



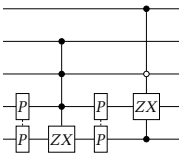
(111)(262)(112)
=



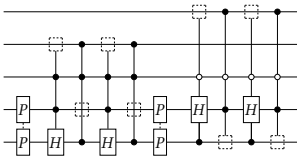
(246)(112)
=



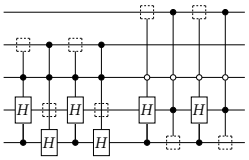
方程证明 (267)：不失一般性，我们可以假设 $\alpha = 1$。如果 $\beta = \gamma = 1$，那么利用引理 B.6（连同方程（81）、（111）和（208）），不失一般性，我们可以假设 $a = 0$ 且 $b = 1$。我们有



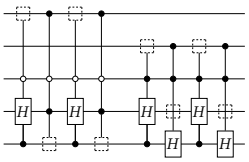
(210)(81)
=



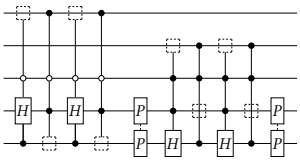
(111)(112)(130)(157)
=



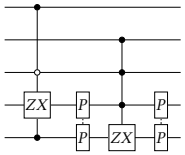
(259)(256)(257)(254)
=



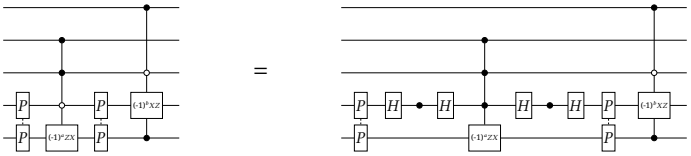
(111)(112)(130)(157)
=



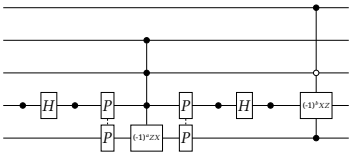
(81)(210)
=



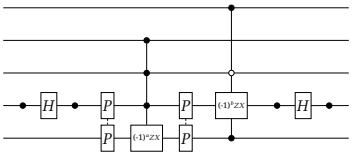
若 $\gamma = 1$ 且 $\beta = 0$，则有



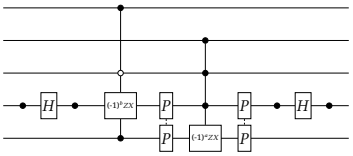
(111)(113)
=



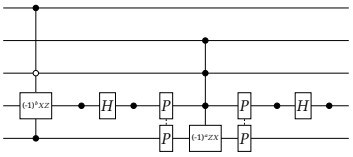
(2)(1)(237)(236)
=



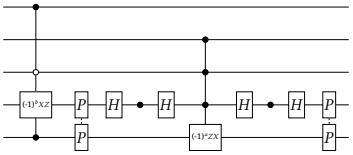
前一种情况
=



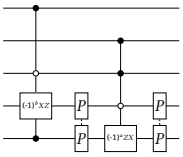
(2)(1)(237)(236)
=



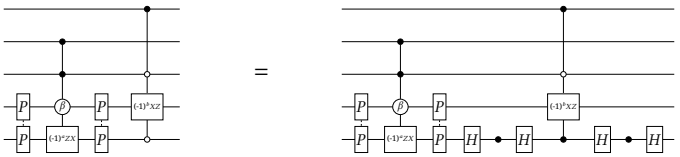
(111)(113)
=



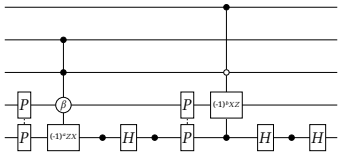
=



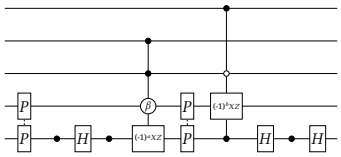
而且如果 $\gamma = 0$，那么我们有



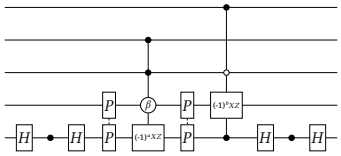
(112)(111)(113)
=



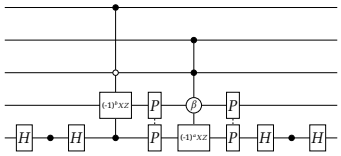
(2)(1)(237)(236)
=



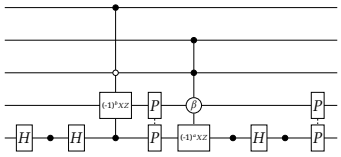
(112)(113)(111)
=



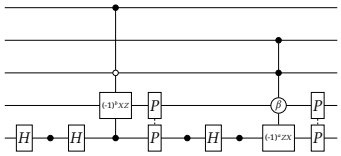
前述情形
=



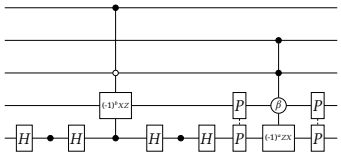
(112)(111)(113)
=



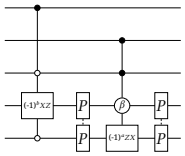
(2)(1)(237)(236)
=



(112)(113)(111)
=

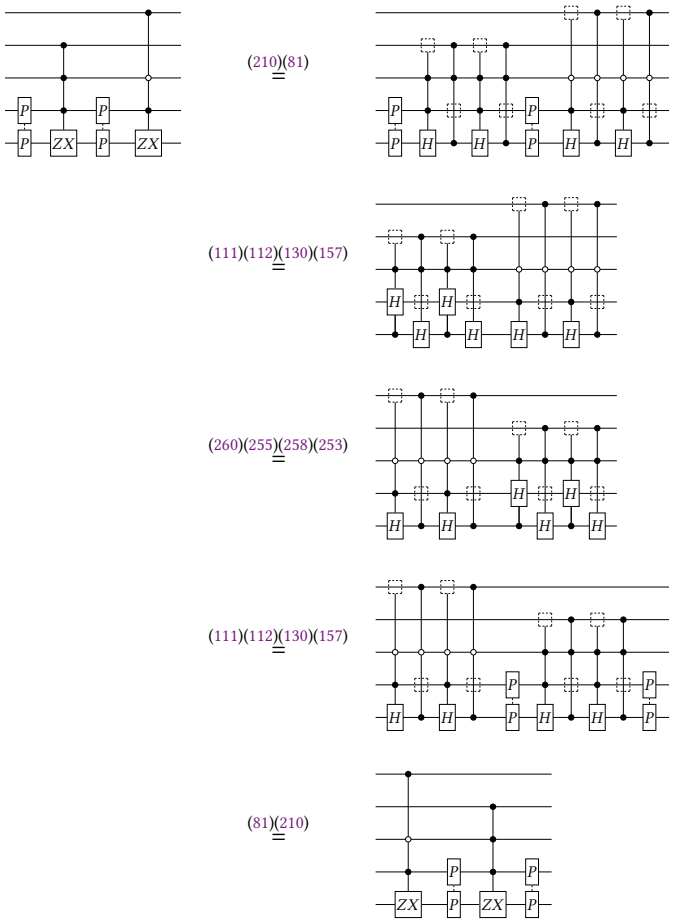


=

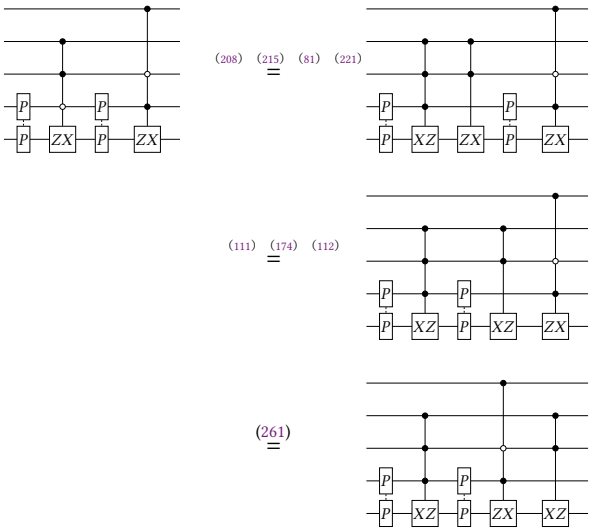


方程证明(268)：不失一般性，我们可以假设 $\alpha = 1$。

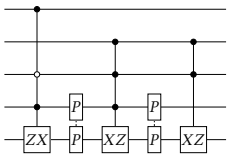
若 $\beta = \gamma = 1$，那么在使用引理 B.6 (以及方程 (81)、(111) 和 (208)) 后，我们不失一般性地假设 $a = 0$ 且 $b = 1$。我们有



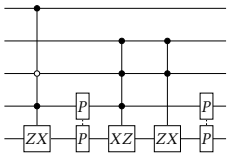
如果 $\gamma = 1$ 和 $\beta = 0$，那么再次利用引理 B.6 （连同方程（81）、（111）和（208）），我们可以不失一般性地假设 $a = 0$ 以及 $b = 1$。我们有



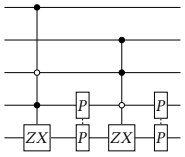
前一种情况
=



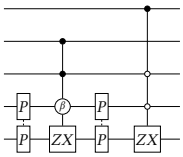
(111)(174)(112)
=



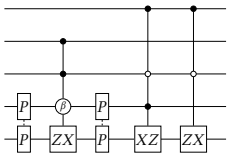
(81)(221)(215)(208)
=



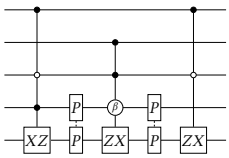
并且若 $\gamma = 0$，那么同样，在使用引理 B.6 (以及方程 (81)、(111) 和 (208)) 后，我们不失一般性地假设 $a = 0$ 且 $b = 1$。我们有



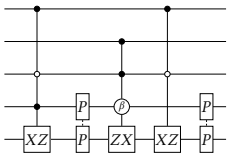
(81)(208)(215)(221)
=



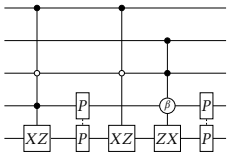
前述情形
=



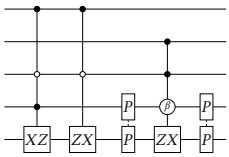
(112)(174)
=



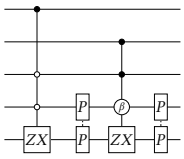
(81)(261)
=



(111)(174)(112)
=



(81)(221)(215)(208)
=



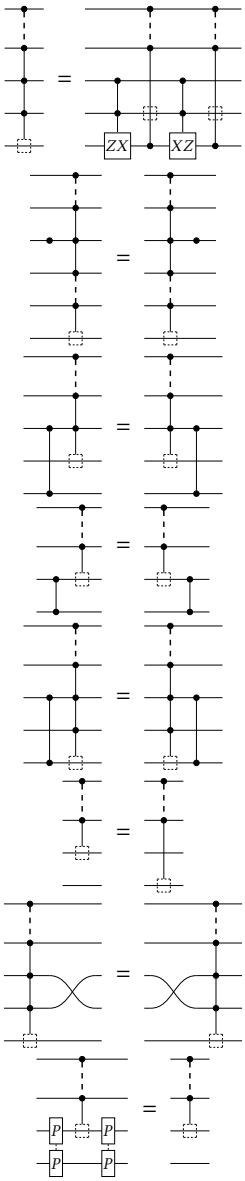
□

D.5 基本辅助方程： n 量子比特及多重受控门的性质

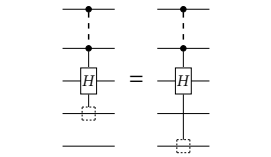
下文中，为方便起见，我们将使用记号 (XX)$_k$ 来指代 k量子比特的多量子比特等式（模式）(XX)。请注意，在推导过程中，我们有时会调用之后才证明的方程的 $n-1$量子比特情形：这应理解为仅仅是调用引理 5.1，这里标出方程编号只是为了更明确地说明所执行的变换。只需检查所有对由 (XX) n表示的n量子比特情形的引用均指向先前已证明的方程，即可验证该证明是良基的。

此外，在进行 3 或 4 量子比特变换时，我们有时会引用引理 D.3 和 D.6： 这同样是调用引理 5.1 (具体而言，这要求量子比特数分别严格大于 3 或 4)。

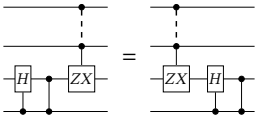
引理D.8。 以下方程是图中方程的推论 *4*:



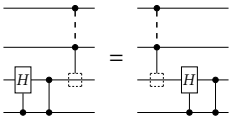
(269)
(270)
(271)
(272)
(273)
(274)
(275)
(276)



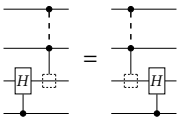
(277)



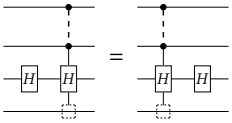
(278)



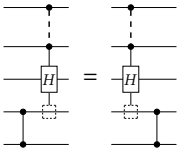
(279)



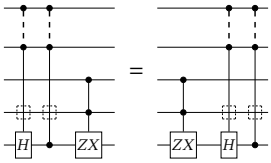
(280)



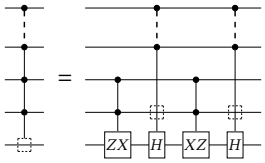
(281)



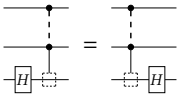
(282)



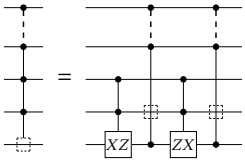
(283)



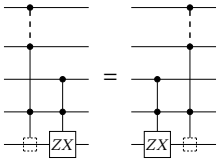
(284)



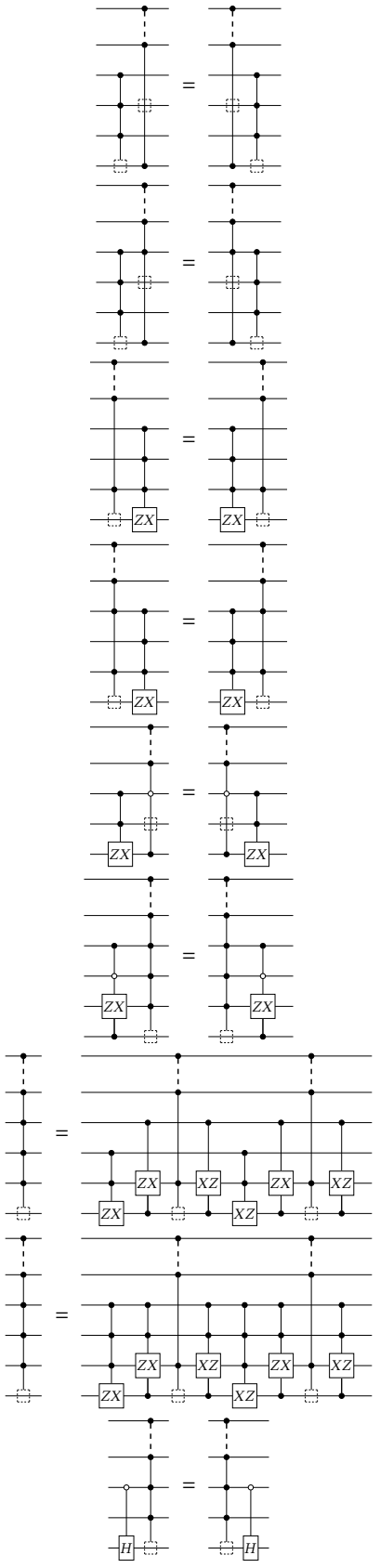
(285)



(286)



(287)



(288)

(289)

(290)

(291)

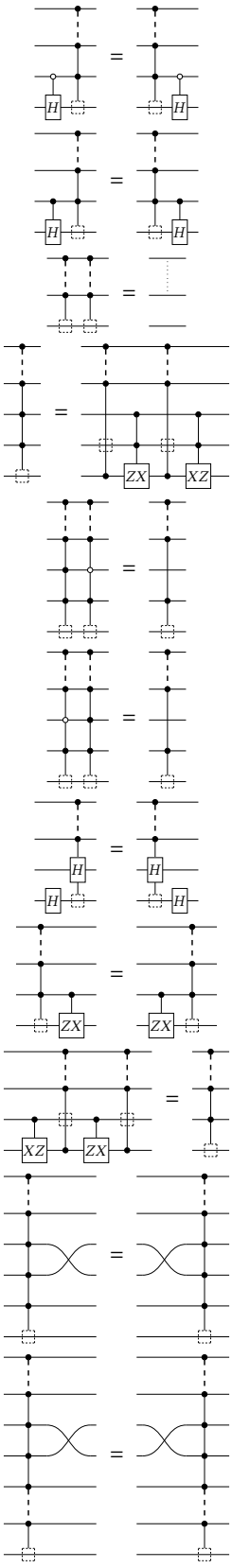
(292)

(293)

(294)

(295)

(296)



(297)

(298)

(299)

(300)

(301)

(302)

(303)

(304)

(305)

(306)

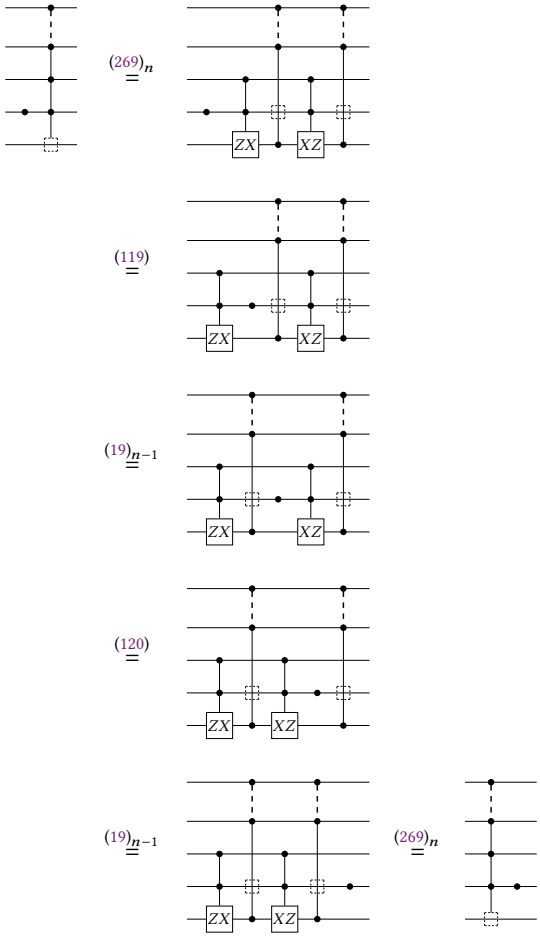
(307)

证明。

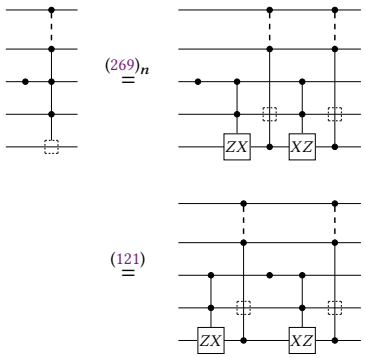
方程证明 (269)$_n$： 方程 (269)$_3$ 就是方程 (126)，而对于 $n \geq 4$，方程 (269)$_n$ 就是

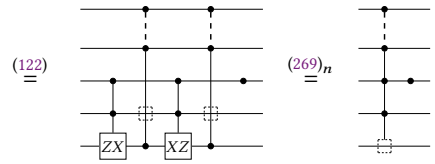


Proof of Eq$_{\text{方程}}$ (270)$_n$: Eq$_{\text{方程}}$ (270)$_2$ 显然。方 q$_{\text{方程}}$ (270)$_3$ 由引理 7.6得出。
若 $n \geq 4$，则根据 Z 门相对于多控制位-Z 门的垂直位置，分为三种情形：如果 Z 门下方没有控制位，则有

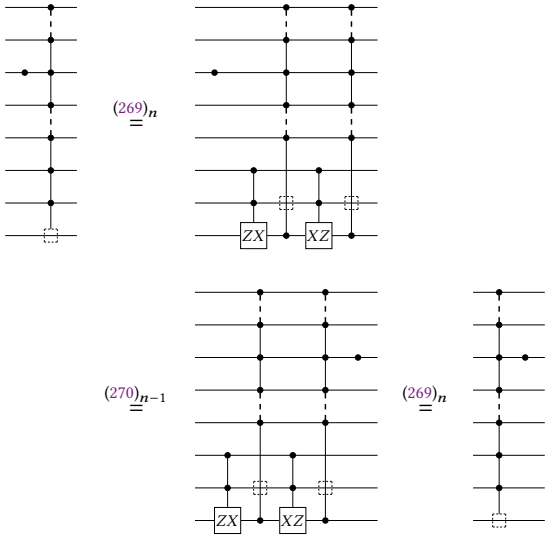


如果它下方恰好有一个控制位，那么我们有

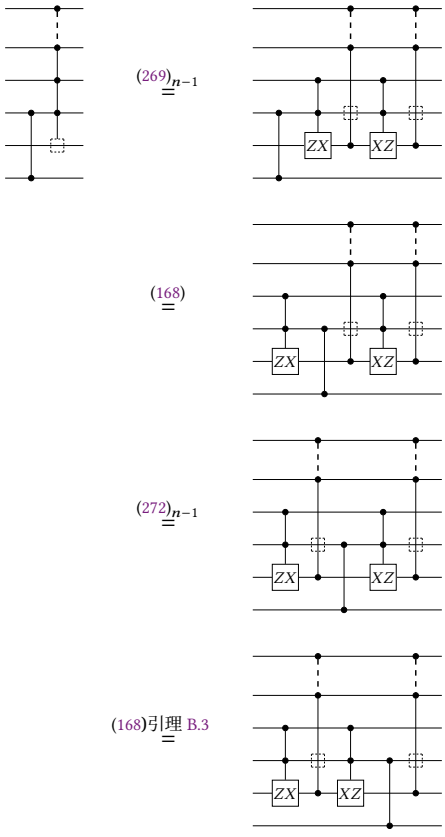


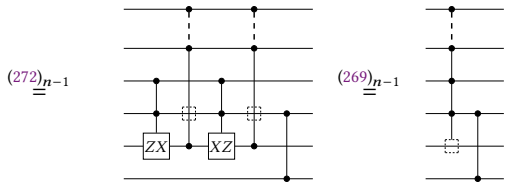


如果它下方有两个或更多控制位，那么我们有

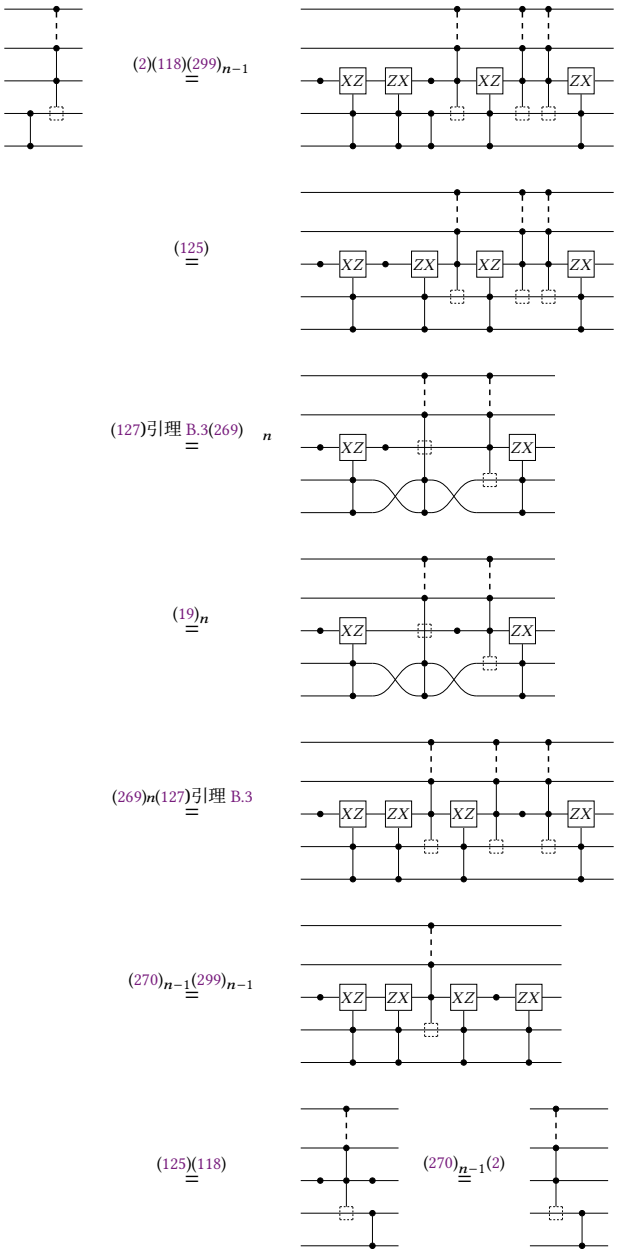


方程证明 (271)$_n$： 方程 (271)$_3$ 由引理 7.6得出。如果 $n \geq 4$，则有

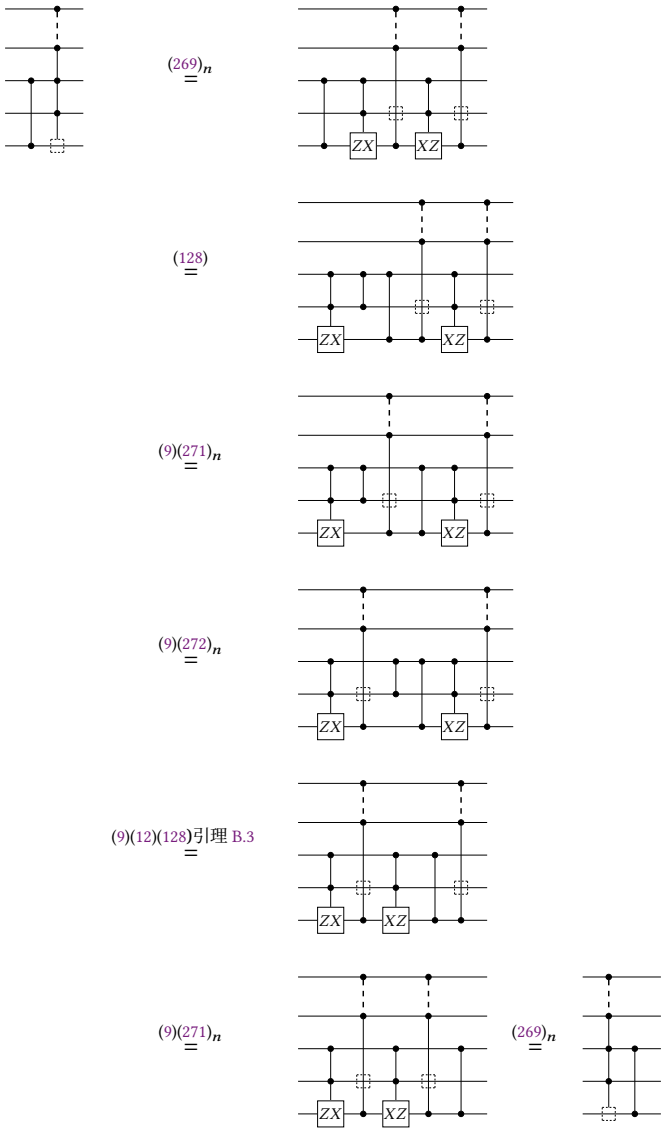




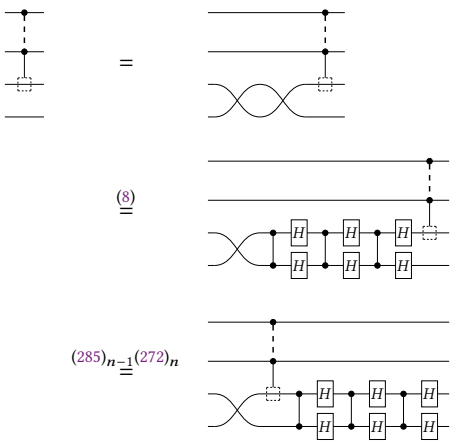
方程证明 (272)$_n$： 方程 (272)$_2$ 由引理 7.6 得出。如果 $n \geq 3$，则有

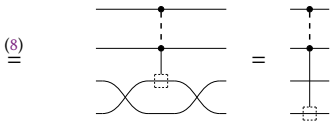


方程证明 $(273)_n$:

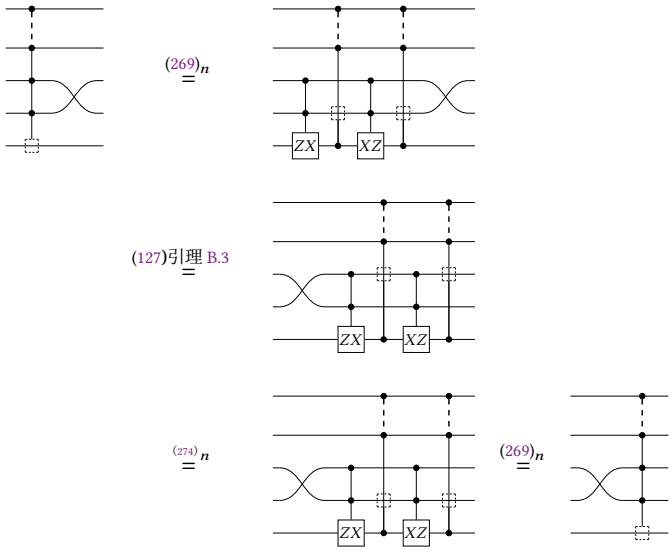


方程证明 $(274)_n$:

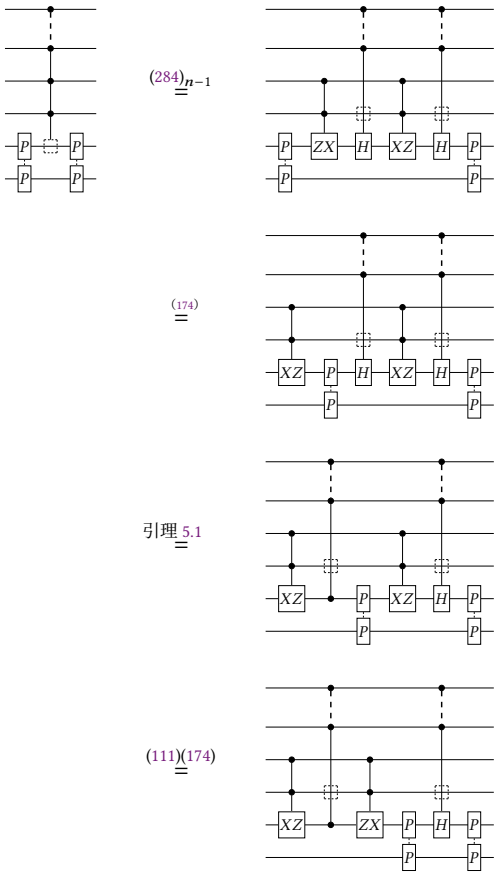




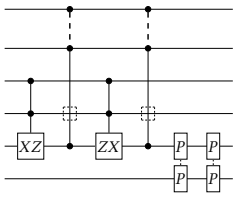
方程证明 (275)$_n$:



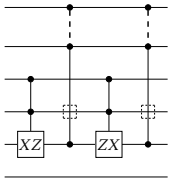
方程证明 (276)$_n$: 方程 （276）$_2$ 由引理 7.6得出。方程（276）$_3$ 由方程（111）得出。如果 $n \geq 4$，那么我们有 e



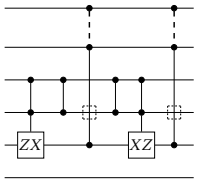
引理 5.1 =



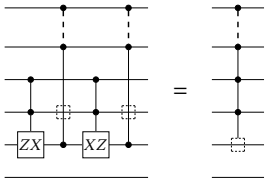
(111) =



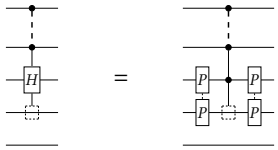
(124)引理 B.3 =



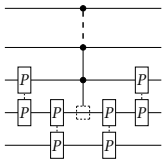
$(272)_{n-1}(4)$ =



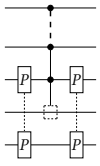
方程（$(277)_n$：方程（277）$_3$ 和方程（277）$_4$ 是显然的。如果 $n \geq 5$，那么我们有



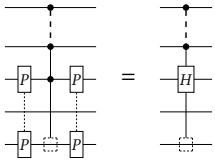
$(276)_n$ =



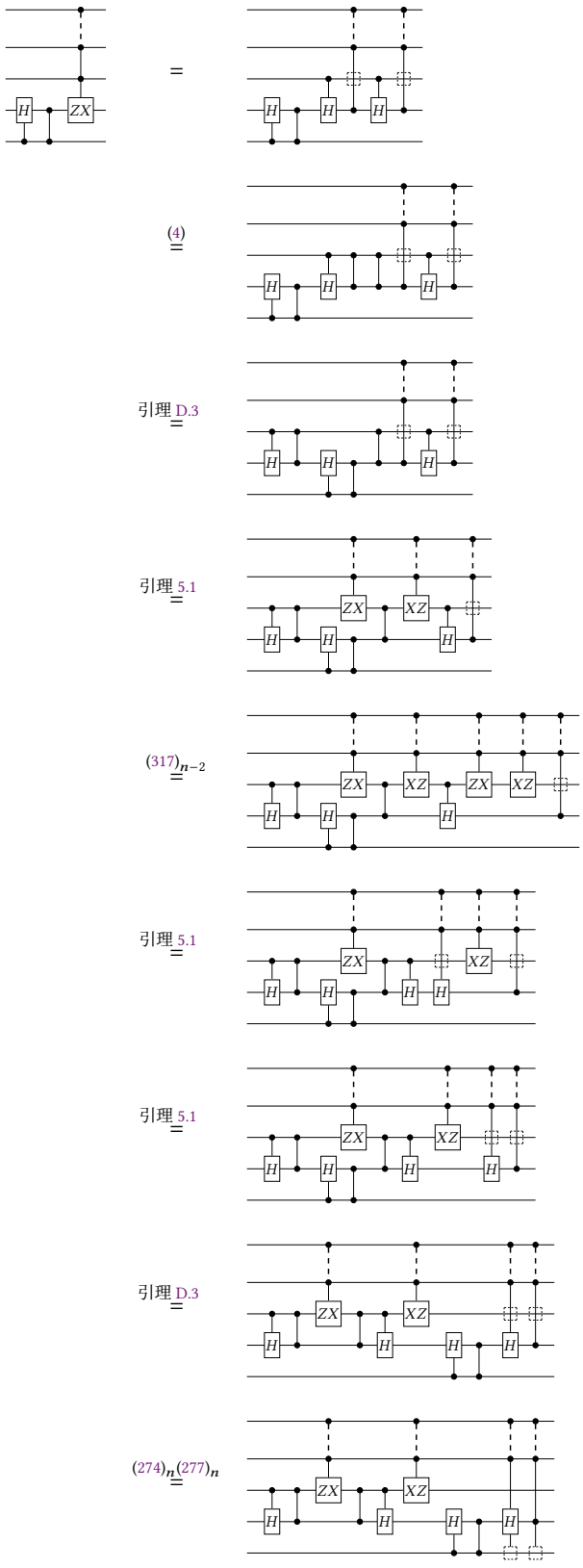
(112) (130) =

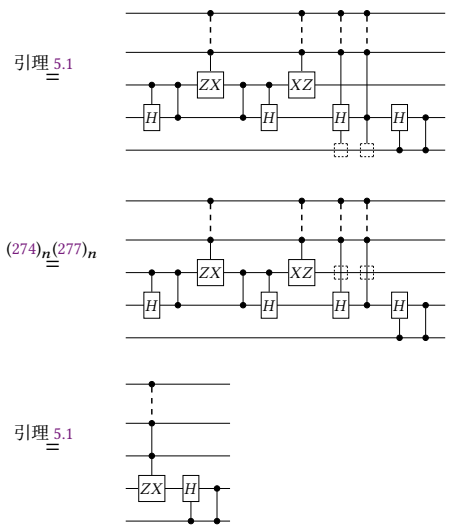


(274) $_n$ =

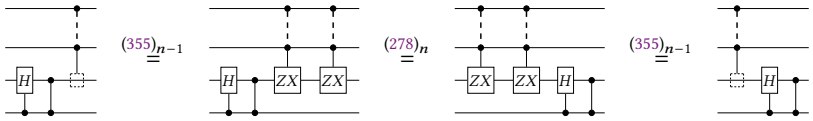


方程证明 (278)$_n$： 方程 (278)$_2$ 由引理 7.6得出。方程 (278)$_3$ 就是方程 (145)。对于 $n \geq 4$，我们有

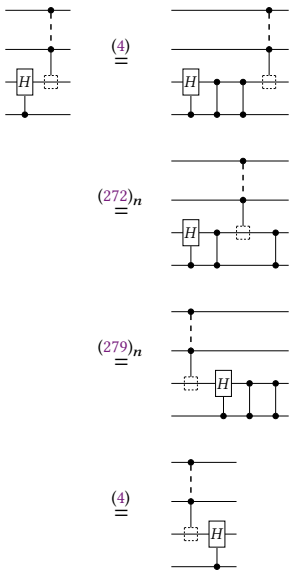




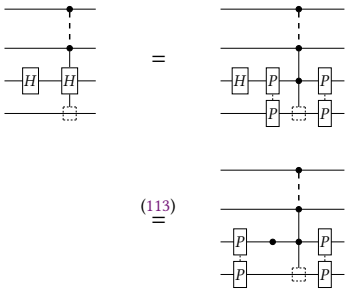
方程证明 $(279)_n$:

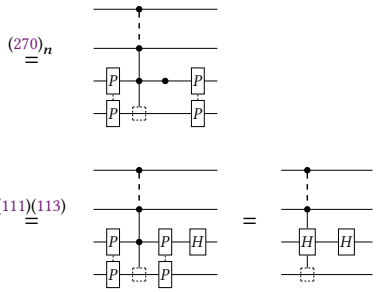


方程证明 $(280)_n$:

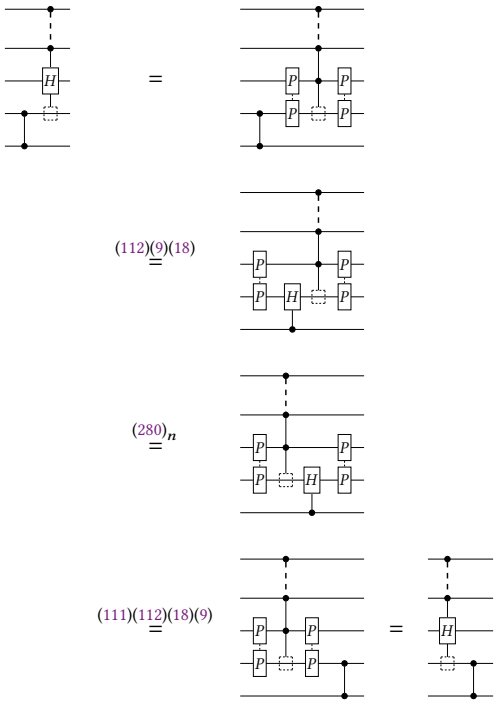


方程证明　　程 $(281)_n$: 方程 $(281)_2$ 显然成立。方程 $(281)_3$ 由方程 (93) 得出。如果 $n \geq 4$，那么我们有　　e

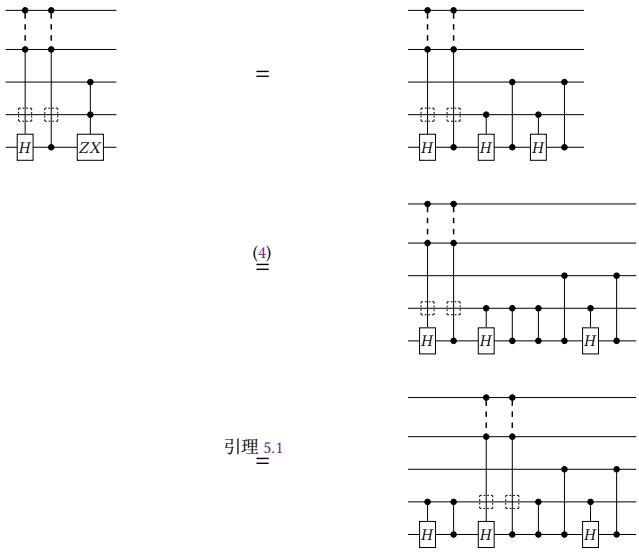




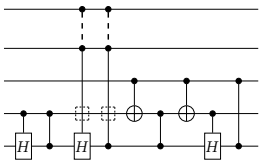
方程证明 (282)$_n$： 方程 (282)$_3$ 和方程 (282)$_4$ 都是平凡的。如果 $n \geq 5$，那么我们有



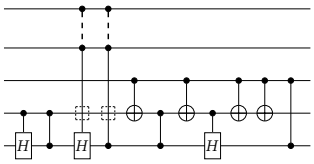
方程证明 (283)$_n$： 方程 (283)$_3$ 就是方程 (144)。对于 $n \geq 4$，我们有



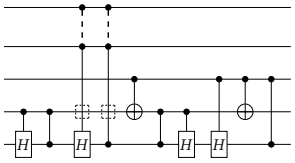
$\overset{(148)}{=}$



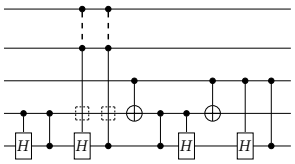
$\overset{(82)}{=}$



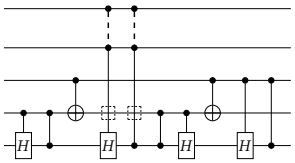
$\overset{\text{引理 D.3}}{=}$



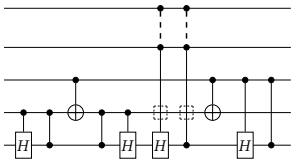
$\overset{\text{引理 D.3}}{=}$



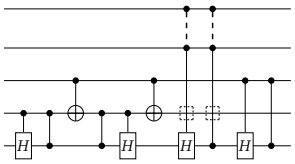
$\overset{(285)_{n-1}(303)_{n-1}(9)(272)_n(282)_n}{=}$



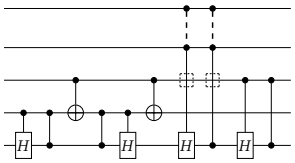
$\overset{\text{引理 5.1}}{=}$

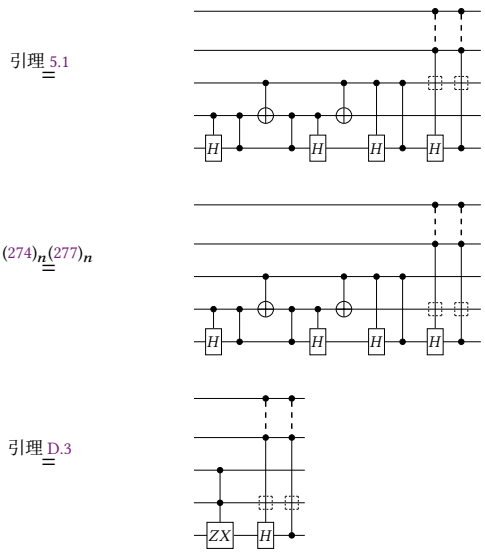


$\overset{(285)_{n-1}(303)_{n-1}(9)(272)_n(282)_n}{=}$

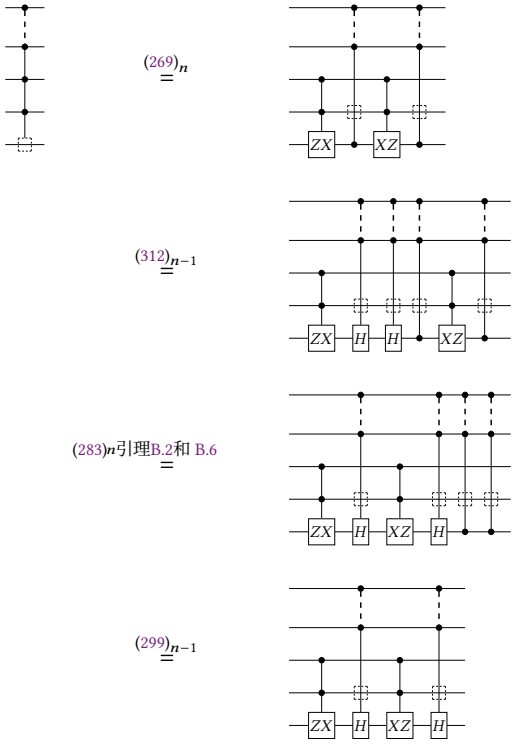


$\overset{(274)_n(277)_n}{=}$

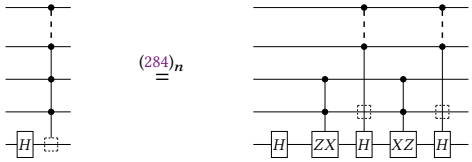


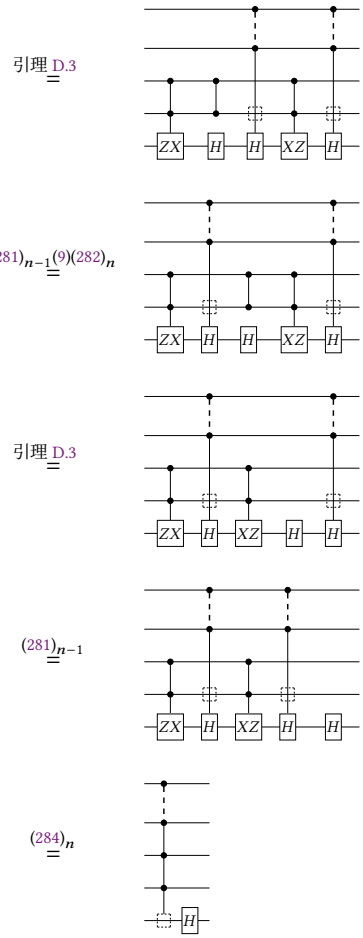


方程证明 (284)$_n$:

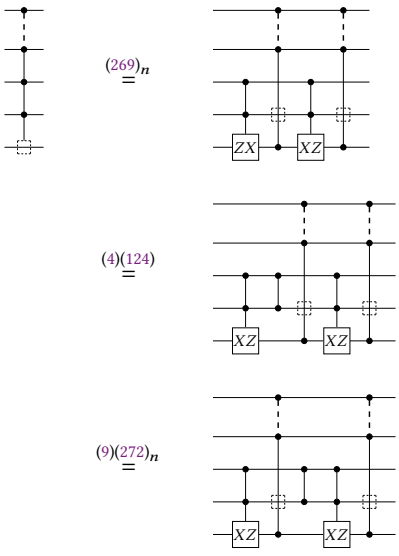


方程（(285)$_n$）：方程（285)$_1$ 由引理 7.1 推得。方程（285)$_2$ 和（285)$_3$ 可由拓扑规则推出。对于 $n \geq 4$，我们有

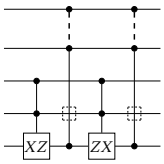



引理 D.3
=
ZX
H
H
XZ
H
(281)n−1(9)(282)n
=
ZX
H
H
XZ
H
引理 D.3
=
ZX
H
XZ
H
H
(281)n−1
=
ZX
H
XZ
H
H
(284)n
=
H

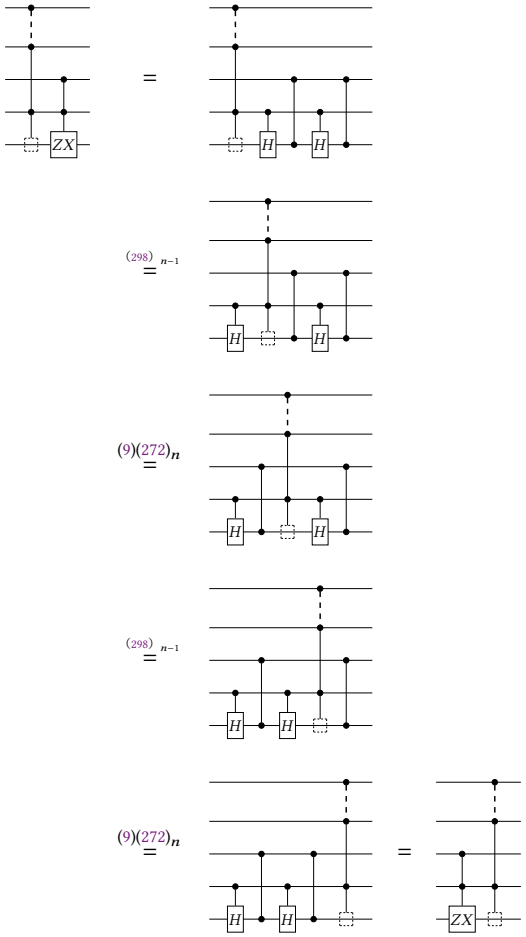
方程证明 (286)$_n$:


(269)n
=
ZX
XZ
(4)(124)
=
XZ
XZ
(9)(272)n
=
XZ
XZ

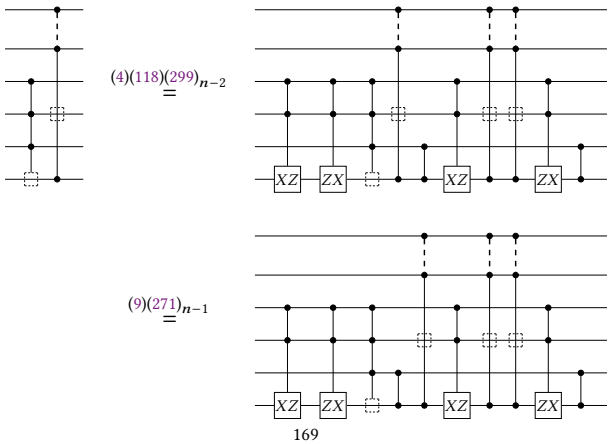
(124)引理 B.3 =



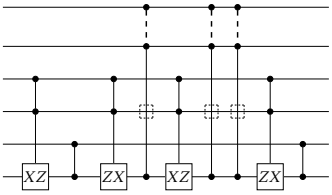
方程证明 (287)$_n$:



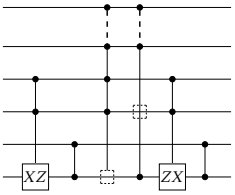
方程证明 (288)$_n$:



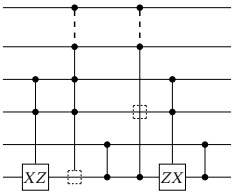
$\overset{(172)}{=}$



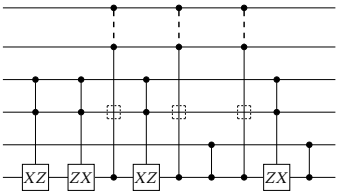
$\overset{(269)_{n-1}}{=}$



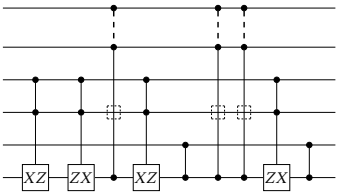
$\overset{(9)(272)_{n}}{=}$



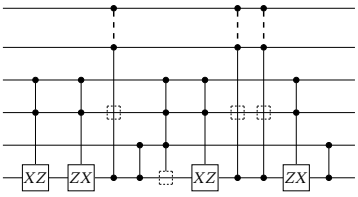
$\overset{(269)_{n-1}}{=}$



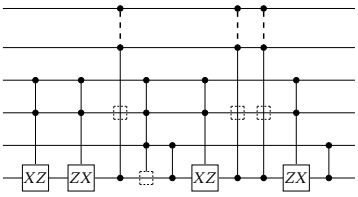
$\overset{(9)(271)_{n-1}}{=}$



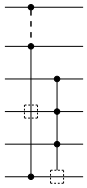
$\overset{(173)}{=}$



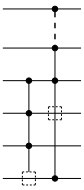
$\overset{(160)}{=}$



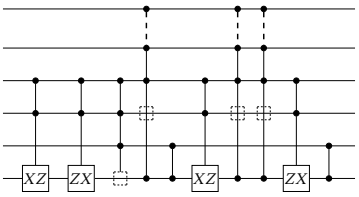
$\overset{(299)_{n-2}(118)(4)}{=}$



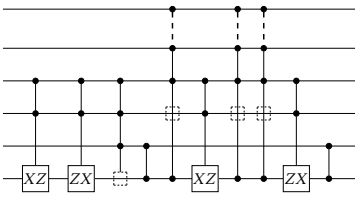
方程证明 $(289)_n$:



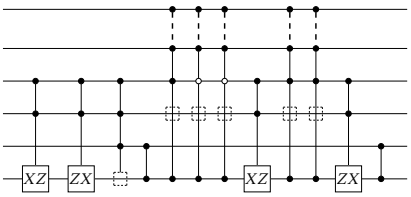
$\overset{(4)(118)(299)_{n-1}}{=}$



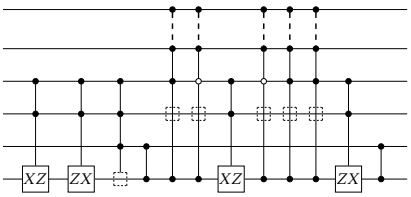
$\overset{(9)(271)_n}{=}$



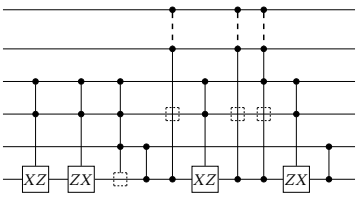
$\overset{(81)(299)_{n-1}}{=}$



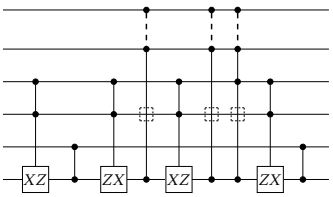
$\overset{(118)(292)_{n-1}(117)}{=}$



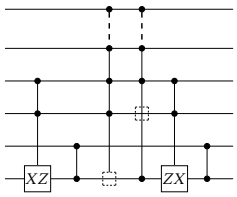
$\overset{(301)_{n-1}(302)_{n-1}}{=}$



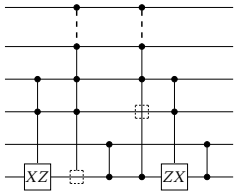
$\overset{(172)}{=}$



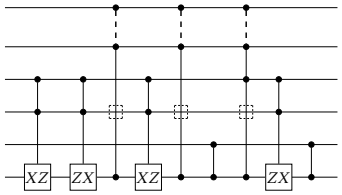
$\overset{(269)_{n-1}}{=}$



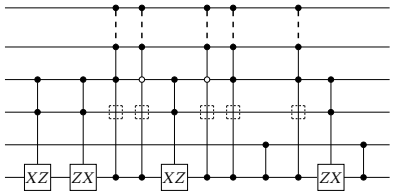
$\overset{(9)(272)_{n}}{=}$



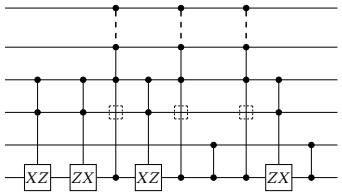
$\overset{(269)_{n-1}}{=}$



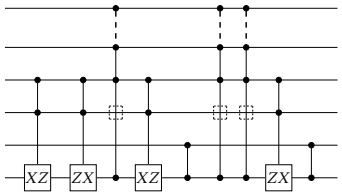
$\overset{(301)_{n-1}(302)_{n-1}}{=}$



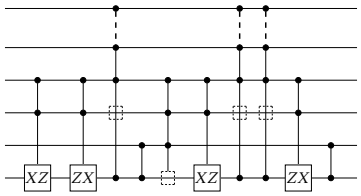
$\overset{(118)(292)_{n-1}(117)}{\underset{(81)(299)_{n-1}}{=}}$

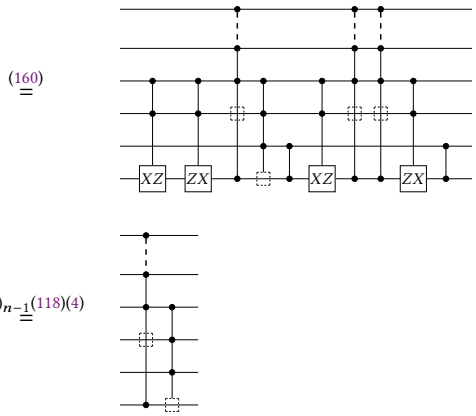


$\overset{(9)(271)_{n}}{=}$

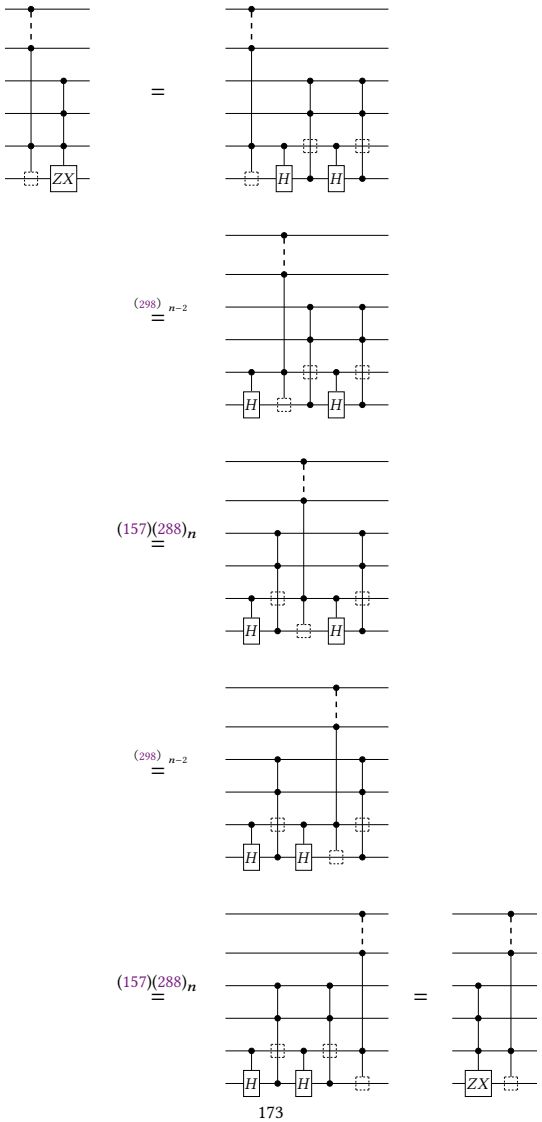


$\overset{(173)}{=}$

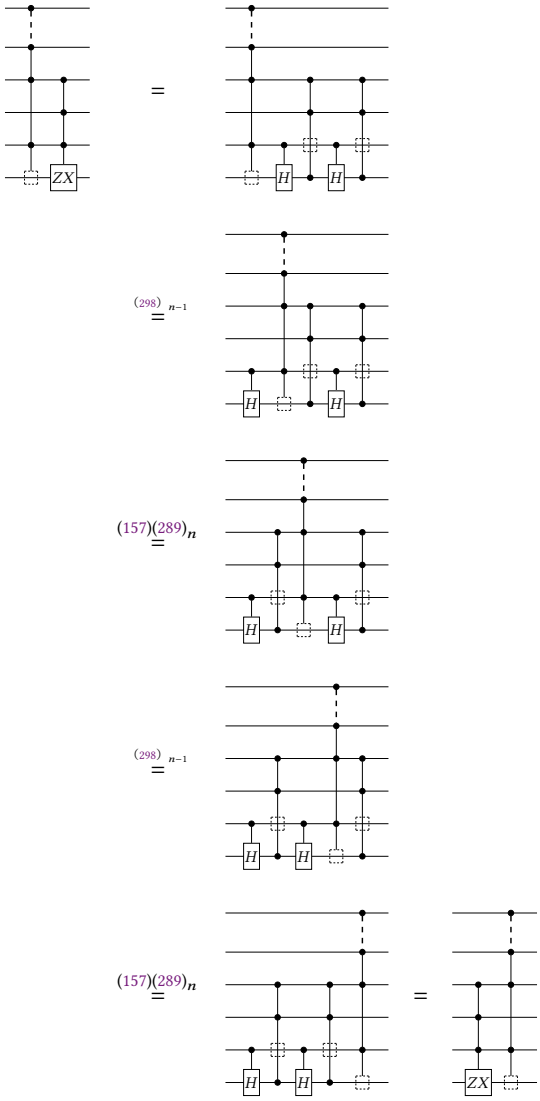



(160)
XZ
ZX
XZ
ZX
(299)$_{n-1}$(118)(4)

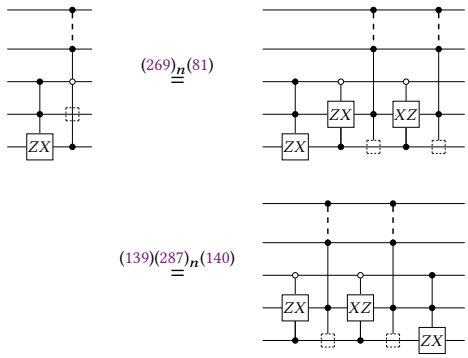
方程证明 (290)$_n$:

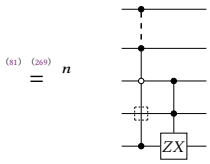

ZX
H
H
(298)$_{n-2}$
(157)(288)$_n$
(298)$_{n-2}$
(157)(288)$_n$
ZX

方程证明(291)$_n$:

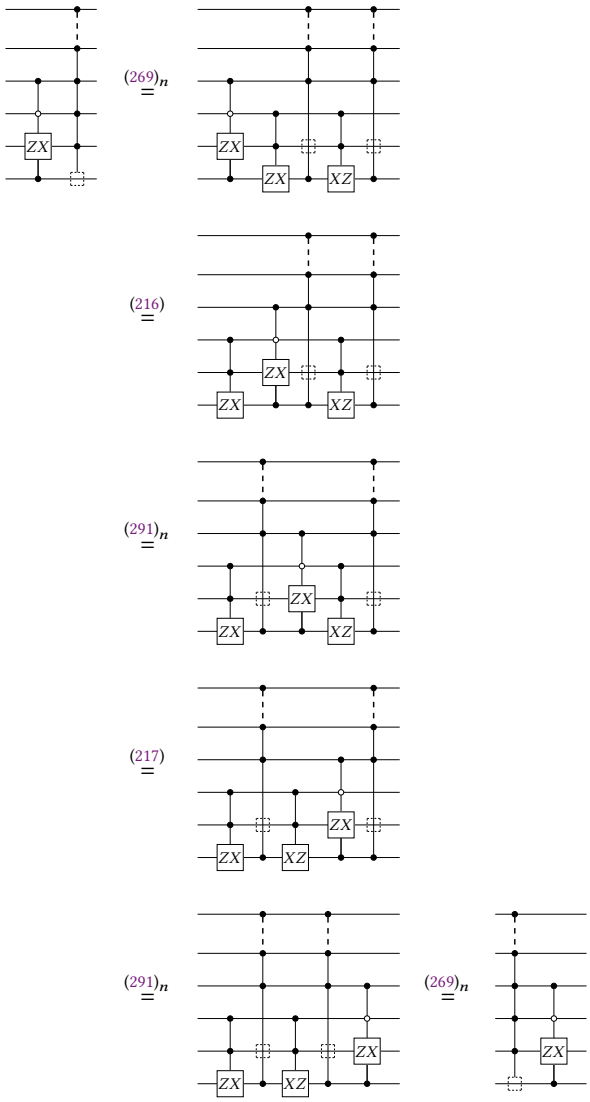


方程证明 (292)$_n$:

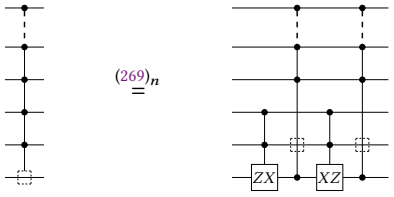




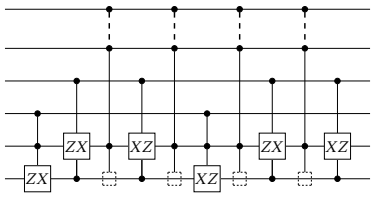
方程证明 (293)$_n$:



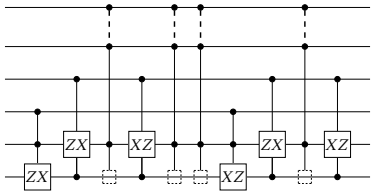
方程证明 (294)$_n$:



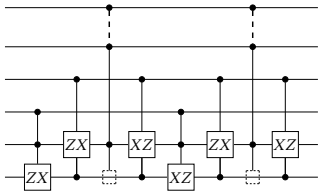
$\overset{(269)_{n-1}(300)_{n-1}}{=}$



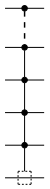
$\overset{(117)(287)_{n-1}(118)}{=}$



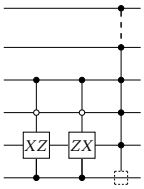
$\overset{(299)_{n-2}}{=}$



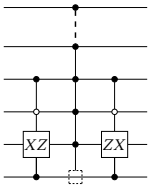
方程证明 $(295)_n$:



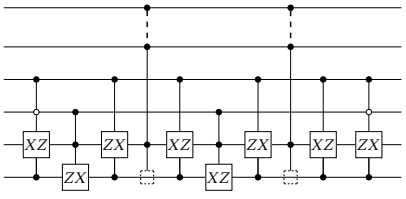
$\overset{(209)}{=}$



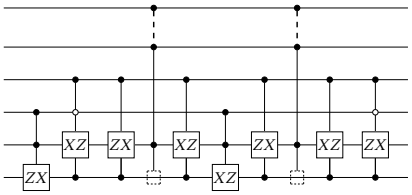
$\overset{(293)_n}{=}$

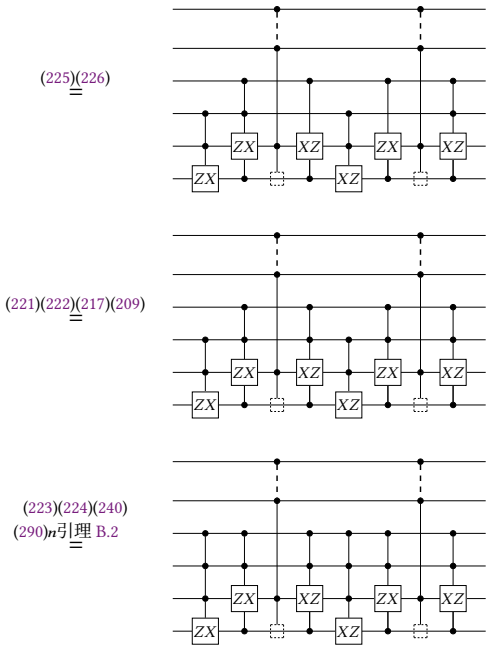


$\overset{(294)_n}{=}$

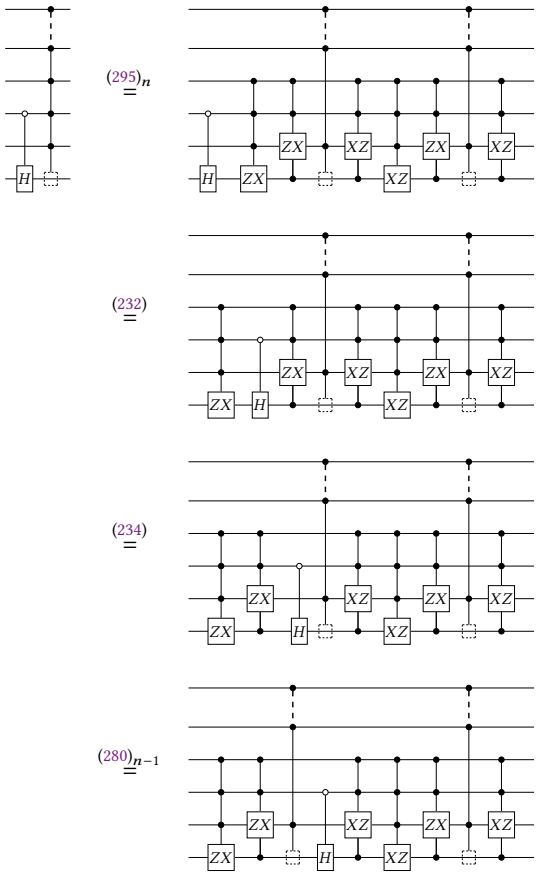


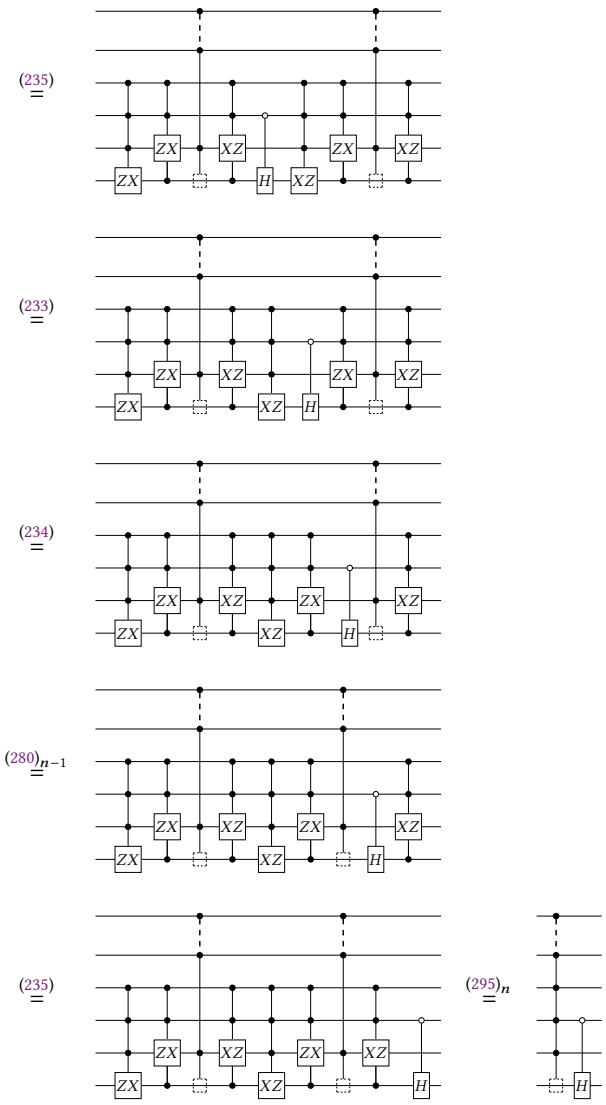
$\overset{(218)}{=}$





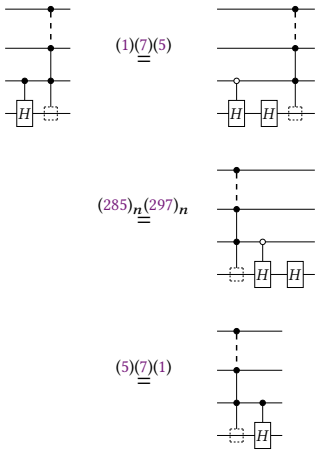
证明 方程 (296)$_n$： 方程 (296)$_3$ 只是方程 (132)。如果 $n \geq 4$，那么要证明方程 (296)$_n$， 我们必 ve



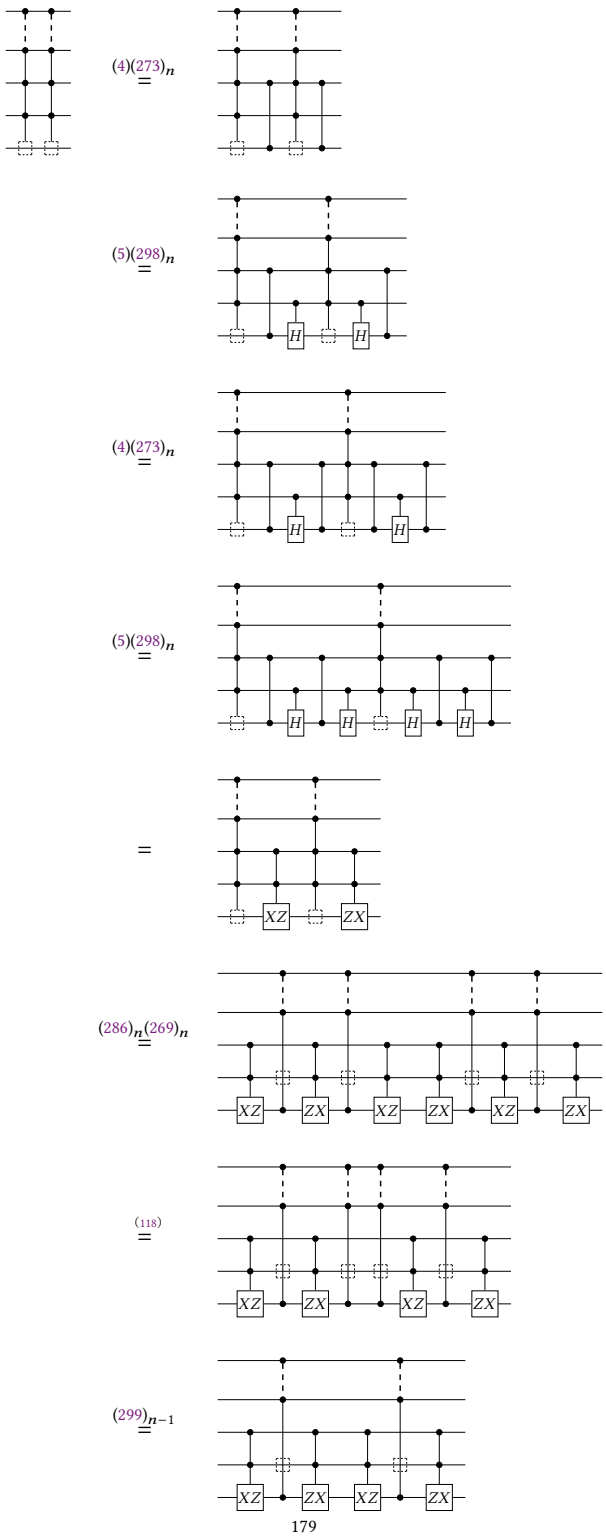


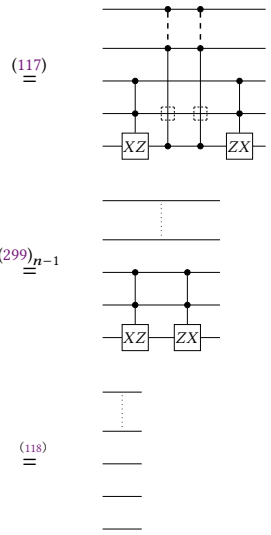
方程证明(297)$_n$：方程 (297)$_2$ 直接由引理7.6得出，并且对于 $n \geq 3$，方程 (297)$_n$ 直接由方程 (275)$_n$ 和 (296)$_n$。

方程证明(298)$_n$：

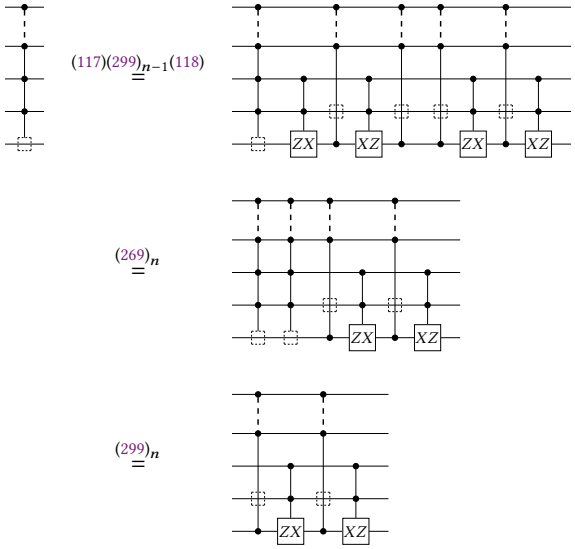


方程证明 (299)$_n$：方程 (299)$_1$ 和 (299)$_2$ 直接由引理 7.1 得出。方程(299)$_3$ 直接由引理 7.6 得出。如果$n \geq 4$，则为证明方程 (299)$_n$，我们有

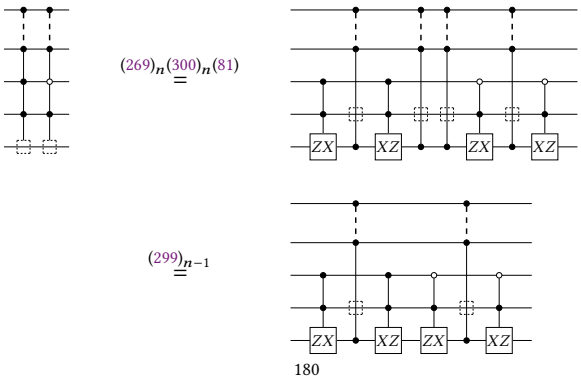




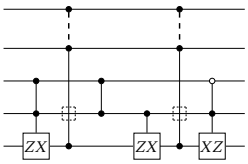
方程证明 (300)$_n$:



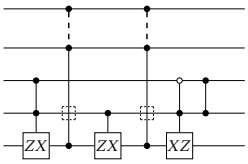
方程证明 (301)$_n$:



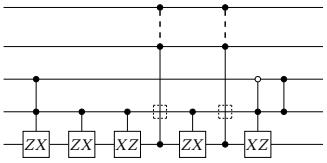
(141)
=



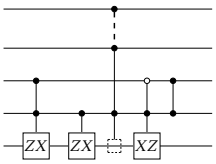
(142)(9)(272)$_n$(143)
=



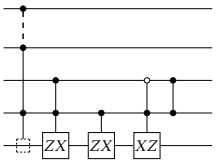
引理 7.6
=



(305)$_{n-1}$
=



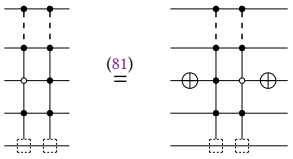
(304)$_{n-1}$(287)$_n$
=

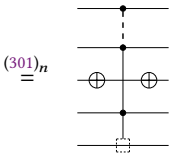


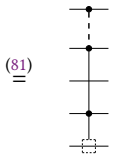
(143)(142)(141)(81)(117)
=



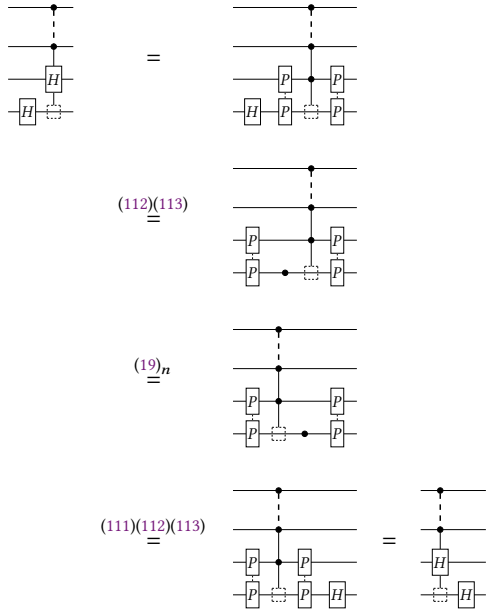
方程证明 (302)$_n$:



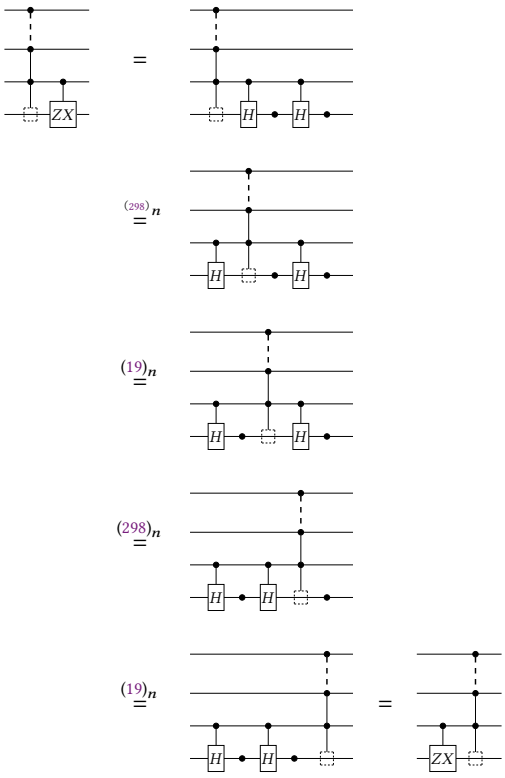




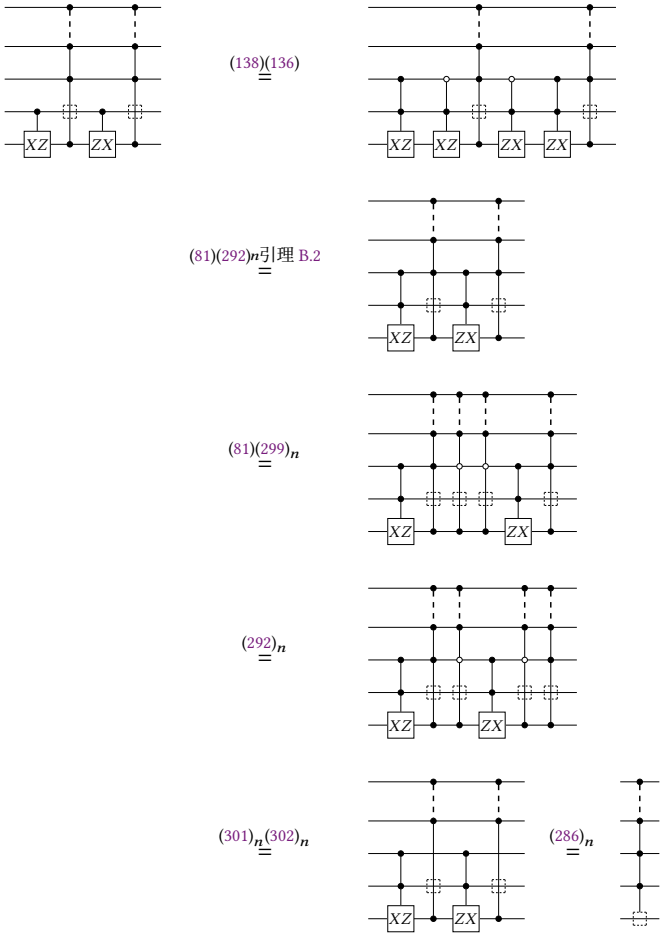
方程证明 (303)$_n$： 方程 (303)$_2$ 和方程 (303)$_3$ 显然成立。若 $n \geq 4$，则有



方程证明（304）$_n$:

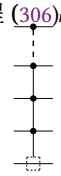


方程证明（305）$_n$：方程（305）$_2$ 由引理7.6得出。如果 $n \geq 3$，则我们有



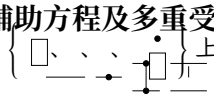
方程证明 (306)$_n$： 方程 (306)$_n$ 可由方程 (295)$_n$ 与方程 (214)直接得出。

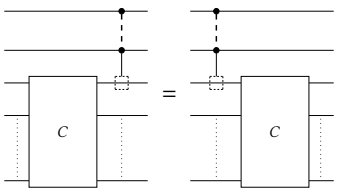
方程证明 (307)$_n$： 我们根据交换下方控制位的数量分类讨论：如果没有控制位，那么方程 (307)$_n$ 就是方程 (275)$_n$。如果恰好有一个控制位，那么方程 (307)$_n$ 就是方程 (306)$_n$。如果有多个控制位，那么展开 的归纳定义后，结果可由方程 (307)$_{n-1}$得出。



□

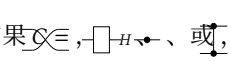
D.6 量子比特上的其他辅助方程及多重受控门的性质

引理 D.9. 对于任意电路（在  上），以下方程是图 4 中方程的推论：



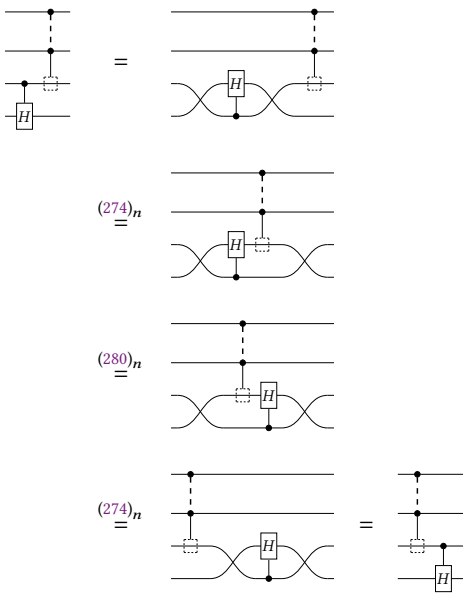
(308)

证明。我们对 C 进行结构归纳。[18]

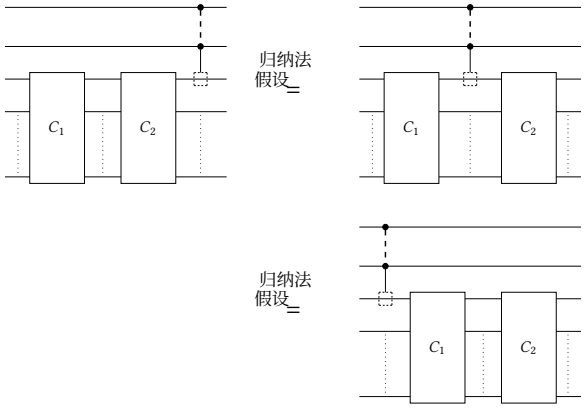
如果 $C =$ ——，那么结果显然是 等。如果  ，、或，则结果分别由（274）$_n$、（19）$_n$、（285）$_n$或（272）$_n$ 得出。

[18]更准确地说，在底层原始电路上。

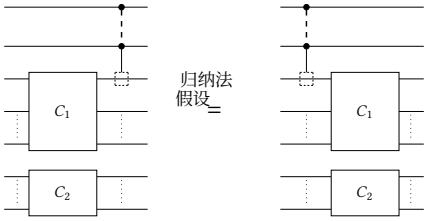
如果 $C =$  ，那么我们有$_H$



若 $C = C_2 \circ C_1$（其中 C_1，C_2 不同于单位元[19]），则有



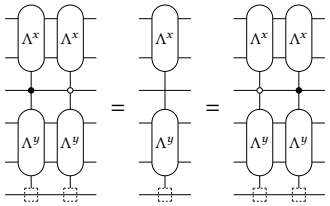
最后，如果 $C = C_1 \otimes C_2$（满足 $C_2 \neq$ ，那么我们有



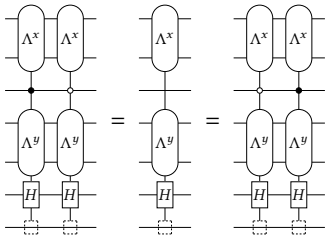
□

[19]也就是说，与$(\,)^{\otimes n}$ if C 不同，它是一个 n 量子比特电路。

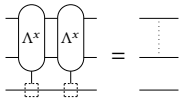
引理 D.10. 以下方程是图 *4* 中方程的推论：



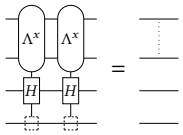
(309)



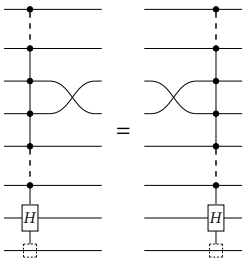
(310)



(311)



(312)

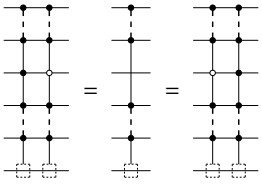


(313)

注记 8. 方程 (277) 与 (313) 的推广（其中虚线黑色控制序列被替换为任意 Λ^x）推导起来是平凡的。然而，我们选择保持这些方程简洁，因为每当在推导中使用其推广版本时，这实际上都相当于使用全黑版本，因为 Λ^x 不过是被某些 包围的黑色控制序列。同样的注记也适用于方程 (274)、(307)、(308) 与 (314)。

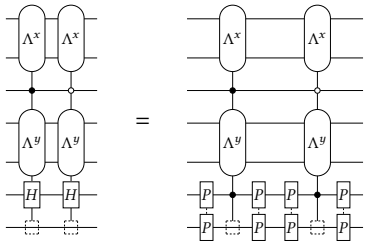
引理 D.10 的证明。

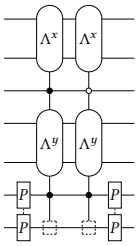
方程证明 (309)：由方程 (81)，只需证明 x 为仅由 1 组成的向量时的方程版本：

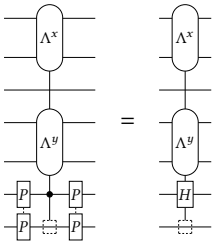


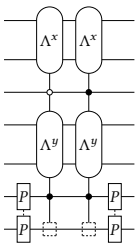
而该方程可直接由方程（301）、（302）和（307）得到 .

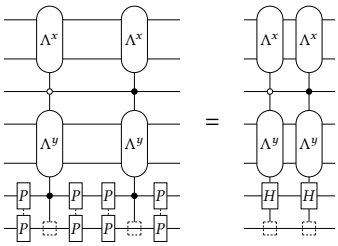
方程证明 (310):





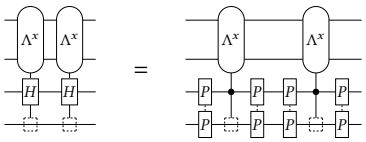


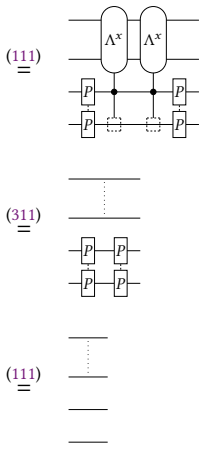




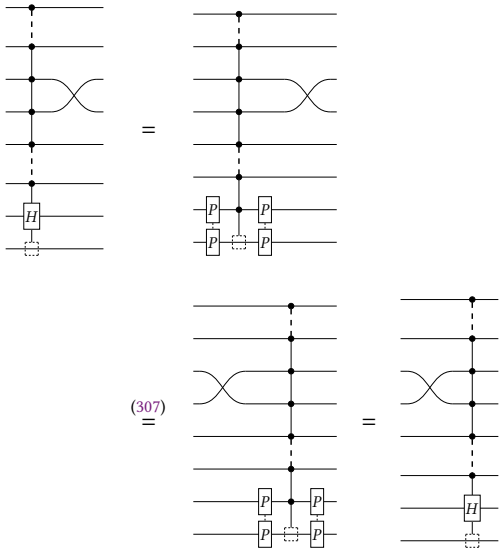
方程证明 (311): 方程 (311) 直接由方程 (81) 和 (299) 得出。

方程（312）的证明:

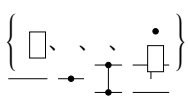


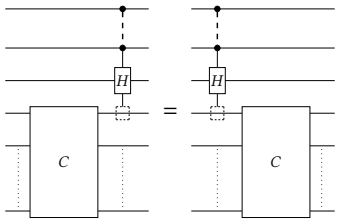


方程证明 (313):



□

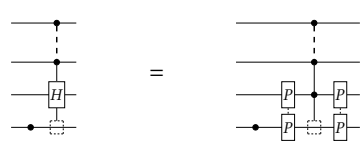
引理D.11。 对于任意电路（基于  ）， 以下方程可由图 4 中的方程推出：



(314)

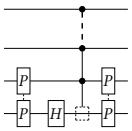
证明。我们对 C进行结构归纳。[20]

若 $C =$  ，则结果显然。若 $C =$  ，H或  ，则分别由方程（277）、（303）或（282）可得。若$C =$  ，则有

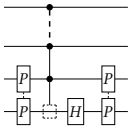


[20]更确切地说，是对底层原始电路进行归纳。

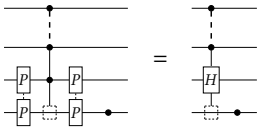
(111)(112)(113)
=



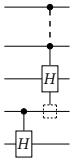
(285)
=



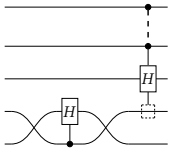
(112)(113)
=



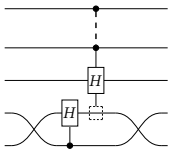
若 $C =$  则有 H



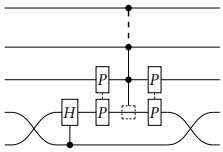
=



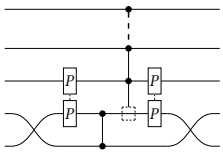
(277)
=



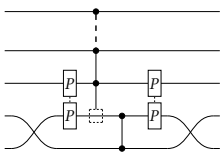
=



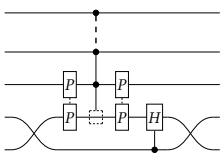
(111)(112)(18)(9)
=

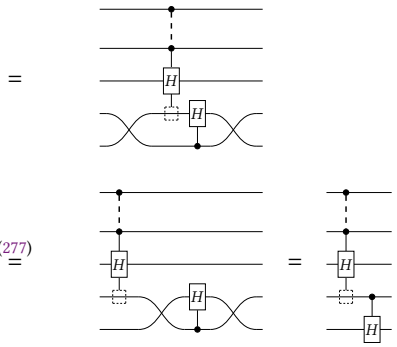


(272)
=

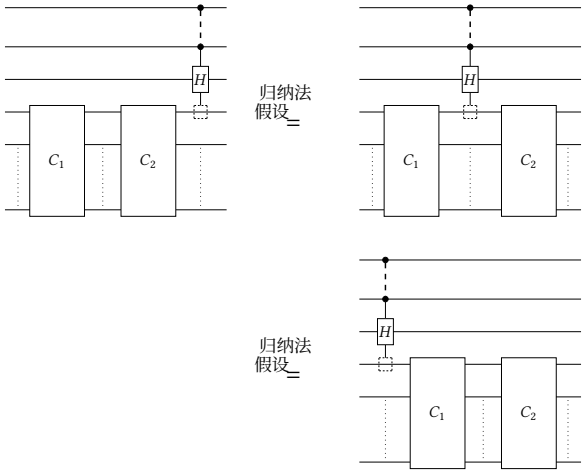


(112)(9)(18)
=

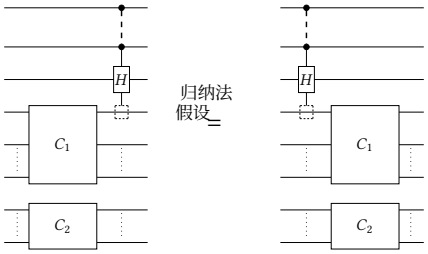




若 $C = C_2 \circ C_1$（其中 C_1, C_2 不同于单位元），则有



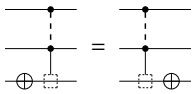
最后，如果 $C = C_1 \otimes C_2$（其中 $C_2 \neq$ ），那么我们有



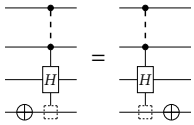
□

D.7 多重控制量子门的对易性质

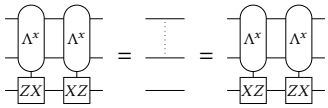
引理 D.12。 以下方程可由图 *4* 的方程推出：



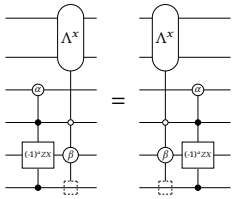
(315)



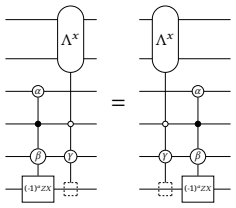
(316)



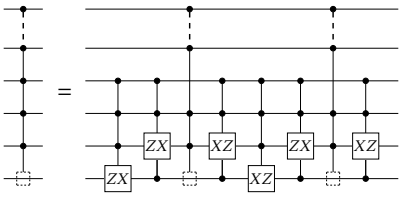
(317)



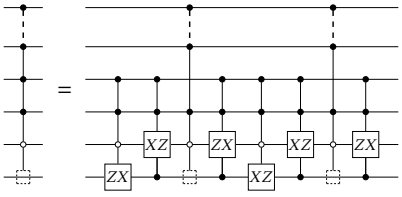
(318)



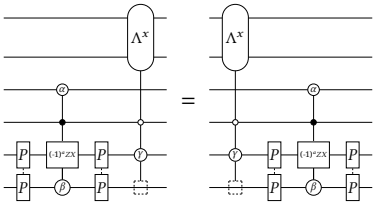
(319)



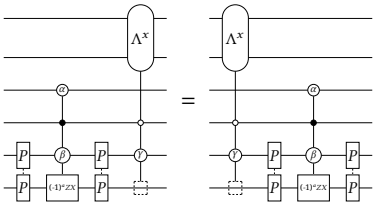
(320)



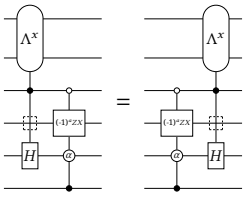
(321)



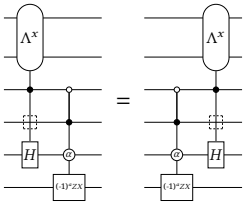
(322)



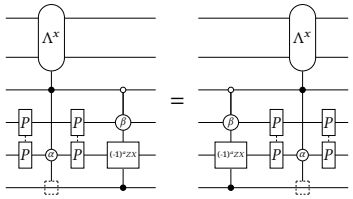
(323)



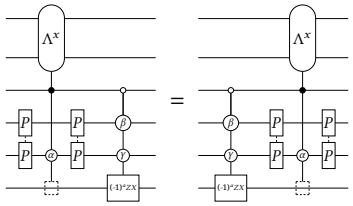
(324)



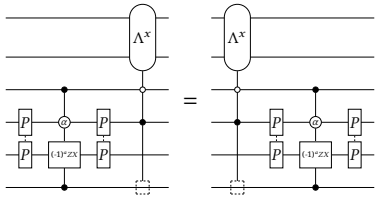
(325)



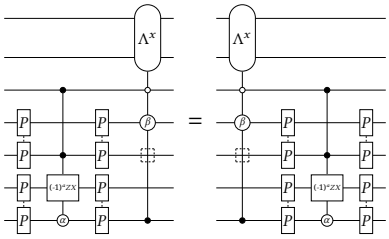
(326)



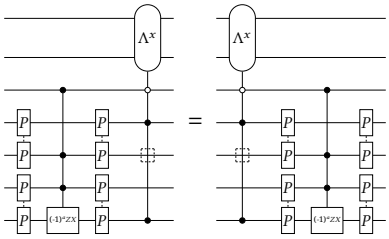
(327)



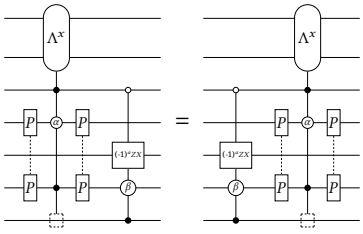
(328)



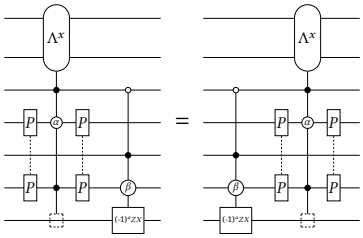
(329)



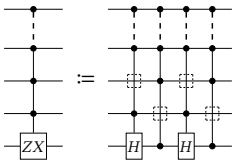
(330)



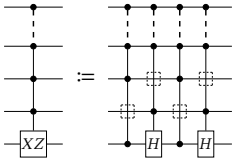
(331)



(332)

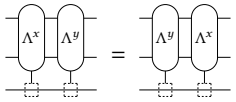


(333)

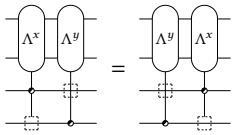


(334)

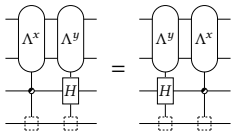
引理 D.13. 以下等式 均是图中方程的推论 *4*，其中 表示黑色控制或白色控制：

$\forall x, y \in \{0,1\}^n,$ 

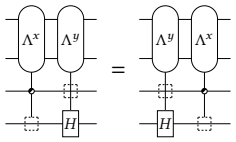
(335)

$\forall x, y \in \{0,1\}^n,$ 

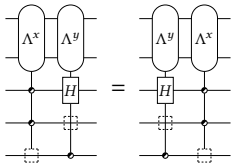
(336)

$\forall x, y \in \{0,1\}^n$ 其中 $x \neq y,$ 

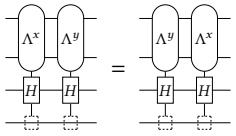
(337)

$\forall x, y \in \{0,1\}^n,$ 

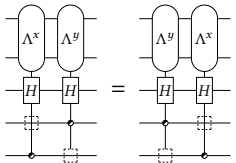
(338)

$\forall x, y \in \{0,1\}^n$ 其中 $x \neq y,$ 

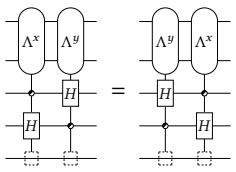
(339)

$\forall x, y \in \{0,1\}^n,$ 

(340)

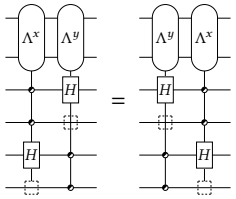
$\forall x, y \in \{0,1\}^n,$ 

(341)

$\forall x, y \in \{0,1\}^n$ 其中 $x \neq y,$ 

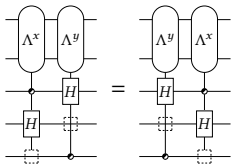
(342)

$\forall x, y \in \{0,1\}^n$ 其中 $x \neq y$,



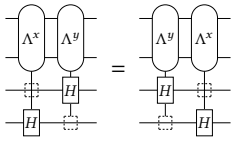
(343)

$\forall x, y \in \{0,1\}^n$ 其中 $x \neq y$,



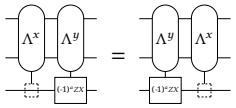
(344)

$\forall x, y \in \{0,1\}^n$,



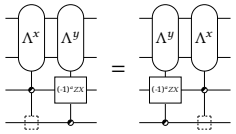
(345)

$\forall x, y \in \{0,1\}^n$,



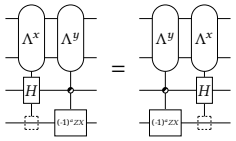
(346)

$\forall x,\ y \in \{0、1\}^n$，其中 $x \neq y$,



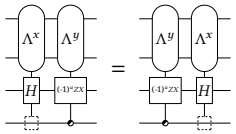
(347)

$\forall x,\ y \in \{0、1\}^n$，其中 $x \neq y$,



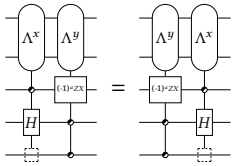
(348)

$\forall x, y \in \{0,1\}^n$ 其中 $x \neq y$,



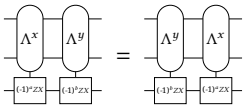
(349)

$\forall x, y \in \{0,1\}^n$ 与 $x \neq \quad y$,



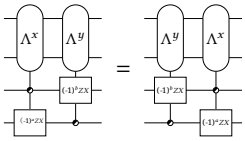
(350)

$\forall x, y \in \{0,1\}^n$,



(351)

$\forall x, y \in \{0,1\}^n$ 其中 $x \neq y$,



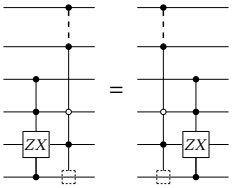
(352)

引理 D.12 和 D.13 的证明。 我们按顺序证明所有方程，但方程 (333) 和 (334) 除外；这两个方程只有在证明了方程 (335) 至 (345) 后才证明。

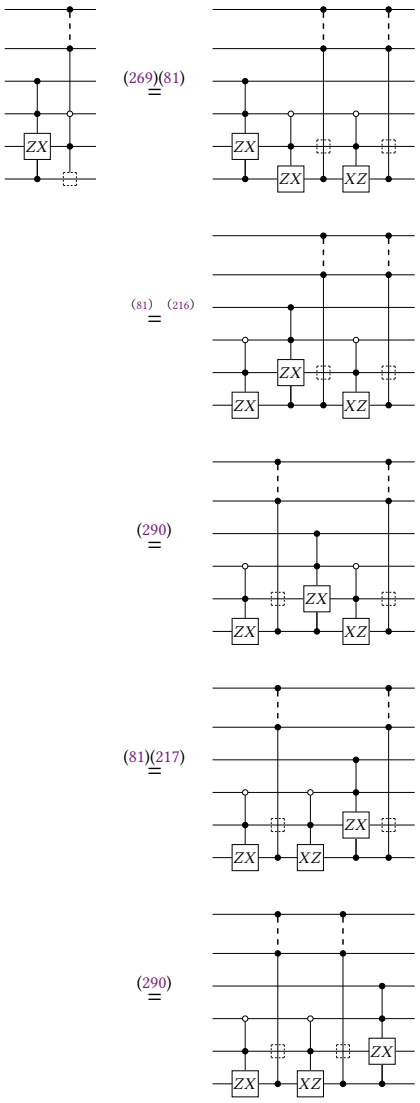
方程的证明 (315) 和 (316)： 方程 (315) 和 (316) 分别只是方程 (308) 和 (314) 的特例。我们将其明确写出，只是为了让后续证明更加清晰。

方程证明 (317)： 方程 (317) 可直接由方程 (5)、(81) 和 (299) 得出。

方程证明 (318)： 首先，我们证明该方程在 $x = \vec{1}$、 $\alpha = \beta = 1$ 和 $a = 0$ 的特殊情形：

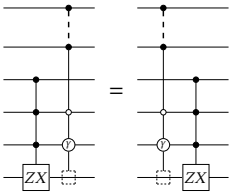


推导如下：

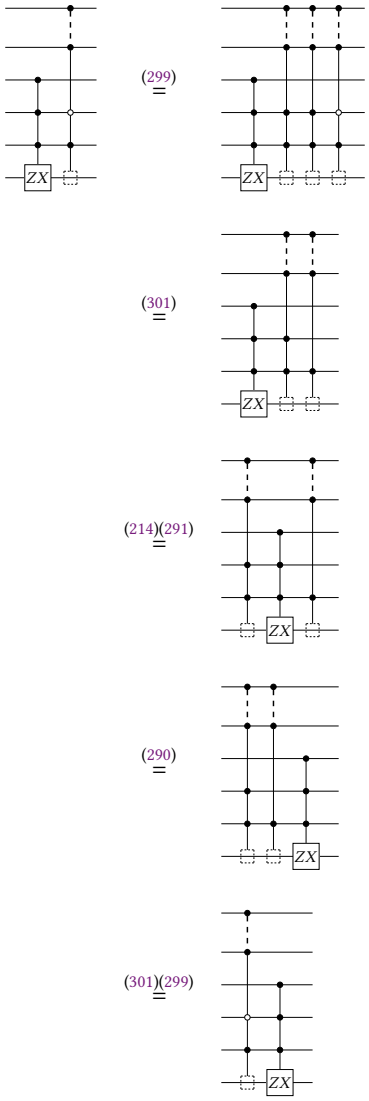


接下来， $x \neq \vec{1}$ 或 $\alpha \neq 1$ 的情形可直接得出。 $a = 1$ 的情形由引理B.5 （结合方程（311）和（317））得出。而 $\beta = 0$ 的情形由方程（238）得出，必要时结合方程（81）。

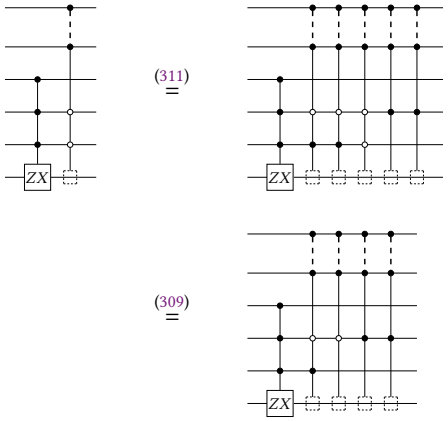
方程证明 (319)： 首先，我们证明该方程在以下情形下的特殊情况： $x = \vec{1}$， $\alpha = \beta = 1$，以及 $a = 0$：



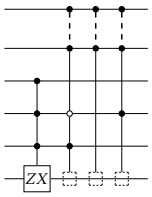
若 $\gamma = 1$，则有



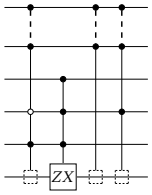
并且如果 $\gamma = 0$，那么我们有



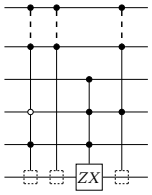
(309)
=



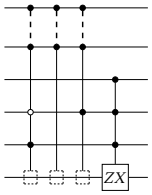
前一种情况
=



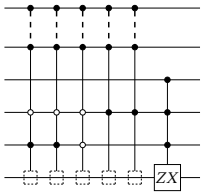
(308)
=



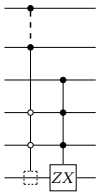
(215)(290)
=



(309)
=



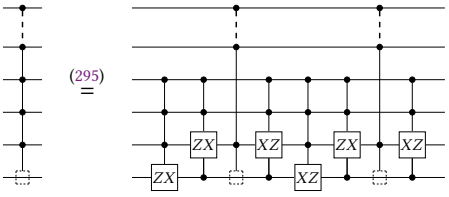
(311)
=

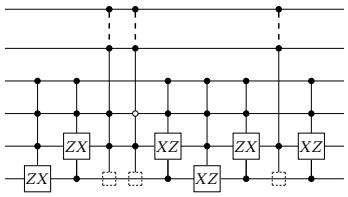


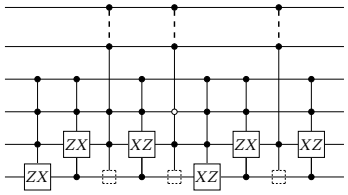
最后， $x \neq \vec{1}$， $\alpha \neq 1$，或 $\beta \neq 1$ 显然成立，或可由方程（81）得出；而 $a = 1$ 则可由引理B.5 （结合方程（311）和（317））得出。

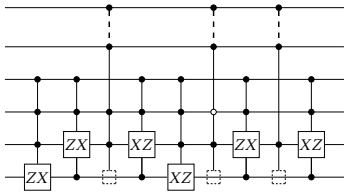
方程证明(320)：

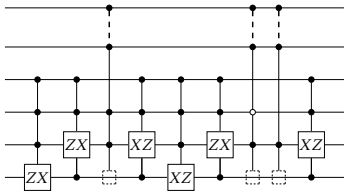
(295)
=

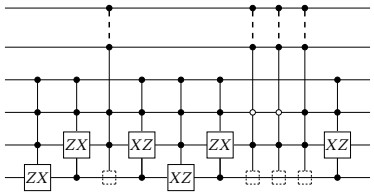


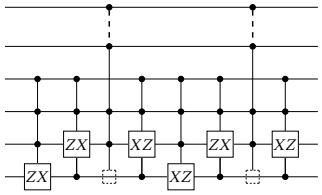
(301)
=


(319)
=


(319)
=


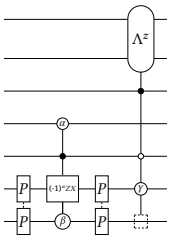
(319)
=


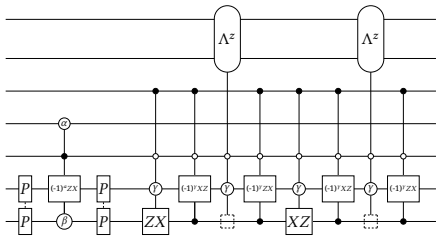
(302)
=


(311)
=


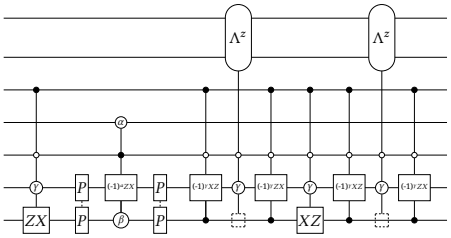
*Pro*方程 (321)： 由方程 (320)，方程 (321) 可由方程 (81) 和 (238) 直接推出。

方程证明(322)： 我们按长度进行归纳 n 的 x。若 $n = 0$，则结论由方程（247）得出。若 $n \geq 1$，则不失一般性地假设 x 的最后一位为 1，即 $x = z1$ 其中 $z \in \{0, 1\}^{n-1}$。于是我们有

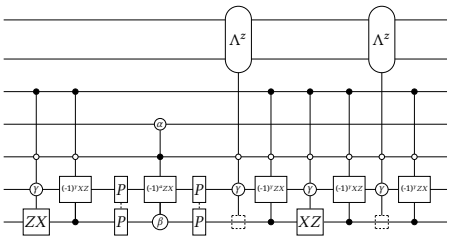


(320)(321)(81)
=


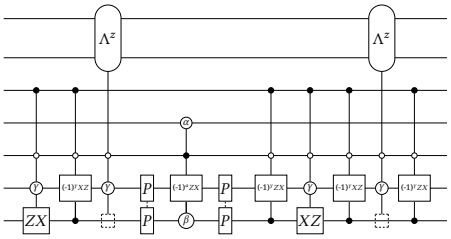
(112)(267)
=



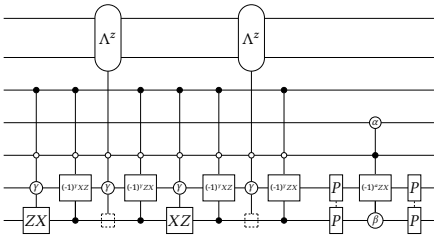
(112)(268)
=



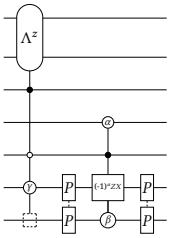
归纳法
假设
=



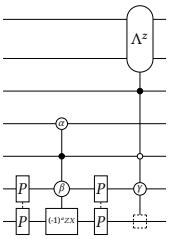
(112)(268)(267)
归纳法
假设
=



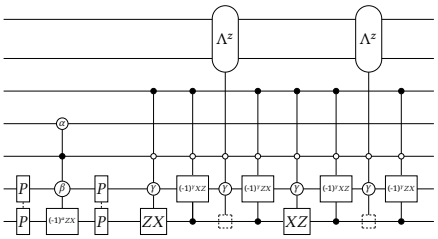
(81)(320)(321)
=



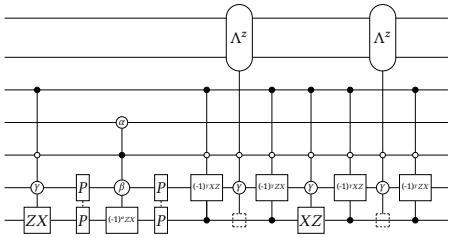
方程证明 (323)： 我们对长度 n 的 x进行归纳。若 $n=0$，则由方程（248）可得结论。若 $n\geq 1$，则不失一般性，我们可以假设 x 的最后一位是1，即 $x=z1$，其中 $z\in\{0,1\}^{n-1}$。于是有



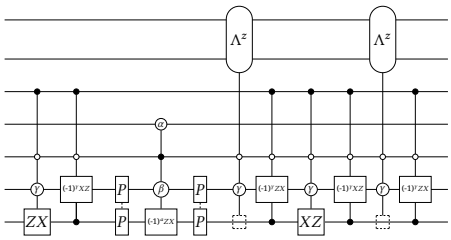
(320)(321)(81)
=



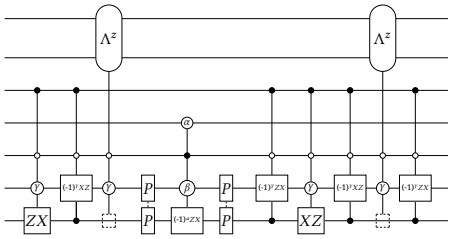
(268)
=



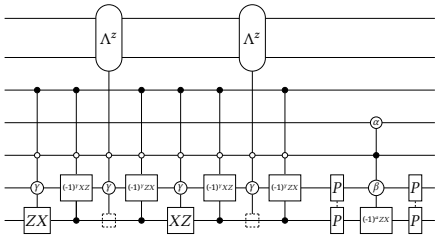
(267)
=



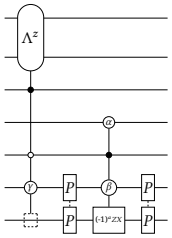
归纳法
假设
=



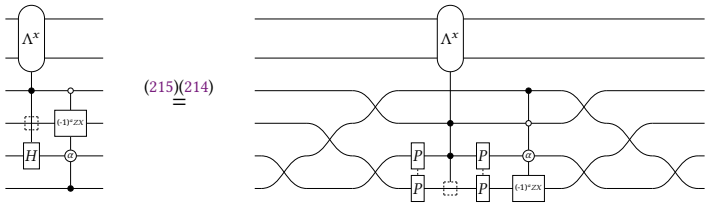
(267)(268)
归纳法
假设
=



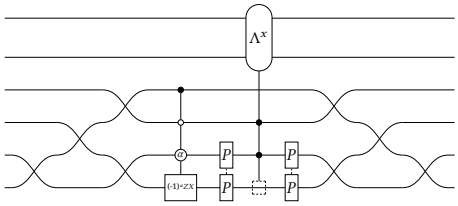
(81)(320)(321)
=



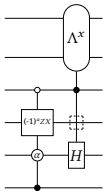
方程证明 (324)*:*



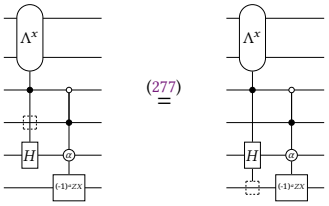
(81)(111)(323)
=



(214)(215)
=

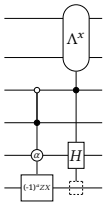


方程证明 (325)*:*

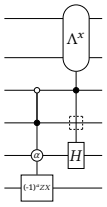


(277)
=

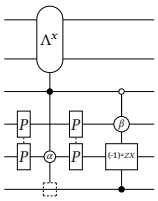
(215)(324)
=



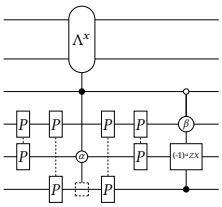
(277)
=



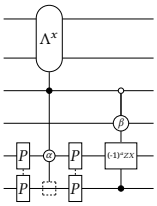
方程证明 (326)*:*



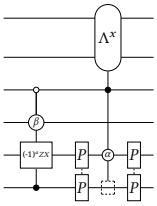
(111)(308)
=



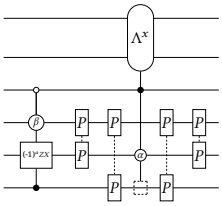
(112)(130)
=



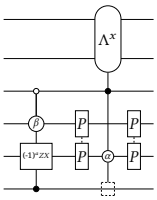
(81)(111)(214)(322)
=



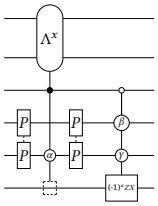
(130)(112)
=



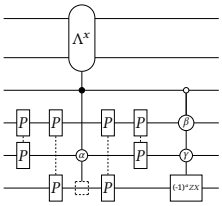
(308)(111)
=



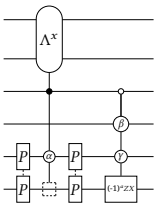
方程证明 (327):



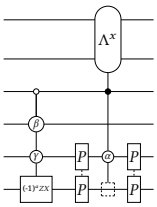
(111)(308)
=



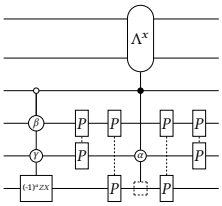
(112)(130)
=



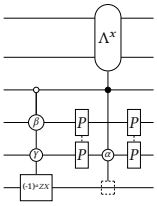
(81)(111)(214)(323)
=



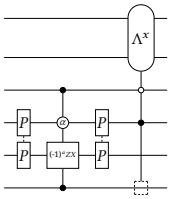
(130)(112)
=



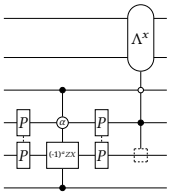
(308)(111)
=



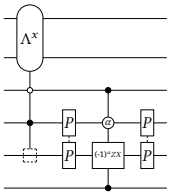
方程证明 (328):



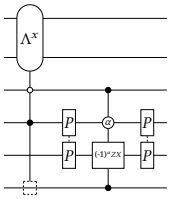
(274)
=



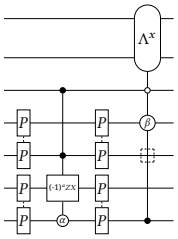
(215)(214)(323)
=



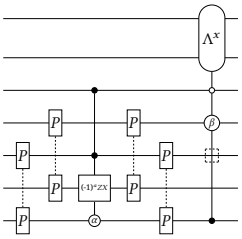
(274)
=



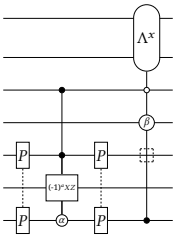
方程证明 (329):



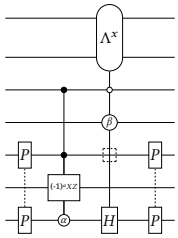
(246)
=



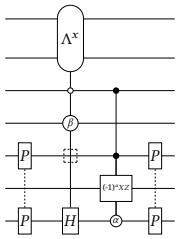
(112)(262)(111)
=



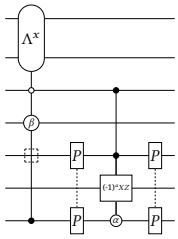
(111)(112)
=



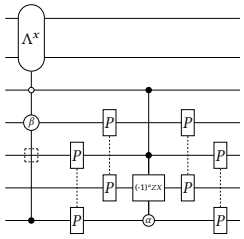
(307) (81) (325)
=



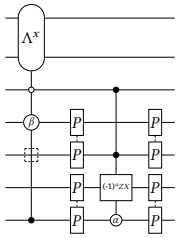
(112)(111)
=



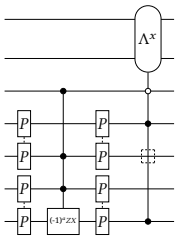
(111)(262)(112)
=



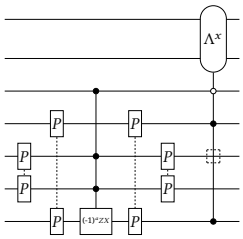
(246)
=



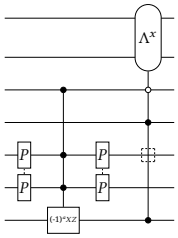
方程证明(330):



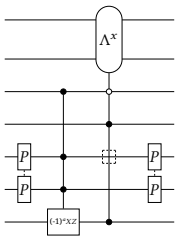
(112)(246)
=



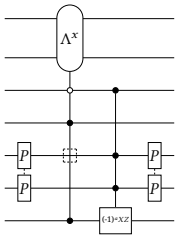
(112)(262)(111)
=



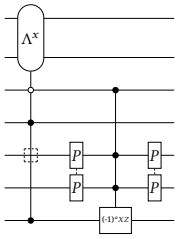
(308)
=



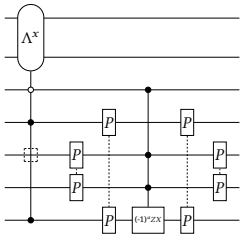
(307)(215)(214)(318)
=



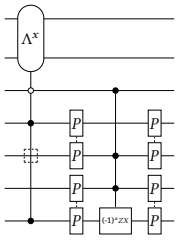
(308)
=



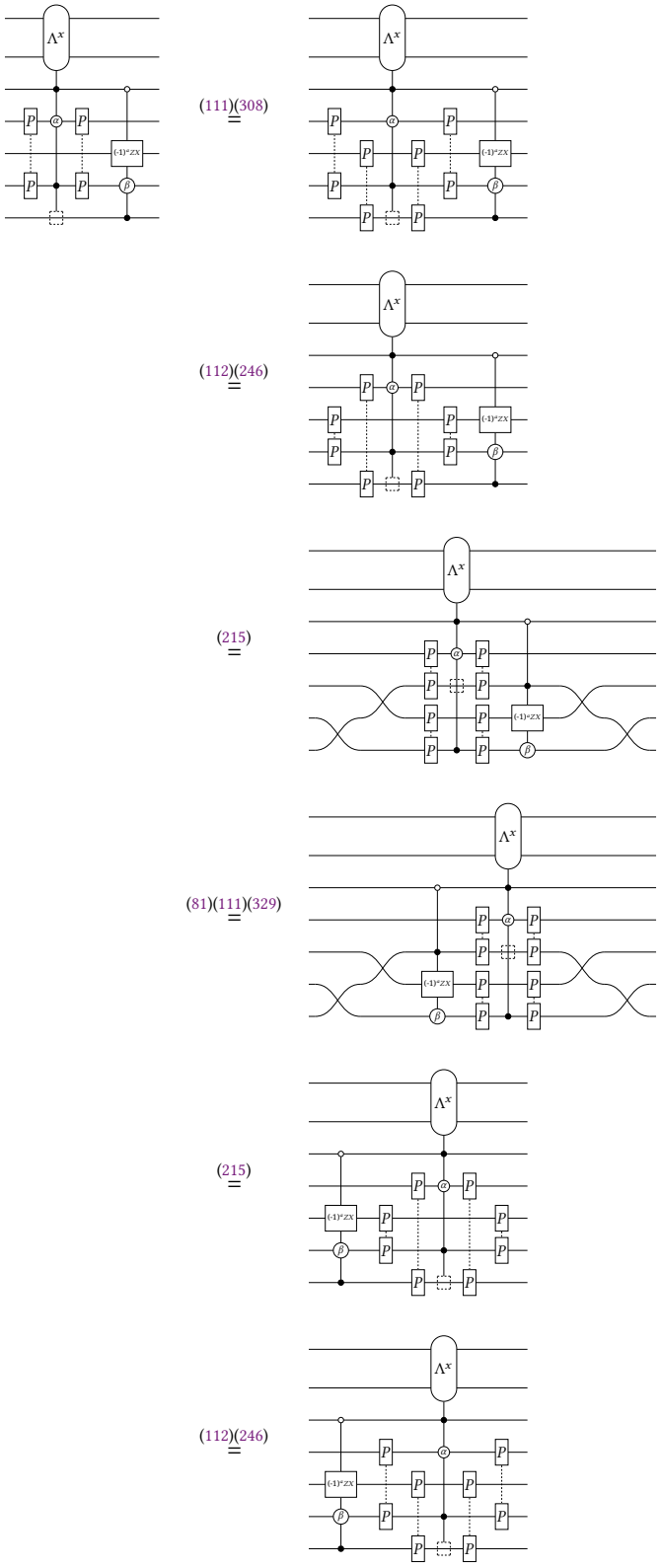
(111)(262)(112)
=



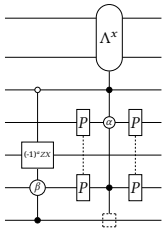
(246)(112)
=



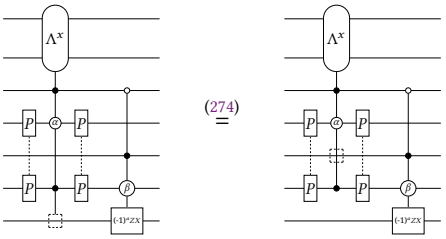
方程证明 (331)：



(308)(111)
=

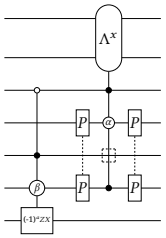


方程证明 (332)*:*

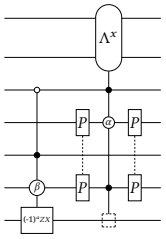


(274)
=

(215)(331)
=



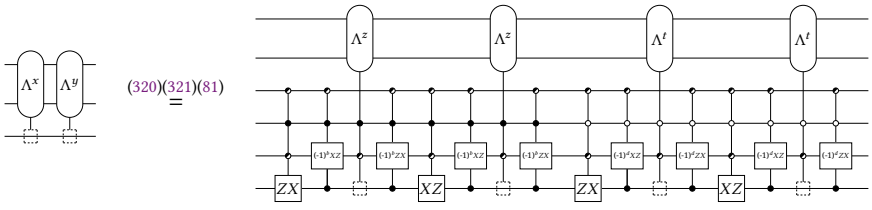
(274)
=



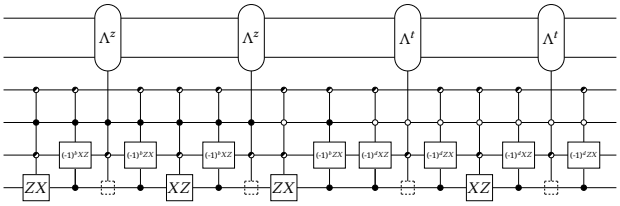
*P*方程的上方 (335)： 如果 $x = y$ 那么该方程为 tr 平凡。

如果 $x \neq y$，那么 x 和 y 至少有一位比特不同，这意味着 Λ^x 的黑色控制位于 Λ^y 的白色控制之前，或者反之。由于该方程是对称的，不失一般性，我们可以假设属于第一种情况。接着，我们对 n 进行归纳（即 x 的长度）。不能有 $n = 0$，因为这将意味着 $x = y$。如果 $n = 1$，则结论由引理 7.1 得出。如果 $n = 2$，则结论由引理 7.6 得出。如果 $n \geq 3$，那么根据等式 (307)，不失一般性，我们可以假设这是 x 和 y 之间倒数第二个不同的比特，也就是说，$x = za1b$ 和 $y = tc0d$，其中 z、$t \in \{0,1\}^{n-3}$ 以及 a、b、c、$d \in \{0,1\}$。于是有

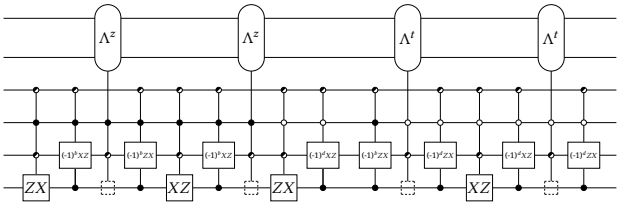
(320)(321)(81)
=



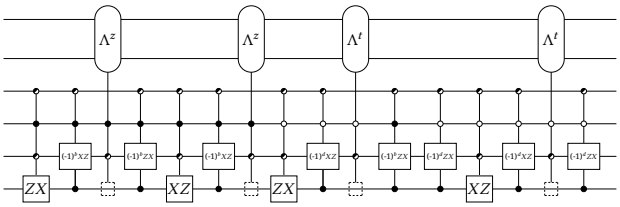
(240)
=



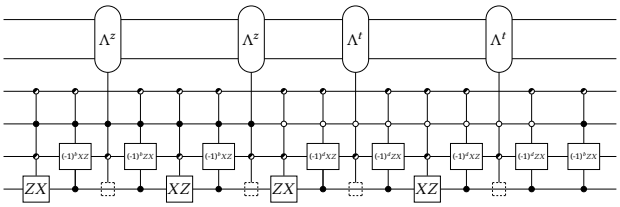
(241)
=



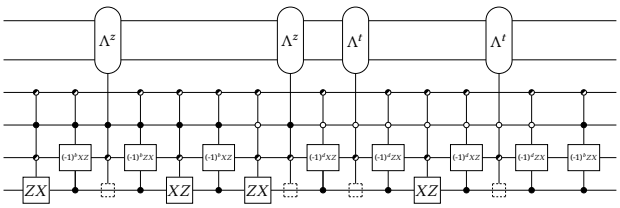
(318)
=



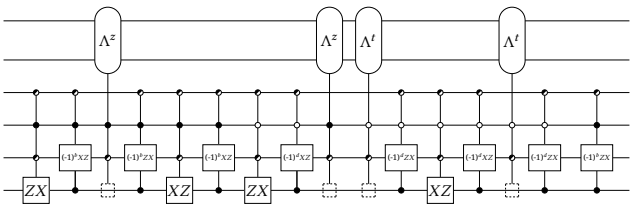
(241)(240)(318)
=



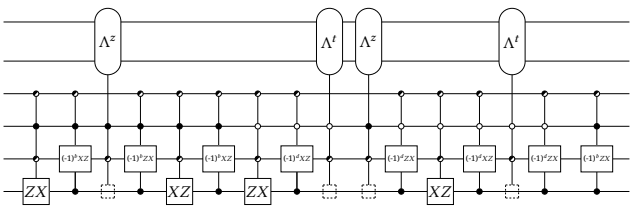
(81)(319)
=



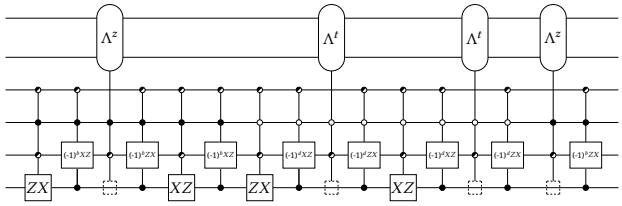
(81)(318)
=



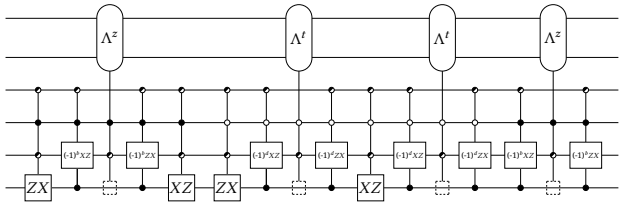
归纳法
假设
=



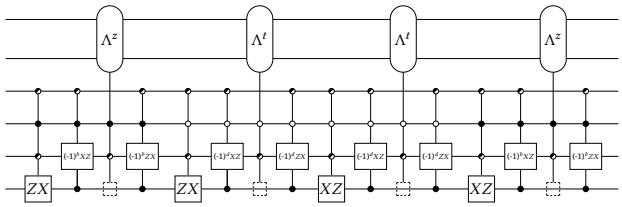
(81)(318)(319)
归纳法
假设
=



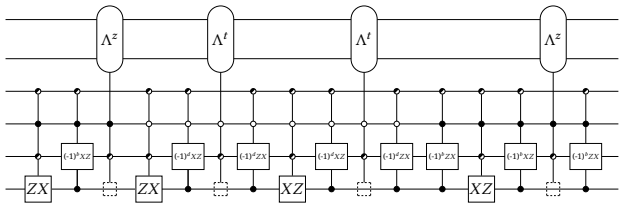
(240)(241)(318)
=



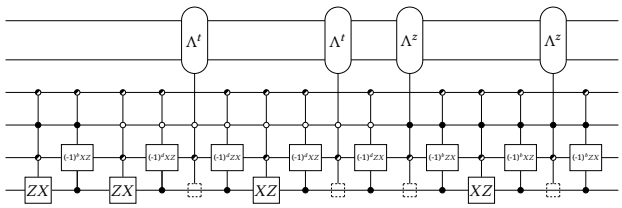
(241) (240) (319)
=



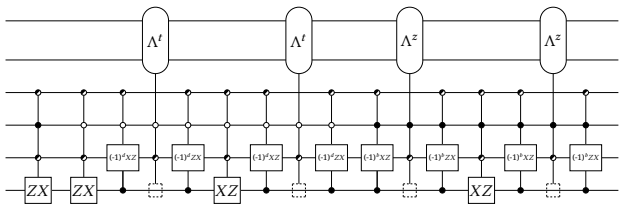
(240)(241)(318)
=



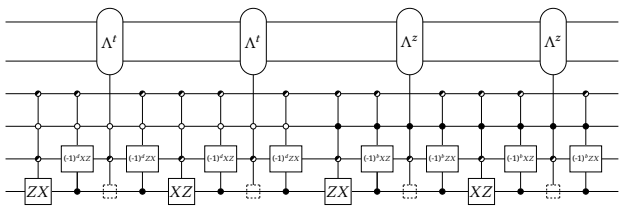
(81)(319)(318)
归纳法
假设
=



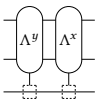
(240)(241)(318)
=



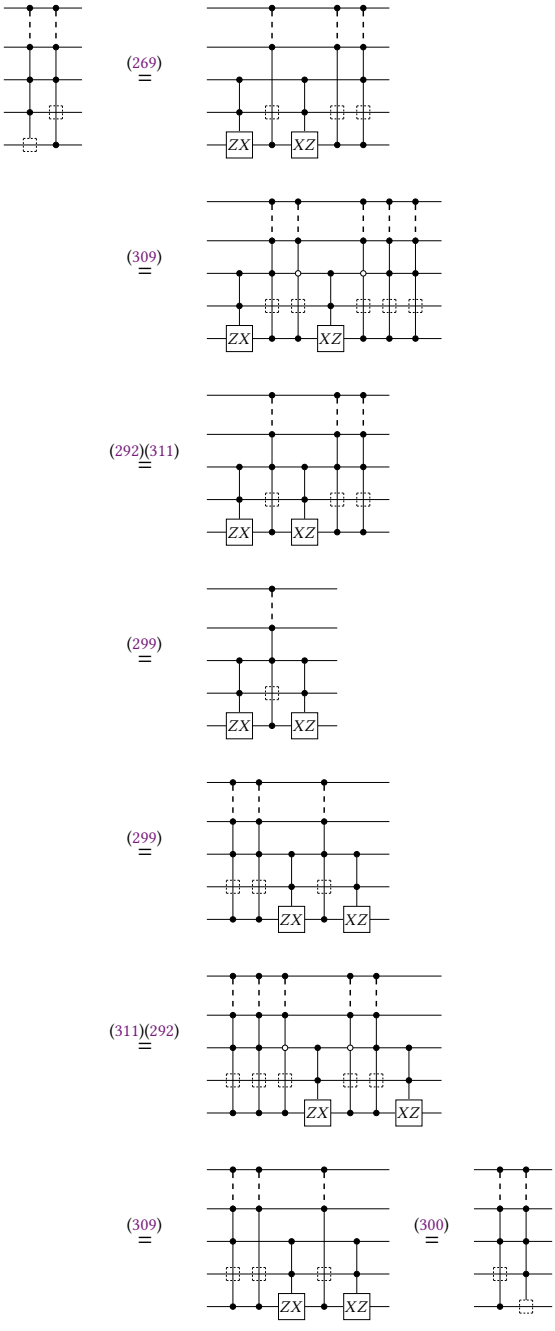
(241) (240) (319)
=



(81)(320)(321) =

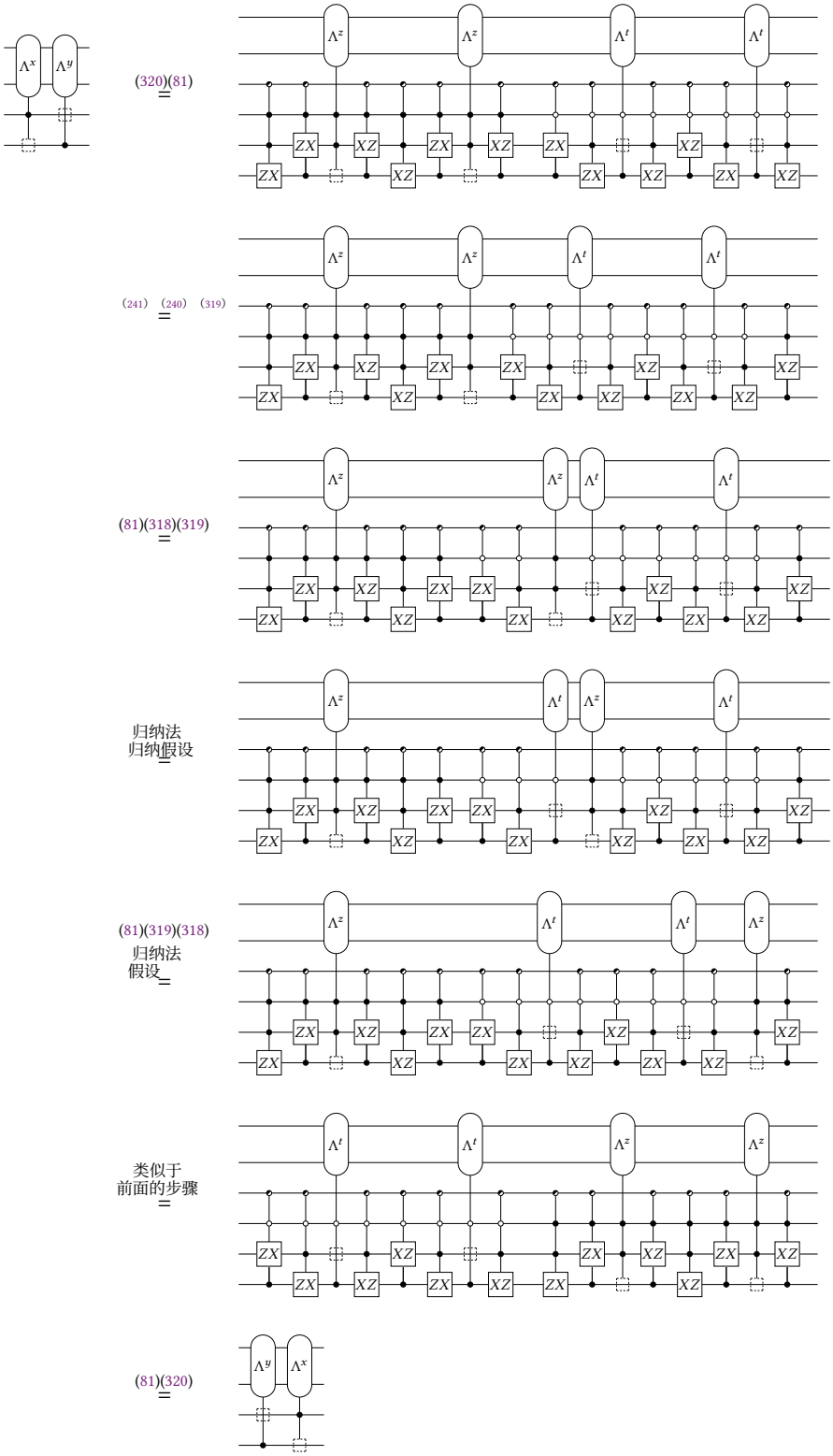


方程证明 (336)：若 $n=0$，则由引理 7.6 可得结论。若 $x=y$ 且 $n\geq 1$，则根据方程 (81)，不失一般性地假设 x(因此 y 也如此) 是仅由 1 组成的向量。根据方程 (315)，还可以不失一般性地假设位于 's 前面的控制位也是黑色的。于是有



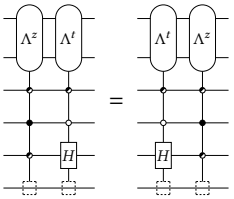
若 $x\neq y$，则我们对 n 使用归纳法。若 $n=1$，则由等式 (12) 和 (131) 以及方程（9）可得结论。若 $n\geq 2$，则根据等式 (307)，不失一般性地假设这是 x和 y之间最后一个不同的比特；根据方程（81），我们可以假设该比特在 x中为 1，在 y中为 0。也就是说，$x=za1$和 $y=tb0$，其中 $z,t\in\{0,1\}^{n-2}$且 $a,b\in\{0,1\}$。那么我们

have

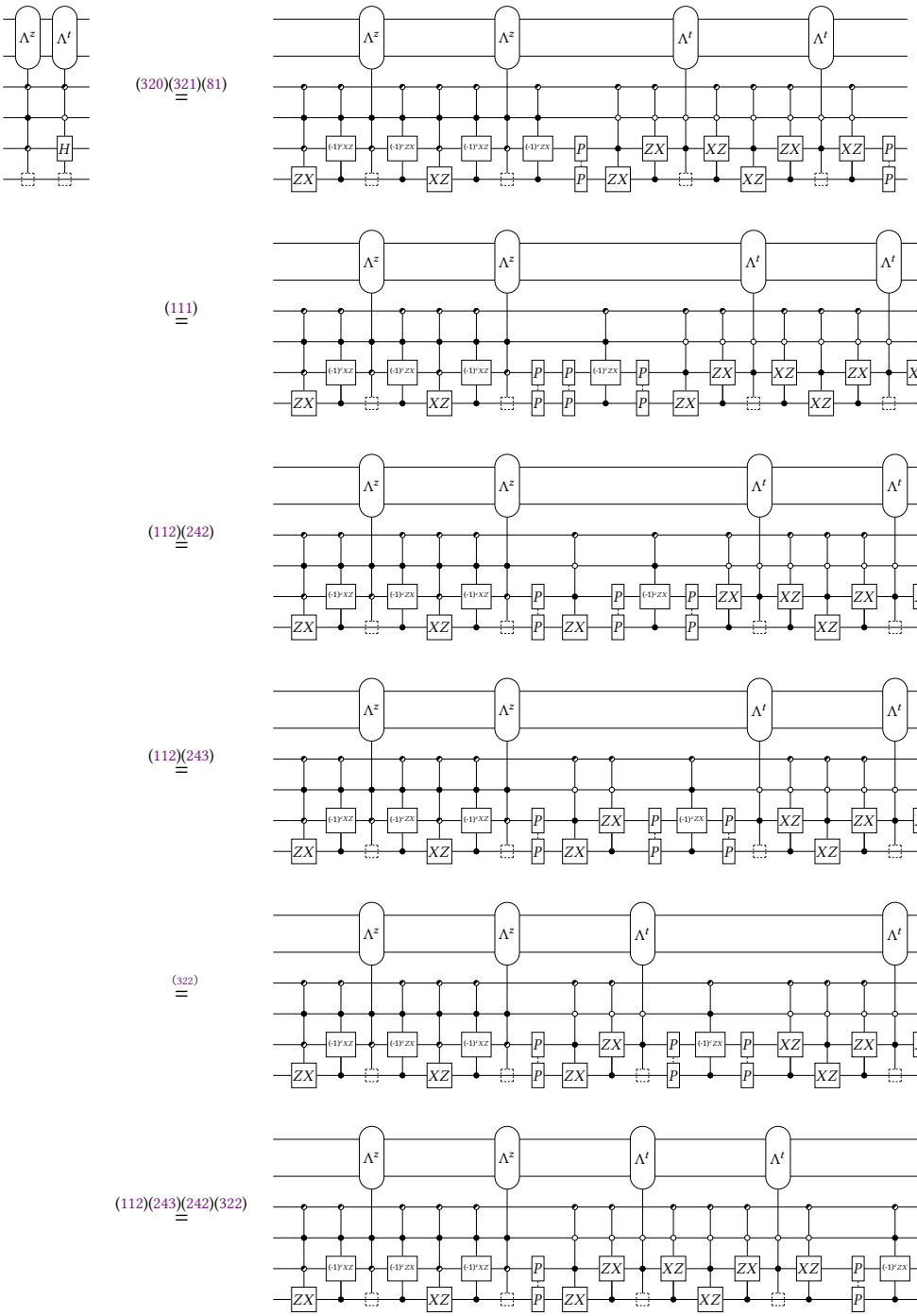


方程证明 (337)： 我们对 n 进行归纳法。如果 $n = 1$，则结论由引理 7.6 得出。如果 $n \geq 2$，则根据方程（307）和（313），不失一般性，我们可以假设 x 和 y 仅最后一位不同；根据方程（81），我们可以假设该位在1 中

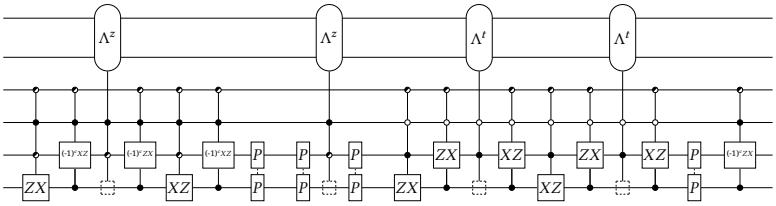
x以及 y 中的 0。也就是说， $x = za1$和 $y = tb0$，其中 z， $t \in \{0, 1\}^{n-2}$以及 a， $b \in \{0, 1\}$。因此，我们需要证明以下方程：



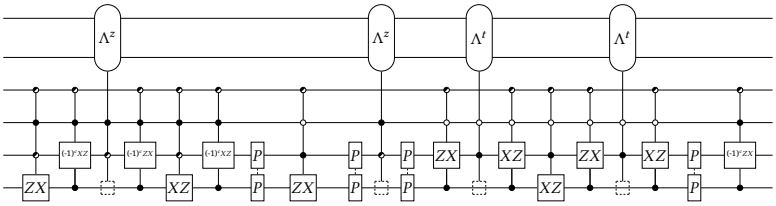
并且我们有（其中 c 表示位于 H 前方的控制所对应的比特）：



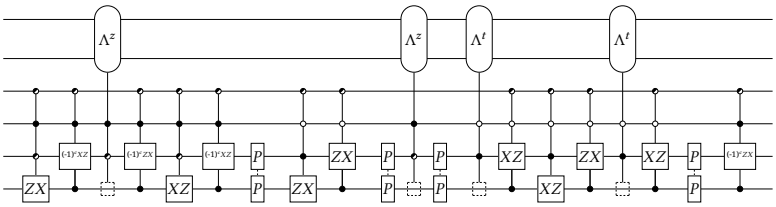
(111)
=



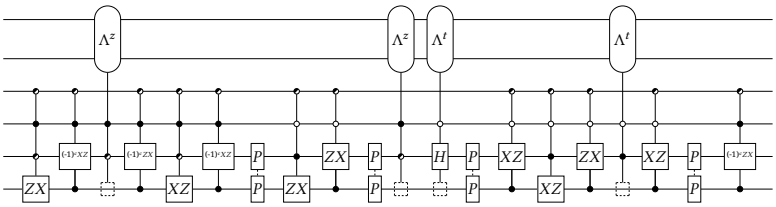
(81)(111)(323)
=



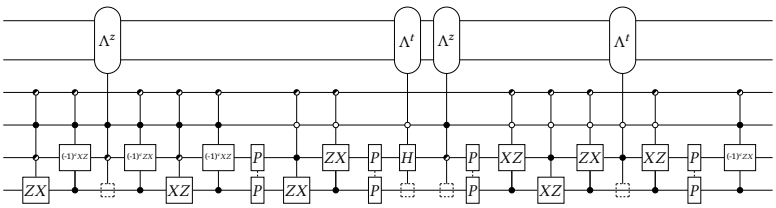
(81)(111)(322)
=



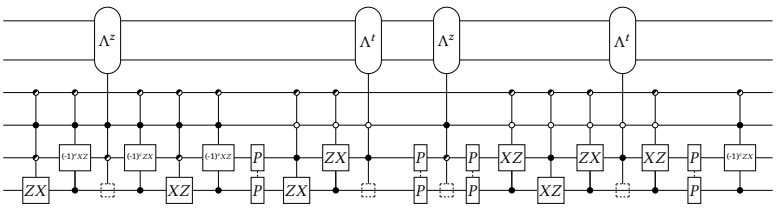
(111)
=



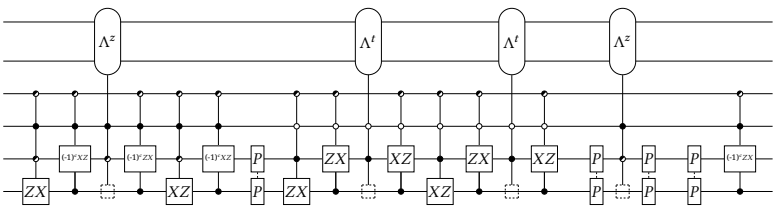
归纳法
假设
=



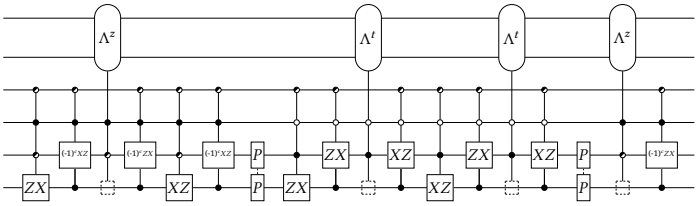
(111)
=



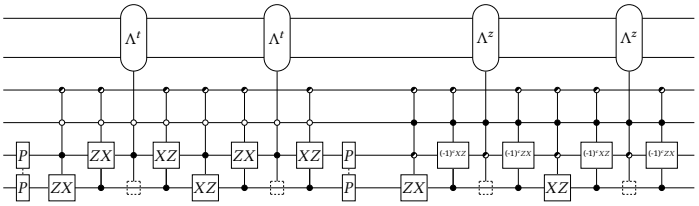
(81)(111)(322)(323)
归纳法
假设
=



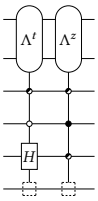
(111)
=



类似于
前面的步骤
=

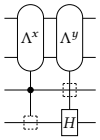


(81) (320) (321)
=

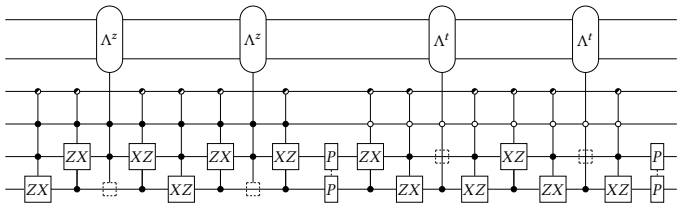


方程证明 （338）： 如果 $n = 0$，那么结果显然成立。

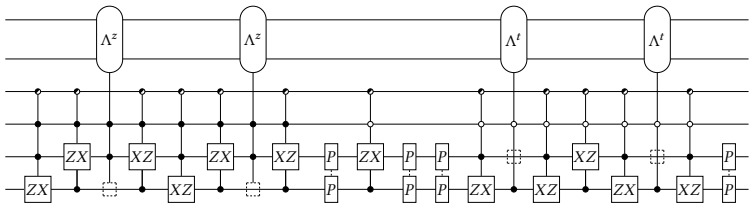
如果 $n \geq 1$和 $x \neq y$，那么我们对 n进行归纳法证明。如果 $n = 1$，则该结果由方程（13）和（132）以及方程（9）和（81）得出。如果 $n \geq 2$，那么根据等式（307）和（313），我们可以不失一般性地假设这是 x和 y之间不同的最后一位；根据方程（81），我们可以不失一般性地假设该位在 x中为 1，在 y中为 0。也就是说， $x = za1$和 $y = tb0$，其中 z、 $t \in \{0,1\}^{n-2}$，以及 a、 $b \in \{0,1\}$。此外，根据方程（316），我们可以不失一般性地假设该控制前面的控制为黑色。于是我们有



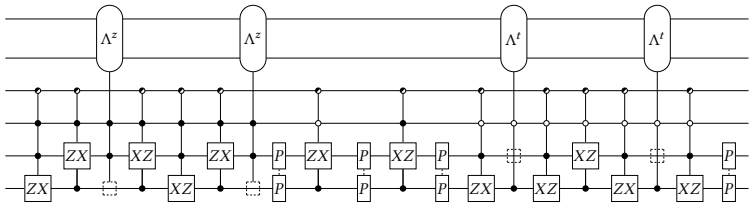
(320)(81)(112)
=



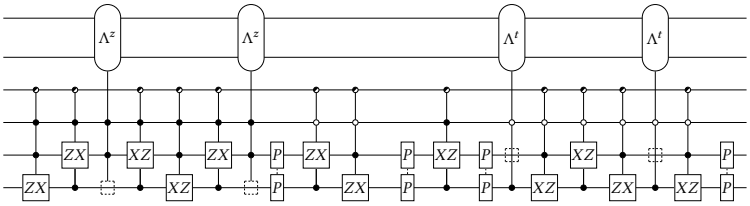
(111)
=



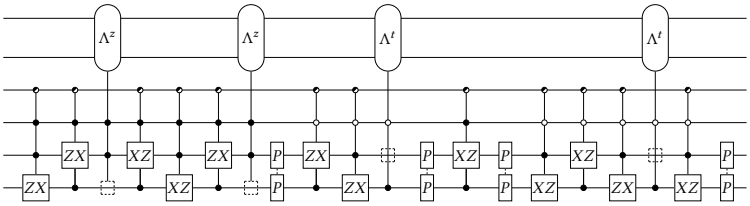
(112)(243)
=



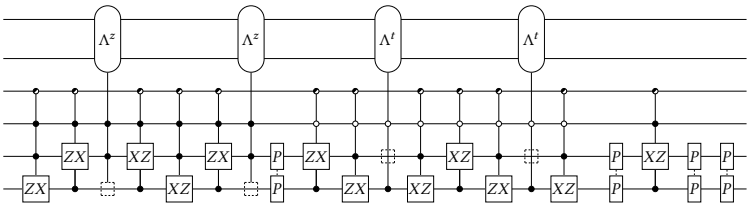
(112)(242)
=



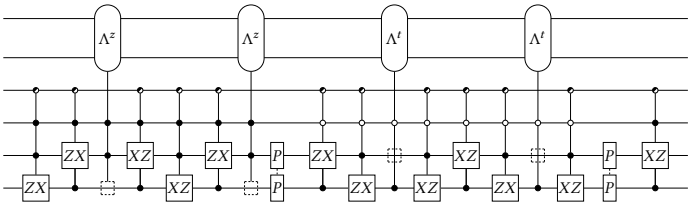
(112)(323)
=



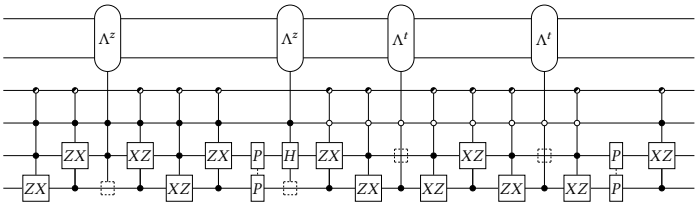
(112)(242)(243)(323)
=



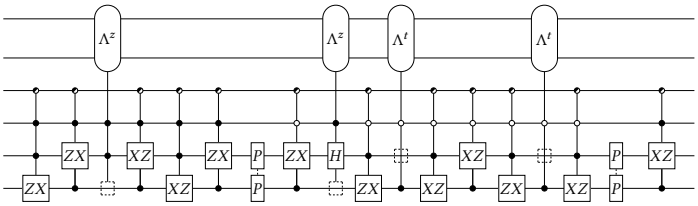
(111)
=



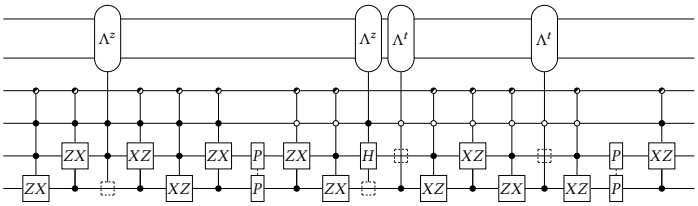
(111)
=



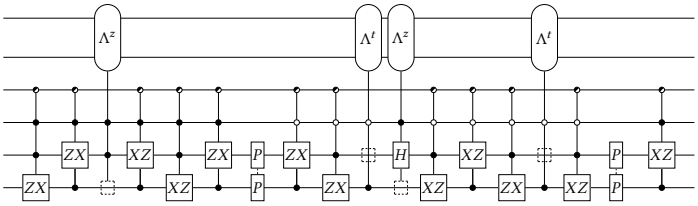
(111)(242)
=



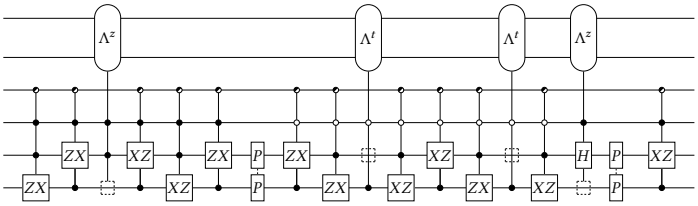
(111)(243)
=



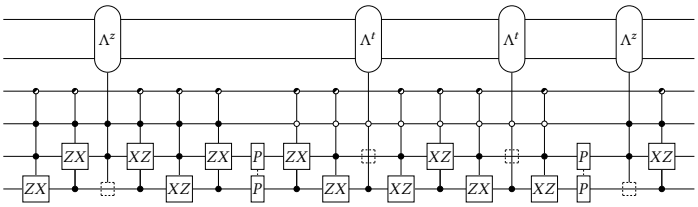
(112)
归纳法
假设
=



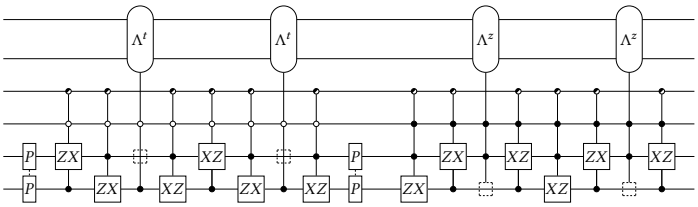
(111)(243)(242)(112)
归纳法
假设
=



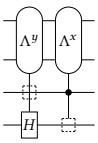
(111)
=

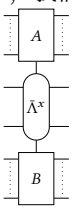
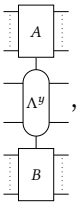


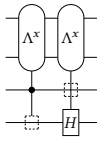
类似于
前面的步骤
=



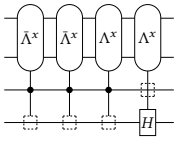
(81)(112)(320)
=



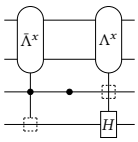
如果 $n \geq 1$ 并且 $x = y$，那么根据方程（316），我们同样可以不失一般性地假设，位于该门前面的控制为黑色。我们有（其中，与 [11], 类似，我们使用记号  $\coloneqq \prod_{y \neq x}$  ，其中乘积按任意顺序取）：



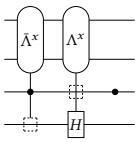
(311)(335)
=



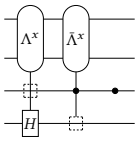
(335)(309)
=



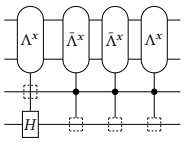
(314)
=



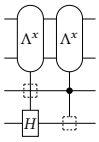
(338) 与 $x \neq y$
=



(309)(335)
=

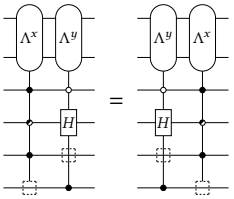


(335)(311)
=

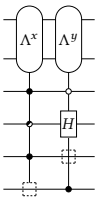


方程（(339)的证明：根据方程（307）和（313），不失一般性，我们可以假设 x 和 y 仅最后一位不同。根据方程（81），我们可以假设该位在 1 中为 x，在 0 中为 y。此外，根据方程（315）和（316），不失一般性，我们可以假设 's 前面的控制位为黑色。因此，只需证明该方程的以下变体：

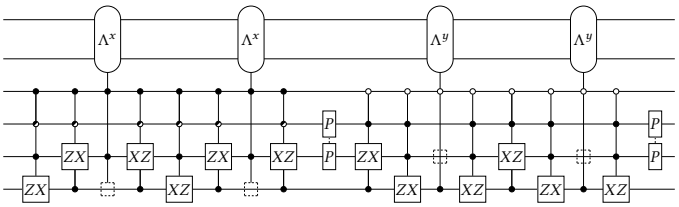
$$\forall x, y \in \{0,1\}^n,$$



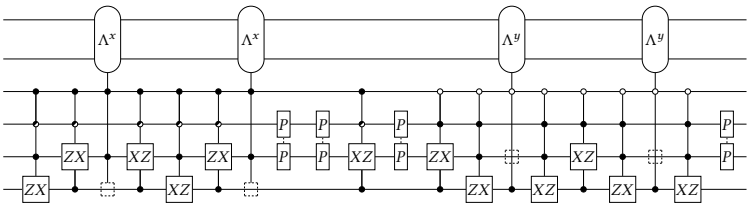
并且我们有



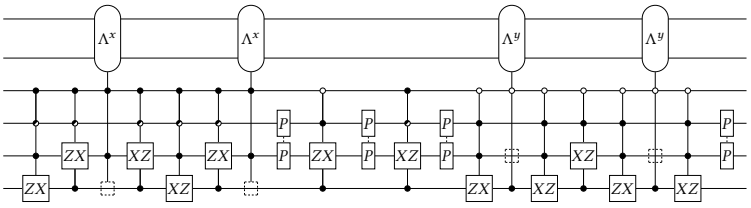
(307)(320)(81)(214)
=



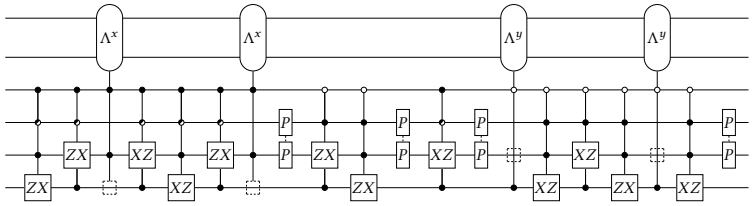
(111)
=



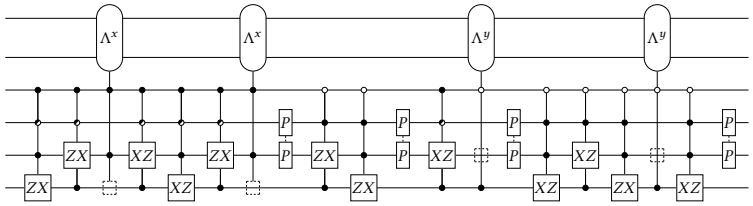
(215)(243)
=



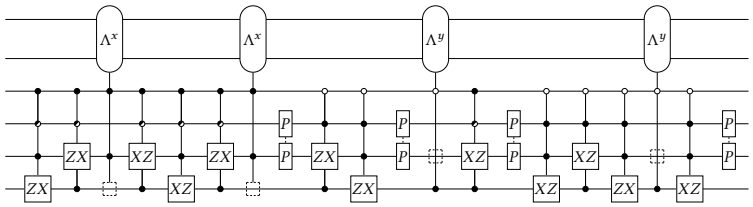
(244)
=



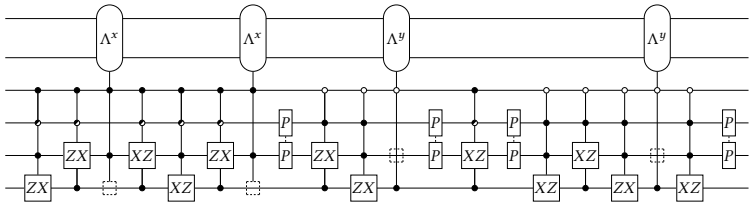
(308)
=



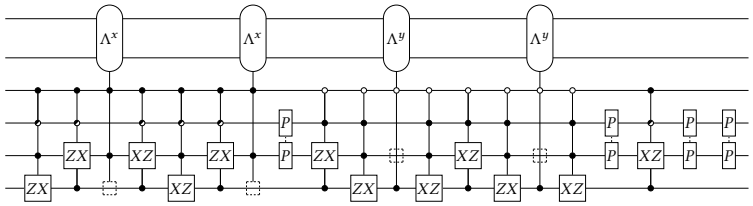
(214)(319)
=



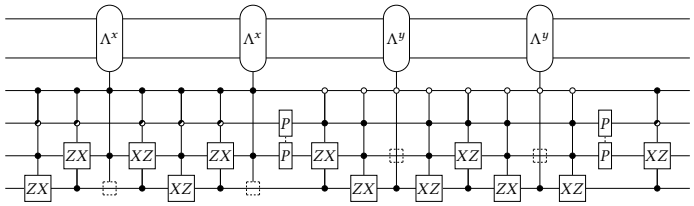
(308)
=



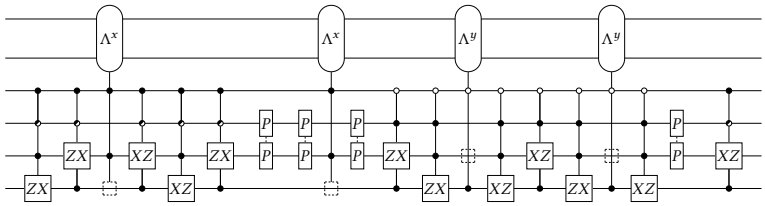
(244)(215)(243)
(308)(214)(319)
=



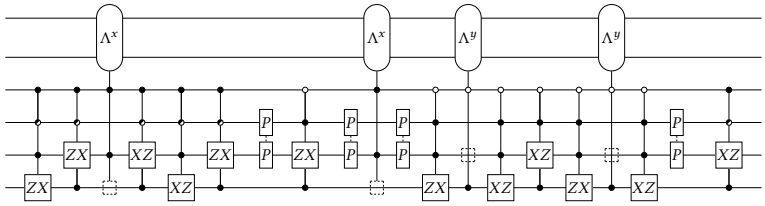
(111)
=



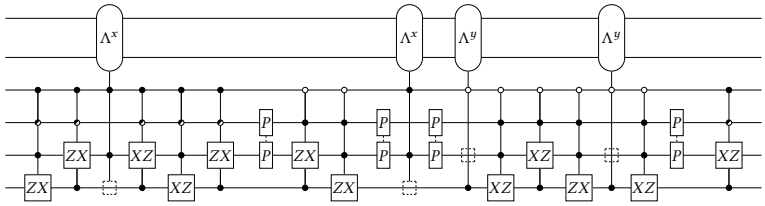
(111)
=



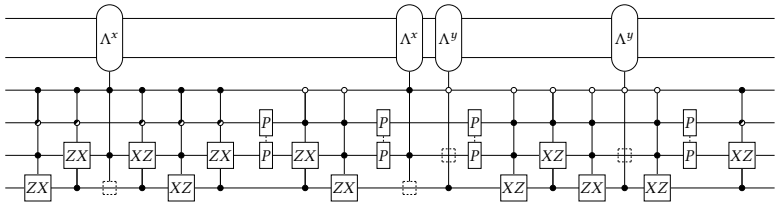
(326)
=



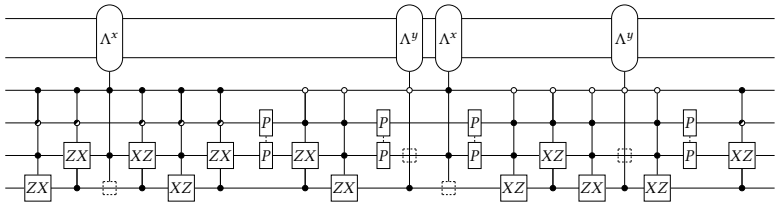
(327)
=



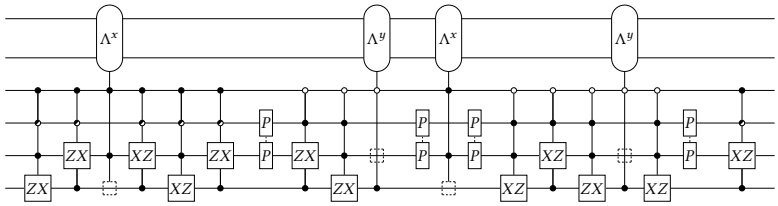
(308)
=



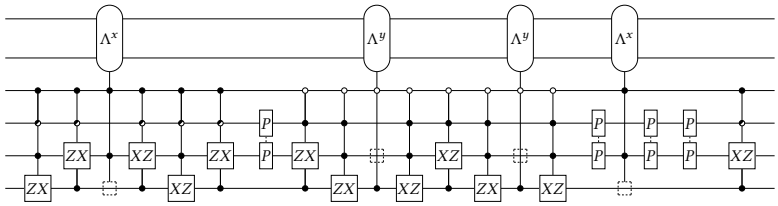
(336)
=



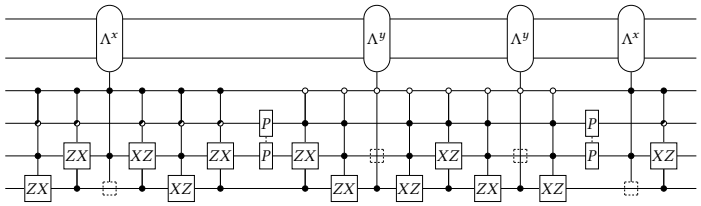
(308)
=



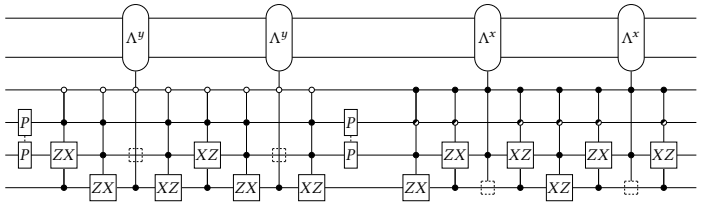
(327)(326)(308)(336)
=



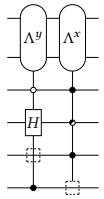
(111)
=



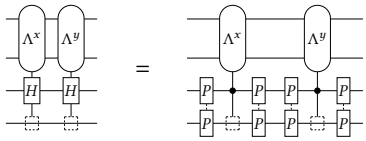
类似于
前面的步骤，
也使用（245）



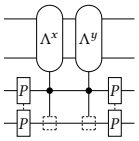
（81）（214）（320）（307）



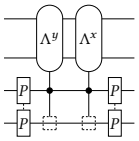
方程证明（340）：



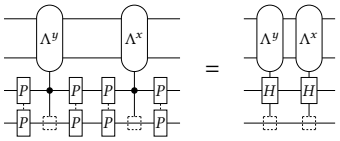
（111）



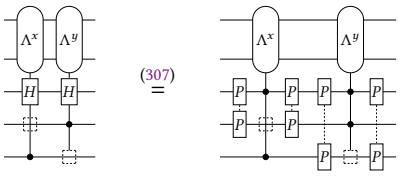
（335）



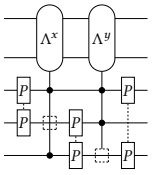
（111）



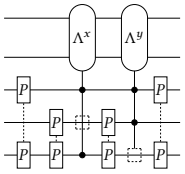
方程（(341)：根据方程（316），不失一般性，我们可以假设这些门前面的控制位都是黑色的。那么我们有□



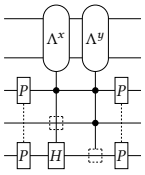
（112）（130）



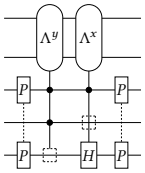
(130)(112) =



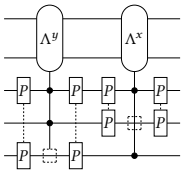
(112) =



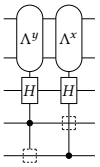
(338) =



(112)(130) =

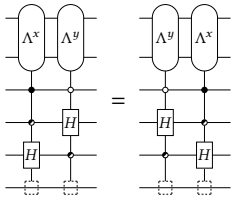


(307) =

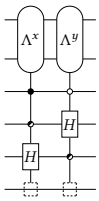


方程证明 (342)： 由方程 (307) 和 (313)，不失一般性，我们可以假设 x 和 y 只在最后一位上不同。根据方程 (81)，不失一般性，我们可以假设该位在 1 中为 x 而在 0 中为 y。也就是说，只需证明该方程的以下变体：

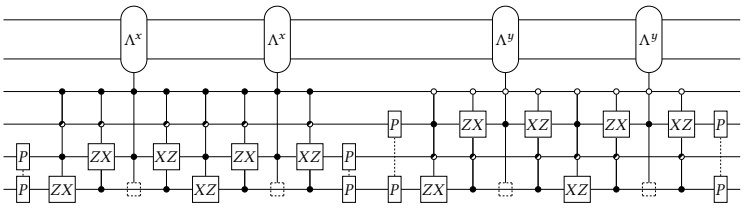
$$\forall x, y \in \{0,1\}^n,$$



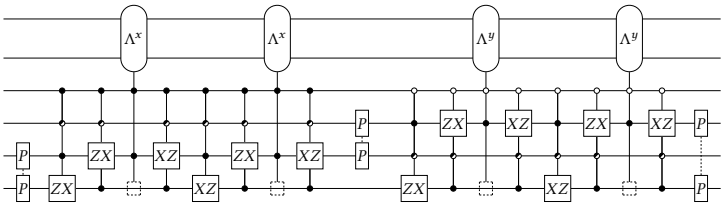
并且我们有



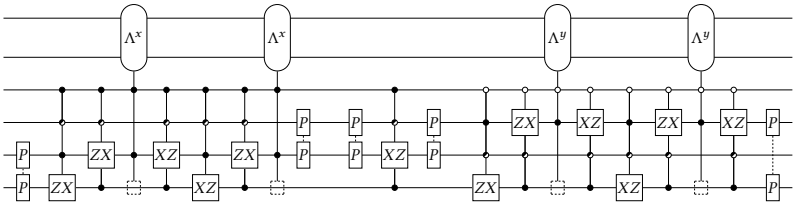
(320) (81) (214) =



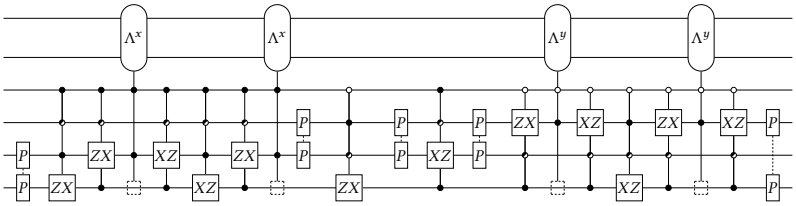
(112)(130) =



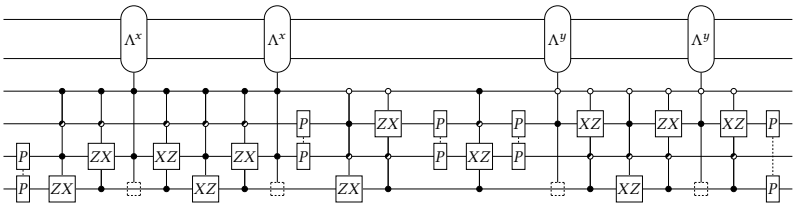
(111)
=



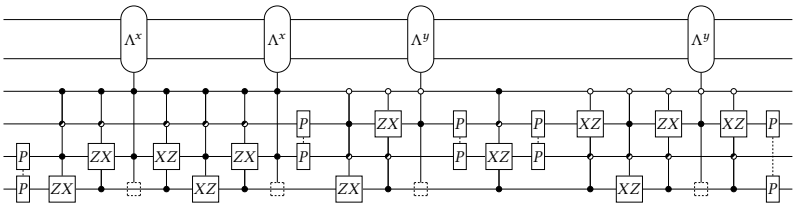
(244)
=



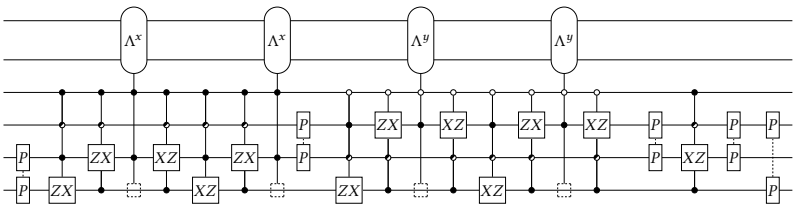
(215)(214)(242)
=



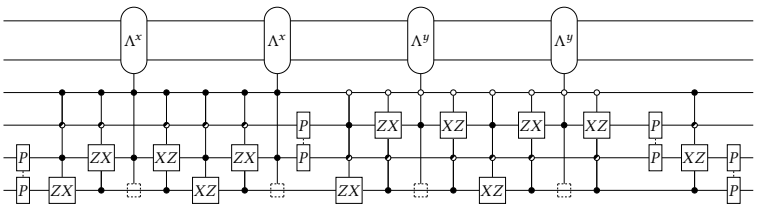
(328)
=



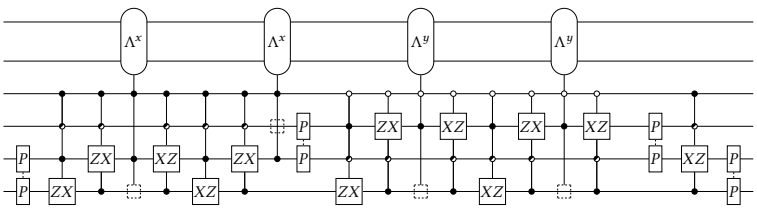
(215)(214)(242)
(244)(328)
=



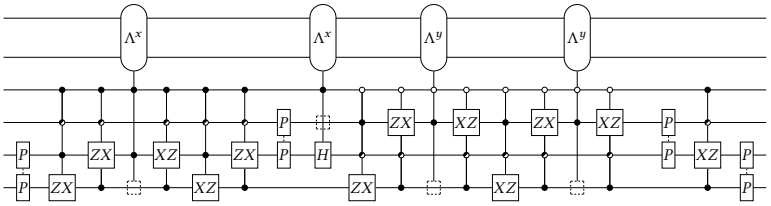
(112)(130)
=



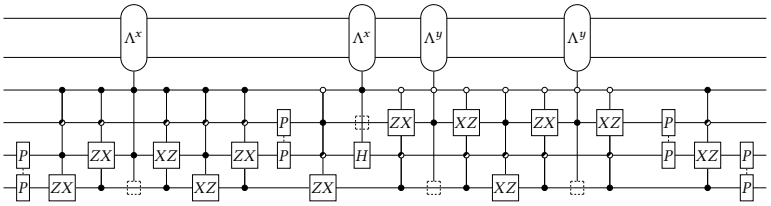
(274)
=



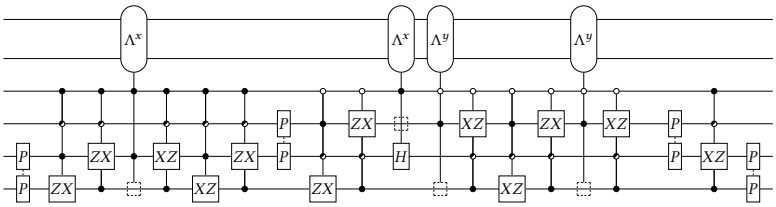
(111)(112)
=



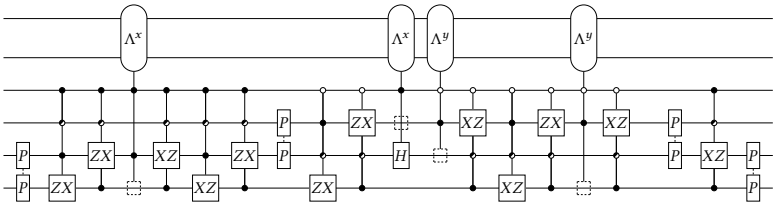
(325)
=



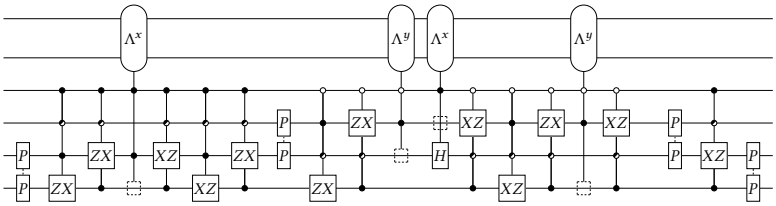
(324)
=



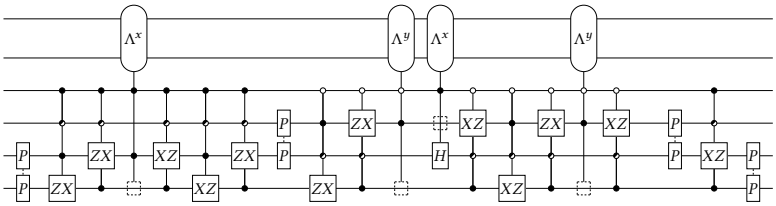
(274)
=



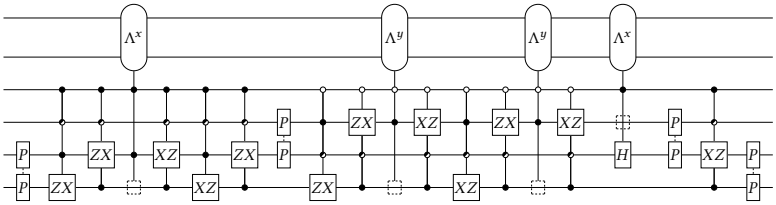
(338)
=



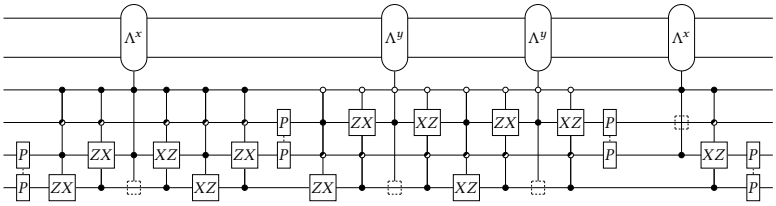
(274)
=



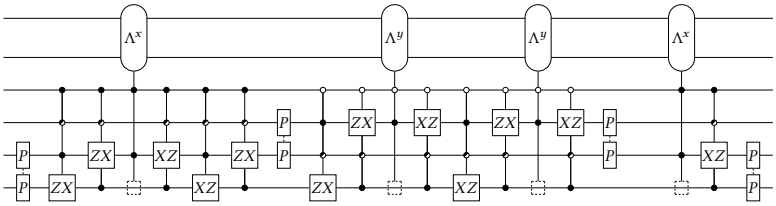
(324)(325)(274)(338)
=



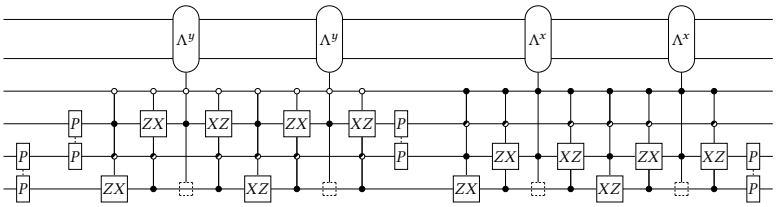
(112)(111)
=



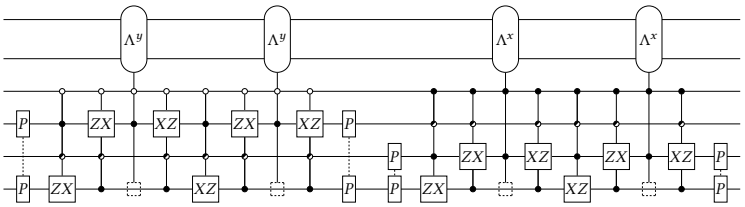
(274)
=



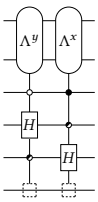
与.....类似
前面的步骤,
还使用了（245）[21]
=



(130)
=

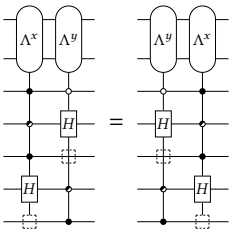


(81)(214)(320)
=



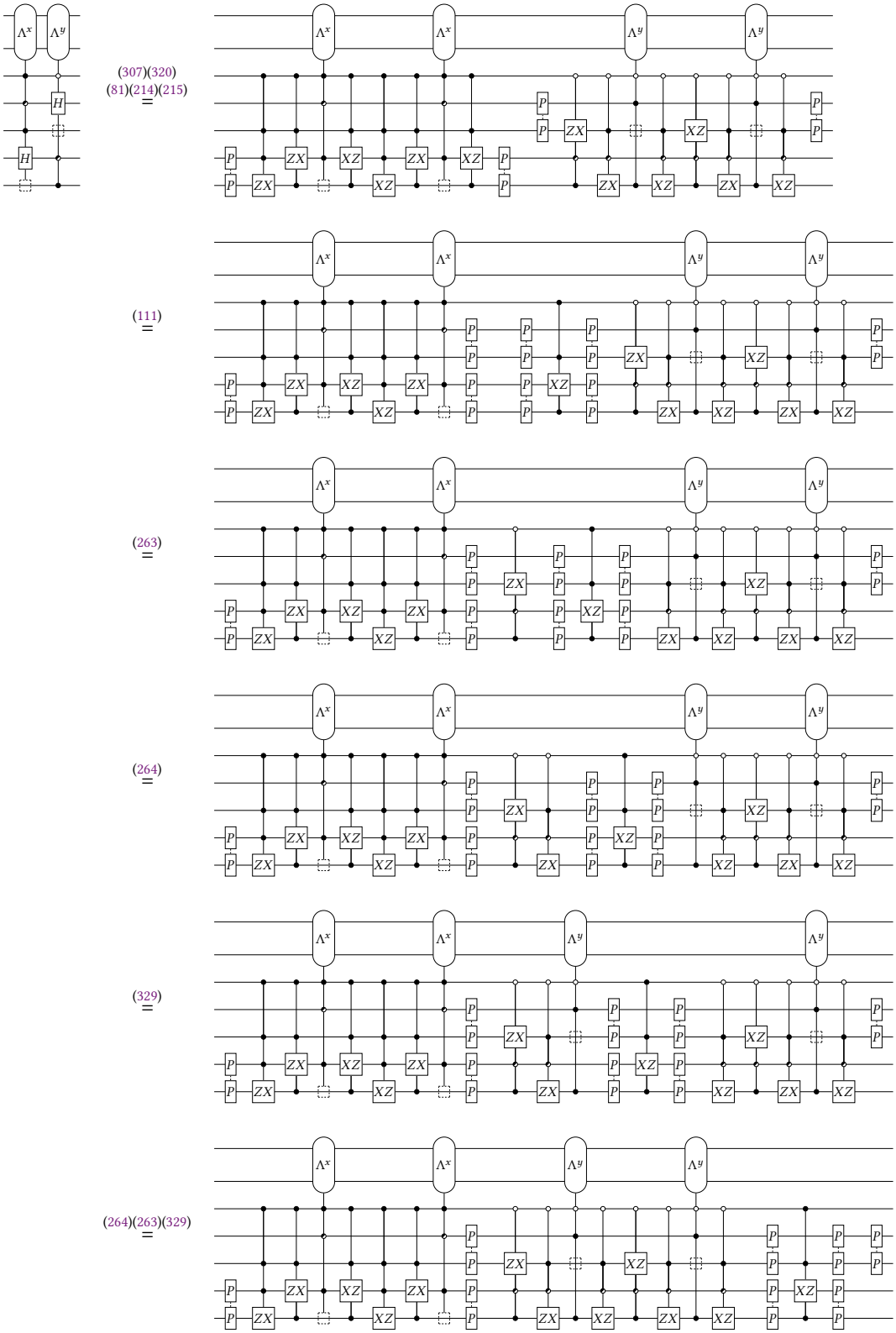
方程证明 (343)：根据方程（307）和（313），不失一般性，假设 x和 y仅最后一位不同；根据方程（81），不失一般性，假设该位在 1 中为 x，而在 0 中为 y。此外，根据方程（316），不失一般性，假设这些 's 前面的控制位均为黑色。因此，只需证明该方程的以下变体：

$\forall x,\ y \in \{0,\ 1\}^n$ 其中 $x \neq y$,

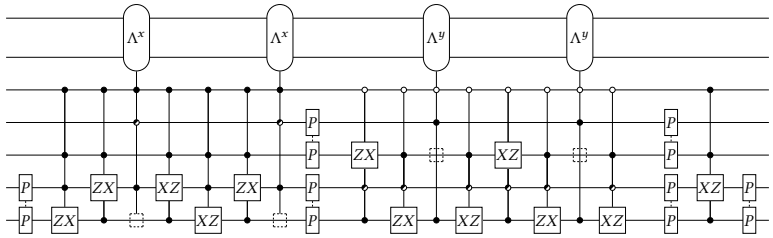


[21]注意，可以像将 $\Lambda^{x11}(-I)$通过 $\Lambda^{01b}ZX$ 一样，将 $\Lambda^{0a1}ZX$和 $\Lambda^{0a1}XZ$量子门通过 $\Lambda^{y01}(-I)$。

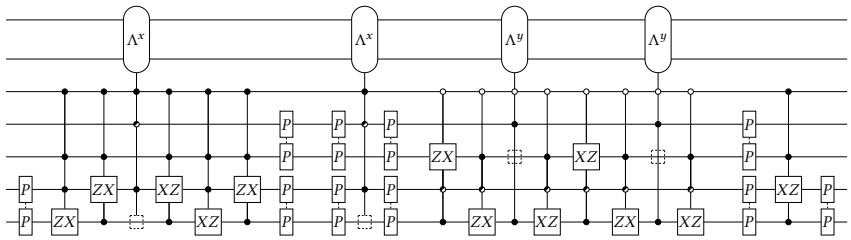
并且我们有



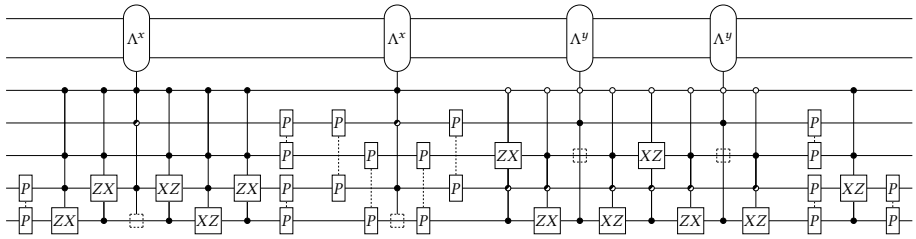
(111)
=



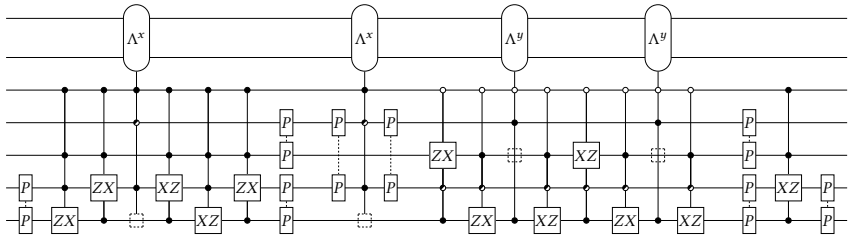
(111)
=



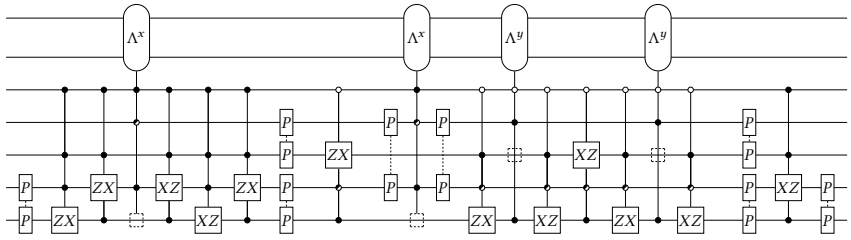
(246)
=



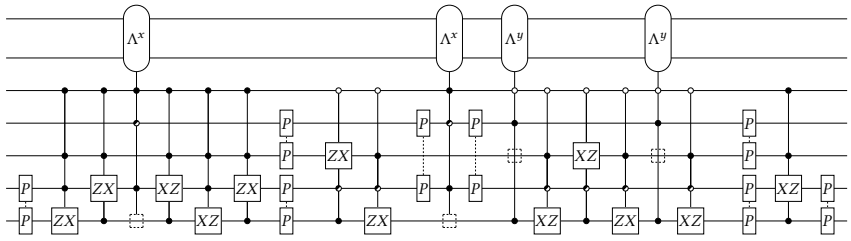
(308)(111)
=



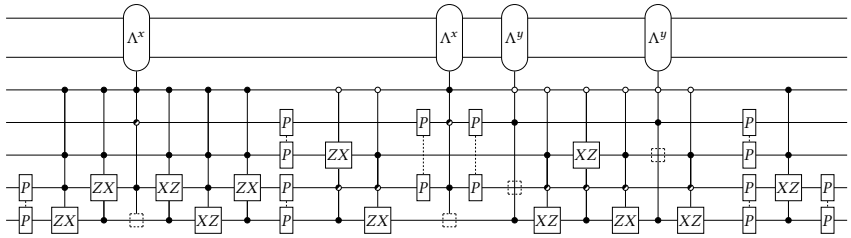
(331)
=



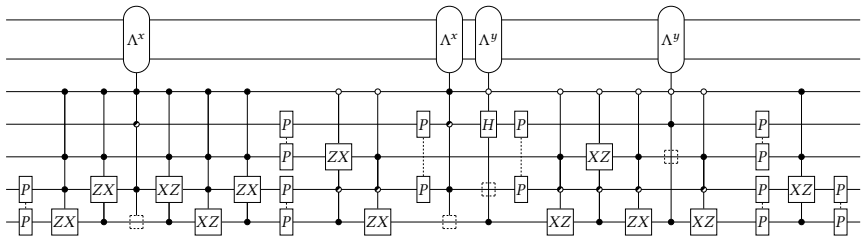
(332)
=



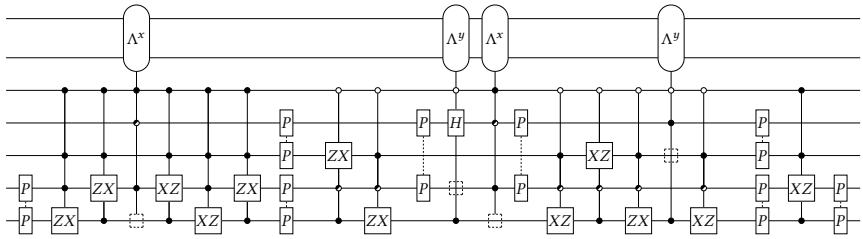
(274)
=



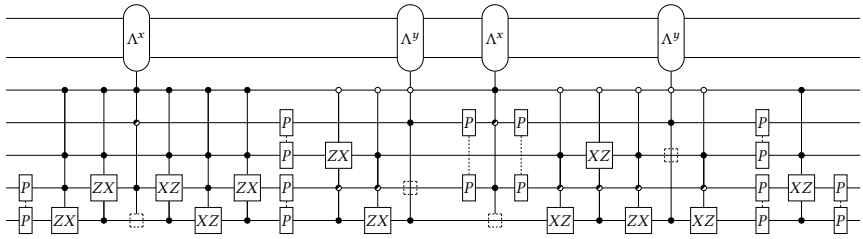
(307)(111)
=



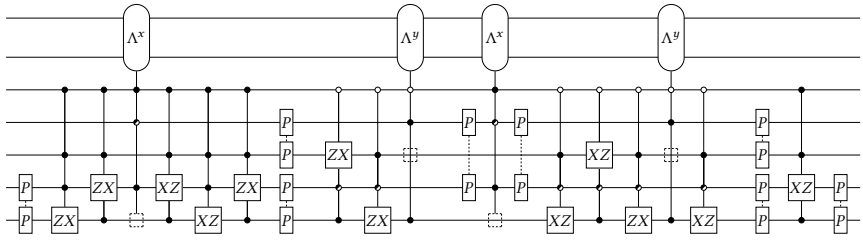
(339)
=



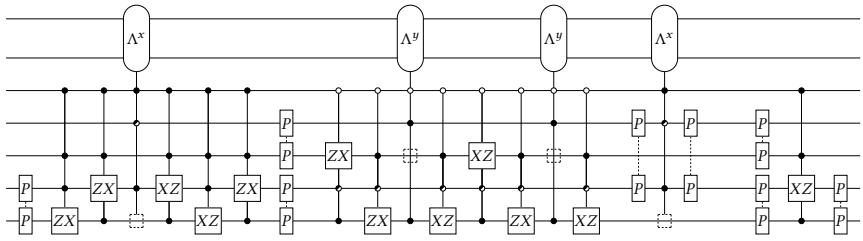
(111) (307)
=



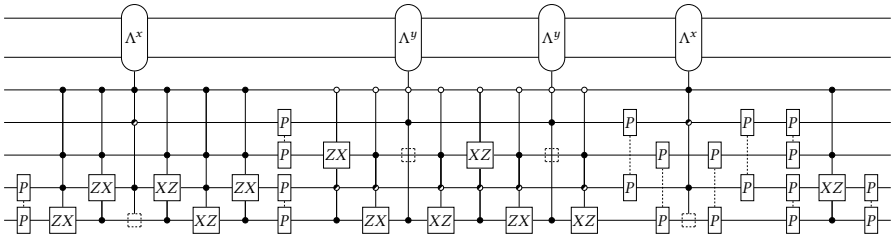
(274)
=



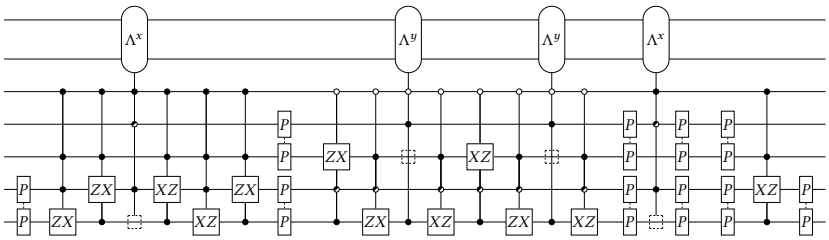
(332)(331)(274)
(307)(111)(339)
=



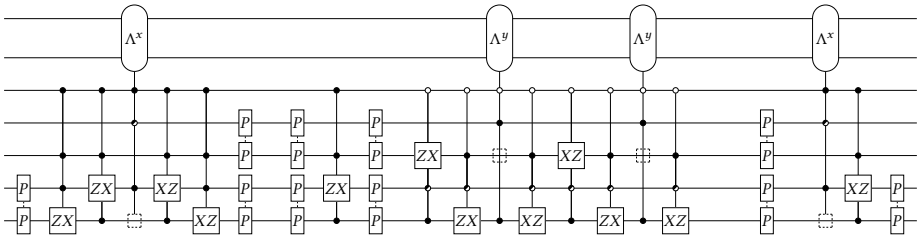
(111)(308)
=



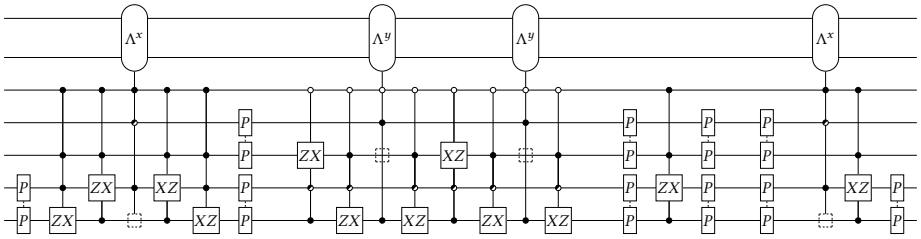
(246)
=



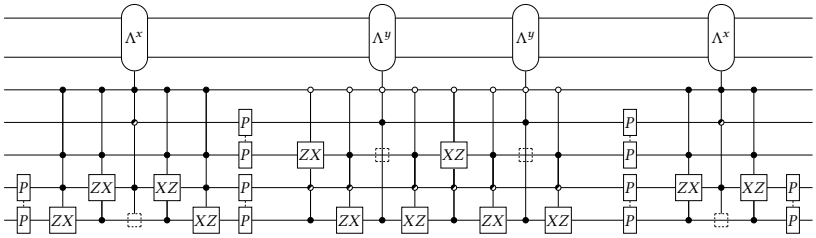
(111)
=



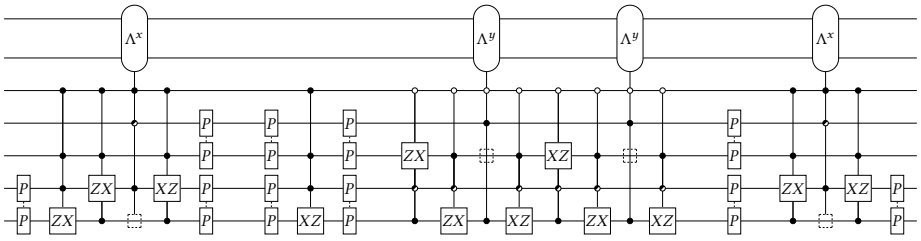
与
之前
=



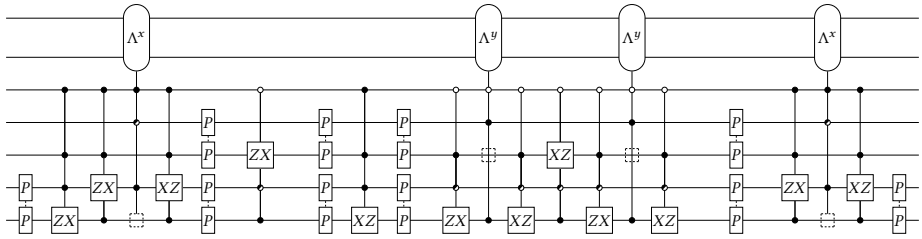
(111)
=



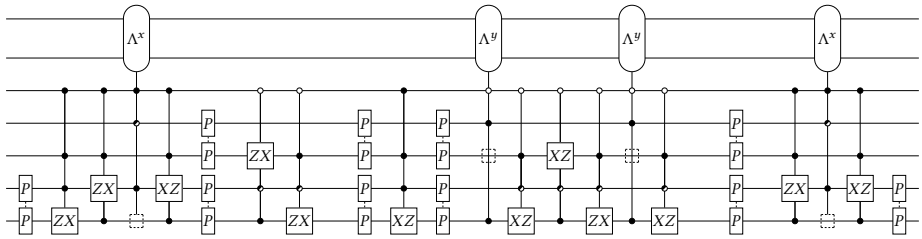
(111)
=



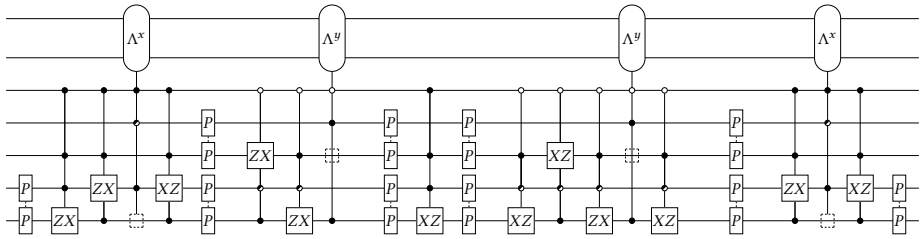
(265)
=



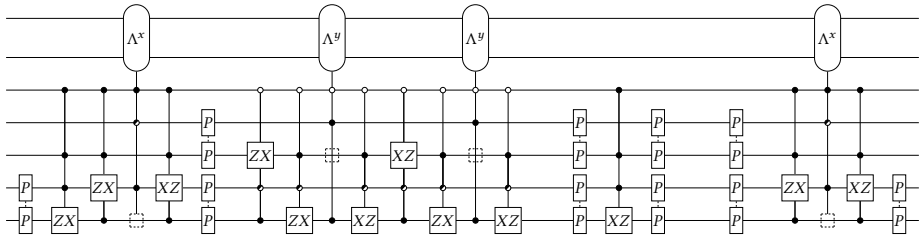
(266)
=



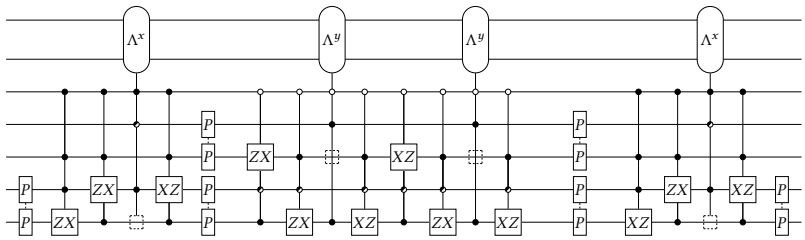
(330)
=



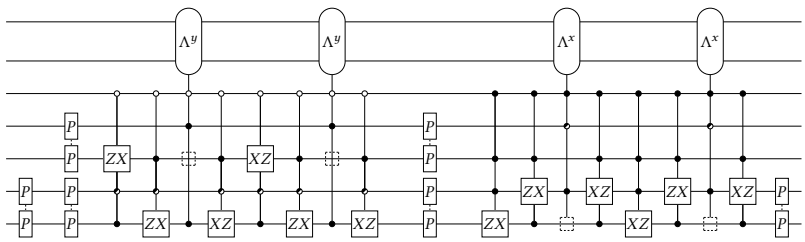
(266) (265) (330)
=

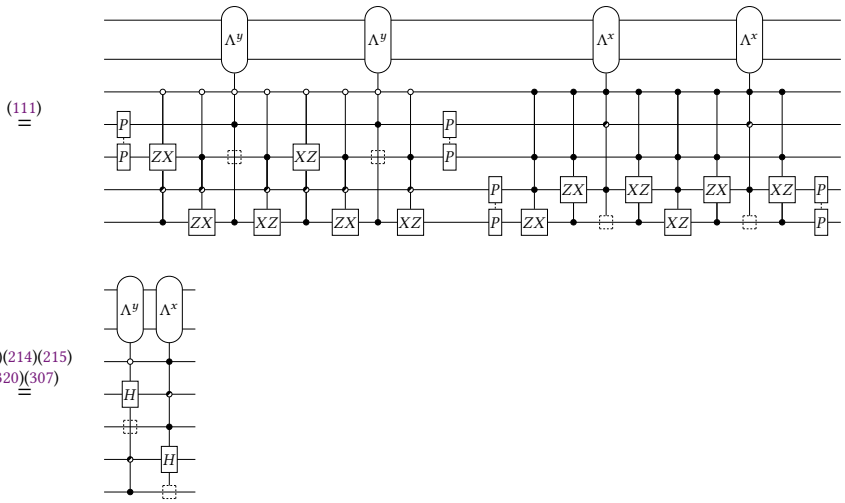


(111)
=

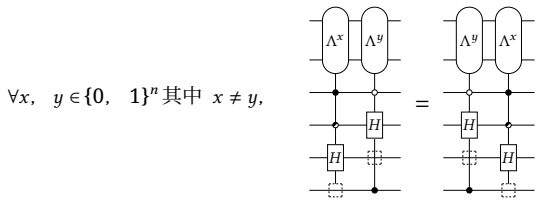


与.....相同
前面的步骤
=

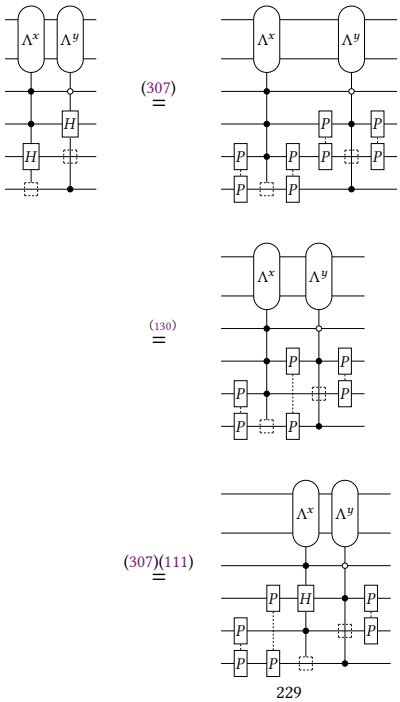




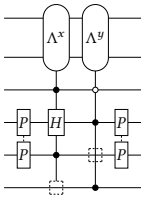
方程证明 (344)： 根据方程 (307) 和 (313)，不失一般性地，我们可以假设 x 和 y 仅在最后一位上不同；根据方程 (81)，不失一般性地，我们可以假设该位在 1 中为 x，在 0 中为 y。此外，根据方程 (316)，不失一般性地，我们可以假设前面的控制为黑色。因此，只需证明该方程的以下变体： □



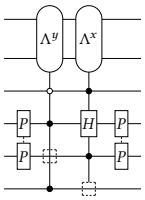
然后我们区分 H 前面的控制是黑色还是白色。如果是黑色，那么我们有



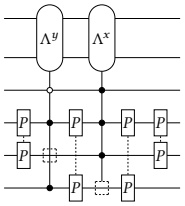
(112)(130) =



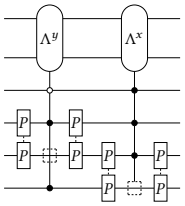
(339) =



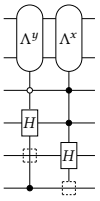
(307) =



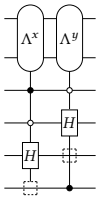
(112)(130) =



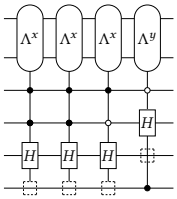
(307) =



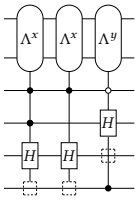
如果它是白色的，那么我们就有



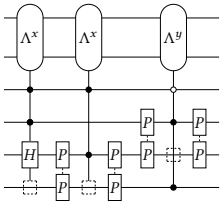
(312) =



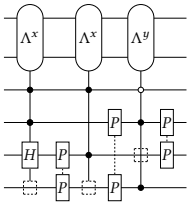
(310) =



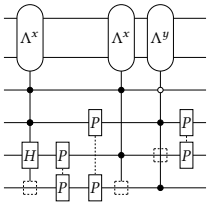
(307) =



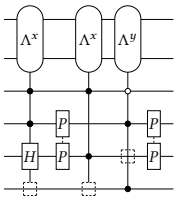
$\overset{(130)}{=}$



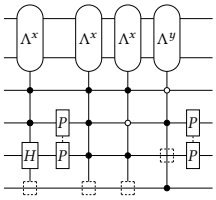
$\overset{(308)}{=}$



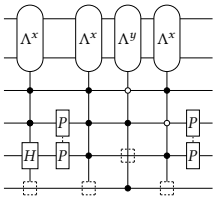
$\overset{(112)(130)}{=}$



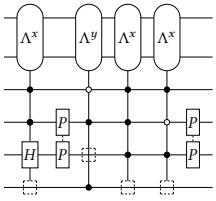
$\overset{(309)}{=}$



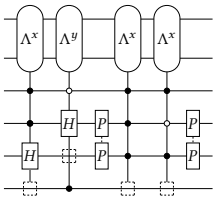
$\overset{(336)}{=}$

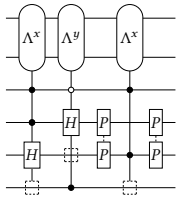


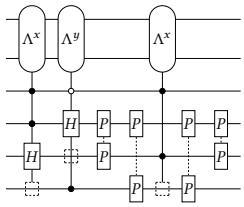
$\overset{(336)}{=}$

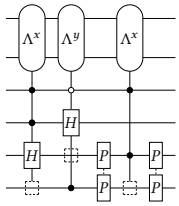


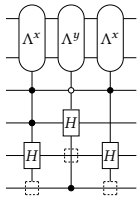
$\overset{(111)\ (307)}{=}$

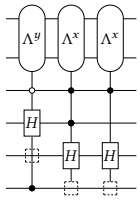


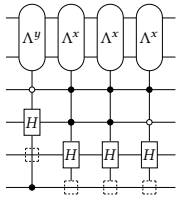
(309)
=


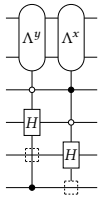
(111)(308)
=


(112)(130)
=


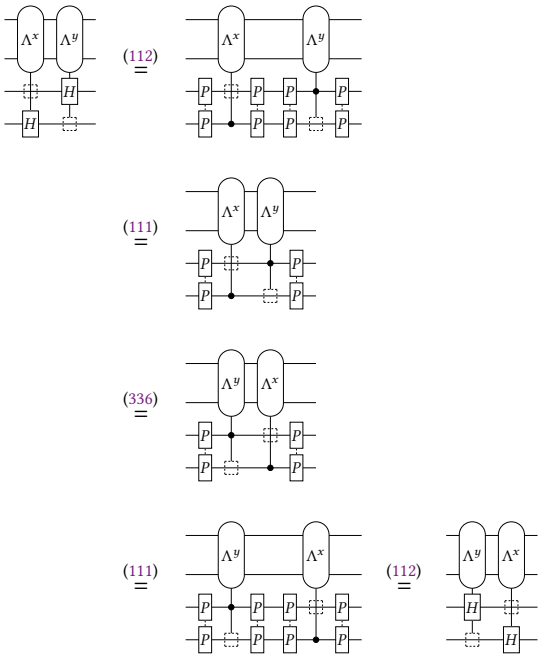
=


黑色外壳
=


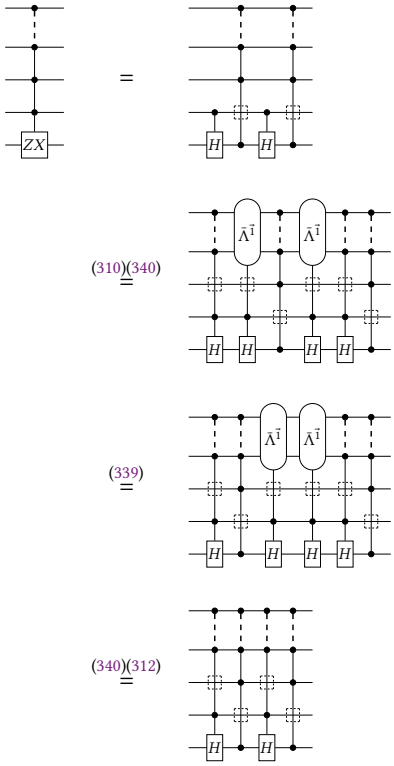
(310)
=


(312)
=


方程证明 (345)：



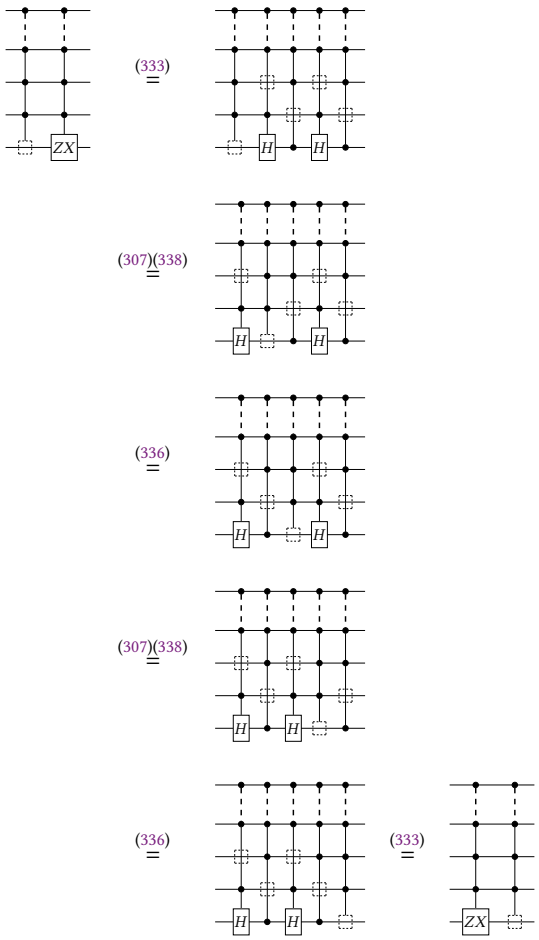
方程证明 (333)：



方程证明 (334)： 方程 (334) 直接由方程 (333) 和引理 B.5 (与方程 (311)、(312) 及 (317) 一起使用）推出。

方程的证明 (346) 至 (352)：这些方程中涉及一个或两个量子比特的特定情形，可直接由引理 7.1 和 7.6,[22] 因此，我们只需讨论至少涉及三个量子比特的情形。

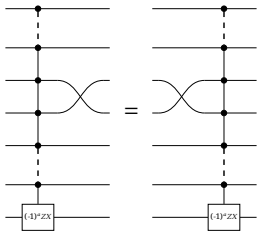
根据方程 (333) 和 (334)（如果存在白色控制，还要结合方程（81）以及可能的方程 (315) 和/或 (316)），任意黑色控制和白色控制组合的多重控制 ZX 或 XZ 门，都可以写成带孔的多重控制（$-I$）门和 H 门的乘积。因此，只要白色控制之前有黑色控制，我们就可以从方程 (335) 至 (345) 推导出方程 (346) 至 (352)，也就是说，除方程 (346) 和 (351) 的特定情形 $x = y$ 外，所有情形都成立。对于方程 (351)，当 $a = b$ 时，该特定情形是平凡的；当 $a \neq b$ 时，则可直接由方程（317）得到。因此，只需处理方程 (346) 的这一情形。根据方程（81），不失一般性地，我们可以假设 x（因此 y 也）是仅由 1 构成的向量；根据引理 B.5（结合方程（317）使用），我们可以不失一般性地假设 $a = 0$。于是有



□

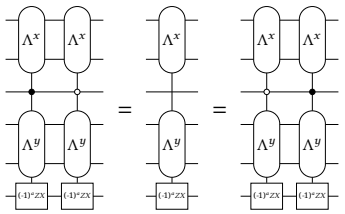
D.8 多重控制 ZX 和 XZ 量子门的性质

引理 D.14。以下方程是图 4中方程的推论：



(353)

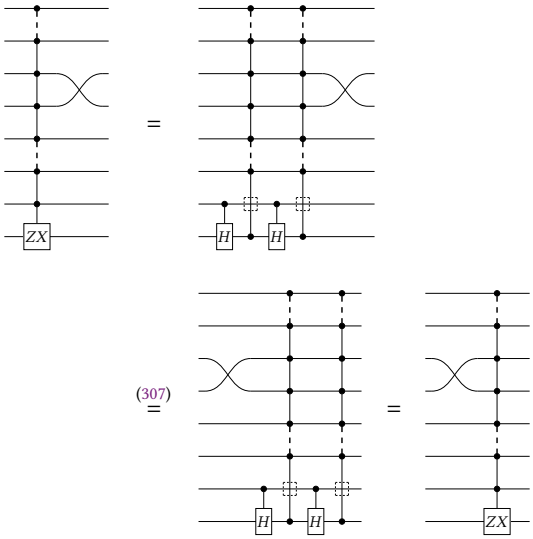
[22]可以注意到，这些情形仅与方程（346）和（351）相关。



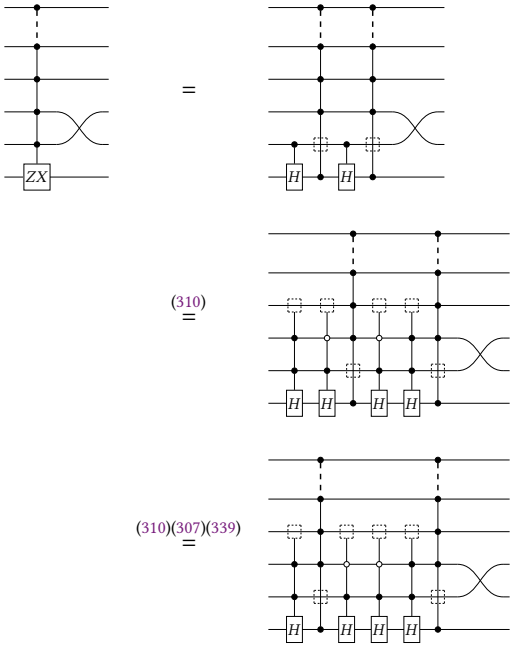
(354)

证明。

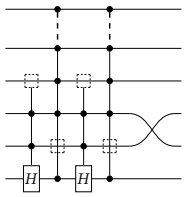
方程证明 (353)： 根据引理 B.5 （结合方程 (317）使用），我们可以不失一般性地假设 $a = 0$。该方程的三量子比特情形（交换上方或下方没有控制位）正是方程 (127)。如果交换下方至少有一个控制位，则有



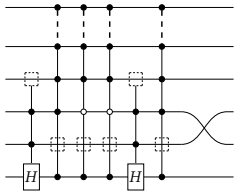
最后，如果交换下方没有控制，但上方至少有一个控制，则有



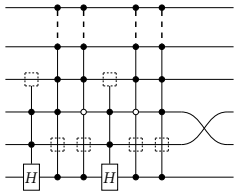
(312)
=



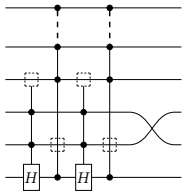
(311)
=



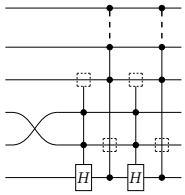
(310)(307)(339)
=



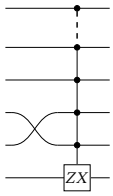
(309)
=



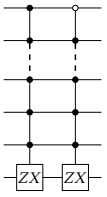
(274)(313)
=



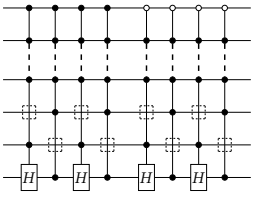
相同于
前面的步骤
=



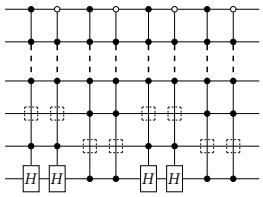
方程证明 (354)： 根据引理 B.5 (结合方程 (317))，不失一般性地，我们可以假设 $a = 0$，并且根据方程 (353)，不失一般性地，我们可以假设 $x = \epsilon$。若 y的长度为 0，则结论由引理 7.6得出。若 y的长度为 1，则结论由方程 (136) 和 (137) 以及方程 (81) 得出。若 y的长度至少为 2，则根据方程 (81)，不失一般性地，我们可以假设它是仅由 1 组成的向量。于是有



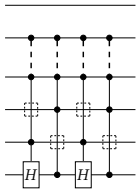
(333)
=



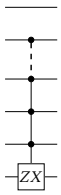
(335)(340)(307)(339)
=



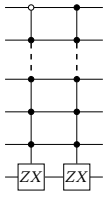
(309)(310)
=



(333)
=



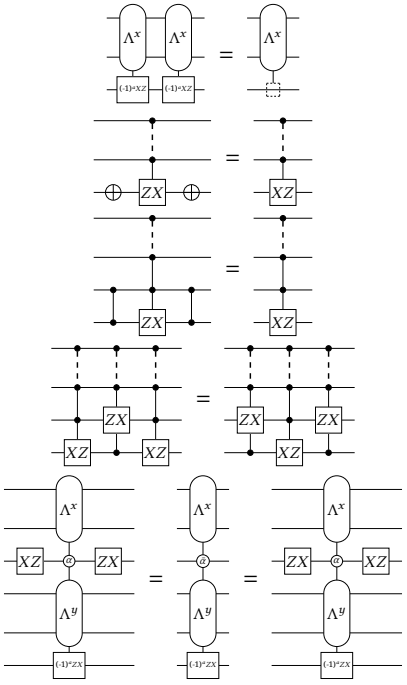
类似于
前面的步骤
=



□

D.9 量子比特上的其他有用辅助方程

引理 D.15. 以下方程是图 *4* 中方程的推论：



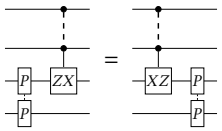
(355)

(356)

(357)

(358)

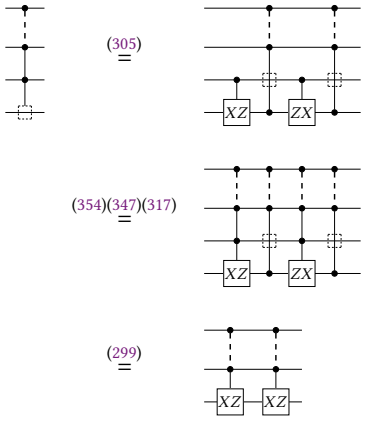
(359)



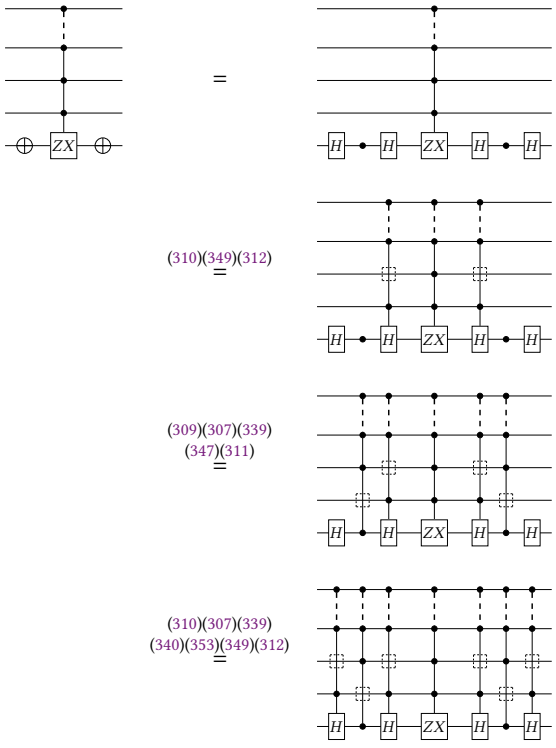
(360)

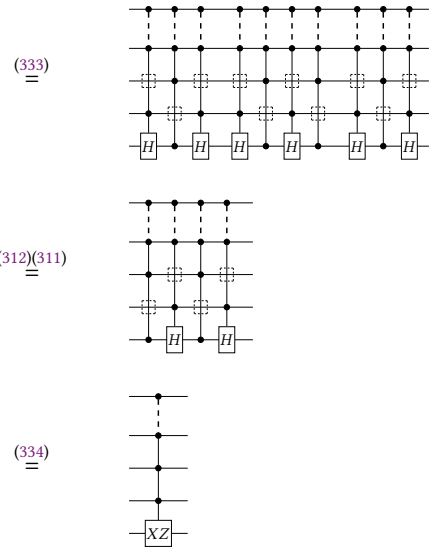
证明。

方程证明 (355)： 如果 x 的长度为 0，则结论由引理 7.1 得出。如果 x 的长度至少为 1，那么根据方程 (81)，不失一般性地假设 x 是仅由 1 组成的向量；并且根据引理 B.5 (结合方程 (317))，不失一般性地假设 $a = 0$。于是我们有

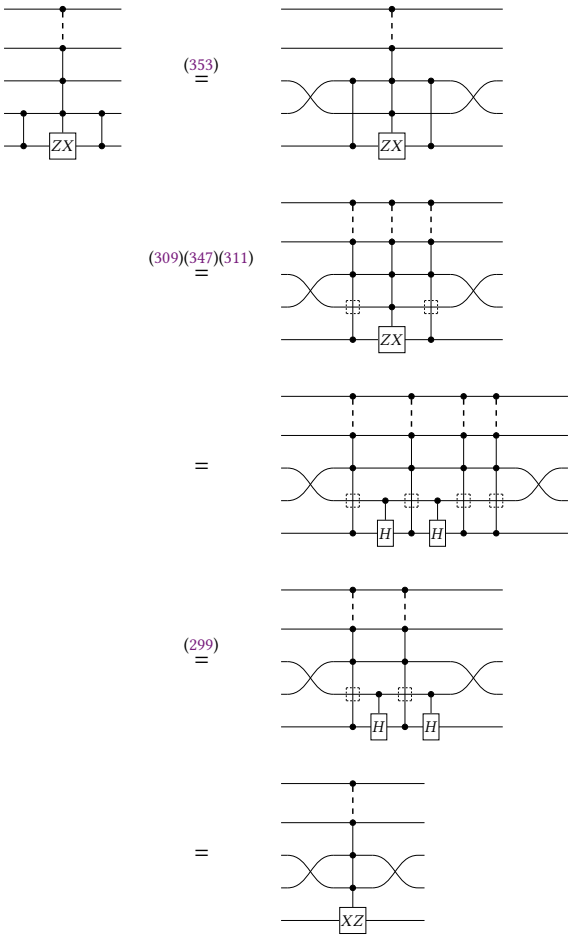


方程证明 (356)： 方程的双量子比特情形（两个底部量子比特上方没有控制位）由引理 7.6 得出。在其他情形（上方至少有一个控制位）中，我们有

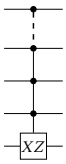




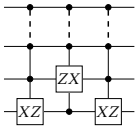
方程 (357)的证明： 该方程的双量子比特情形（即两个底部量子比特上方没有控制位）可由引理 7.6推出。在其他情形下（即上方至少有一个控制位时），我们有



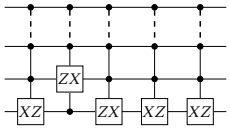
(353)
=



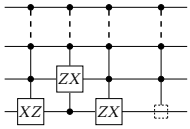
方程证明 (358):



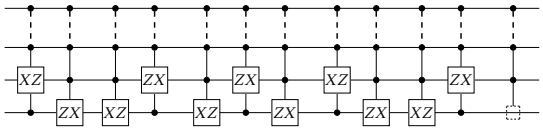
(317)
=



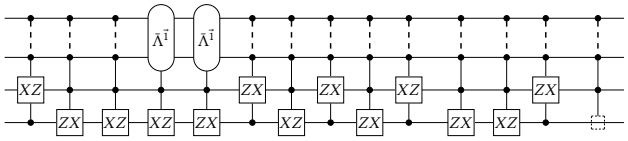
(355)
=



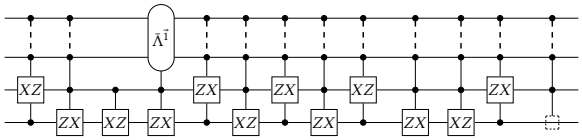
(317)
=



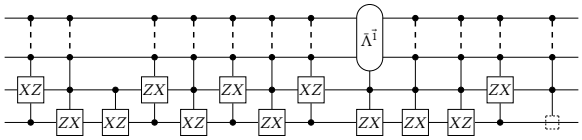
(317)(351)
=



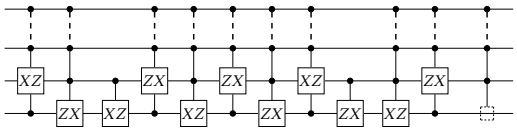
(351)(354)
=



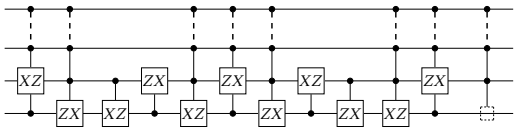
(351)(352)
=



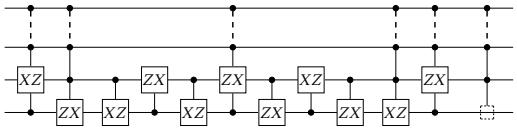
(351)(354)
=



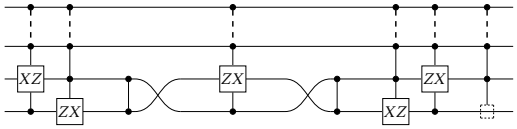
类似于
最后 4 个步骤
=



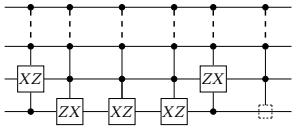
再次相似
=



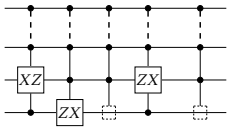
(115)(116)
=



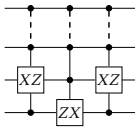
(357)
=



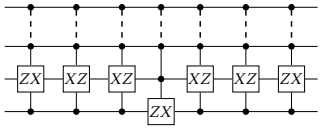
(355)
=



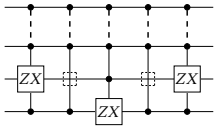
(299)
=



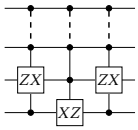
(317)
=



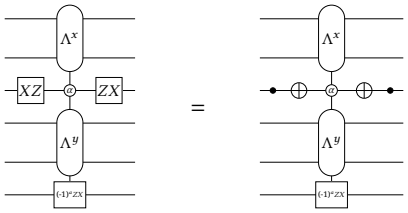
(355)
=



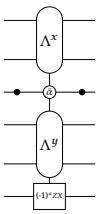
(299)
=

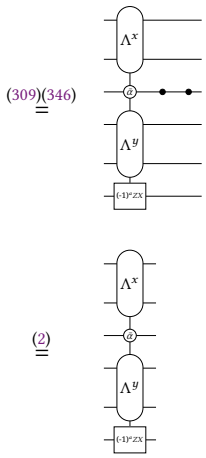


方程证明 (359)*:*

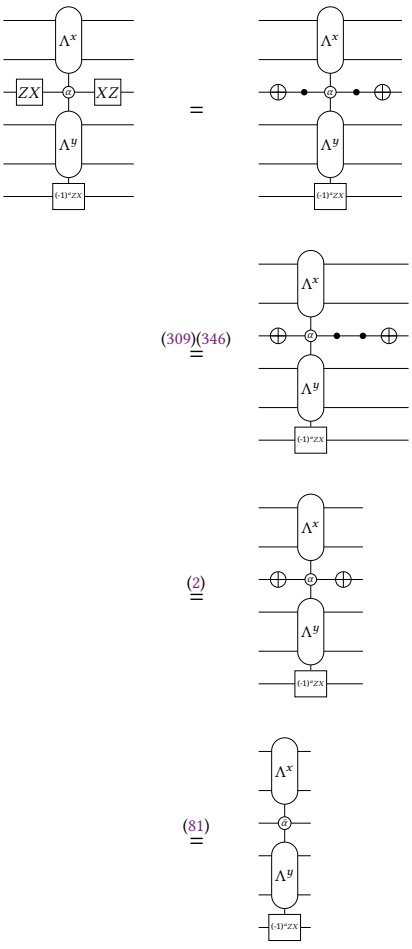


(81)
=

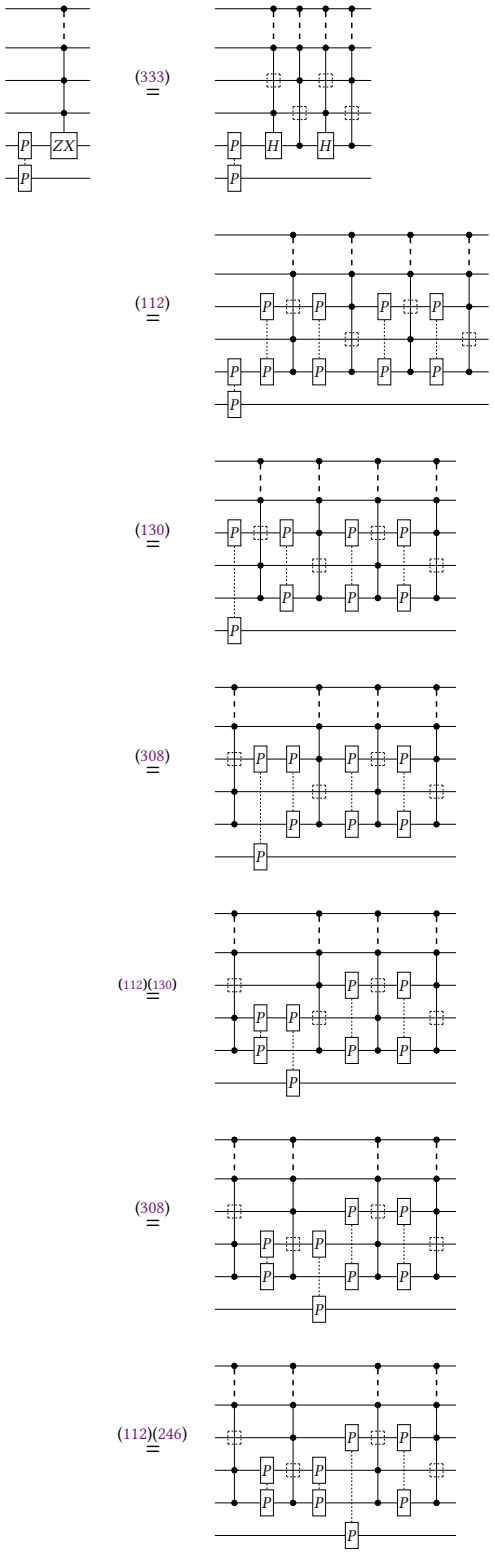



(309)(346)
=
Λ^x
a
Λ^y
(-1)^zx
(2)
=
Λ^x
a
Λ^y
(-1)^zx

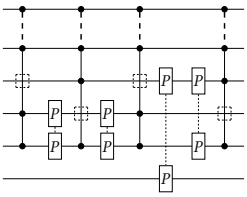
and


Λ^x
ZX
a
XZ
Λ^y
(-1)^zx
=
Λ^x
a
Λ^y
(-1)^zx
(309)(346)
=
Λ^x
a
Λ^y
(-1)^zx
(2)
=
Λ^x
a
Λ^y
(-1)^zx
(81)
=
Λ^x
a
Λ^y
(-1)^zx

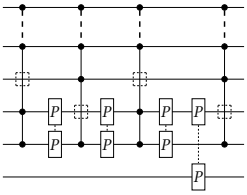
方程证明 (360)： 该方程的双量子比特情形（其中 ZX门没有控制位）可由引理 7.6 得出。该方程的三量子比特情形（其中 ZX门恰有一个控制位）就是方程（129）。在其他情形下，我们有



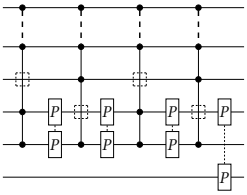
(308)
=



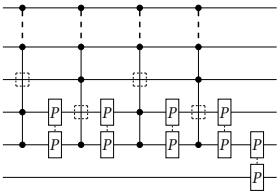
(112)(130)
=



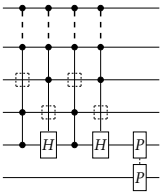
(308)
=



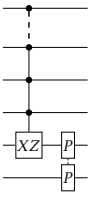
(112)(130)
=



(112)
=



(334)(353)
=



□

E 一般情形下的完备性

E.1 $\Sigma_{a,b,c,d}$ 和 $\Sigma_{a,b,c,d}$的定义

我们需要给出 P_N 上的两个字 $\Sigma_{a,b,c,d}$和 $\Sigma'_{a,b,c,d}$，它们不包含任何形如 $\left(H_{[e,f]}H_{[g,h]}\right)$的生成元，并满足 $\left[\!\left[\Sigma'_{a,b,c,d}\right]\!\right] = \left[\!\left[\Sigma_{a,b,c,d}\right]\!\right]^{-1}$；此外，存在 $\mu \notin \{0,1,3,2\}$ 以及一个置换矩阵 σ，分别将 $|0\rangle\ |1\rangle\ |3\rangle\ |2\rangle$映射为 $|a\rangle\ |b\rangle\ |c\rangle\ |d\rangle$，使得$\left[\!\left[\Sigma_{a,b,c,d}\right]\!\right] = \sigma$ 或$\left[\!\left[\Sigma_{a,b,c,d}\right]\!\right] = \sigma \circ \left[\!\left[(-1)_{[\mu]}\right]\!\right]$。以下定义满足这些性质：

定义 E.1。

$$\Sigma_{a,b,c,d} = \left((-1)_{[m_0]}X_{[a,i_0]}\right)^{e_0}\left((-1)_{[m_1]}X_{[b,i_1]}\right)^{e_1}\left((-1)_{[m_2]}X_{[c,i_2]}\right)^{e_2}\left((-1)_{[m_3]}X_{[d,2]}\right)^{e_3}$$

$$\Sigma'_{a,b,c,d} = \left((-1)_{[4]}X_{[d,2]}\right)^{e_3}\left((-1)_{[m'_2]}X_{[c,i_2]}\right)^{e_2}\left((-1)_{[m'_1]}X_{[b,i_1]}\right)^{e_1}\left((-1)_{[m'_0]}X_{[a,i_0]}\right)^{e_0}$$

其中

- $e_3 = \begin{cases}1 & if\, d \neq 2\\ 0 & if\, d = 2\end{cases}$
- $m_3 = m'_2 = \tau_{d,2}^{e_3}(4)$
- $i_2 = \tau_{d,2}^{e_3}(3)$
- $e_2 = \begin{cases}1 & if\, c \neq i_2\\ 0 & if\, d = i_2\end{cases}$
- $m_2 = m'_1 = \tau_{c,i_2}^{e_2}(\tau_{d,2}^{e_3}(4))$
- $i_1 = \tau_{c,i_2}^{e_2}(\tau_{d,2}^{e_3}(1))$
- $e_1 = \begin{cases}1 & if\, b \neq i_1\\ 0 & if\, b = i_1\end{cases}$
- $m_1 = m'_0 = \tau_{b,i_1}^{e_1}(\tau_{c,i_2}^{e_2}(\tau_{d,2}^{e_3}(4)))$
- $i_0 = \tau_{b,i_1}^{e_1}(\tau_{c,i_2}^{e_2}(\tau_{d,2}^{e_3}(0)))$
- $e_0 = \begin{cases}1 & if\, a \neq i_0\\ 0 & if\, a = i_0\end{cases}$
- $m_0 = \tau_{a,i_0}^{e_0}(\tau_{b,i_1}^{e_1}(\tau_{c,i_2}^{e_2}(\tau_{d,2}^{e_3}(4))))$

其中 $\tau_{k,i}\colon\{0,\ldots,2^n-1\}\to\{0,\ldots,2^n-1\}$ 表示交换 k 和 i 的换位，并且我们允许在 $\left((-1)_{[m]}X_{[k,i]}\right)^e$ 中使用 $k=i$，只要 $e=0$（在这种情况下它仍然等于单位元）。

E.2 引理 8.4 的证明

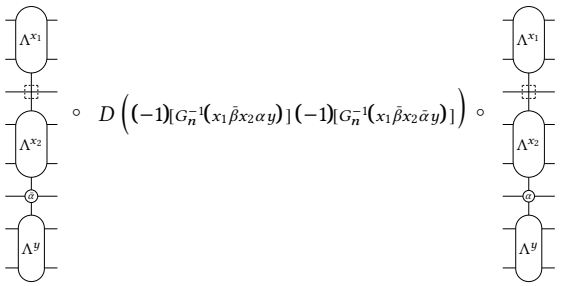
我们对 $\left|G_n^{-1}(x0y)-G_n^{-1}(x1y)\right|$ 进行归纳。注意，根据格雷码的一个基本性质，[23]，因为 $x0y$ 和 $x1y$ 相差 b
y 为奇数个比特（即 1 个），$\left|G_n^{-1}(x0y)-G_n^{-1}(x1y)\right|$ 必为奇数。

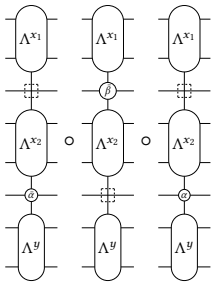
如果 $\left|G_n^{-1}(x0y)-G_n^{-1}(x1y)\right|=1$，则结论可直接由定义 8.3得到。

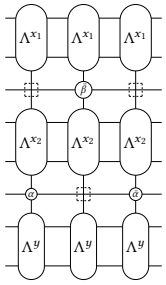
如果 $\left|G_n^{-1}(x0y)-G_n^{-1}(x1y)\right|\geq 3$，令 $\alpha\in\{0,1\}$ 满足 $G_n^{-1}(x\alpha y)<G_n^{-1}(x\bar{\alpha}y)$。根据格雷码的性质，$G_n(G_n^{-1}(x\alpha y)+1)$ 与 $x\alpha y$恰好相差一个比特（该比特位于 x或 y中，因为 $G_n^{-1}(x\alpha y)+1\neq G_n^{-1}(x\bar{\alpha}y)$），此外，$G_n(G_n^{-1}(x\bar{\alpha}y)-1)$ 与 $x\bar{\alpha}y$也相差同一个比特。我们假设变化的比特位于 x中（若位于 y中，证明相同）。换句话说，存在两个比特串 $x_1\in\{0,1\}^{k_1}$、$x_2\in\{0,1\}^{k_2}$以及一个比特 $\beta\in\{0,1\}$，使得 $x=x_1\beta x_2$、$G_n(G_n^{-1}(x\alpha y)+1)=x_1\bar{\beta}x_2\alpha y$以及 $G_n(G_n^{-1}(x\bar{\alpha}y)-1)=x_1\bar{\beta}x_2\bar{\alpha}y$。于是有

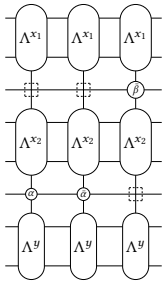
$$\begin{aligned}
& D\left((-1)_{[G_n^{-1}(x0y)]}(-1)_{[G_n^{-1}(x1y)]}\right)\\
=\ & \prod_{k=G_n^{-1}(x\alpha y)}^{\overleftarrow{G_n^{-1}(x\bar{\alpha}y)-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right)\\
=\ & D\left((-1)_{[G_n^{-1}(x\bar{\alpha}y)-1]}(-1)_{[G_n^{-1}(x\bar{\alpha}y)]}\right)\circ\prod_{k=G_n^{-1}(x\alpha y)+1}^{\overleftarrow{G_n^{-1}(x\bar{\alpha}y)-2}} D\left((-1)_{[k]}(-1)_{[k+1]}\right)\circ D\left((-1)_{[G_n^{-1}(x\alpha y)]}(-1)_{[G_n^{-1}(x\alpha y)+1]}\right)\\
=\ & D\left((-1)_{[G_n^{-1}(x\bar{\alpha}y)-1]}(-1)_{[G_n^{-1}(x\bar{\alpha}y)]}\right)\circ D\left((-1)_{[G_n^{-1}(x\alpha y)+1]}(-1)_{[G_n^{-1}(x\bar{\alpha}y)-1]}\right)\circ D\left((-1)_{[G_n^{-1}(x\alpha y)]}(-1)_{[G_n^{-1}(x\alpha y)+1]}\right)\\
=\ & D\left((-1)_{[G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y)]}(-1)_{[G_n^{-1}(x_1\beta x_2\bar{\alpha}y)]}\right)\circ D\left((-1)_{[G_n^{-1}(x_1\bar{\beta}x_2\alpha y)]}(-1)_{[G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y)]}\right)\circ D\left((-1)_{[G_n^{-1}(x_1\beta x_2\alpha y)]}(-1)_{[G_n^{-1}(x_1\bar{\beta}x_2\alpha y)]}\right)
\end{aligned}$$

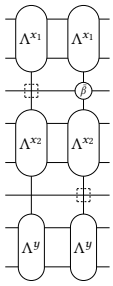
[23]也就是说，自然数的奇偶性始终等于其格雷码中 1 的个数的奇偶性。

$=$ 

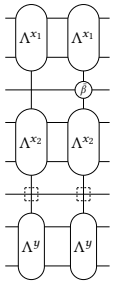
归纳法假设 $=$ 

$=$ 

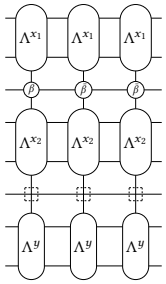
(307)(336) $=$ 

(309) $=$ 

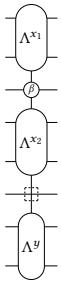
$\overset{(274)}{=}$



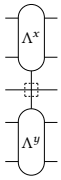
$\overset{(309)}{=}$



$\overset{(311)}{=}$



$=$



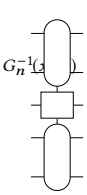
E.3 引理 8.5 的证明

我们对 $\left|G_n^{-1}(x0y) - G_n^{-1}(x1y)\right|$ 进行归纳。注意，出于与引理 8.4 的证明中相同的原因，$\left|G_n^{-1}(x0y) - G_n^{-1}(x1y)\right|$ 必定是奇数。

If $\left|G_n^{-1}(x0y) - G_n^{-1}(x1y)\right| = 1$，则结果可直接由定义 8.3.

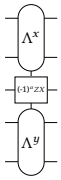
注意到，对于任意 $D\left(-1_{[a]}X_{[b,a]}\right) = D\left(-1_{[b]}X_{[a,b]}\right) = D\left(-1_{[b]}X_{[b,a]}\right)$ a b $D\left(-1_{[a]}X_{[a,b]}\right) =$，，有 ( ) ( ) 与 ( ) ( )。因此，我们要证明的结果等价于

Λ^x量子计算 $\vdash D\left((-1)_{[G_n^{-1}(x\alpha y)]}X_{[G_n^{-1}(x\alpha y)\ G_n^{-1}(x\alpha y)]}\right) =_{(-1)^{\alpha}XZ}\Lambda^y$



若 $\left|G_n^{-1}(x0y) - G_n^{-1}(x1y)\right| \geq 3$，令 $\alpha \in \{0, 1\}$ 满足 $G_n^{-1}(x\alpha y) < G_n^{-1}(x\bar{\alpha}y)$.

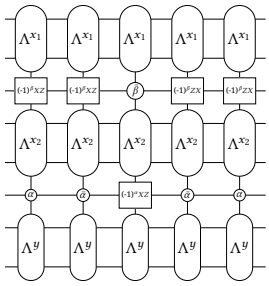
$$\mathrm{QC} \vdash D\left((-1)^{[G_n^{-1}(x\bar{\alpha}y)]}X_{[G_n^{-1}(x\alpha y)\, G_n^{-1}(x\bar{\alpha}y)]}\right) =$$



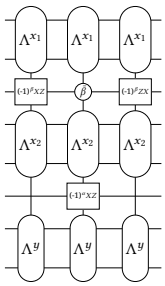
与引理 8.4 的证明类似，由格雷码的性质可知，$G_n(G_n^{-1}(x\alpha y) + 1)$ 与 $x\alpha y$恰好相差一个比特（该比特要么在 x中，要么在 y中，因为 $G_n^{-1}(x\alpha y) + 1 \neq G_n^{-1}(x\bar{\alpha}y)$），并且 $G_n(G_n^{-1}(x\bar{\alpha}y) - 1)$ 与 $x\bar{\alpha}y$相差同一个比特。我们再次假设变化的比特位于 x（若它位于 y，证明相同）。换言之，存在两个比特串 $x_1 \in \{0,1\}^{k_1}$、$x_2 \in \{0,1\}^{k_2}$以及一个比特 $\beta \in \{0,1\}$，使得 $x = x_1\beta x_2$、$G_n(G_n^{-1}(x\alpha y) + 1) = x_1\bar{\beta}x_2\alpha y$以及 $G_n(G_n^{-1}(x\bar{\alpha}y) - 1) = x_1\bar{\beta}x_2\bar{\alpha}y$。于是我们有

$$\begin{aligned}
& D\left((-1)_{[G_n^{-1}(x\alpha y)]}X_{[G_n^{-1}(x\alpha y),G_n^{-1}(x\bar{\alpha}y)]}\right) \\
= \quad & D\left((-1)_{[G_n^{-1}(x\alpha y)+1]}X_{[G_n^{-1}(x\alpha y),G_n^{-1}(x\alpha y)+1]}\right) \circ D\left((-1)_{[G_n^{-1}(x\bar{\alpha}y)-1]}X_{[G_n^{-1}(x\bar{\alpha}y)-1,G_n^{-1}(x\bar{\alpha}y)]}\right) \circ \\
& D\left((-1)_{[G_n^{-1}(x\alpha y)+1]}X_{[G_n^{-1}(x\alpha y)+1,G_n^{-1}(x\bar{\alpha}y)-1]}\right) \circ \\
& D\left((-1)_{[G_n^{-1}(x\bar{\alpha}y)]}X_{[G_n^{-1}(x\bar{\alpha}y)-1,G_n^{-1}(x\bar{\alpha}y)]}\right) \circ D\left((-1)_{[G_n^{-1}(x\alpha y)]}X_{[G_n^{-1}(x\alpha y),G_n^{-1}(x\alpha y)+1]}\right) \\
= \quad & D\left((-1)_{[G_n^{-1}(x_1\bar{\beta}x_2\alpha y)]}X_{[G_n^{-1}(x_1\beta x_2\alpha y),G_n^{-1}(x_1\bar{\beta}x_2\alpha y)]}\right) \circ D\left((-1)_{[G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y)]}X_{[G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y),G_n^{-1}(x_1\beta x_2\bar{\alpha}y)]}\right) \circ \\
& D\left((-1)_{[G_n^{-1}(x_1\bar{\beta}x_2\alpha y)]}X_{[G_n^{-1}(x_1\bar{\beta}x_2\alpha y),G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y)]}\right) \circ \\
& D\left((-1)_{[G_n^{-1}(x_1\beta x_2\bar{\alpha}y)]}X_{[G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y),G_n^{-1}(x_1\beta x_2\bar{\alpha}y)]}\right) \circ D\left((-1)_{[G_n^{-1}(x_1\beta x_2\alpha y)]}X_{[G_n^{-1}(x_1\beta x_2\alpha y),G_n^{-1}(x_1\bar{\beta}x_2\alpha y)]}\right)
\end{aligned}$$

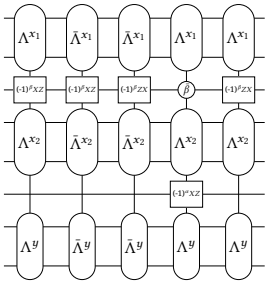
归纳法假设 =



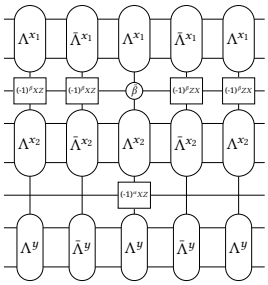
(354) =



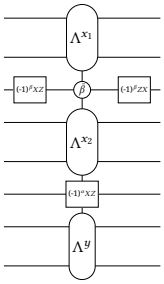
(317)(351)
=



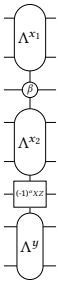
(352)
=

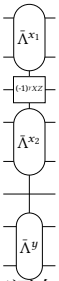
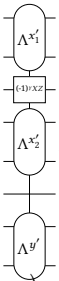


(351)(354)
=



(359)
=



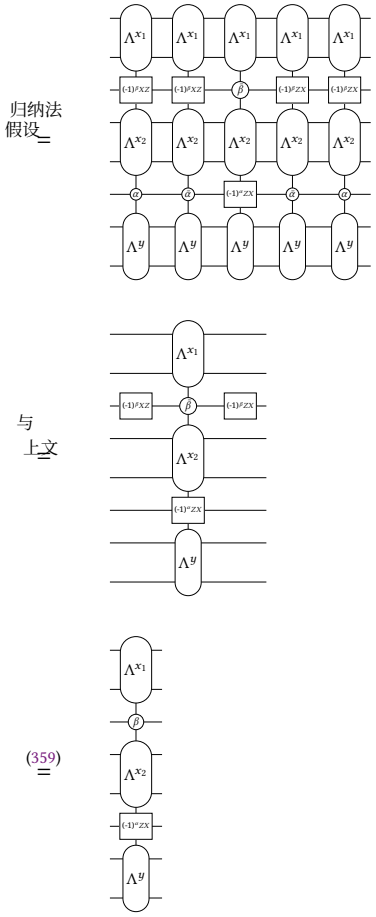
其中  是一个滥用记号的写法，表示 $\prod_{\substack{x'_1\in\{0,1\}^{k_1}\\ x'_2\in\{0,1\}^{k_2}\\ y'\in\{0,1\}^{\ell}\\ x'_1x'_2y\neq x_1x_2y}}$  ，其中乘积的顺序未作规定。

我们还有

$$D\left((-1)^{[G_n^{-1}(x\bar{\alpha}y)]}X_{[G_n^{-1}(x\alpha y)\ G_n^{-1}(x\bar{\alpha}y)]}\right)$$

$$=D\left((-1)^{[G_n^{-1}(x\alpha y)+1]}X_{[G_n^{-1}(x\alpha y)\ G_n^{-1}(x\alpha y)+1]}\right)\circ D\left((-1)^{[G_n^{-1}(x\bar{\alpha}y)-1]}X_{[G_n^{-1}(x\bar{\alpha}y)-1,G_n^{-1}(x\bar{\alpha}y)]}\right)\circ$$

$$D\left((-1)^{[G_n^{-1}(x\bar{\alpha}y)-1]}X_{[G_n^{-1}(x\alpha y)+1,G_n^{-1}(x\bar{\alpha}y)-1]}\right)\circ D\left((-1)^{[G_n^{-1}(x\bar{\alpha}y)]}X_{[G_n^{-1}(x\bar{\alpha}y)-1,G_n^{-1}(x\bar{\alpha}y)]}\right)\circ D\left((-1)^{[G_n^{-1}(x\alpha y)}X_{[G_n^{-1}(x\alpha y)\,G_n^{-1}(x\alpha y)+1]}\right)= D\left((-1)^{[G_n^{-1}(x_1\bar{\beta}x_2\alpha y)]}X_{[G_n^{-1}(x_1\beta x_2\alpha y)\,G_n^{-1}(x_1\bar{\beta}x_2\alpha y)]}\right)\circ D\left((-1)^{[G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y)]}X_{[G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y)\,G_n^{-1}(x_1\beta x_2\bar{\alpha}y)]}\right)\circ D\left((-1)^{[G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y)]}X_{[G_n^{-1}(x_1\bar{\beta}x_2\alpha y)\,G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y)]}\right)\circ D\left((-1)^{[G_n^{-1}(x_1\beta x_2\bar{\alpha}y)]}X_{[G_n^{-1}(x_1\bar{\beta}x_2\bar{\alpha}y)\,G_n^{-1}(x_1\beta x_2\alpha y)]}\right)\circ D\left((-1)^{[G_n^{-1}(x_1\beta x_2\alpha y)]}X_{[G_n^{-1}(x_1\beta x_2\alpha y)\,G_n^{-1}(x_1\bar{\beta}x_2\alpha y)]}\right)$$



这就完成了证明。

E.4 引理的证明 8.6

更准确地说，我们将证明以下等价命题：对于任意满足 $|||C''||| = C$ 的原始电路 C''，都有 QC $D\ E_{k\,\ell}\ \|C''\| = id_k \otimes C \otimes id_\ell$ $\|C''\|$ $|||C''|||$ $\|C''\|$ $\vdash$ $(.\ (\,))$，其中 (分别) 表示经由典范投影到 $\mathbf{QC}^{\mathbf{seq}}$（分别投影到 $\mathbf{QC}$）所得的像。为简单起见，在证明余下部分中，我们滥用记号，省略典范投影 $\|\cdot\|$。我们对 C'' 进行结构归纳。

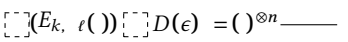
对于任意两个 n量子比特原始电路 C_1，C_2 使得 $k+n+\ell \geq 3$，其中一个 has

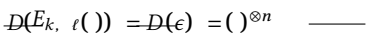
$$D(E_{k,\ell}(C_2 \circ C_1)) = D(E_{k,\ell}(C_2)) \circ D(E_{k,\ell}(C_1))$$

并且对于任意 n 比特原始电路 C_1 和 m 比特原始电路 C_3，使得 $k+n+m+\ell \geq 3$,

$$D(E_{k,\ell}(C_1 \otimes C_3)) = D(E_{k+n,\ell}(C_3)) \circ D(E_{k,\ell+m}(C_1)).$$

因此，剩下的是基例：

情形： 

情形： 

情形：如果 $\ell \geq 1$，则由定义 8.2 和引理 8.4 可知

$$\mathrm{QC} \vdash D(E_{k,\ell}(\bullet\!-\!)) = \prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^{\ell-1}}} \Lambda^x \;\square\; \Lambda^y .$$

根据方程（335），可以将这些因子按适当顺序排列，从而能够利用方程（309）将它们全部合并。可得 $id_k \otimes \bullet \otimes id_\ell$，即为所需结果。

如果 $\ell = 0$，则由定义 8.2 和引理 8.4 可知

$$\mathrm{QC} \vdash D(E_{k,0}(\bullet\!-\!)) = \prod_{x\in\{0,1\}^{k-1}} \square\; \Lambda^x .$$

同样可以合并一个 将所有因子合并起来，使用方程 (335) 和 (309)，从而得到 $id_k \otimes$ ，这就是所需的结果 t.

情形：若 $\ell \geq 1$，则由定义 8.2 和引理 8.4 可得

$$\mathrm{QC} \vdash D(E_{k,\ell}(\;\square\;)) = \prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^{\ell-1}}} \Lambda^x \;\square\; \Lambda^y .$$

根据方程 (335)，可以将各因子按适当顺序排列，从而能够使用方程 (309) 将它们全部合并。于是得到 $id_k \otimes \bullet \otimes id_\ell$，这就是所需的结果。

若 $\ell = 0$，则由定义 8.2 和引理 8.4 可得

$$\mathrm{QC} \vdash D(E_{k,0}(\;\square\;)) = \prod_{x\in\{0,1\}^{k-1}} \square\; \Lambda^x .$$

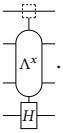
同样可以合并一个 将所有因子合并起来，使用方程 (335) 和 (309)，从而得到$id_k \otimes$ ，这就是所需的结果 t.

情形 H 若 $\ell \geq 1$，则由定义 8.2 和 8.3 可得

$$D(E_{k,\ell}(-\boxed{H}-)) = \prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^{\ell-1}}} \Lambda^x \;\square\; H \;\square\; \Lambda^y .$$

根据方程（340），可以将各个因子按适当顺序排列，从而能够利用方程（310）将它们全部合并。于是得到 $id_k \otimes \square \otimes id_\ell$，这正是所需结果。

若 $\ell = 0$，则由定义 8.2 和 8.3 可知

$$D(E_{k,0}(\bullet\!-\!)) = \prod_{x\in\{0,1\}^{k-1}}$$ 

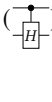
类似地，可以利用方程（340）和（310）将所有因子合并在一起，从而得到 $id_k \otimes$  ，这就是所需的结果。

情形 H : 若 $\ell \geq 1$，则由定义 8.2 和 8.3 可知

$$D(E_{k,\ell}($$ 

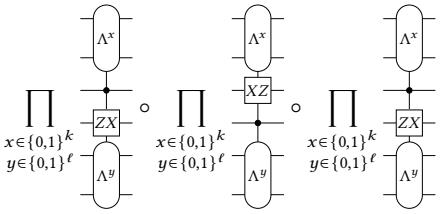
根据方程 (340)，可以将各因子按适当顺序排列，从而利用方程 (310) 将它们合并起来。得到 $id_k \otimes$  $\otimes\, id_\ell$，这就是所需结果。

若  $\ell = 0$，则由定义 8.2 和 8.3 可得

$$D(E_{k,0}($$ 

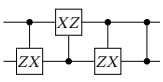
类似地，可以利用方程 (340) 和 (310) 将所有因子合并起来，从而得到 $id_k \otimes$  ，这就是所需结果。

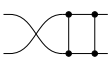
情形：由定义 8.2 和引理 8.5，以及上面的情形，可得 

$$\mathsf{QC} \vdash D(E_{k,\ell}($$  $)) = (id_k \otimes$  $\otimes\, id_\ell) \circ$ 

在每个乘积中，根据方程 (351)，可以将各因子按适当顺序排列，从而利用方程 (354) 将它们合并起来。得到

$$(id_k \otimes$$  $\otimes\, id_\ell) \circ (id_k \otimes$  $\otimes\, id_\ell) \circ (id_k \otimes$  $\otimes\, id_\ell) \circ (id_k \otimes$  $\otimes\, id_\ell)$

$$= \quad id_k \otimes$$  $\otimes\, id_\ell$

$$\overset{(116)}{=} \quad id_k \otimes$$  $\otimes\, id_\ell$

$$\overset{(4)}{=} \quad id_k \otimes$$  $\otimes\, id_\ell$

E.5 引理8.8的证明

要证明引理 8.8，只需证明对于图 8 中形如 $w_1 = w_2$ 其中 $w_1,\ w_2 \in \mathcal{G}_{2^n}^*$ 的每条规则，以及任意两个字 $w_0,\ w_3 \in \mathcal{G}_{2^n}^*$，均有 $\mathsf{QC} \vdash D(w_0 w_1 w_3) = D(w_0 w_2 w_3)$。由于 D 是幺半群同态，只需证明 $\mathsf{QC} \vdash D(w_1) = D(w_2)$。

解码方程 (20)： $D\left((-1)_{[a]}(-1)_{[a]}\right) = id_n = D(\epsilon)$。

解码方程 (21)： 结果可由以下定义得出： $D\left((-1)_{[a]}(-1)_{[b]}\right)$。

解码方程 (22)： 我们根据 a、 b、 c 的相对顺序分别讨论。

- 若 $a \le b \le c$，则有

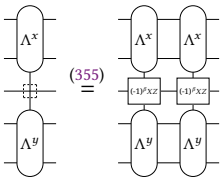
$$\begin{aligned} D\Big(\big((-1)_{[a]}(-1)_{[b]}\big)\big((-1)_{[b]}(-1)_{[c]}\big)\Big) &= \overleftarrow{\prod_{k=a}^{b-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \circ \overleftarrow{\prod_{k=b}^{c-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \\ &\overset{(335)(336)}{=} \overleftarrow{\prod_{k=b}^{c-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \circ \overleftarrow{\prod_{k=a}^{b-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \\ &= \overleftarrow{\prod_{k=a}^{c-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \\ &= D\left((-1)_{[a]}(-1)_{[c]}\right) \end{aligned}$$

- 若 $a \le c \le b$，则有

$$\begin{aligned} D\Big(\big((-1)_{[a]}(-1)_{[b]}\big)\big((-1)_{[b]}(-1)_{[c]}\big)\Big) &= \overleftarrow{\prod_{k=a}^{b-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \circ \overleftarrow{\prod_{k=c}^{b-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \\ &= \overleftarrow{\prod_{k=c}^{b-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \circ \overleftarrow{\prod_{k=a}^{c-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \circ \overleftarrow{\prod_{k=c}^{b-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \\ &\overset{(335)(336)}{=} \overleftarrow{\prod_{k=a}^{c-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \circ \overleftarrow{\prod_{k=c}^{b-1}} \Big(D\left((-1)_{[k]}(-1)_{[k+1]}\right) \circ D\left((-1)_{[k]}(-1)_{[k+1]}\right)\Big) \\ &= \overleftarrow{\prod_{k=a}^{c-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \\ &= D\left((-1)_{[a]}(-1)_{[c]}\right) \end{aligned}$$

- 其他情形（$b \le a \le c$、 $b \le c \le a$、 $c \le a \le b$ 和 $c \le b \le a$）类似。

解码方程 (23)：

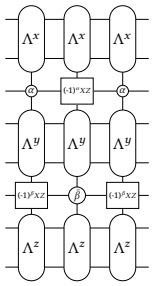
$$D\left((-1)_{[a]}(-1)_{[a+1]}\right) =$$  $$\overset{(355)}{=}$$ $$= D\Big(\big((-1)_{[a]}X_{[a,a+1]}\big)\big((-1)_{[a]}X_{[a,a+1]}\big)\Big)$$

其中 $G_n(a) = x\beta y$和 $G_n(a+1) = x\bar{\beta}y$， 且 $\beta \in \{0,1\}$、 $x \in \{0,1\}^k$ 和 $y \in \{0,1\}^{n-k-1}$。

解码方程 (24)：根据格雷码的性质，存在比特串 x, y, z（总长度为 $n-2$）以及比特 $\alpha, \beta \in \{0,1\}$，使得 $G_n(a) = x\alpha y\beta z$，且要么 $G_n(a+1) = x\alpha y\bar{\beta}z$，要么 $G_n(a+1) = x\bar{\alpha}y\beta z$，并且 $G_n(a+2) = x\bar{\alpha}y\bar{\beta}z$。我们只讨论 $G_n(a+1) = x\alpha y\bar{\beta}z$ 的情形，

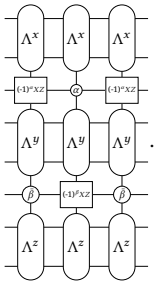
另一种情况类似。可得

$$D\left(\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\right) =$$



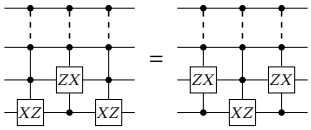
and

$$D\left(\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\right) =$$



.

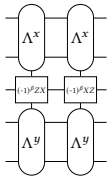
为了推导二者之间的等式，除了使用方程 (81) 和 (356) 外，我们不失一般性地假设 $\alpha = 1$ 且 $\beta = 0$。此外，除了使用方程 (81) 外，我们不失一般性地假设 x， y， z仅由 1组成；并且，除了使用方程 (353) 外，我们不失一般性地假设 y和 z的长度为零。因此，只需证明以下方程：



这恰好是方程（358）。

解码方程（25）：该结果直接由 $D\left((-1)_{[a]}X_{[a,c]}\right)$ 和 $D\left((-1)_{[a+1]}X_{[a+1,c]}\right)$的定义得出。解码方程（26）：该结果直接由 $D\left((-1)_{[c]}X_{[a,c]}\right)$ 和 $D\left((-1)_{[c]}X_{[a+1,c]}\right)$的定义得出。解码方程（27）：该结果直接由 $D\left((-1)_{[a]}X_{[a,c]}\right)$ 和 $D\left((-1)_{[a+1]}X_{[a+1,c]}\right)$的定义得出。解码方程（ 28 ）：该结果直接由 $D\left((-1)_{[c]}X_{[a,c]}\right)$ 和 $D\left((-1)_{[c]}X_{[a+1,c]}\right)$的定义得出。解码方程（29）：

$$D\Big(\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a+1]}X_{[a+1,a+2]}\right)\Big) =$$



$$\overset{(317)}{=} id_n = D(\epsilon)$$

其中 $G_n(a) = x\beta y$和 $G_n(a+1) = x\beta y$,¯ 其中 $\beta \in \{0,1\}$、 $x \in \{0,1\}^k$ 和 $y \in \{0,1\}^{n-k-1}$。

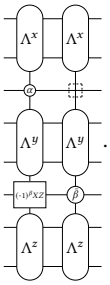
解码方程 (30)：根据 $D\left((-1)_{[c]}X_{[a,b]}\right)$的定义，结果可直接得到，因为 $c \neq a$， b。解码方程 (31)：我们只讨论 $c > a+1$的情况，另一种情况（其中 $c < a$）类似。我们有

$$D\Big(\left((-1)_{[a+1]}(-1)_{[c]}\right)\left((-1)_{[a]}X_{[a,a+1]}\right)\Big)$$

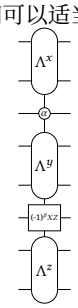
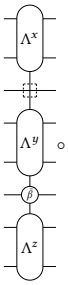
$$= \prod_{k=a+1}^{\overleftarrow{c-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \circ D\Big(\left((-1)_{[a]}X_{[a,a+1]}\right)\Big)$$

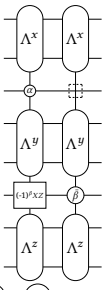
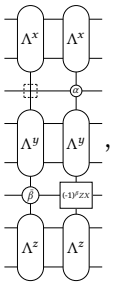
$$= \overleftarrow{\prod_{k=a+2}^{c-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \circ D\left((-1)_{[a+1]}(-1)_{[a+2]}\right) \circ D\Big(\left((-1)_{[a]}X_{[a,a+1]}\right)\Big)$$

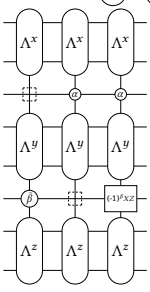
根据格雷码的性质，存在比特串 x，y，z（总长度为 $n-2$）以及比特 α，$\beta \in \{0,1\}$，使得 $G_n(a) = x\alpha y\beta z$，要么是 $G_n(a+1) = x\alpha y\bar{\beta}z$，要么是 $G_n(a+1) = x\bar{\alpha}y\beta z$，并且 $G_n(a+2) = x\bar{\alpha}y\bar{\beta}z$。我们只考虑 $G_n(a+1) = x\alpha y\bar{\beta}z$ 这种情况，另一种情况类似。我们有

$D\left((-1)_{[a+1]}(-1)_{[a+2]}\right) \circ D\Big(\left((-1)_{[a]}X_{[a,a+1]}\right) =$  .

利用方程（81）和（356），我们可以假定由 β 参数化的控制位为黑色；再利用方程（315），我们也可以假定由 α 参数化的控制位为黑色。然后利用方程（353）、（307）和（313），我们可以适当地交换控制位，使得

利用方程（333）和（334）（以及（81）），我们展开  使结果包含  。随后便很容易

将其变换为  into  ，可能还需要借助方程（317）。根据方程（317）和（355），我们便可以进一步将其变换为

into  ，这等于 $D\left((-1)_{[a]}X_{[a,a+1]}\right) \circ D\left((-1)_{[a]}(-1)_{[a+1]}\right) \circ D\left((-1)_{[a+1]}(-1)_{[a+2]}\right)$。因此，我们得 t

$$\overleftarrow{\prod_{k=a+2}^{c-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right) \circ \left((-1)_{[a]}X_{[a,a+1]}\right) \circ D\left((-1)_{[a]}(-1)_{[a+1]}\right) \circ D\left((-1)_{[a+1]}(-1)_{[a+2]}\right).$$

最后，注意对于任意 $k \notin \{a-1, a, a+1\}$，$D\left((-1)^{[k]}(-1)_{[k+1]}\right)$根据方程（346）或（347）（以及等式 (307)）与 $D\left((-1)_{[a]}X_{[a,a+1]}\right)$对易。事实上，$G_n(k)$ 与 $G_n(k+1)$ 恰好相差一个比特，并且 $G_n(a)$ 与 $G_n(a+1)$ 也恰好相差一个比特。由于$G_n(a)$ $G_n(a+1)$ $G_n(k)$ $G_n(k+1)$均互不相同，因此至少存在一个比特，使得 $G_n(k)$ 与 $G_n(k+1)$ 一致，$G_n(a)$ 与 $G_n(a+1)$ 一致，但 $G_n(k)$ $G_n(k+1)$ 与 $G_n(a)$ $G_n(a+1)$ 不同（否则，通过在 $G_n(k)$ 与 $G_n(k+1)$ 之间以及在 $G_n(a)$ 与 $G_n(a+1)$ 之间适当地选择，我们便能得到两个相同的向量，这与这四个向量均互不相同的事实相矛盾）。这对应于 $D\left((-1)^{[k]}(-1)_{[k+1]}\right)$的一个控制位于相反颜色的 $D\left((-1)_{[a]}X_{[a,a+1]}\right)$的一个控制之前。

因此，我们得到

$$D\left((-1)_{[a]}X_{[a,a+1]}\right)\circ\overleftarrow{\prod_{k=a+2}^{c-1}}D\left((-1)_{[k]}(-1)_{[k+1]}\right)\circ D\left((-1)_{[a]}(-1)_{[a+1]}\right)\circ D\left((-1)_{[a+1]}(-1)_{[a+2]}\right)$$

由方程（336）可得

$$\begin{aligned}
&D\left((-1)_{[a]}X_{[a,a+1]}\right)\circ\overleftarrow{\prod_{k=a+2}^{c-1}}D\left((-1)_{[k]}(-1)_{[k+1]}\right)\circ D\left((-1)_{[a+1]}(-1)_{[a+2]}\right)\circ D\left((-1)_{[a]}(-1)_{[a+1]}\right)\\
=\;& D\left((-1)_{[a]}X_{[a,a+1]}\right)\circ\overleftarrow{\prod_{k=a}^{c-1}}D\left((-1)_{[k]}(-1)_{[k+1]}\right)\\
=\;& D\Big(\left((-1)_{[a]}X_{[a,a+1]}\right)\left((-1)_{[a]}(-1)_{[c]}\right)\Big).
\end{aligned}$$

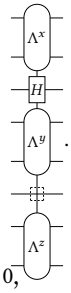
解码方程（32）： $G_n(a)$ 恰好与 $G_n(a+1)$ 相差一个比特，而 $G_n(b)$ 也恰好与 $G_n(b+1)$ 相差一个比特。由于 $G_n(a)\ G_n(a+1)\ G_n(b)\ G_n(b+1)$ 各不相同，因此至少存在一个比特，使得 $G_n(a)$ 与 $G_n(a+1)$ 相同， $G_n(b)$ 与 $G_n(b+1)$ 相同，但 $G_n(a)\ G_n(a+1)$ 与 $G_n(b)\ G_n(b+1)$ 不同（否则，我们就可以在 $G_n(a)$ 和 $G_n(a+1)$ 之间以及 $G_n(b)$ 和 $G_n(b+1)$ 之间适当选择，从而得到两个相同的向量，这与四者各不相同的事实矛盾）。这对应于将 $D\left((-1)_{[a]}X_{[a,a+1]}\right)$ 的控制置于颜色相反的 $D\left((-1)_{[b]}X_{[b,b+1]}\right)$ 的控制之前，因此两者可根据方程（351）或方程（352）（结合方程（353））交换。

解码方程 (33)：T 该结果可直接由 $D\left((-1)_{[a]}X_{[a,b]}\right)$ 和 $D\left((-1)_{[b]}X_{[a,b]}\right)$ 在 $a>b$ 情形下的定义得出 .

解码方程 (34)：该结果可直接由 $D\left(X_{[a,b]}X_{[c,d]}\right)$。

解码方程 (35)：当元组 $(G_n(a)\ G_n(b)\ G_n(c)\ G_n(d))$ 既不是 $(x0y0z, x1y0z, x0y1z, x1y1z)$ 的形式，也不是 $(x0y0z, x0y1z, x1y0z, x1y1z)$ 的形式时，该结果可直接由 $D\left(H_{[a,b]}H_{[c,d]}\right)$ 的定义得出。

解码方程(36)： 一方面，根据 $D\left(H_{[a,b]}H_{[c,d]}\right)$的定义，当元组$(G_n(a)\ G_n(b)\ G_n(c)\ G_n(d))$具有

形式 $(x0y0z,\ x1y0z,\ x0y1z,\ x1y1z)$，左侧的解码为 $D\left(H_{[a,b]}H_{[c,d]}\right)=$ 

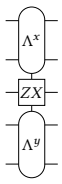
.

另一方面，为了解读右端，首先注意 $D\left(\mathrm{E}_{k\,\ell}^{1-x},(\,)\right)$ 在 $x=1$时为单位元，并且如果 $x=0$,



$$D\left(\mathcal{E}_{k,\ell}^{1-x}(\ \ )\right)\quad=\quad D(E_{k,\ell}(\ \ ))\circ\overrightarrow{\prod_{\substack{x\in\{0,1\}^k\\ y\in\{0,1\}^\ell}}}D\left((-1)_{[G_n^{-1}(x1y)]}X_{[G_n^{-1}(x0y),G_n^{-1}(x1y)]}\right)$$

$$\overset{\text{Lemmas 8.5 and 8.6}}{=}\quad (id_k\otimes\ \ \otimes id_\ell)\circ\overrightarrow{\prod_{\substack{x\in\{0,1\}^k\\ y\in\{0,1\}^\ell}}}$$

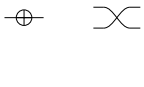


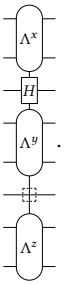
$$\overset{(351)(354)}{=}\quad (id_k\otimes\ \ \otimes id_\ell)\circ(id_k\otimes\ \ \otimes id_\ell)$$

$$=\quad id_k\otimes\ \ \otimes id_\ell$$

$\overset{(2)}{=}$ $id_k \otimes$ $\otimes\, id_\ell$

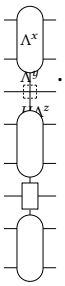
结合引理 8.6 应用于 ，并结合方程(34)，这意味着方程 (36) 右侧的解码可以

通过 和 的组合进行共轭变换，从而对应于H的定义 

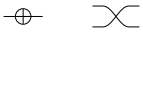


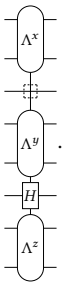
解码方程 (37)： 一方面，根据以下情形下 $D\left(H_{[a,b]}H_{[c,d]}\right)$ 的定义，其中元组 $(G_n(a)\ G_n(b)\ G_n(c)\ G_n(d))$属于

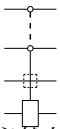
形式为 $(x0y0z, x0y1z, x1y0z, x1y1z)$，左侧的解码为 $D\left(H_{[a,b]}H_{[c,d]}\right) =$



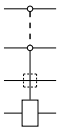
另一方面，使用与方程 (36) 相同的论证，可以证明方程 (37) 右侧的解码

可以通过 和 的组合进行共轭变换，从而对应于H的定义 



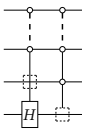
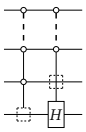
解码方程 (38)： 一方面， $D\left(H_{[0,1]}H_{[3,2]}\right) =$ 。 

另一方面，对于任意 $a \geq 4$, $G_n(a)$ 和 $G_n(a+1)$，它们必然有一个值为 1 且不属于最后两位的公共比特。事实上，否则，由于它们仅相差一位，至少其中一个会等于 0...000、0...001、0...011 或 0...010（更确切地说，如果变化的比特位于最后两位中，那么 $G_n(a)$ 和 $G_n(a+1)$ 都会等于这些编码之一；如果变化的比特位于前 $n-2$ 位中，那么 $G_n(a)$ 和 $G_n(a+1)$ 中恰好有一个会等于这些编码之一）。但这些分别已经是 $0,1,2,3$ 的格雷码。

因此， $D\left((-1)_{[a]}X_{[a,a+1]}\right)$ 在 的某个白色控制前有一个黑色控制，因此根据 H 与它对易 

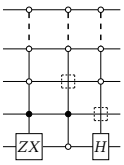
方程（348）、（349）或（350）。

解码方程 (39)：

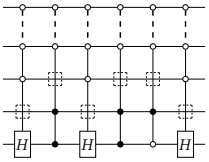
$D\Big(\left((-1)_{[0]}(-1)_{[1]}\right)\left(H_{[0,1]}H_{[3,2]}\right)\Big)$ =  $\overset{(338)}{=}$  $= D\Big(\left(H_{[0,1]}H_{[3,2]}\right)\left((-1)_{[0]}(-1)_{[1]}\right)\Big)$

解码方程 (40)：

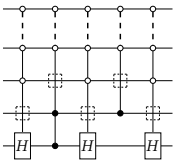
$$D\Big(\big(H_{[0,1]}H_{[3,2]}\big)\,\big((-1)_{[3]}(-1)_{[4]}\big)\,\big((-1)_{[2]}X_{[2,3]}\big)\Big) =$$



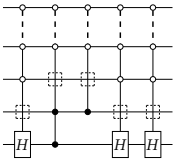
(353)(333)(81)(315)=



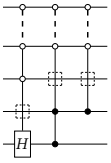
(309)=



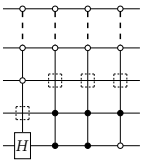
(274)(309)(338)=



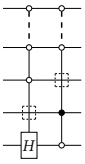
(312)=



(309)=



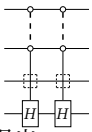
(311)=



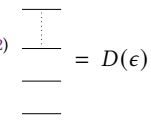
$$= D\Big(\big((-1)_{[3]}(-1)_{[4]}\big)\,\big(H_{[0,1]}H_{[3,2]}\big)\Big)$$

解码方程 (41)：

$$D\Big(\big(H_{[0,1]}H_{[3,2]}\big)\,\big(H_{[0,1]}H_{[3,2]}\big)\Big) =$$



(312)=

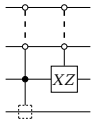


$= D(\epsilon)$

解码方程 (42)：结果可直接由以下情形下 $D\left(H_{[a,b]}H_{[c,d]}\right)$的定义得出：$|\{a,\ b,\ c,\ d\}| \leq 3$。

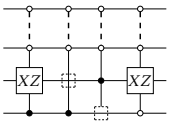
解码方程 (43)： 首先，我们证明以下辅助方程是图 4 中方程的推论：

$$D\left(X_{[0,3]}X_{[1,2]}\right) \;=\; \tag{361}$$

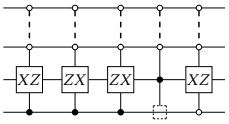


$$\begin{aligned}
D\left(X_{[0,3]}X_{[1,2]}\right) &= D\Big(\left((-1)_{[0]}X_{[0,3]}\right)\left((-1)_{[3]}X_{[1,2]}\right)\Big)\\
&= D\Big(\left((-1)_{[0]}X_{[0,3]}\right)\left((-1)_{[3]}(-1)_{[1]}\right)\left((-1)_{[1]}X_{[1,2]}\right)\Big)\\
&= D\Big(\left((-1)_{[0]}X_{[0,3]}\right)\left((-1)_{[2]}(-1)_{[3]}\right)\left((-1)_{[1]}(-1)_{[2]}\right)\left((-1)_{[1]}X_{[1,2]}\right)\Big)
\end{aligned}$$

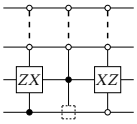
引理 8.5 =



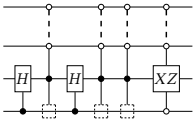
(355) =



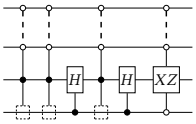
(317) =



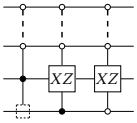
(81) =



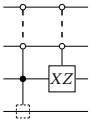
(311) =



(81) =

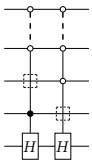


(354) =

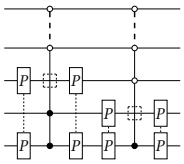


于是，我们可以如下证明该结果：

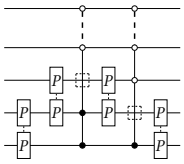
$$D\Big(\left(H_{[0,1]}H_{[3,2]}\right)\left(H_{[3,2]}H_{[4,5]}\right)\Big) =$$



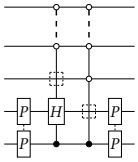
$\overset{(112)}{=}$



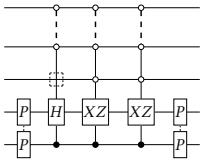
$\overset{(112)(130)}{=}$



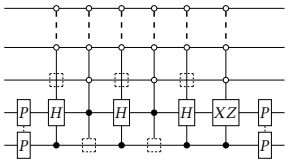
$\overset{(112)(307)}{=}$



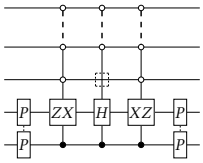
$\overset{(355)}{=}$



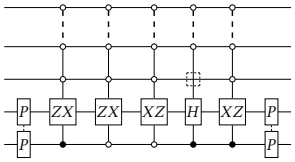
$\overset{(334)(81)(316)}{=}$



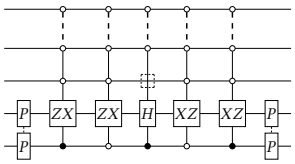
$\overset{(316)(81)(333)}{=}$



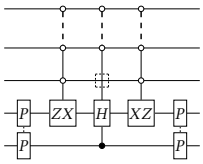
$\overset{(317)}{=}$



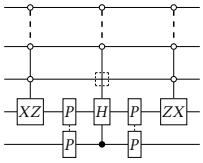
(353)(349)
=



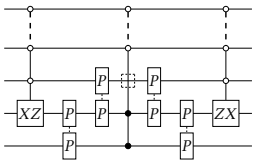
(354)
=



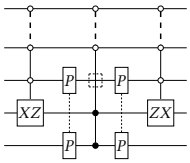
(360)
=



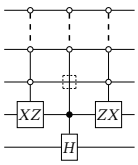
(112)(307)
=



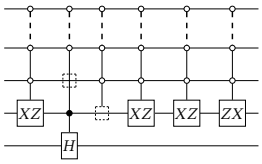
(112)(130)
=



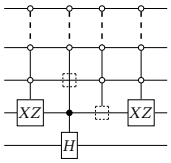
(112)
=



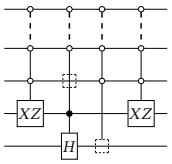
(311)(355)
=



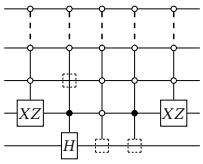
(317)
=



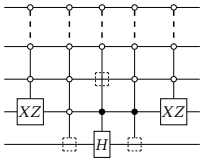
(274)
=



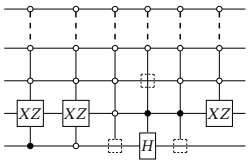
(309)
=



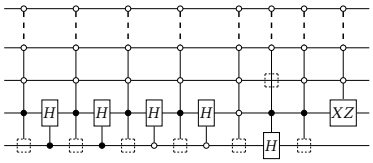
(307)(338)
=



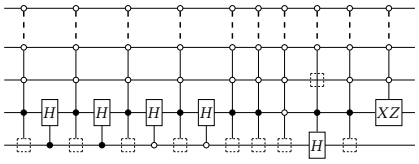
(354)
=



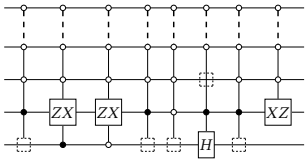
(81)(315)
=



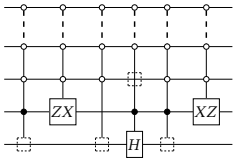
(311)
=



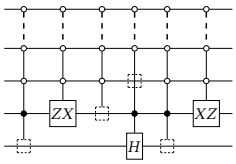
(315)(81)
=



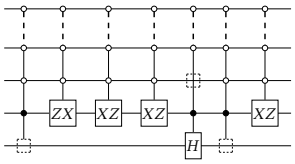
(309)(354)
=



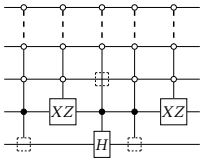
(274)
=



(355)
=



(317)
=



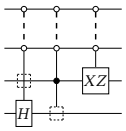
(361)
=

$$D\Big(\big(X_{[0,3]}X_{[1,2]}\big)\,\big(H_{[3,2]}H_{[4,5]}\big)\,\big(X_{[0,3]}X_{[1,2]}\big)\Big)$$

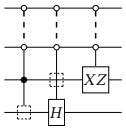
解码方程 (44):

$$D\Big(\big(X_{[0,3]}X_{[1,2]}\big)\,\big(H_{[0,1]}H_{[3,2]}\big)\Big)$$

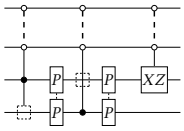
(361)
=



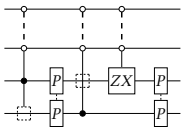
(338)
=



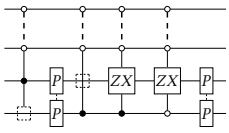
(112)
=



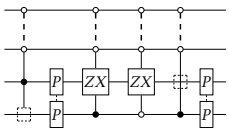
(111)(360)
=

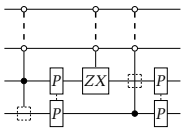


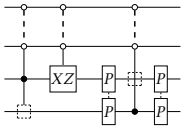
(354)
=

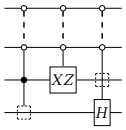


(346)
=



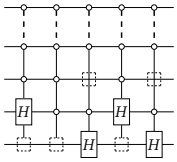
$\overset{(354)}{=}$ 

$\overset{(360)}{=}$ 

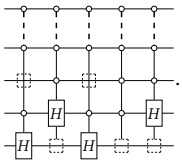
$\overset{(112)}{=}$ 

$\overset{(361)}{=} \quad D\Big(\big(H_{[0,1]}H_{[3,2]}\big)\,\big(X_{[0,3]}X_{[1,2]}\big)\Big)$

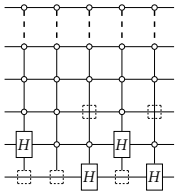
解码方程 (45)： 左侧的解码结果为

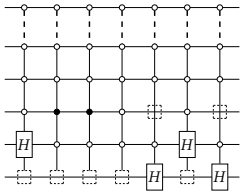


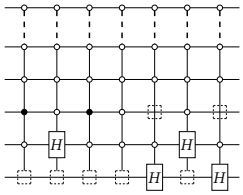
且左侧的解码结果为

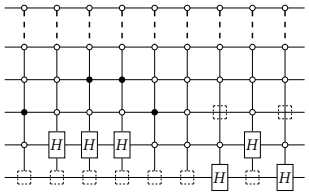


若 $n = 3$，则结果由方程 (146) 给出。若 $n \geq 4$，则有



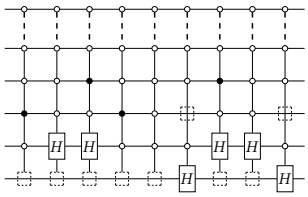
$\overset{(311)}{=}$ 

$\overset{(337)}{=}$ 

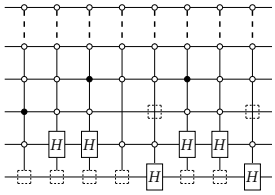
$\overset{(312)}{=}$ 

(I)

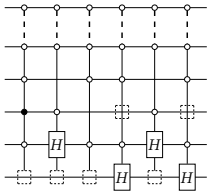
(337)(344)
=



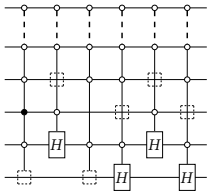
(309)
=



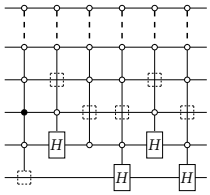
(310)
=



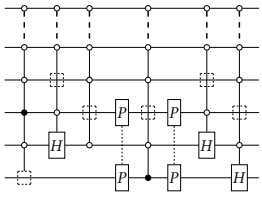
(277)
=



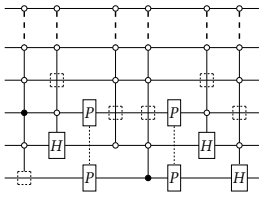
(274)
=



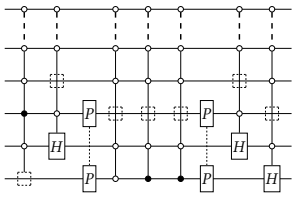
(112)
=



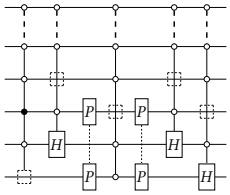
(308)
=



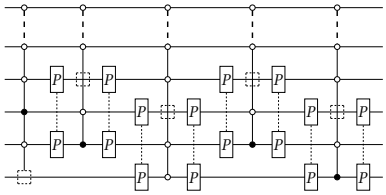
(309)
=



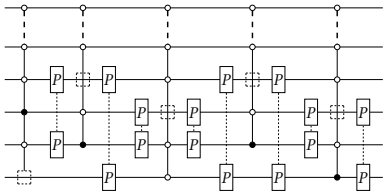
(311)
=



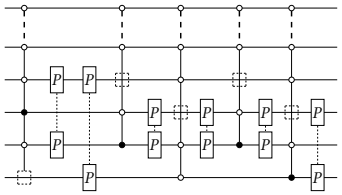
(112)
=



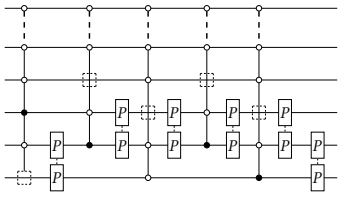
(112)(246)
=



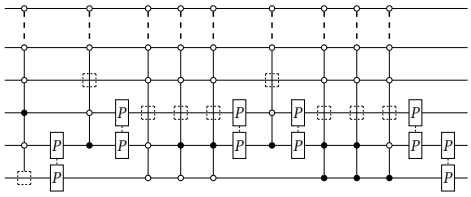
(308)(111)
=



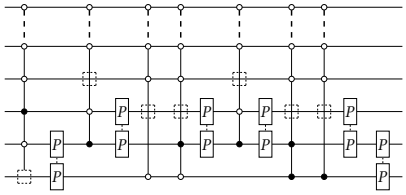
(112)(130)
=



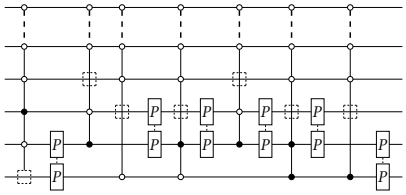
(311)
=



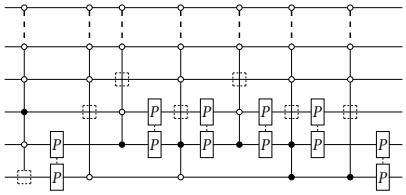
(309)
=



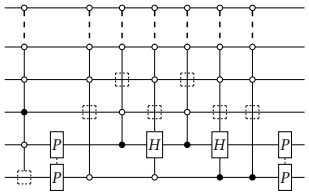
(308)
=



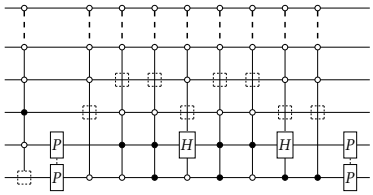
(309)(307)(336)
=



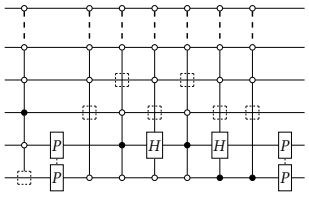
(112)
=



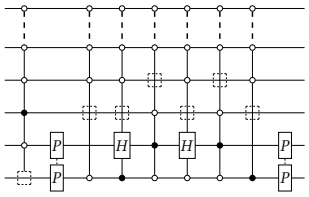
(309)
=



(307)(313)(339)(311)
=

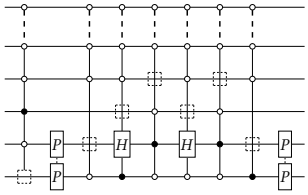


(307)(313)(339)(340)
=

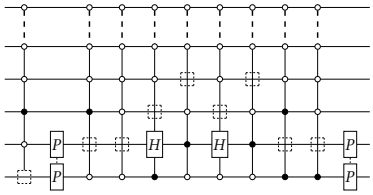


(II)

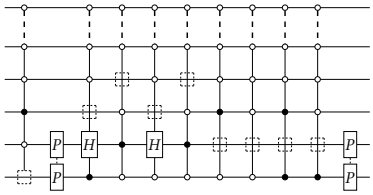
(274)
=



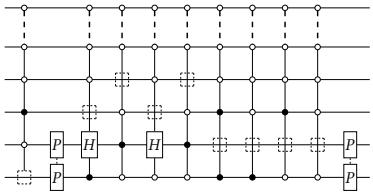
(309)
=



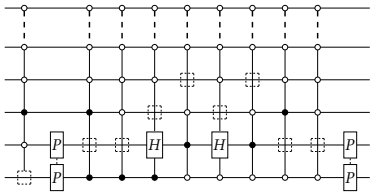
(307)(338)(336)
=



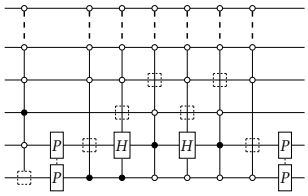
(335)
=



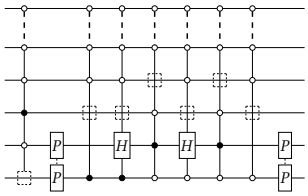
(307)(336)(338)
=



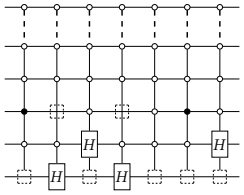
(309)
=



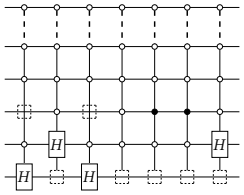
(274)
=



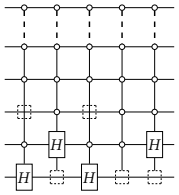
相同的步骤
从 (I) 到 (II),
镜像
按逆序
=



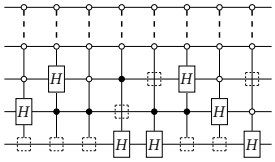
(307)(338)(337)(335)
=



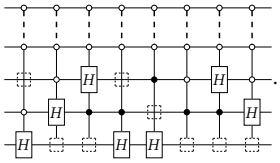
(311)
=



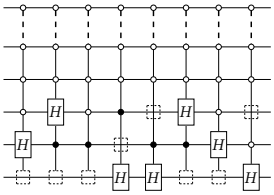
解码方程 (46)： 左侧的解码结果为



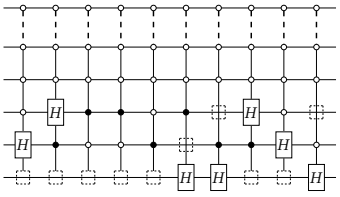
左侧的解码结果为



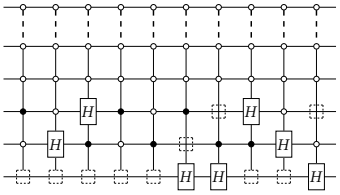
若 $n = 3$，则结果由方程 (147) 给出。若 $n \geq 4$，则有



(311)
=

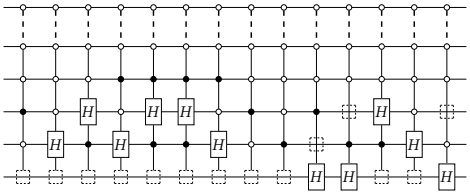


(307)(337) =

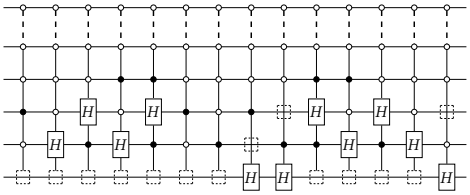


(III)

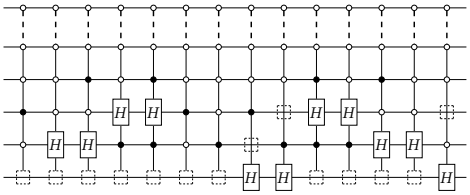
(312) =



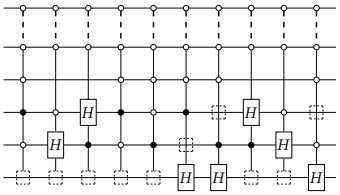
(337)(307)(345)(344) =



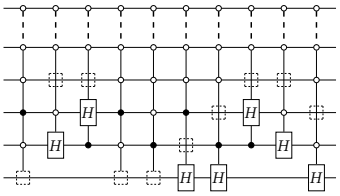
(342) =



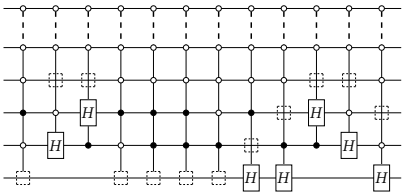
(310) =



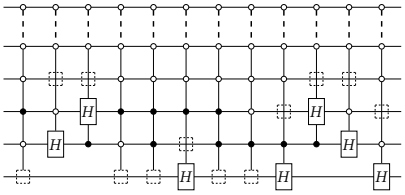
(277) =



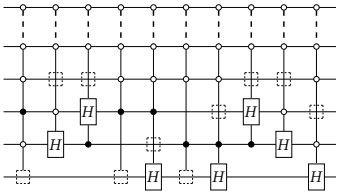
(311) =



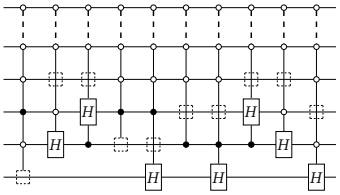
(338)
=



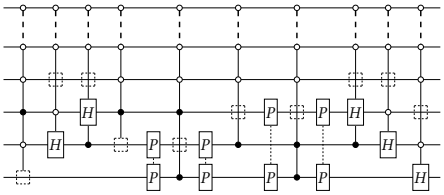
(309)
=



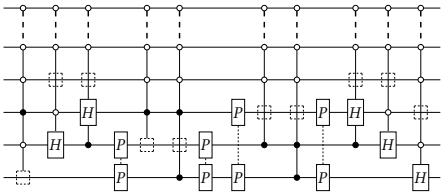
(274)
=



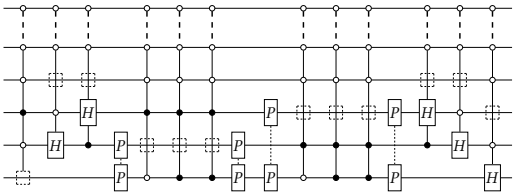
(112)
=



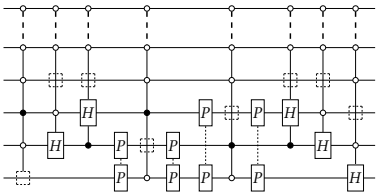
(308)
=



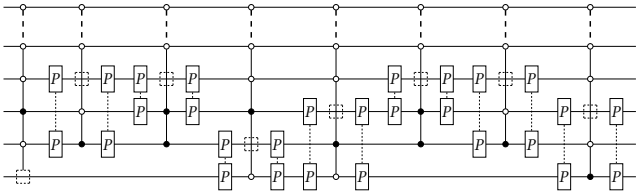
(309)
=



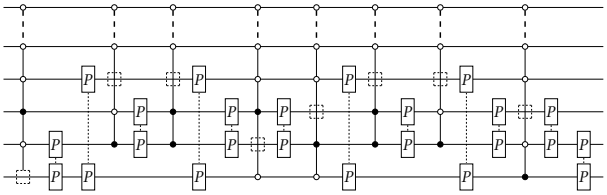
(311)
=



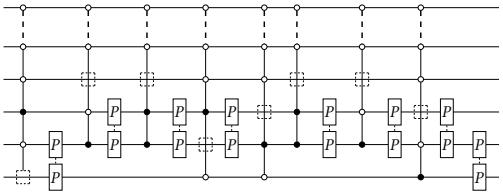
(112)(307)
=



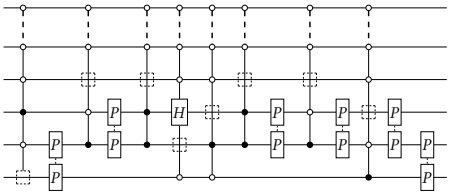
(112)(130)
=



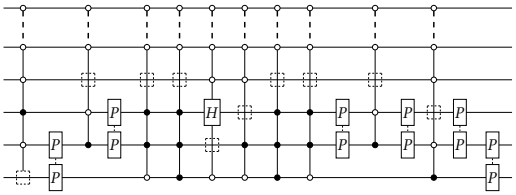
(308)(111)
=



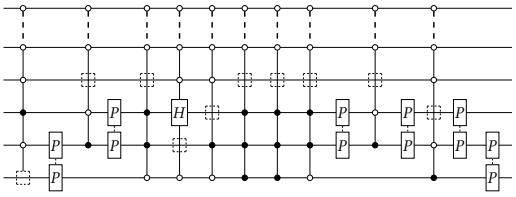
(307)
=



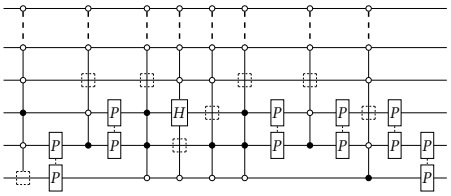
(309)
=



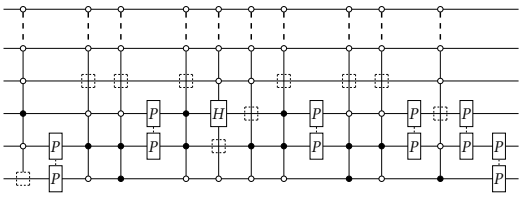
(307)(313)(339)(336)
=



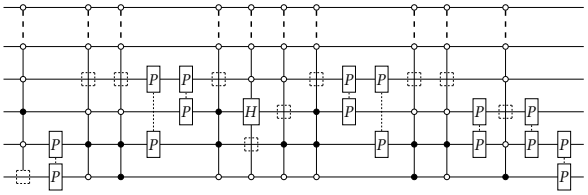
(311)
=



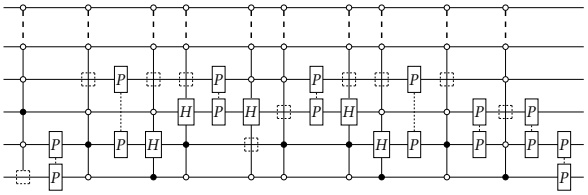
(309)
=



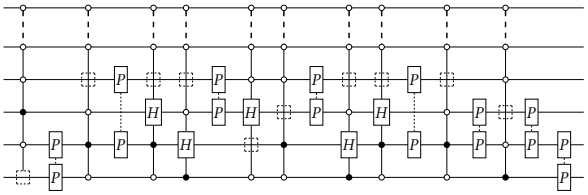
(130)(112)
=



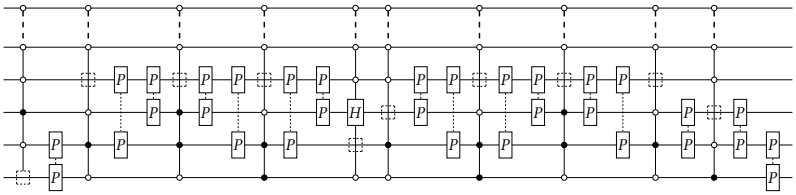
(111)(112)(307)
=



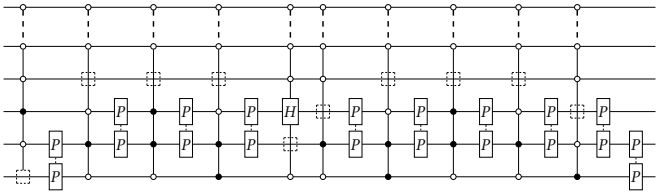
(313)(342)
=



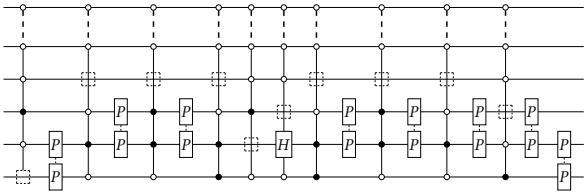
(112)(307)
=



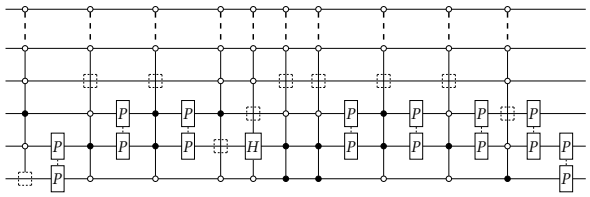
(112)(130)
=



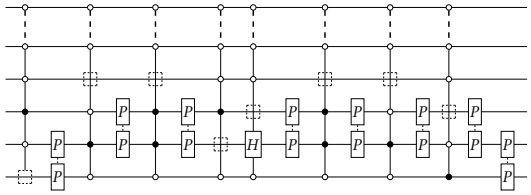
(111)(112)
=



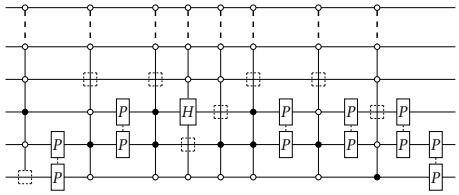
(307)(313)(336)(339)
=



(311)
=

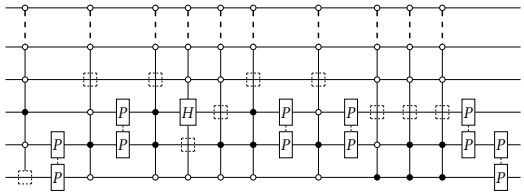


(112)(111)
=

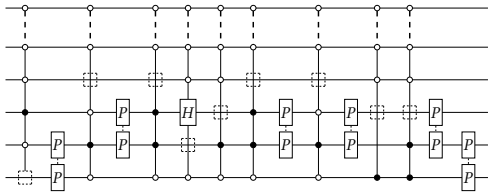


(IV)

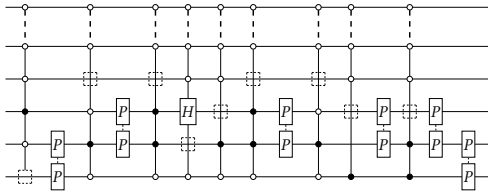
(311)
=



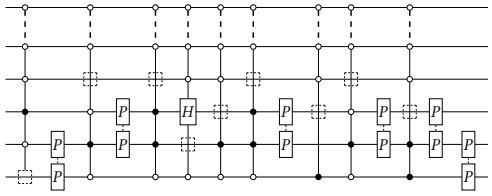
(309)
=



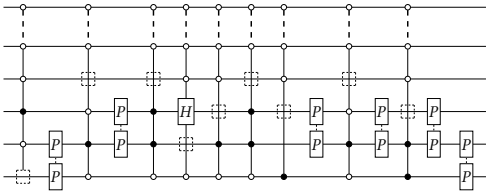
(308)
=



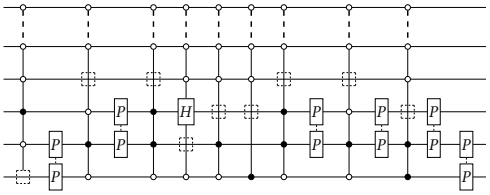
(309)(307)(336)
=



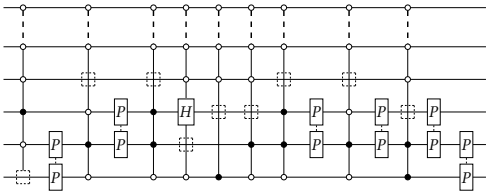
(308)
=



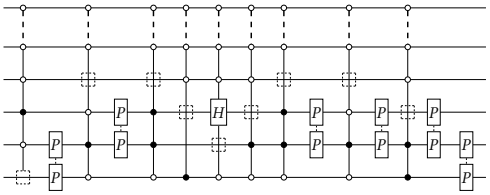
(309)(307)(336)
=



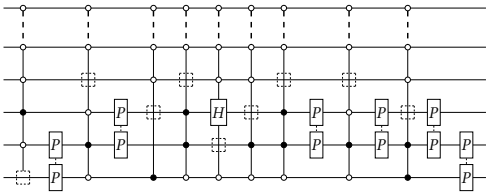
(309)(335)
=



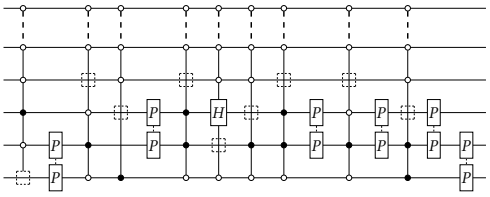
(309)(338)
=



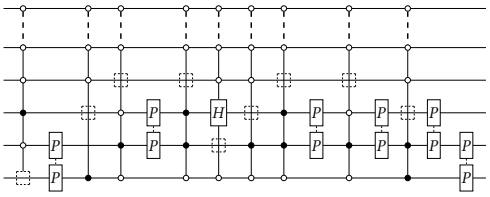
(309)(307)(336)
=



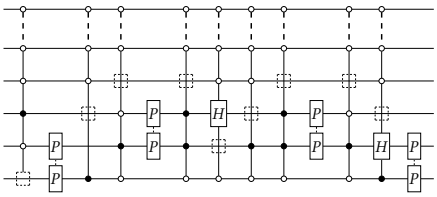
(308)
=



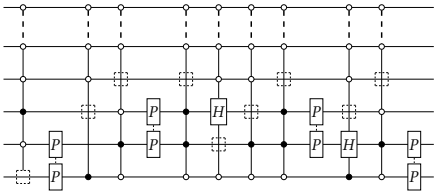
(309)(307)(336)
=



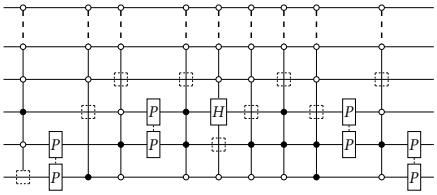
(307)(112)
=



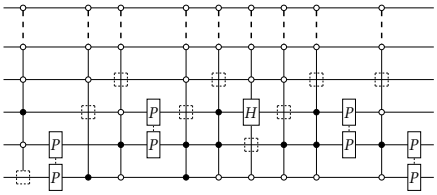
(307)(313)(339)
=



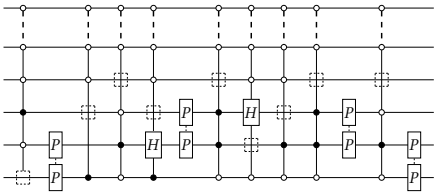
(112)(111)
=



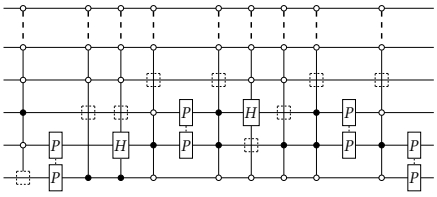
(307)(336)(335)(338)
=



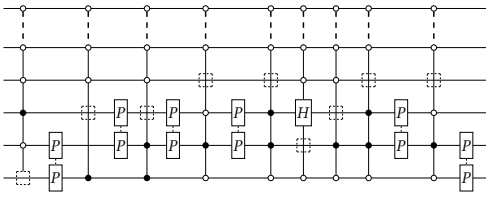
(111)(112)
=



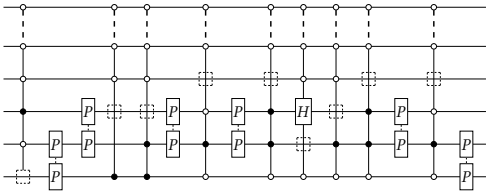
(307)(313)(339)
=



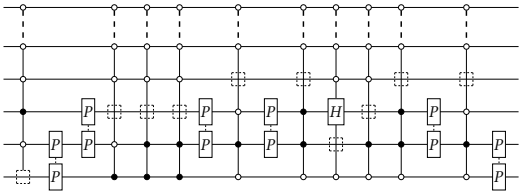
(112)(307)
=



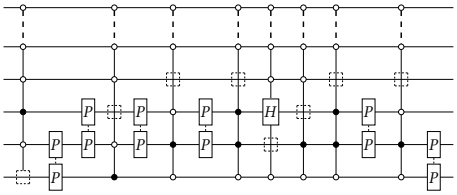
(308)
=



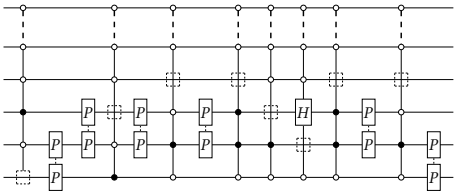
(309)
=



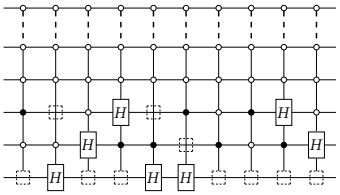
(311)
=



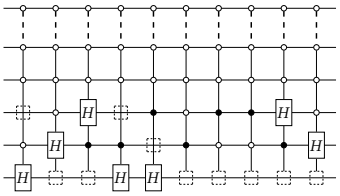
(307)(338)
=



与.....相同的步骤
从 (III) 到 (IV),
镜像 ,
逆序
=



(307)(338)(337)(335)
=



(311)
=

