arXiv:2602.16927v1 [quant-ph] 18 Feb 2026

自由量子计算

JACQUES CARETTE、CHRIS HEUNEN、ROBIN KAARSGAARD、NEIL J. ROSS 和 AMR SABRY

Abstract. 量子计算在多种重要问题上显著优于已知的经典算法，但我们尚未充分理解量子计算与经典计算之间关系的本质。自由模型能够厘清这种关系：它只为经典计算添加足以表示量子计算的物理原理，不多也不少。本文提出一种量子计算公理化方案，以少量离散方程取代标准的连续公设；同时提出一种自由模型，以范畴论模型取代标准的线性代数模型。这些公理和模型以可逆经典计算为基础，将量子优势归结为能够求取某些性质良好的平方根，并与多种量子计算硬件平台相联系。这种方法使组合优化（包括计算机穷举搜索）能够用于优化量子计算。自由模型可被诠释为一种量子计算机编程语言，其表达能力和计算普适性与标准模型相同，同时还支持自动验证与推理。

量子计算在某些问题上大幅改进了已知的经典算法 [7] ，包括质因数分解 [49], 、玻色子采样 [38], 和哈密顿量模拟 [2]。经典计算与量子计算之间关系的本质尚未得到充分理解。文献仅识别出若干本身并不能解释这一差异的概念 [52], ，包括叠加 [19], 、纠缠 [53], 、非定域性 [30], 、情境性 [26], 和干涉 [21]。量子计算相对于经典计算的优势通常从定量角度加以考量：某一特定量子算法相对于经典算法究竟具有多大优势 [1]? 本文则从定性角度加以考量：一种计算模型是否允许存在优于经典算法的算法，抑或并不允许?

这一问题之所以困难，部分原因在于量子计算往往被隐含地限定于一种使用复线性映射的标准模型 [44]。为进行有意义的比较，经典计算与量子计算都必须置于更广阔的模型图景之中。我们以双置换范畴作为模型，这是最为宽松的一种可能的计算模型概念。在此框架内，我们识别出量子计算的一种统一自由模型，它能够表达所有相对于经典算法具有优势的量子算法。

为了通过例子解释模型的自由性质，我们来看看组合学。自然数可以用多种方式补入负数： $\mathbb{N}$嵌入到 $\mathbb{Z}$ 中，并将加法保留为 $n \mapsto n$，但也可以保留为 $n \mapsto -n$ 或 $n \mapsto 2n$。

我们感谢 John Baez 和 Jørgen Ellegaard Andersen 指出了公理（2）的拓扑性质。Robin Kaarsgaard 获得了 Sapere Aude：DFF-Research Leader 项目资助（编号 5251-00024B）。Neil J. Ross 获得了加拿大自然科学与工程研究委员会（NSERC）的资助。

这些是补入负数的完备化，意味着为数字 1 添上了一个加法逆元，并且这意味着所有这些嵌入实际上都相同，至多相差一个无关紧要的全局标量。它是自由完备化，则意味着任何其他完备化都必须包含它。实数也包含 $\mathbb{N}$ 并允许减法，但还具有许多其他对计数而言多余的性质。任何保加法的嵌入 $\mathbb{N} \to \mathbb{R}$ 都唯一地经由自由模型 $\mathbb{Z}$ （由自然数及其负数组成）分解。在这个意义上，整数是自然数及其负数构成的最小模型，不带任何多余的假设或约束。这正是自由模型所体现的含义。见图 1。一般来说，自由模型是唯一的：它们由其定义性质（例如具有负数）完全决定，且至多相差一个唯一同构（例如一个无关紧要的全局标量）。

本文以类似的方式阐释经典计算与量子计算之间的关系。正如向自然数中添加 -1一样，我们为可逆经典计算添加少量具有物理意义的生成元，并表明可逆量子计算可由此作为自由完备化得到。类似于实数，任何其他可逆量子计算模型，包括复酉矩阵的标准模型，都必须唯一地通过这个自由模型分解。反过来，我们可以借助量子计算模型的（双置换）结构，在任何此类模型中规范地识别出经典计算。该自由模型具有与标准模型相同的计算普适性：它能够以任意所需的精度表达任何量子算法。不过，它还有其他优点。

与标准模型相比，这个自由模型的主要优势在于它能够对量子算法进行自动化推理。例如，判断两个量子电路是否表示相同的量子计算，是一个难以处理的问题 [29], ，原因之一是自由度有无穷多个。但由于自由模型完全是离散的，且只涉及有限多个方程，因此可以充分运用组合优化和计算机科学中的等式重写方法 [42]。举一个简单的例子，我们将证明哈达玛门是一个对合；这个事实并不深奥，但关键在于，这个等式可以自动推导出来，其他所有等式也同样如此。

自由模型的第二个优势在于其基础性：它不会混淆物理概念。因此，我们得以将量子计算与经典计算的区别归结为能够求取性质良好的平方根，换言之，就是能够将某些经典计算进行到一半便停止。自由模型是从操作性第一原理出发加以阐释的，不像依赖复数那样在基础层面令人难以满意 [17]。同样，它既不需要也不允许使用中间的非物理矩阵，再在之后的阶段将其重新变为酉矩阵，从而避开了其他方法所面临的电路综合效率低下问题 [16]。

自由模型的第三个优势在于其实用性：它不诉诸那些无法在有限时间内以任意精度通过实验测定的非经验数，而是能够精确地处理精度。我们不会讨论各类计算模型中的定量结果，例如稠密性定理 [31, 46] ；这些定理表明，如何利用量子电路高效近似酉矩阵。不过，作为一个例子，我们将分析自由模型中的精度与其实现量子傅里叶变换的效率之间的关系。

大量文献探讨了量子计算的结构化方法和方程式方法，其中最著名的是范畴量子力学 [3, 25] 和

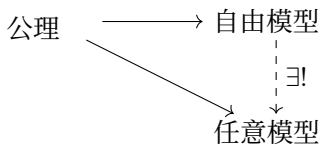


FIGURE 1. 自由模型的定义特性是：它实现了我们的量子计算公理，而且在任何其他满足这些公理的模型中，都存在对自由模型的唯一解释。从这个意义上说，自由模型恰好包含构成一个模型所需的一切，不多也不少。

ZX演算 [13]等图示形式体系。这些框架以生成元和重写规则取代矩阵，从而支持符号操作和电路优化。我们的目标与此相关，但在概念上有所不同。我们并非为特定模型（通常是希尔伯特空间或其片段）提供可靠且往往完备的表示，而是构造由一组具有物理内涵的公理生成的自由模型。其结果并非用于在固定量子模型内推理的演算，而是适用于该公理化的通用量子编程语言。

AUXILIARY QUBITS

量子计算文献主要关注有限门集的普适性，而非与经典计算进行明确比较 [48]。本文关注的是复用经典计算基础设施，并由一组有限公理构建的量子计算模型。我们固定一组公理，其中包含平方根和一个精度参数 k，并研究其自由模型。我们证明，精度级别可以通过 n 提高，代价是使用 n辅助量子比特。对于 $k = 2$自由模型涵盖 Clifford+Toffoli 量子电路； $k = 3$ 涵盖 Clifford+T 量子电路； $k = 4$ 涵盖 Clifford+T+$\sqrt{T}$ 量子电路；而更高精度则涵盖 Clifford 圆分量子电路 [4]。其他公理（例如使用立方根的公理）会产生其他自由模型。参见图 2。一般而言，比较基于不同公理的模型并无意义，但我们猜想，当 k 趋于无穷大时，使用平方根的公理所对应的自由模型将与使用立方根或其他任何基数的根的公理所对应的自由模型一致。我们的公理之所以独具特色，是因为除上述数学和计算优势外，它们还具有物理联系。

除了提高精度，辅助量子比特还提供了一个机会，让我们可以在可逆量子计算的自由模型中加入量子测量。第二种自由构造允许计算中途测量控制量子计算的流程 [23]。我们将证明，测量并移除辅助量子比特的能力增强了自由模型的完备性：两个不可逆量子计算相等，当且仅当它们可以由我们的公理推出，而无需使用任何辅助量子比特。

AXIOMS

可逆量子计算的标准公设可以替换为以下内容；我们稍后会讨论（不可逆的）量子测量。公理

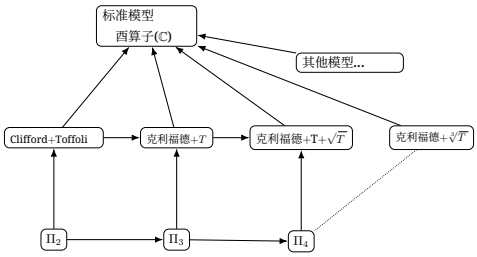


FIGURE 2. 量子计算模型及其关系的全貌。实线箭头表示一个模型包含于另一个模型中。不可比较的模型之间用虚线连接。对于每个 k， Π_k 都是满足双置换范畴公理并加入公理 (1)–(3) 后的自由模型。复数上的酉算子标准模型也满足这些公理。对于每个 k, Π_k 都嵌入任何满足相同公理的模型中。另一个例子是，克利福德+$\sqrt[3]{T}$ 电路模型在计算上也是通用的 [43] ，但与任何 Π_k都不可比较。

精度级别为 k 的可逆量子计算，通过两个生成元 ζ_k 和 V 以及三个关系扩展了可逆经典计算

$$V^2 = X \tag{1}$$

$$V\,S\,V = S\,V\,S \tag{2}$$

$$\zeta_k^{2^k} = 1 \tag{3}$$

其中， X 是经典非门的相干量子版本，而 S 是用 ζ_k定义的，详情见下文 [10]。经典可逆计算对应于不附加任何其他假设的自由双置换范畴，它嵌入任何其他双置换范畴中。

这些公理将（性质良好的）平方根单独确定为量子计算与经典计算之间任何差异的唯一来源。我们还将考虑一种较弱形式的等价性 $\approx_k$ ，它在存在辅助量子比特时判定计算是否相等。当纳入（不可逆的）量子测量和态制备后，这种弱等价性便无关紧要了。

INTERPRETATION

在详细讨论之前，请注意这种公理化的优势。它由有限个方程组成，不包含连续变量或逻辑量词。因此，这些方程非常适合自动化处理，并且能够受益于组合优化，包括计算机穷举搜索 [34]。

此外，全部三个方程都能在重要的计算物理模型中得到直接实现，并与概念性原理相联系，尤其是叠加和干涉。

公理 (1) 可以理解为： X 门有一个平方根。在囚禁离子量子计算中，这是通过将激光脉冲持续时间或强度设为实现 X 门所需的一半来实现的 [54]。类似地，$\sqrt{X}$ 是超导量子计算机中的原生门 [7]。 X 门具有平方根会产生叠加，但在这里，主要的是能够让某些计算在进行到一半时停止，



FIGURE 3. 公理（2）的示意图：将 V 解释为交换最左侧的两条线，将 S 解释为交换最右侧的两条线。

而某些叠加态的存在则只是推导出来的结果。在仅用有限条公理扩展经典可逆计算的模型中，不可能构造出所有叠加态。

公理（2）是 3股辫群的定义方程，将这一公理化与任意子量子计算联系起来 [50]。参见图 3。

公理（3）关注可构造性。原则上，要以无限精度确定一般复数需要无穷长的时间。自由模型则使用可以通过经验构造或精确测量的数。假定存在一个非平凡相位，并结合 V所提供的叠加，会产生干涉。我们选择一个本原 2^k次单位根 $\zeta_k = e^{2\pi i/2^k}$ 作为本原非平凡相位。因此，自由模型中的标量（定义见下文“《双置换范畴：形式化主要结果》”）是阶为 2^k的循环群，由 ζ_k的幂构成。显然，通过选择足够大的 k，便能用这类可构造标量逼近单位圆上的任意复数；此外，这些标量还适用于参数化旋转门、光子量子计算和变分量子算法。请注意，自由模型不需要对标量进行加法，而酉矩阵的标准模型则使用更多种标量。

REVERSIBLE CLASSICAL COMPUTING

为了理解公理化，并更详细地解释我们所说的模型 是什么，我们首先讨论可逆经典计算。在这一范式中，无论正向还是反向运行，计算都是确定性的 [20]。这与物理学相关，因为实验已经证实，不可逆地改变计算机中存储的信息会散发热量 [9], ，这符合兰道尔原理 [35, 36]。

经典可逆计算的标准模型由可逆布尔门构成的电路给出。例如，门 CCX，也称为 Toffoli 门，它将三个输入比特 $(x, y, z) \in \{0, 1\}^3$ 变换为 $(x, y, xy + z \mod 2)$，具有普适性，也就是说，任何布尔函数都可以通过由 CCX 门构成的电路实现。

经典可逆计算的一般模型可以用双置换范畴这一概念来描述。它包含对象和过程，并可通过组合子 $\oplus$和 $\otimes$ [12]将它们组合起来。这是任何计算模型所需具备的最低要求：能够按顺序组合指令（使用 $\circ$），能够考虑并行的数据（使用 $\otimes$），以及能够利用一份并发数据来影响另一份数据（使用 $\oplus$）。在标准模型中， $\otimes$ 的单位对象 $\mathbf{1}$ 类似于单元素集合，而 $2 = 1 \oplus 1$ 则表示

比特。交换过程 $X\colon 1\oplus 1 \to 1\oplus 1$ 表示一个非门，而 CCX 则是将受控运算建模为 $\mathsf{id}\oplus X\colon 2\oplus 2\oplus 2\oplus 2 = 2\otimes 2\otimes 2 \to 2\otimes 2\otimes 2$ 的典型方式。

经典可逆计算的自由模型由有限集的置换组成，或者等价地说，由置换矩阵组成。由于有限集的每个置换都是若干对换的复合，非门 X 生成了所有这些置换。因此，自由双置换范畴可视为经典可逆计算的自由模型： X 和 CCX 门已由双置换范畴的公理建模。

Reversible quantum computing

类似的组合子 $\oplus$ 和 $\otimes$ 将量子计算从单个量子比特扩展到多个受控量子比特。现在我们可以详细理解公理 (1)–(3)。从自由双置换范畴（即 经典可逆计算的自由模型）开始，并选取一个整数 $k \geq 2$。添加生成元 $\zeta_k\colon 1 \to 1$ 和 $V\colon 2 \to 2$，并考虑满足公理 (1)–(3) 的自由双置换范畴，其中 $S = \mathsf{id}\oplus\zeta_k^{2^{k-2}}$。下面的定理 1 表明这个自由模型存在。请注意，如果我们只使用 $\otimes$，添加 ζ_k 只会产生在物理上无关紧要的全局相位；正是由于存在 $\oplus$，才会产生具有非平凡计算后果的相对相位。组合子 $\oplus$使我们能够表示任意维数的 d维量子比特，而不仅仅是量子比特；这也符合量子算法（例如 Shor素数分解）需要为数值分配最接近的 2 的幂次的存储空间的要求，其中有些空间在实际计算中不会用到。

酉矩阵的标准模型也满足公理 (1)–(3)，并且

$$\zeta_k = e^{2\pi i/2^k}, \qquad V = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

因此，自由模型在标准矩阵模型中有一个解释（见图 1）。下文的定理 2 表明，当 $k = 2$ 到标准矩阵模型的一个子集时，这个解释实际上是一个同构。自由模型在唯一同构意义下是唯一的：给定两个自由模型，将其中一个设为“自由模型”，并将图 1 中的“任意模型”实例化为另一个，反之亦然，就会得到两个互为逆映射的映射。由此可知，自由模型（其中有$k = 2$）由元素取自包含ζ_2 和$_1$ $_2$的最小环的酉矩阵构成。反过来，对于每个 k，我们都可以将自由模型视为一种编程语言，用它来构造可逆量子程序。

标准矩阵解释回答了关于这种量子编程语言的两个计算机科学问题 [18]。首先，字问题是可判定的：给定编程语言中的两个表达式，可以通过比较它们所诱导的矩阵，使用一种算法来判定它们是否计算出相同的函数。其次，求值归一化 [8] 是可行的：可以根据量子程序所诱导的矩阵合成范式，从而优化量子程序。这与量子电路优化类似。

最后，舍弃矩阵并采用自由模型，不会损失任何推理能力。由下文的定理 2 可知，两个量子程序表示同一矩阵，当且仅当它们能够通过使用公理 (1)–(3) 进行替换而被证明相等。因此，我们可以自动验证量子程序，并使用自动化证明助手 [45] 来构造、变换量子计算并对其进行推理。

Precision and conditional circuits with auxiliary qubits

定理 3 证明，对于每个 $k \geq 2$，自由模型在复数域上的酉矩阵标准模型中拓扑稠密。换言之，任意目标酉算子都可以由自由模型中的程序以任意精度逼近，这也证明了自由模型作为（可逆）量子计算模型的合理性。

定理 4 进一步表明，一旦具备干净辅助量子比特，精度参数 k 就不会影响表达能力： Π_{k+1} 可以使用单个辅助量子比特由Π_k 精确模拟。因此， k 只会影响项的规模和便利性，而不会影响哪些酉算子是可定义的。特别是， $k = 2$ 已经足以实现通用逼近。更大的 k 可以为同一目标酉算子生成更短得多的 Π_k 项，并且由于必须通过较长的编译序列表达的恒等式更少，也能让程序推理和在语法内证明代数性质变得更加容易。事实上，某些高度结构化的酉算子会显著受益于更多的基本相位。一个显著的例子是量子傅里叶变换（QFT），其相位角是 $1/2$的精确幂，因此是研究 k 对综合成本影响的理想案例。

每个 n量子比特的量子傅里叶变换（QFT）包含 $O(n^2)$个受控相位门，其角度为 $2\pi/2^d$ ，其中$2 \leq d \leq n$ [44]。由于 Π_k 将分母为 2^k 的所有相位都作为基本相位，只有较小角度的旋转需要近似；每个旋转的代价为 $O(\log_2(1/\varepsilon))$，其中 ε是近似 [32, 46]的精度。增加 k 会减少需要近似的旋转数量，直到 k 达到 n；此后，所有旋转都可直接使用，规模稳定在 $O(n^2)$。这一明显的截断点源于 QFT 角度的结构性；对于缺乏这种对齐关系的一般酉变换，增加 k 只能改善常数因子，并不能消除 $O(\log(1/\varepsilon))$的综合开销。

除了降低相位综合的成本， Π_k 形式体系还能生成规模更小的受控电路。近期的编译技术表明，利用高阶根并将闲置量子比特重复用作临时工作空间，可以在线性复杂度下分解多重受控运算，而无需辅助量子比特 [27]。这意味着，提高 k 不仅能缩短程序中相位综合部分的长度，还能降低条件语句和受控子程序的开销，进一步放大高精度带来的实际优势。

Measurement

最后，我们讨论如何通过将（计算过程中的）量子测量、辅助量子比特的初始化以及经典控制纳入上述可逆量子计算论述，免费替换关于测量的标准公设。测量要求我们处理混合态，而非纯态。这意味着，自由模型的对象不再能是表示维度的自然数，而应是自然数列表，用来表示按测量结果分支的维度，从而实现经典控制。

从 m 到 n 个量子比特的不可逆量子计算，可以通过从 $m+n$ 到 $m+n$ 个量子比特的可逆量子计算，利用量子信息效应 [23] 完美模拟。这是另一种自由构造，它引入了以一种同时符合顺序复合（$\circ$）和并行复合（$\otimes$）的方式隐藏信息的能力，这遵循退相干的指针态选择解释 [56]。可以将其视为另一种编程语言，在

这种编程语言中，辅助量子比特、经典控制和测量可以在量子程序的任何位置随意使用，随后编译成仅在末尾进行一次测量的量子程序。下文的定理 5 指出，两个包含测量的此类程序表示相同的量子信道，当且仅当它们能够通过使用一组有限方程进行代换而被证明相等——详情请参阅补充信息。在这一构造中，全局相位在物理上无关紧要，这是因为信息隐藏具有均匀性，将所有全局相位压缩为同一个点。

与 n 量子比特的混合态对应于量子信道 $\mathbb{C} \to (\mathbb{C}^2)^{\otimes n}$ 类似， A 自由模型中某个对象的状态对应于态射 $1 \to A$。输入态 $\rho\colon 1 \to A$ 沿着运算 $f\colon A \to B$ 复合演化，从而得到输出态 $f \circ \rho\colon 1 \to B$。因此，概率是自由模型中的一个派生概念，混合态由其纯化的等价类表示。

Bipermutative categories: formalising the main results

现在，我们先概述技术发展过程，详细内容请参阅补充信息。范畴由对象以及对象之间的态射组成，使得态射 $f\colon A \to B$ 和 $g\colon B \to C$ 可以复合为 $g \circ f\colon A \to C$（通常简写为 gf），且复合满足结合律；每个对象 [40]上都有恒等态射 $\mathsf{id}\colon A \to A$ 。范畴无需借助标准模型 [24]，便能完整刻画量子理论。严格对称幺半范畴还具有对象 $A \otimes B$，适用于任意两个对象 A 和 B；对于任意态射 $f\colon A \to C$ 和 $g\colon B \to D$，还具有态射 $f \otimes g\colon A \otimes B \to C \otimes D$；此外，它有一个单位对象 $\mathsf{1}$，满足 $1 \otimes A = A$，以及一个交换态射 $\sigma\colon A \otimes B \to B \otimes A$，使得 $(\mathsf{id} \otimes g) \circ (f \otimes \mathsf{id}) = (f \otimes \mathsf{id}) \circ (\mathsf{id} \otimes g)$ 且 $\sigma \circ \sigma = \mathsf{id}$ [25]。态射 $s\colon 1 \to 1$ 称为标量，任意态射 $f\colon A \to B$ 都可以乘以标量 s 进行缩放，得到 $s \cdot f\colon A \to B$，且这种标量乘法与所有其他运算 [25]可交换。双置换范畴是一个以两种方式成为严格对称幺半范畴的范畴，分别为 $(\otimes, \mathsf{1})$ 和 $(\oplus, 0)$，并且满足 $(A \oplus B) \otimes C = (A \otimes C) \oplus (A \otimes B)$，以及三个自然方程 [41]。当一个范畴满足图 1 [40]中的条件时，它在某种性质下称为自由范畴。

定理 1. 存在一个自由双置换范畴 Π_k，其生成元为 $\zeta_k\colon 1 \to 1$ 和 $V\colon 1 \oplus 1 \to 1 \oplus 1$，满足公理(1)–(3)。

回顾一下，与任何自由模型一样， Π_k 在唯一同构的意义下是唯一的。例如，Π_0 是这样一个范畴：其对象是自然数，其态射是 $\{1, \ldots, n\}$的排列，并且它只有一个平凡标量。双置换范畴的另一个例子是**酉算子**(R)，其中对象是自然数，态射是带对合环 R上的酉矩阵，标量是 R的元素。例如， R 可以是二进有理数环 $\mathbb{D} = \mathbb{Z}[\frac{1}{2}] = \{2^{-n} z \mid n \in \mathbb{N}, z \in \mathbb{Z}\}$，并附加一个本原 2^k次单位根 ζ_k。

定理 2. 存在一个同构 $\Pi_2 \simeq$ **酉算子**$(\mathbb{D}[\zeta_2])$ 的双置换范畴。

证明概要。 Π_2 的自由性给出了一个从 Π_2 到**酉算子**$(\mathbb{D}[\zeta_2])$的函子，并且该函子在对象上是双射。它在态射上也是双射，因为 Π_2 满足生成**酉算子**$(\mathbb{D}[\zeta_2])$的方程 [10]。□

正如量子电路只是一种形式化图表， Π_k 中的态射也是量子程序的源代码。要实际执行计算，必须为其赋予含义，就像将量子电路解释为酉矩阵一样。这种含义的赋予保留了计算的结构。

定理 3. 对于任意精度级别 k，都存在一个从 $[\![-]\!]$ 到 **酉算子**$(\mathbb{C})$ 的嵌入 Π_k，且对于 $k \geq 2$，其像是稠密的。

证明概要。 在精度 $k = 2$下，范畴 Π_2 已经包含 CCX 门以及所有克利福德门（相差一个全局相位）。这足以在不使用辅助量子比特的情况下近似任意复酉矩阵 [5]。□

类似地，双置换范畴之间的平移是一个保留 $\circ$和 $\oplus$的函数。

定理 4. 存在一个从 Π_{k+1} 到 Π_k 的平移 Φ，对于 $k \geq 2$，使得 f 和g在 Π_{k+1} 中满足 $[\![f]\!] = [\![g]\!]$，当且仅当 $[\![\Phi(f)]\!] = [\![\Phi(g)]\!]$ 属于 Π_k。

证明概要。 这一构造通过使用一个辅助量子比特来模拟给定标量的平方根，并注意到 Π_{k+1} 满足这一点，从而推广了 [48] 。□

补充信息详细介绍了一种自由构造，它向双置换范畴 Π_k 添加初始化态射、退相干态射和经典控制，从而将其转化为严格幺半范畴 $\mathbf{Split(LR(\Pi_k))}$ [23], ，并给出一种等价关系 $\approx_k$，该关系在存在辅助量子比特时将相等的计算视为相同。

定理 5。 对于任意精度级别 k，都存在一个包含映射 $[\![-]\!]$，将$\mathrm{Split}(\mathrm{LR}(\Pi_k))$ 映入有限维 C^*-代数之间完全正线性映射所构成的范畴；并且， $[\![f]\!] = [\![g]\!]$ 当且仅当 $f = g$ 属于 $\mathrm{Split}(\mathrm{LR}(\Pi_k))$。计算 f 和g 在 Π_k 中相等，当且仅当 $f \approx_k g$ 仅相差一个全局相位。

证明概要。量子信道范畴有一种已知的表示法 [51]„ 只需验证 $\mathbf{Split(LR(\Pi_k))}$ 满足其方程即可。□

Reasoning

在 Π_k 中的推理是精确的、符号化的，而且完备。即使是像 $HH = \mathsf{id}$ 这样看似简单的恒等式，标准方法也会遇到困难。一种做法是使用元素涉及代数数的矩阵，这使得精确证明极为棘手，而且本质上属于数论范畴。虽然存在针对这些问题的判定程序，但其复杂度令人难以应付。根本问题在于，代数数理论无法用有限多个公理公理化。相比之下， H 以及所有其他门在 Π_k 中都表示为由一小组有限方程支配的组合对象。这些方程既可靠（所有可推导的等式在满足这些公理的所有模型中都成立），又完备（这类模型中所有成立的等式都可以推导出来）。因此，从最简单的恒等式到最复杂的优化，所有推理都无需近似、无需专用常数，也无需脱离符号框架。

举一个简单的例子，让我们完全在 Π_k 内证明恒等式 $HH = \mathsf{id}$。在Π_k 中结合 $k \geq 3$, 定义

$$\omega := \zeta_k^{2^{k-3}}, \qquad S := \mathrm{id} \oplus \omega^2, \qquad H := \omega^{-1} \cdot (VSV).$$

从 H^2 开始:

$$\begin{aligned} H^2 &= \left(\omega^{-1} \cdot VSV\right)\left(\omega^{-1} \cdot VSV\right) \\ &= \omega^{-2} \cdot VSVVSV && \text{（标量的中心性）} \\ &= \omega^{-2} \cdot V\left(SXS\right)V && \text{（根据公理 (1)）。} \end{aligned}$$

展开定义 $S = \mathsf{id} \oplus \omega^2$，并利用 $\oplus$-交换尊重 $\circ$这一事实，可得:

$$\begin{aligned} SXS &= \left(\mathrm{id} \oplus \omega^2\right) X \left(\mathrm{id} \oplus \omega^2\right) \\ &= \left(\mathrm{id} \oplus \omega^2\right)\left(\omega^2 \oplus \mathrm{id}\right) X \\ &= \left(\omega^2 \oplus \omega^2\right) X \\ &= \omega^2 \cdot X && \text{（标量的分配性）。} \end{aligned}$$

代回:

$$\begin{aligned} H^2 &= \omega^{-2} \cdot V\left(\omega^2 \cdot X\right)V \\ &= VXV && \text{（标量的中心性）} \\ &= V^4 && \text{（根据公理 (1)）} \\ &= X^2 \\ &= \mathrm{id} && (\text{since } X^2 = \sigma_\oplus^2 = \mathrm{id}). \end{aligned}$$

因此，对于所有 $k \geq 3$，仅使用三条公理 (1)–(3) 以及双置换范畴的公理（其中包括所用标量的所有代数性质，例如中心性和分配律），即可在 Π_k 中推导出 $HH =$id。

Conclusion

我们为量子计算提供了一种等式公理化及其配套的自由模型，该模型不使用复数，其本质完全是离散且组合性的。由此得到的量子编程语言足以表达任何量子计算（如定理 3 所述），并且相对于标准模型，不会损失任何普适性或推理能力。无需复线性代数；在这一量子计算的普适模型中，可以充分运用组合优化的全部能力，以自动化方式操作量子程序，从而进行优化、规约和正确性验证。判断两个布尔电路是否等价，在最坏情况下是一个难以处理的问题 [14], ，但实践中出现的情形可以通过启发式方法高效解决 [15]。判断两个量子电路是否等价则是一个更难处理的问题 [29], ，因为这还需要比较两个实数是否相等。由于判断 $\mathbb{D}[\zeta_2]$ 中的两个元素是否相等是高效的，因此可以通过启发式方法高效处理我们的自由模型。此外，这种公理化在基础层面令人满意：它建立在经典可逆计算之上，与各种量子计算硬件平台相联系，并将量子优势归结为能够求取性质良好的平方根。

文献大多研究由量子比特数 n参数化的酉群 $U_{2^n}(\mathbb{C})$，但除此之外并不考察该族中各个群之间的任何关系。若改用双置换范畴

则意味着定理 1 的自由模型在电路规模或门数方面的完备性不受任何限制。更精确地说，公理 (1)–(3) 这一集合并非随量子比特数或门数 [55], 增长并依赖于它们的方程集合，而是对所有可在 Π_k 中表达的电路同时完备。

References

[1] S. Aaronson 和 L. Chen。量子霸权实验的复杂性理论基础。载于 *Computational Complexity Conference*，第 22:1–67 页，2017 年。[2] D. S. Abrams 和 S. Lloyd。在通用量子计算机上模拟多体费米系统。*Physical Review Letters*，97:2586–2589，1997 年。[3] S. Abramsky 和 B. Coecke。量子协议的范畴语义。载于 *Proceedings of the IEEE Symposium on Logic in Computer Science* 415 425, 2004，第 – 页。

[4] M. Amy、A. N. Glaudell、S. Kelso、W. Maxwell、S. S. Mendelson 和 N. J. Ross。多量子比特Clifford-分圆电路的精确综合。载于 *Reversible Computation*，*Lecture Notes in Computer Science* 第 14680 卷，第 238–245 页，海德堡，2024 年。Springer出版社。[5] M. Amy、A. N. Glaudell 和 N. J. Ross。某些受限 Clifford+T 电路的数论刻画。*Quantum*，4:252，2020 年。[6] P. Andres-Martinez、C. Heunen 和 R. Kaarsgaard。部分量子映射的泛性质。载于 *Quantum Physics and Logic*，*Electronic Proceedings in Theoretical Computer Science* 第 394 卷，第 192–207 页，2023 年。[7] F. Arute、K. Arya、R. Babbush、D. Bacon、J. C. Bardin、R. Barends、R. Biswas、S. Boixo、F. G. S. L. Brandao、D. A. Buell、B. Burkett、Y. Chen、Z. Chen、B. Chiaro、R. Collins、W. Courtney、A. Dunsworth、E. Farhi、B. Foxen、A. Fowler、C. Gidney、M. Giustina、R. Graff、K. Guerin、S. Habegger、M. P. Harrigan、M. J. Hartmann、A. Ho、M. Hoff mann、T. Huang、T. S. Humble、S. V. Isakov、E. Jeffrey、Z. Jiang、D. Kafri、K. Kechedzhi、J. Kelly、P. V. Klimov、S. Knysh、A. Korotkov、F. Kostritsa、D. Landhuis、M. Lindmark、E. Lucero、D. Lyakh、S. Mandr`a、J. R. McClean、M. McEwen、A. Megrant、X. Mi、K. Michielsen、M. Mohseni、J. Mutus、O. Naaman、M. Neeley、C. Neill、M. Y. Niu、E. Ostby、A. Petukhov、J. C. Platt、C. Quintana、E. G. Rieffel、P. Roushan、N. C. Rubin、D. Sank、K. J. Satzinger、V. Smelyan-skiy、K. J. Sung、M. D. Trevithick、A. Vainsencher、B. Villalonga、T. White、Z. J. Yao、P. Yeh、A. Zalcman、H. Neven 和 J. M. Martinis。使用可编程超导处理器实现量子霸权。*Nature*，574:505–510，2019 年。[8] U. Berger 和 H. Schwichtenberg。类型化 lambda 演算求值泛函的逆。载于 *[1991] Proceedings Sixth Annual IEEE Symposium on Logic in Computer Science*，第 203–211 页，1991 年。[9] A. B´erut、A. Arakelyan、A. Petrosyan、S. Ciliberto、R. Dillenschneider 和 E. Lutz。实验验证兰道尔原理：信息与热力学之间的联系。*Nature*，483:187–190，2012 年。[10] J. Carette、C. Heunen、R. Kaarsgaard 和 A. Sabry。只需几个平方根，量子计算就能像 Π 一样简单。载于 *Proceedings ACM on Programming Languages*，第 8 卷，第 564 页，2024 年。[11] E. G. Cate 和 D. W. Twigg。原位转置分析。*ACM Transactions on Mathematical Software* 3 104 110, 1977，：–。[12] V. Choudhury、J. Karwowski 和 A. Sabry。可逆编程中的对称性。载于 *Proceedings ACM on Programming Languages* 6, 6, 2022，卷，页。[13] B. Coecke 和 R. Duncan。交互式量子可观测量：范畴代数与图示法。*New Journal of Physics*，13:043016，2011 年。[14] S. Cook。定理证明过程的复杂性。载于 *ACM Symposium on Theory of Computing* 151 158, 1971，第 – 页。[15] M. Davis、G. Logemann 和 D. Loveland。用于定理证明的机器程序。*Communications of the ACM* 5 394 397, 1962，：–。[16] N. de Beaudrap、A. Kissinger 和 J. van de Wetering。ZX图的电路提取是#P难的。载于 *International Colloquium on Automata Languages and Programming*，*Leibniz International Proceedings in Informatics* 第 229 卷，第 119:1–19 页，2022 年。

[17] F. Del Santo 和 N. Gisin。无决定论的物理学：经典物理学的替代性解释。 *Physical Review A*, 100:062107，2019 年。[18] N. Dershowitz 和 J. P. Jouannaud。 *Handbook of Theoretical Computer Science (vol B): formal models and semantics* 1990 ，章节：重写系统。爱思唯尔，。[19] D. Deutsch。量子理论、丘奇–图灵原理与通用量子计算机。 *Proceedings of the Royal Society A*，400:97–117，1985 年。[20] R. Gl¨uck 和 T. Yokoyama。从编程语言视角看可逆计算。*Theoretical Computer Science*，953:113429，2023 年。[21] D. Gottesman。量子计算机的海森堡表示。载于 *International Colloquium on Group Theoretical Methods in Physics* *Proceedings of the* 32 43, 1999 ，第 – 页。[22] C. Hermida 和 R. D. Tennent。幺半群范畴不定元与可能世界范畴。*Theoretical Computer Science*, 430:3–22，2012 年。[23] C. Heunen 和 R. Kaarsgaard。量子信息效应。载于 *Proceedings ACM on Programming Languages* 6, 1 27, 2022 ，卷，页 –。[24] C. Heunen 和 A. Kornell。希尔伯特空间范畴的公理。 *Proceedings of the National Academy of Sciences* 119 2117024119, 2022 ，:e。[25] C. Heunen 和 J. Vicary。 *Categories for Quantum Theory*。牛津大学出版社，牛津，2019 年。[26] M. Howard、J. Wallman、V. Veitch 和 J. Emerson。情境性为量子计算提供了“魔力”。 *Nature*，510:351–355，2014 年。[27] K. Huang 和 J. Palsberg。不使用辅助量子比特编译条件量子门。 *Proceedings ACM on Programming Languages*，8，2024 年。[28] G. Janelidze 和 G. M. Kelly。关于幺半范畴作用的一则短注。 *Theory and Applications of Categories* 9 61 91, 2001 ，:–。[29] D. Janzing、P. Wocjan 和 T. Beth。“非恒等性检验”是QMA完全问题。 *International Journal of Quantum Information* 3 3 463 473, 2005 ，( ): –。[30] R. Jozsa 和 N. Linden。纠缠在量子计算加速中的作用。*Proceedings of the Royal Society of London A*, 459:2011–2032，2003 年。[31] A. Yu Kitaev。量子计算：算法与纠错。 *Russian Mathematical Surveys* 52 6 1191 1249, 1997 ，( ): –。[32] A. Yu. Kitaev、A. H. Shen 和 M. N. Vyalyi。 *Classical and Quantum Computation*。美国数学学会，2002 年。[33] Vadym Kliuchnikov、Dmitri Maslov 和 Michele Mosca。使用常数数量的辅助量子比特，通过 Clifford 和 T 电路对单量子比特酉变换进行渐近最优近似。 *Phys. Rev. Lett.*，110:190502，2013 年 5 月。[34] B. Korte 和 J. Vygen。 *Combinatorial optimization*。Springer出版社，海德堡，2000 年。[35] R. Landauer。计算过程中的不可逆性与热产生。 *IBM Journal of Research and Development* 5 183 191, 1961 ，:–。[36] R. Landauer。信息具有物理性。 *Physics Today*，44:23–29，1991 年。[37] M. L. Laplaza。分配律的相干性。载于 *Coherence in Categories*，第 29–65 页，海德堡，1972 年。Springer出版社。[38] A. P. Lund、A. Laing、S. Rahimi-Keshari、T. Rudolph、J. L. O’Brien 和 T. C. Ralph。基于高斯态的玻色子采样。 *Physical Review Letters*，113:100502，2014 年。[39] S. Mac Lane。范畴代数。 *Bulletin of the American Mathematical Society* 71 40 106, , :–。[40] S. Mac Lane。 *Categories for the Working Mathematician*。Springer出版社，海德堡，1969 年。[41] J. P. May。 *E_∞ Ring spaces and E_∞ ring spectra*。Springer出版社，海德堡，1977 年。[42] Y. Nam、N. J. Ross、Y. Su、A. M. Childs 和 D. Maslov。带连续参数的大型量子电路自动优化。 *npj Quantum Information*，4:23，2018 年。[43] Gabriele Nebe、E. M. Rains 和 N. J. A. Sloane。Clifford群的不变量。*Designs Codes and Cryptography*，24(1):99–122，2001 年 9 月。[44] M. A. Nielsen 和 I. L. Chuang。 *Quantum computation and quantum information*。剑桥大学出版社，剑桥，2010 年。[45] U. Norrell。Agda 中的依赖类型编程。载于 *Proceedings ACM on Types in Language Design and Implementation* 1 2, 2009 ，第 – 页。[46] N. J. Ross 和 P. Selinger。对 z 旋转进行最优的无辅助量子比特 Clifford+T 近似。 *Quantum Information and Computation*，16:901–953，2016 年。

[47] P. Selinger。dagger 范畴中的幂等元。载于 *Quantum Physics and Logic*, *Electronic Notes in Theoretical Computer Science*第 210 卷，第 107–122 页，阿姆斯特丹，2008。爱思唯尔。[48] Y. Shi。Toffoli 与受控非门只需少量辅助即可实现通用量子计算。*Quantum Information and Computation*，3(1):84–92，2003。[49] P. W. Shor。量子计算机上素因数分解与离散对数的多项式时间算法。 *SIAM Journal on Computing*，26:1484–1509，1997。[50] S. H. Simon。*Topological Quantum*。牛津大学出版社，牛津，2023。[51] S. Staton。代数效应、线性性与量子编程语言。载于 *Proceedings ACM on Programming Languages* 395 406, 2015 ，第 – 页。[52] V. Vedral。量子加速难以捉摸的来源。 *Foundations of Physics* 40 1141 1154, , : –。[53] G. Vidal。轻度纠缠量子计算的高效经典模拟。 *Physical Review Letters* 91 147902, 2003 2010 , : 。[54] D. J. Wineland、C. Monroe、W. M. Itano、D. Leidfried、B. E. King 与 D. M. Meekhof。囚禁原子离子相干量子态操控中的实验问题。 *Journalof Research of the National Institute of Standards and Technology*，103:259–328，1998。[55] M. Xu、Z. Li、O. Padon、S. Lin、J. Pointing、A. Hirth、H. Ma、J. Palsberg、A. Aiken、U. A. Acar 与 Z. Jia。Quartz：量子电路的超优化。载于 *Proceedings ACM on Programming Language Design and Implementation*，第 625–640 页，2022。[56] W. H. Zurek。退相干以及从量子到经典的转变。 *Physics Today*，10 36：–44，1991。

Appendix A. Supporting Information

本补充信息包含一项证明，证明文中所述的量子计算自由模型是可靠且完备的（定理 35），并证明有关项大小随精度变化的渐近标度的论断。前一项证明分三步进行：首先，我们将问题化简为仅含和的情形，从而无需考虑积；然后，我们在可逆设定下证明可靠性和完备性，直至辅助量子比特；最后，我们证明包括测量在内的完整模型的可靠性和完备性。我们假设读者熟悉量子计算中使用的范畴方法 [25] thoughout。

首先回顾双置换范畴的定义 [41, 37]。

定义 6. 双置换范畴 是一个范畴**C**，具有两种严格对称幺半结构 $(\otimes, I)$ 和 $(\oplus, O)$，其中

- 对于所有对象 A, B 以及所有态射 $f\colon A \to B$:

$$O \otimes A = O = A \otimes O$$
$$\mathrm{id}_O \otimes f = \mathrm{id}_O = f \otimes \mathrm{id}_O$$

- 对于所有对象 A, B, C 以及态射 f, g, h:

$$(A \oplus B) \otimes C = (A \otimes C) \oplus (B \otimes C)$$
$$(f \oplus g) \otimes h = (f \otimes h) \oplus (g \otimes h)$$

且下列图表交换：

$$\begin{array}{ccc} (A \oplus B) \otimes C & \xrightarrow{=} & (A \otimes C) \oplus (B \otimes C) \\ {\scriptstyle \sigma_\oplus \otimes \mathrm{id}}\downarrow & & \downarrow{\scriptstyle \sigma_\oplus} \\ (B \oplus A) \otimes C & \xrightarrow{=} & (B \otimes C) \oplus (A \otimes C) \end{array}$$

• 对于所有对象 A, B, C, D 该图表

$$\begin{array}{ccc}
(A \oplus B) \otimes (C \oplus D) & \xrightarrow{\quad = \quad} & (A \otimes (C \oplus D)) \oplus (B \otimes (C \oplus D)) \\
\downarrow{\scriptstyle \delta_L} & & \downarrow{\scriptstyle \delta_L \oplus \delta_L} \\
((A \oplus B) \otimes C) \oplus ((A \oplus B) \otimes D) & & (A \otimes C) \oplus (A \otimes D) \oplus (B \otimes C) \oplus (B \otimes D) \\
& \searrow^{=} & \downarrow{\scriptstyle \mathrm{id} \oplus \sigma_\oplus \oplus \mathrm{id}} \\
& & (A \otimes C) \oplus (B \otimes C) \oplus (A \otimes D) \oplus (B \otimes D)
\end{array}$$

交换，其中 δ_L 是复合

$$A \otimes (B \oplus C) \xrightarrow{\sigma_\otimes} (B \oplus C) \otimes A \xrightarrow{=} (B \otimes A) \oplus (C \otimes A) \xrightarrow{\sigma_\otimes \oplus \sigma_\otimes} (A \otimes B) \oplus (A \otimes C).$$

严格双置换函子是一个函子，它对于 $(\otimes, I)$ 和 $(\oplus, O)$ 都是严格对称幺半的。

当一个双置换范畴的对象是自然数，且其幺半结构为 $n \otimes m = nm$ （单位元为 1）和 $n \oplus m = n + m$（单位元为 0）时，它是半单的。

我们所有的自由模型都是双置换范畴，但有些其他模型的结构较弱，例如有限维 C*-代数与量子信道的标准模型。它们是*rig* 范畴，其中（$A \oplus B$）$\otimes C$ 不一定等于（$A \otimes C$）$\oplus$（$B \otimes C$），而可能仅与之同构。无妨：任何 rig 范畴都与某个双置换范畴 rig 等价 [41, 37]。

在任意幺半范畴（$\mathbf{C}$ $\otimes, I$）中，都可以将任意态射 $f\colon\ A \to B$与一个标量 $s\colon\ I \to I$ 相乘，得到 $s \cdot f\colon\ A \to B$，如下列复合所示。

$$A \cong I \otimes A \xrightarrow{s \otimes f} I \otimes B \cong B$$

Tensor products

请注意，公理（1）–（3）只涉及 $\circ$ 和 $\oplus$，不涉及 $\otimes$。此外，Π_k 的对象只是自然数。我们将证明，在每个这样的范畴中，$\otimes$ 都可以由 $\oplus$重构。准确地说，我们使用*PROP*s（积与置换范畴） [39]：严格对称幺半范畴（$\mathbf{C}$ $\oplus, 0$），其中对象是自然数，对象的和就是自然数的加法。*PROP* 的态射是 PROPs 之间保持对象不变的严格对称幺半函子。

对于自然数 n 和 m，在 PROP 的对象上定义乘积 $n \cdot m$：将 n 与自身进行 m 重求和；并定义态射的克罗内克积 $f \otimes g\colon\ m \to m'$ 和 $g\colon\ n \to n'$ 为

$$mn \xrightarrow{n \cdot f} nm' \xrightarrow{\pi_{n,m'}} m'n \xrightarrow{m' \cdot g} m'n' \xrightarrow{\pi_{m',n'}} n'm'$$

其中 $n \cdot f = f \overbrace{\oplus \cdots \oplus f}^{n \text{ times}}$和 $\pi_{m,n}$是重新索引 $mn \to nm$，它将序数 $m \times n$ 上的字典序映射到序数 $n \times m$上的字典序。具体而言， [11]:

$$\pi_{m,n}(x) = \begin{cases} nx \bmod mn - 1 & \text{if } x \neq mn - 1, \\ mn - 1 & \text{if } x = mn - 1. \end{cases}$$

一般而言，无法保证 $(f \otimes \mathrm{id}) \circ (\mathrm{id} \otimes g) = (\mathrm{id} \otimes g) \circ (f \otimes \mathrm{id})$。因此，PROP 不一定会以这种方式诱导出一个半单双置换范畴，但是

任何半单双置换范畴都是满足额外方程的 PROP。为确立这一主张，我们将证明每个态射——即使表面上是以积定义的——都等于一个仅以和定义的态射。对于对象而言，这一点根据构造已然成立。对于态射而言：

$$\begin{aligned} f \otimes g &= (f \otimes \mathrm{id}_n) \circ (\mathrm{id}_m \otimes g) \\ &= \sigma_\otimes \circ (\mathrm{id}_n \otimes f) \circ \sigma_\otimes \circ (\mathrm{id}_m \otimes g) \\ &= \sigma_\otimes \circ (\underbrace{f \oplus \cdots \oplus f}_{n \text{ times}}) \circ \sigma_\otimes \circ (\underbrace{g \oplus \cdots \oplus g}_{m \text{ times}}). \end{aligned}$$

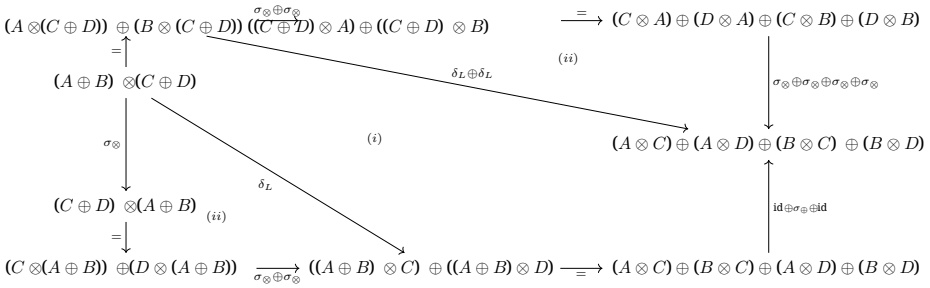
根据定理 6 中的三个相干态射，只需证明 $\sigma_\otimes$ 总能表示为若干 $\sigma_\oplus$ 的和的复合；因为 δ_L 已由若干个它的和导出，而 $\sigma_\oplus$ 已按该和定义。

引理 7。 在半单双置换范畴中，乘法对称性

$$\sigma_\otimes \colon (A \oplus B) \otimes (C \oplus D) \to (C \oplus D) \otimes (A \oplus B)$$

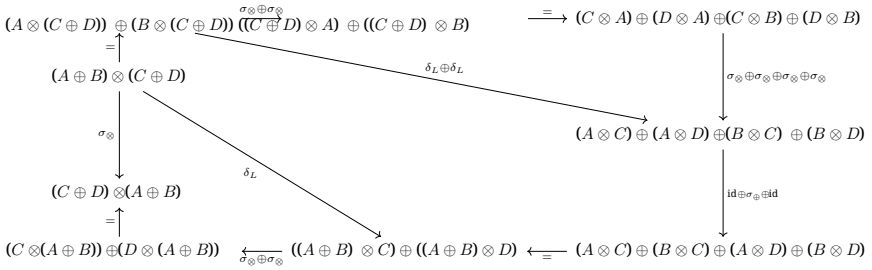
可用严格更小对象 $A \otimes (C \oplus D)$、 $B \otimes (C \oplus D)$、 $C \otimes (A \oplus B)$、 $D \otimes (A \oplus B)$、 $C \otimes A$、 $D \otimes A$、 $C \otimes B$、$D \otimes B$ 上的对称性 $\sigma_\otimes$ ，以及加法对称性 $\sigma_\oplus$ 来表示。

证明。 对于基础情形，注意到对称性 $\sigma_\otimes \colon 1 \otimes n \to n \otimes 1$ 和 $\sigma_\otimes \colon n \otimes 1 \to 1 \otimes n$ 对任意 n 都是恒等态射。对于 $m > 1$，注意以下图表是可交换的：



事实上，(i) 根据相干条件 [37, (IX)] 交换，而 (ii) 根据 δ_L 的定义交换。因为 $\sigma_\otimes \colon B \otimes A \to A \otimes B$ 是 $\sigma_\otimes \colon A \otimes B \to B \otimes A$ 的逆，所以下面的图表也交换：

(1)



□

引理 8。 在半单双置换范畴中，每个乘法对称性$\sigma_\otimes \colon \ m \otimes n \to n \otimes m$ 都可以构造为恒等态射之和与加法对称性的复合 $\sigma_\oplus$。

证明。 我们在字典序下对序对 $[m,n]$ 进行良基归纳。记 $\sigma_{\otimes[m,n]}$ 为乘法对称性 $m \otimes n \to n \otimes m$。

基础情形 $m = n = 0$ 是平凡成立的，因为此时 $\sigma_\otimes = \mathrm{id}_0$。对于归纳步骤，假设 $\sigma_{\otimes[m',n']}$ 是由恒等式之和与加法对称组成的复合 $\sigma_\oplus$，其中所有 (m',n') 均按字典序先于 (m,n)。根据上文证明中的图表 (1)，$\sigma_{\otimes[m,n]}$ 是由恒等式之和以及 $\sigma_{\otimes[n-1,m]}$、$\sigma_{\otimes[1,m]}$、$\sigma_{\otimes[n-1,m-1]}$、$\sigma_{\otimes[n-1,1]}$、$\sigma_{\otimes[1,m-1]}$、$\sigma_{\otimes[1,1]}$、$\sigma_{\otimes[m-1,n]}$ 和 $\sigma_{\otimes[n,1]}$ 的复合，同时还包括 $\sigma_{\oplus}$。除 $[m-1,n]$ 外，所有这些指标的字典序都先于 $[n,m]$。因此，对于除 $\sigma_{\otimes[m-1,n]}$ 之外的所有乘法对称，我们都可以应用归纳假设，将它们写成恒等式之和与加法对称的复合。

为构造 $\sigma_{\otimes[m-1,n]}$，注意到 $\sigma^{-1}_{\otimes[m-1,n]} = \sigma_{\otimes[n,m-1]}$。运用归纳法，将 $\sigma_{\otimes[n,m-1]}$ 构造为恒等态射之和与加法对称的复合。由于恒等态射和加法对称的逆仍分别是恒等态射和加法对称，因此我们可以立即构造出形式正确的 $\sigma_{\otimes[m-1,n]}$。 □

定理 9. 半单双置换范畴是 *PROPs*，而且半单双置换范畴之间的函子是严格双置换函子，当且仅当它是 *PROP* 态射。

证明。 根据定义，半单双置换范畴的对象恰好是自然数。至于态射，根据分配律，每个态射的幺半积都可化为幺半群和与乘法对称的形式；根据定理 8，半单双置换范畴的每个相干同构——进而，双置换范畴的每个相干条件——都可以用严格对称幺半群结构 $(\oplus, 0)$ 表示。

若 $F\colon \mathbf{C} \to \mathbf{D}$ 是半单双置换范畴之间的函子，则立即可知，如果 F 是一个严格双置换函子，那么它也是一个 PROP 态射。反之，设 F 是一个 PROP 态射。由于 $F(n) = n$ 在态射上尤其有 $F(1) = 1$，因此在对象上它保持乘法单位元。在态射上，由定理 8 可得 $F(\sigma_\otimes) = \sigma_\otimes$，因为 $\sigma_\otimes$（在**C**和**D**中）完全由严格对称幺半结构（$\oplus$，0）构造而成，而该结构由 F 精确保持。此外，F 严格保持幺半积:

$$
\begin{aligned}
F(f \otimes g) &= F((f \otimes \mathrm{id}_n) \circ (\mathrm{id}_m \otimes g)) \\
&= F(\sigma_\otimes \circ (\mathrm{id}_n \otimes f) \circ \sigma_\otimes \circ (\mathrm{id}_m \otimes g)) \\
&= F(\sigma_\otimes \circ (\underbrace{f \oplus f \oplus \cdots \oplus f}_{n \text{ times}}) \circ \sigma_\otimes \circ (\underbrace{g \oplus g \oplus \cdots \oplus g}_{m \text{ times}}) \\
&= F(\sigma_\otimes) \circ F(\underbrace{f \oplus f \oplus \cdots \oplus f}_{n \text{ times}}) \circ F(\sigma_\otimes) \circ F(\underbrace{g \oplus g \oplus \cdots \oplus g}_{m \text{ times}}) \\
&= F(\sigma_\otimes) \circ \underbrace{F(f) \oplus F(f) \oplus \cdots \oplus F(f)}_{n \text{ times}} \circ F(\sigma_\otimes) \circ \underbrace{F(g) \oplus F(g) \oplus \cdots \oplus F(g)}_{m \text{ times}} \\
&= \sigma_\otimes \circ \underbrace{F(f) \oplus F(f) \oplus \cdots \oplus F(f)}_{n \text{ times}} \circ \sigma_\otimes \circ \underbrace{F(g) \oplus F(g) \oplus \cdots \oplus F(g)}_{m \text{ times}} \\
&= \sigma_\otimes \circ (\mathrm{id}_n \otimes F(f)) \circ \sigma_\otimes \circ (\mathrm{id}_m \otimes F(g)) \\
&= (F(f) \otimes \mathrm{id}_n) \circ (\mathrm{id}_m \otimes F(g)) \\
&= F(f) \otimes F(g).
\end{aligned}
$$

因此，对于（$\otimes$，$\mathbf{1}$），F 也是一个严格对称幺半函子，进而使其成为严格双置换函子。□

由于已知自由 PROP 存在 [39], ，这证明了主文的定理 1。

命题 10. 存在一个自由双置换范畴 $\langle \zeta_k, S, V\rangle$，其生成元为$\zeta_k\colon 1 \to 1$ 与 $V\colon 1 \oplus 1 \to 1 \oplus 1$（对于 $k \geq 2$）。记 X 为对称态射$\sigma\colon 1 \oplus 1 \to 1 \oplus 1$，并记 S 为 $1 \oplus \zeta_k^{2^{k-2}}\colon 1 \oplus 1 \to 1 \oplus 1$。存在商 Π_k，即 $\langle \zeta_k, S, V\rangle$ 关于包含方程 (1)–(3) 的双置换范畴最小同余 $\sim_k$ 的商，且它是一个双置换范畴。

Cancellativity

请注意，在本节中，我们用 a, a', b, b', c 表示范畴 $\mathbf{C}$ 的态射。

接下来，我们将逐步证明 Π_k的可靠性和完备性。我们的证明将利用辅助对象，并依赖于以下性质。

定义 11. 若幺半范畴（$\mathbf{C}$ $\oplus, O$）满足以下条件，则称其具有强消去性

$$a \oplus b = a' \oplus b' \implies a = a' \text{ and } b = b'$$

对所有态射 $a, a'\colon A \to A'$ 以及 $b, b'\colon B \to B'$均成立。

任何嵌入到一个使 $\oplus$ 成为双积的范畴中的幺半范畴，都具有强消去性。这包括带对合环 R 上酉矩阵构成的 PROP **酉算子**(R)；该 PROP 嵌入到 R-模的幺半环范畴中，其中 $a \oplus b$ 是分块对角酉矩阵。我们认为，对于所有 k，Π_k 本身都具有强消去性（已知 $k = 2$ 的情形成立），但将其证明留作一个开放问题。我们在此只需使一个 PROP 具有强消去性。

命题 12. 任意对称幺半范畴 ($\mathbf{C}$ $\oplus, O$) 都有一个定义在 $a, a'\colon A \to A'$ 上的幺半同余：

$$a \approx a' \qquad \iff \qquad \exists b, b'\colon B \to B'\colon a \oplus b = a' \oplus b'$$

证明。 我们验证关系 $\approx$是一个幺半同余：

- 自反性。取 $b = b' = \mathrm{id}_I$ 可得 $a \approx a$。
- 对称性。假设 $a \approx a'$，也就是说，因为 $a \oplus b = a' \oplus b'$。那么也有$a' \oplus b' = a \oplus b$，因此 $a' \approx a$。
- 传递性。假设 $a \approx a'$，因为 $a \oplus b = a' \oplus b'$；并且 $a' \approx a''$，因为 $a' \oplus c' = a'' \oplus c''$。那么 $a \approx a''$，因为

$$\begin{aligned} a \oplus (c' \circ b) &= (1 \oplus c') \circ (a \oplus b) \\ &= (1 \oplus c') \circ (a' \oplus b') \\ &= (a' \oplus c') \circ (1 \oplus b') \\ &= (a'' \oplus c'') \circ (1 \oplus b') \\ &= a'' \oplus (c'' \circ b'). \end{aligned}$$

- 组合性。假设 $a \approx a'$因为 $a \oplus b = a' \oplus b'$对于 a，$a'\colon A \to A'$，并且 $c \approx c'$因为 $c \oplus d = c' \oplus d'$对于 c，$c'\colon A' \to A''$。那么 $ca \approx c'a'$因为

$$ca \oplus db = (c \oplus d)(a \oplus b) = (c' \oplus d')(a' \oplus b') = c'a' \oplus d'b'.$$

• 幺半性。假设 $a \approx a'$ 因为 $a \oplus b = a' \oplus b'$，并且 $c \approx c'$因为 $c \oplus d = c' \oplus d'$。那么

$$a \oplus b \oplus c \oplus d = a' \oplus b' \oplus c' \oplus d'$$

并通过与对称性复合，因此也

$$a \oplus c \oplus b \oplus d = a' \oplus c' \oplus b' \oplus d',$$

也就是说， $a \oplus c \approx a' \oplus c'$。

□

推论 13. 如果$(\mathbf{C}\ \oplus、\ O)$ 是一个对称幺半范畴，那么$\mathbf{C}/\approx$是一个定义良好的强消去对称幺半范畴。如果$\mathbf{C}$ 满足某个方程，那么$\mathbf{C}/\approx$也满足该方程。

证明。 第一条结论直接由定理 12 得出。第二条结论源于（对称）幺半函子 $\mathbf{C} \to \mathbf{C}/\approx$ 保持方程这一事实。□

现在我们可以定义主文中定理 2 和定理 3 所述的函子。

命题 14。 以下定义了一个对称幺半函子 $[\![-]\!]\colon \Pi_k \to$**酉算子**$(\mathbb{D}[\zeta_k])$：

$$[\![\zeta_k]\!] = e^{2\pi i/2^k} \qquad [\![V]\!] = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

证明。 注意，这些矩阵满足 (1)–(3)。 □

由于 **酉算子**$(\mathbb{D}[\zeta_k])$ 具有强消去性，因此还存在一个对称幺半函子 $\langle \zeta_k, S, V\rangle \to$ **酉算子**$(\mathbb{D}[\zeta_k])$。

定义 15。 对于 $k \geq 2$，在 Π_k 中定义以下标准态射：

$$-1 = \zeta_k^{2^{k-1}} \colon 1 \to 1 \qquad X = \sigma_\oplus \colon 2 \to 2$$

$$H = (\zeta_k^{2^{k-3}})^7 \bullet T_k^{2^{k-2}} V T_k^{2^{k-2}} \colon 2 \to 2 \ \ (k \geq 3) \qquad T_k = \mathrm{id} \oplus \zeta_k \colon 2 \to 2$$

环 $\mathbb{D}[\zeta_k]$ 有共轭 $x + \zeta_k y \mapsto (x + \zeta_k y)^* = x - \zeta_k y$，这个环自同构逐分量扩展为一个矩阵环上的自同构，其中矩阵的元素属于 $\mathbb{D}[\zeta_k]$。现在我们定义一种语法类比。

定义 16. 设 $a \in \Pi_k$ for $k \geq 2$。 a 的共轭 a^* 归纳定义如下：

- $(\mathrm{id}_n)^* = \mathrm{id}_n$;
- $(\sigma)^* = \sigma$;
- $(\zeta_k)^* = -\zeta_k$;
- $(V)^* = V$;
- $(ab)^* = (a)^*(b)^*$，对任意 a， b： $m \to m$;
- $(a \oplus b)^* = (a)^* \oplus (b)^*$，对任意 a： $m \to m$和 b： $n \to n$。

显然，利用归纳法可得 $[\![a^*]\!] = [\![a]\!]^*$。

定义 17。令 $k \geq 3$。催化嵌入 Φ_k： $\Pi_k \to \Pi_{k-1}$ 是一个对称幺半函子，其在对象上的定义为 $\Phi_k(n) = 2n$ ，在态射上的定义为

- $\Phi_k(\mathrm{id}_n) = \mathrm{id}_n \oplus \mathrm{id}_n$;
- $\Phi_k(\sigma) = \sigma \oplus \sigma$;

- $\Phi_k(\zeta_k) = X \circ (\mathrm{id} \oplus \zeta_{k-1})$;
- $\Phi_k(V) = V \oplus V$;
- $\Phi_k(ab) = \Phi_k(a)\Phi_k(b)$ 对于 $a,\ b\colon\ n \to n$;
- $\Phi_k(a \oplus b) = \sigma_{2,\ m+n}^{\otimes} \Phi_k(a) \oplus \Phi_k(b) \sigma_{2,\ m+n}^{\otimes}$，对于 $a\colon\ m \to m$ 和 $b\colon\ n \to n$。

对于 $n \in \mathbb{N}$，催化剂 $c_{k,\ n}\colon\ 2n \to 2n$ 是 $c_{k,\ n} = (H \circ T_k) \otimes \mathrm{id}_n$。

引理 18。如果 $a\colon\ n \to n$ 在 Π_k 中对于 $k \geq 3$，那么 $c_{k,\ n} \Phi_k(a) c_{k,\ n}^{\dagger} \sim_k a \oplus a^*$。

证明。对 a 进行结构归纳法。如果 $a = \mathrm{id}_n$，那么

$$\begin{aligned}
c_{k,n} \circ \Phi_k(a) \circ c_{k,n}^{\dagger} &\sim_k c_{k,n} \circ \Phi_k(\mathrm{id}_n) \circ c_{k,n}^{\dagger} \\
&\sim_k (HT \otimes \mathrm{id}_n) \circ \mathrm{id}_n \oplus \mathrm{id}_n \circ (T^{\dagger} H^{\dagger} \otimes \mathrm{id}_n) \\
&\sim_k (HT \otimes \mathrm{id}_n) \circ \mathrm{id}_2 \otimes \mathrm{id}_n \circ (T^{\dagger} H^{\dagger} \otimes \mathrm{id}_n) \\
&\sim_k (HT \circ \mathrm{id}_2 \circ T^{\dagger} H^{\dagger}) \otimes \mathrm{id}_n \\
&\sim_k \mathrm{id}_2 \otimes \mathrm{id}_n \\
&\sim_k \mathrm{id}_n \oplus \mathrm{id}_n \\
&\sim_k a \oplus a^*.
\end{aligned}$$

如果 $a = \sigma_{m,\ n}$，那么

$$\begin{aligned}
c_{k,m+n} \circ \Phi_k(a) \circ c_{k,m+n}^{\dagger} &\sim_k c_{k,m+n} \circ \Phi_k(\sigma_{m,n}) \circ c_{k,m+n}^{\dagger} \\
&\sim_k (HT \otimes \mathrm{id}_{m+n}) \circ \sigma_{m,n} \oplus \sigma_{m,n} \circ (T^{\dagger} H^{\dagger} \otimes \mathrm{id}_{m+n}) \\
&\sim_k (HT \otimes \mathrm{id}_{m+n}) \circ \mathrm{id}_2 \otimes \sigma_{m,n} \circ (T^{\dagger} H^{\dagger} \otimes \mathrm{id}_{m+n}) \\
&\sim_k (HT \circ \mathrm{id}_2 \circ T^{\dagger} H^{\dagger}) \otimes \sigma_{m,n} \\
&\sim_k \mathrm{id}_2 \otimes \sigma_{m,n} \\
&\sim_k \sigma_{m,n} \oplus \sigma_{m,n} \\
&\sim_k a \oplus a^*
\end{aligned}$$

如果 $a = \zeta_k$，那么

$$\begin{aligned}
c_{k,1} \circ \Phi_k(a) \circ c_{k,1}^{\dagger} &\sim_k c_{k,1} \circ \Phi_k(\zeta_k) \circ c_{k,1}^{\dagger} \\
&\sim_k (HT \otimes \mathrm{id}_1) \circ (X \circ (\mathrm{id} \oplus \zeta_{k-1})) \circ (T^{\dagger} H^{\dagger} \otimes \mathrm{id}_1) \\
&\sim_k HT \circ (X \circ (\mathrm{id} \oplus \zeta_{k-1})) \circ T^{\dagger} H^{\dagger} \\
&\sim_k H \circ T \circ X \circ T^2 \circ T^{\dagger} \circ H^{\dagger} \\
&\sim_k H \circ T \circ X \circ T \circ H^{\dagger} \\
&\sim_k H \circ (\zeta_k \oplus \zeta_k) \circ X \circ H^{\dagger} \\
&\sim_k (\zeta_k \oplus \zeta_k) \circ Z \\
&\sim_k \zeta_k \oplus -\zeta_k \\
&\sim_k a \oplus a^*
\end{aligned}$$

如果 $a = V$，那么

$$\begin{aligned} c_{k,2} \circ \Phi_k(a) \circ c_{k,2}^\dagger &\sim_k c_{k,2} \circ \Phi_k(V) \circ c_{k,2}^\dagger \\ &\sim_k (HT \otimes \mathrm{id}_2) \circ V \oplus V \circ (T^\dagger H^\dagger \otimes \mathrm{id}_2) \\ &\sim_k (HT \otimes \mathrm{id}_2) \circ \mathrm{id}_2 \otimes V \circ (T^\dagger H^\dagger \otimes \mathrm{id}_2) \\ &\sim_k (HT \circ \mathrm{id}_2 \circ T^\dagger H^\dagger) \otimes V \\ &\sim_k \mathrm{id}_2 \otimes V \\ &\sim_k V \oplus V \\ &\sim_k a \oplus a^* \end{aligned}$$

若 $a = a_1 a_2$，对于 a_1，a_2：$m \to m$ 属于 Π_k，则根据归纳法，

$$\begin{aligned} c_{k,m} \circ \Phi_k(a) \circ c_{k,m}^\dagger &\sim_k c_{k,m} \circ \Phi_k(a_1 a_2) \circ c_{k,m}^\dagger \\ &\sim_k c_{k,m} \circ \Phi_k(a_1)\Phi_k(a_2) \circ c_k^\dagger \\ &\sim_k c_{k,m} \circ \Phi_k(a_1) \circ c_{k,m} \circ c_{k,m}^\dagger \Phi_k(a_2) \circ c_k^\dagger \\ &\sim_k a_1 \oplus a_1^* \circ a_2 \oplus a_2^* \\ &\sim_k (a_1 a_2) \oplus (a_1^* a_2^*) \\ &\sim_k a \oplus a^* \end{aligned}$$

最后，考虑这种情况：$a = a_1 \oplus a_2$，对于 a_1：$m \to m$ 以及 a_2：$n \to n$ 属于 $\Pi_{k\circ}$ 注意

$$\begin{aligned} c_{k,m+n} \circ \sigma_{2,m+n}^\otimes &\sim_k (HT \otimes \mathrm{id}_{m+n}) \circ \sigma_{2,m+n}^\otimes \\ &\sim_k \sigma_{2,m+n}^\otimes \circ (\mathrm{id}_{m+n} \otimes HT) \\ &\sim_k \sigma_{2,m+n}^\otimes \circ ((\mathrm{id}_m \oplus \mathrm{id}_n) \otimes HT) \\ &\sim_k \sigma_{2,m+n}^\otimes \circ ((\mathrm{id}_m \otimes HT) \oplus (\mathrm{id}_n \otimes HT)) \\ &\sim_k \sigma_{2,m+n}^\otimes \circ (c_{k,m} \oplus c_{k,n}). \end{aligned}$$

因此，根据归纳法，

$$\begin{aligned} c_{k,m+n} \circ \Phi_k(a) \circ c_{k,m+n}^\dagger &\sim_k c_{k,m+n} \circ \Phi_k(a_1 \oplus a_2) \circ c_{k,m+n}^\dagger \\ &\sim_k c_{k,m+n} \circ (\sigma_{2,m+n}^\otimes \Phi_k(a) \oplus \Phi_k(b) \sigma_{2,m+n}^\otimes) \circ c_{k,m+n}^\dagger \\ &\sim_k \sigma_{2,m+n}^\otimes (c_{k,m} \oplus c_{k,n}) \Phi_k(a) \oplus \Phi_k(b) (c_{k,m}^\dagger \oplus c_{k,n}^\dagger) \sigma_{2,m+n}^\otimes \\ &\sim_k \sigma_{2,m+n}^\otimes (a_1 \oplus a_1^*) \oplus (a_2 \oplus a_2^*) \sigma_{2,m+n}^\otimes \\ &\sim_k (a_1 \oplus a_2) \oplus (a_1^* \oplus a_2^*) \\ &\sim_k a \oplus a^*. \end{aligned}$$

□

现在我们可以证明主文中的定理 4。

引理 19. 若 $k \geq 3$，且 a，$b \in \Pi_k$ 满足 $[\![a]\!] = [\![b]\!]$，则 $[\![\Phi_k(a)]\!] = [\![\Phi_k(b)]\!]$。证明。令 a，$b \in \Pi_k$ 并假设 $[\![a]\!] = [\![b]\!]$，根据定理 18，

$$c_k \Phi_k(a) c_k^\dagger \sim_k a \oplus a^* \quad \text{and} \quad c_k \Phi_k(b) c_k^\dagger \sim_k b \oplus b^*.$$

由于公理相对于该解释是可靠的，因此

$$\begin{aligned}\llbracket c_k\rrbracket\llbracket\Phi_k(a)\rrbracket\llbracket c_k^\dagger\rrbracket &= \llbracket c_k\Phi_k(a)c_k^\dagger\rrbracket\\ &= \llbracket a\oplus a^*\rrbracket\\ &= \llbracket a\rrbracket\oplus\llbracket a\rrbracket^*\\ &= \llbracket b\rrbracket\oplus\llbracket b\rrbracket^*\\ &= \llbracket b\oplus b^*\rrbracket\\ &= \llbracket c_k\Phi_k(b)c_k^\dagger\rrbracket.\end{aligned}$$

我们得出结论：

$$\llbracket\Phi_k(a)\rrbracket = \llbracket c_k^\dagger\rrbracket\llbracket c_k\rrbracket\llbracket\Phi_k(a)\rrbracket\llbracket c_k^\dagger\rrbracket\llbracket c_k\rrbracket = \llbracket c_k^\dagger\rrbracket\llbracket c_k\rrbracket\llbracket\Phi_k(b)\rrbracket\llbracket c_k^\dagger\rrbracket\llbracket c_k\rrbracket = \llbracket\Phi_k(b)\rrbracket. \qquad \square$$

记 $\approx_k$ 为包含 $\sim_k$和 $\approx$的双置换范畴的最小同余。显然，若对 $a,b\in\Pi_k$有 $a\approx_k b$，则 $\llbracket a\rrbracket=\llbracket b\rrbracket$，也就是说， Π_k 的方程是可靠的。下面的定理表明完备性，即其逆命题。

定理 20。 设 $k\geq 2$。若 a、 $b\in\Pi_k$ 满足 $\llbracket a\rrbracket=\llbracket b\rrbracket$，则 $a\approx_k b$。

证明。 该证明通过对 k使用归纳法进行。基础情形 $k=2$ 已知 [10]。现假设该性质对 k成立，并设 $a,b\in\Pi_{k+1}$ 满足$\llbracket a\rrbracket=\llbracket b\rrbracket$。则 $\Phi_k(a)$ $\Phi_k(b)$ $\in\Pi_k$，并且由定理 19， $\llbracket\Phi_k(a)\rrbracket=\llbracket\Phi_k(b)\rrbracket$。因此，由归纳假设， $\Phi_k(a)\approx_k\Phi_k(b)$。故 $\Phi_k(a)$ $\approx_{k+1}$ $\Phi_{k+1}(b)$，从而 $C\Phi_k(a)C^\dagger\approx_{k+1}C\Phi_{k+1}(b)C^\dagger$。定理 18 现给出 $a',b'\in\Pi_{k+1}$，使其满足

$$a\oplus a'\approx_{k+1}C\Phi_{k+1}(a)C^\dagger\approx_{k+1}C\Phi_{k+1}(b)C^\dagger\approx_{k+1}b\oplus b'.$$

因此，根据强消去律 $a\approx_{k+1}b$。 $\square$

本补充信息其余部分的目标，是在下文的定理 35 中证明包含测量的自由模型的完备性。主要思路是将其归约为现有的代数公理化 [51]。这一过程分为四个阶段。在定义测量的自由模型之后，我们将精确定义模型如何验证方程。为了使这一点成立，随后我们将通过首先将问题归约为对有限集之间单射的操作，证明包含测量的自由模型支持经典控制。最后，我们即可验证所需的公理。

测量可以通过以下三个步骤自由地添加到任意模型中 [23, 6]。设**C** 为一个幺半环范畴。

(1) 自由添加初始化状态的能力。这将得到一个范畴 R(**C**)，其对象与**C**相同，但**C**中的态射 $A\to B$ 是来自**C** 的态射 {v10>，其中某个堆 对象为 H；当两个态射在预处理堆的意义下相等时，将它们视为相同。对于每个对象 A，在 R(**C**) 中都有唯一一个初始化状态的态射 $O\to A$。如果**C** 是酉矩阵的 PROP，那么 R(**C**) 就是等距映射范畴。

(2) 自由添加退相干。由此得到一个范畴 LR(**C**)，它与 **C** 具有相同的对象，但 LR(**C**) 中的态射 $A\to B$ 是 R(**C**) 中的态射 $A\to B\otimes G$，其中某个 辅助 对象 G；当态射在对辅助对象进行后处理后相等时，它们被视为相同。对于每个对象 A，LR(**C**) 中都有唯一的态射$A\to I$，它根据.....将系统 A 从实验者的控制中移除并交由环境，从而丢弃该系统。

Zurek 对退相干的解释 [56]。如果 C是酉矩阵的 PROP，那么 LR(C) 就是有限维希尔伯特空间和完全正线性映射构成的范畴，也称为量子信道。

(3) 自由加入经典控制，即 根据测量结果进行分支的能力。这会得到一个范畴 Split(LR(C))，其中对象是 LR(C) 中的投影 $p^\dagger = p^2 = p$：$A \to A$，而态射 $p \to p'$ 是 LR(C) 中满足条件 $p'fp = f$ 的 f：$A \to A'$。这也称为柯西完备化 或*Karoubi* 包络 [47]，，它具有如下泛性质：LR(C) 中对象 B 上的投影对应于 Split(LR(C)) 中的嵌入 $A \to B$。如果C 是酉矩阵的 PROP，那么 Split(LR(C)) 就是有限维 C*-代数与量子信道构成的范畴。

原幺半环范畴C的 $\oplus$ 在 Split(LR(C)) 中成为余积；要实现这一点，这些步骤的执行顺序没有选择余地 [23, 6]。

Algebraic theories

量子计算公理化中的一个重要步骤是 Staton 的量子计算代数理论 [51]。该理论表明，有限维 C*-代数和量子信道的理论可以归结为少量生成空间、信道以及它们之间的方程。简而言之，代数理论由两部分组成：

- 一些运算，每个运算都有一个元数 $p \to (n_1, \dots, n_m)$，这意味着该运算接受 p 个参数，并产生列表 $n_1, \dots, n_m$ 中指定数量的结果。运算既可以按顺序组合（参数数量相匹配时），也可以并行组合，从而形成项 t，用于描述计算。
- 一些方程，用于说明哪些项彼此相等。

顾名思义，这种结构与代数中的结构完全类似——例如组合群论，其中群是通过若干基本运算（生成元）以及群元素之间的方程（关系）来描述的。

量子计算代数理论由三种运算（以及十二个方程，此处暂且不予考虑）组成。这些运算是：

- 新建：$0 \to 1$ 分配一个处于状态 $|0\rangle$ 的新量子比特。
- 测量：$1 \to (0, 0)$，在计算基下测量一个量子比特，并将结果记录在输出的选择中。
- 应用U：$n \to n$ 应用一个 n 量子比特酉算子 U。

代数理论可以在具有足够结构以支持这些运算和方程的范畴中进行解释：

(1) 它必须具有余积，必须有一个特选对象 X，并且对于每个运算 O：$n \to n_1$，……，n_m，都有一个态射 $[\![O]\!]$：$n \bullet X \to (n_1 \bullet X + \cdots + n_m \bullet X)$ 对于 PROP **FinPerm** 的一个作用 $n \bullet -$，其态射$n \to n$ 是 $\{1, \dots, n\}$ 的排列（如果 $n \neq n'$，则不存在态射 $n \to n'$ ） [28]。（2）对于每个方程 $s = t$，态射 $[\![s]\!]$ 和$[\![t]\!]$ 必须相同：$[\![s]\!] = [\![t]\!]$。

这样的范畴称为该代数理论的模型 。

量子计算代数理论有一个自然的模型，即由有限维 C*-代数和量子信道构成的范畴。在这里，一个元数为（$p \mid n_1$、……、n_m）的项 t描述了一个量子信道 $[\![t]\!]$，它从代数 $M_p(\mathbb{C})$（由 2^p 行、2^p 列的矩阵构成）映射到矩阵代数的直和 $M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_m}(\mathbb{C})$。方程 $t = u$ 断言量子信道 $[\![t]\!]$ 和 $[\![u]\!]$执行相同的操作，即 $[\![t]\!] = [\![u]\!]$。令人惊讶的是，这个模型是完备的：如果 $[\![t]\!] = [\![u]\!]$ 成立（对任意选取的量子信道 t 和 u都如此），那么仅通过应用该代数理论的方程，就能证明这一点。

我们的目标是证明 Split(LR(Π_k)) 同样是 Staton 的量子计算代数理论的完备模型。为了使这一点有意义，我们首先详细解释范畴如何诠释代数理论。

若一个范畴$\mathbf{C}$ 要承载一个代数理论签名的结构，就必须具有一个作用 于 $\mathbf{FinPerm}$的作用：必须存在一个函子 $\bullet\colon \mathbf{FinPerm} \times \mathbf{C} \to \mathbf{C}$，以及自然同构 $0 \bullet X \cong X$ 和 $(n+m) \bullet X \cong n \bullet (m \bullet X)$，并满足某些相容条件。我们首先证明，任意对称幺半范畴$\mathbf{C}$ 都会为$\mathbf{FinPerm}$导出一族规范作用。

令 $A^{\otimes n}$ 表示对象 A 与自身的 n 重幺半积（选取一种规范的加括号方式，例如将所有括号向左结合），其中 $A^{\otimes 0} = I$。定义指数作用 为$\mathbf{C}$中对象 S的函子 $\bullet\colon \mathbf{FinPerm} \times \mathbf{C} \to \mathbf{C}$，其在对象上的作用由 $n \bullet X = S^{\otimes n} \otimes X$ 给出；对于态射 $(\pi\colon n \to n) \bullet (f\colon X \to Y) = \lceil \pi \rceil \otimes f$，其中 $\lceil \pi \rceil\colon S^{\otimes n} \to S^{\otimes n}$ 是唯一的置换，它利用自然对称 $\sigma_{X,\,Y}\colon X \otimes Y \to Y \otimes X$，按照置换 $\pi\colon n \to n$ 对 n 条不同的 S-线进行置换。

引理 21. 当$(\mathbf{C}, \otimes, I)$ 是一个对称幺半范畴，且 S 是$\mathbf{C}$的一个对象时，指数作用 S 在 $\otimes$ 上是$\mathbf{FinPerm}$ 在$\mathbf{C}$上的一个作用。

证明. 为看出 $\bullet\colon \mathbf{FinPerm} \times \mathbf{C} \to \mathbf{C}$ 具有双函子性，我们注意到

$$\mathrm{id}_n \bullet \mathrm{id}_X = \lceil \mathrm{id}_n \rceil \otimes \mathrm{id}_X = \mathrm{id}_{S^{\otimes n}} \otimes \mathrm{id}_X = \mathrm{id}_{S^{\otimes n} \otimes X} = \mathrm{id}_{n \bullet X}$$

and

$$\begin{aligned}(\pi_2 \bullet g) \circ (\pi_1 \bullet f) &= (\lceil \pi_2 \rceil \otimes g) \circ (\lceil \pi_1 \rceil \otimes f) \\ &= (\lceil \pi_2 \rceil \circ \lceil \pi_1 \rceil) \otimes (g \circ f) \\ &= \lceil \pi_2 \circ \pi_1 \rceil \otimes (g \circ f) \\ &= (\pi_2 \circ \pi_1) \bullet (g \circ f)\end{aligned}$$

利用如下事实：先按 π_1 、再按 π_2 置换 n 条线，与按它们的复合 $\pi_2 \circ \pi_1$置换这些线完全相同。为看出这是一个作用，我们首先注意到

$$0 \bullet X = S^{\otimes 0} \otimes X = I \otimes X \cong X$$

and

$$\begin{aligned}(n+m) \bullet X &= S^{\otimes n+m} \otimes X \\ &\cong S^{\otimes n} \otimes (S^{\otimes m} \otimes X) \\ &= n \bullet (m \bullet X)\end{aligned}$$

其中同构 $S^{\otimes n+m} \otimes X \cong S^{\otimes n} \otimes (S^{\otimes m} \otimes X)$ 利用结合律相应地移动括号。至于相容条件，我们可以不失一般性地假设 $\mathbf{C}$ 是严格对称幺半的，并注意到$\mathbf{FinPerm}$ 已经

是严格对称幺半的。在这个严格情形下，我们注意到上文给出的同构$\vartheta : (n + m) \bullet X \to n \bullet (m \bullet X)$和 $\nu\colon\ 0 \bullet X \to X$，以及 $\mathbf{C}$ 和$\mathbf{FinPerm}$的所有相干同构，都是恒等映射，因此三个相干条件 [28] 显然交换（因为涉及的每个态射都是恒等映射）。□

我们现在可以定义签名的结构了。我们将使用薛定谔绘景，而不是海森堡绘景 [51], 。为使下述定义有意义，必须存在余积，我们将在下文的定理 30 中使用它们。

定义 22. 一个签名 是一组具有元数 O 的运算： $p \to (m_1,\ \ldots\ldots,\ m_k)$，直观地表明运算 O 接受 p 个输入，并且可以产生 m_1、 m_2、.....或 m_k 个输出。设 $\mathbf{C}$ 具有 $\mathbf{FinPerm}$ 的作用。$\mathbf{C}$ 中签名的结构是一个对象 X，并且对每个运算 $O\colon\ p \to (m_1,\ \ldots\ldots,\ m_k)$ 配有一个态射 $p \bullet X \to (m_1 \bullet X) + \cdots + (m_k \bullet X)$。

The free coaffine rig category

我们感兴趣的许多方程很容易看出在 PROP $\mathbf{FinInj}$ 中成立，其态射 $m \to n$ 是单射 $\{1, \ldots, m\} \rightarrowtail \{1, \ldots, n\}$。其对象上的半环结构由自然数的加法和乘法给出。对于态射 $f\colon\ n \to m$ 和 $g\colon\ p \to q$，它们的和 $f \oplus g\colon\ n + p \to m + q$为

$$(f \oplus g)(a) = \begin{cases} f(a) & \text{if } a \leq n \\ m + g(a - n) & \text{otherwise} \end{cases}$$

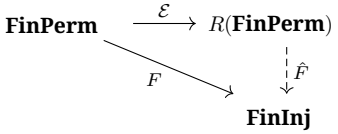
而它们的积 $f \otimes g\colon\ np \to mq$ 由函数给出

$$p_{f,g} \colon n \times p \to m \times q$$
$$(a, b) \mapsto (f(a), g(b))$$

经康托尔置换 $\{1, \ldots, np\} \to \{1, \ldots, n\} \times \{1, \ldots, p\}$共轭得到。

引理 23。 $R(\mathbf{FinPerm})$ 与 $\mathbf{FinInj}$半环同构。

证明。 由 R-构造的泛性质可知，遗忘函子 $F\colon \mathbf{FinPerm} \to \mathbf{FinInj}$ 分解为



ˆ 对唯一的 rig 函子 F。由于 F 和 $\mathcal{E}$ 在对象上都为恒等，因此 ˆ ˆ F 在对象上也为恒等（具体而言，是双射）：因此， F 是 rig 范畴的同构，当且仅当它是满且忠实的。

根据 Expansion-Raw 态射分解 [22, 引理 2.8], ， $R(\mathbf{FinPerm})$中的每个态射都能唯一分解为一个典范单射 $\amalg_1\colon\ n \to n + k$，后接 ˆ 一个双射 $\pi\colon\ n + k \to m$。由此可知， F 是满的，当且仅当有限集之间的每个单射都存在这样的分解；而它是忠实的，当且仅当该分解在仅对 k应用双射的意义下唯一。

设 $f\colon\ n \to m$ 是某个单射，并考虑集合 $m \setminus \mathrm{im}(f)$，其中 $k = |m \setminus \mathrm{im}(f)|$。注意，$m \setminus \mathrm{im}(f)$ 是有序集 m 的有限子集，因此是有序的

的。也就是说，我们可以定义一个双射 $\psi\colon k \to m \setminus \mathrm{im}(f)$：将 $\psi(1)$ 映射到 $m \setminus \mathrm{im}(f)$ 中最小的元素，将 $\psi(1)$ 映射到第二小的元素，依此类推。现在定义 $\pi\colon n+k \to m$，使得

$$\pi(a) = \begin{cases} f(a) & \text{if } a \leq n \\ \psi(a-n) & \text{otherwise} \end{cases}$$

这是单射，因为 f 和 ψ 均为单射，且它们的像不相交，依据

$$\mathrm{im}(f) \cap \mathrm{im}(\psi) = \mathrm{im}(f) \cap (m \setminus \mathrm{im}(f)) = \emptyset,$$

并且它是满射，因为

$$\mathrm{im}(\pi) = \mathrm{im}(f) \cup \mathrm{im}(\psi) = \mathrm{im}(f) \cup (m \setminus \mathrm{im}(f)) = m$$

所以是双射。但随后由于 $\mathrm{II}_1\colon\ n \to n+k$ 由 $\mathrm{II}_1(n) = n$给出，根据 π 的ˆ定义可得 $\pi \circ \mathrm{II}_1 = f$。因此 F是满的。

为了看出它也是忠实的，假设存在另一个 $\pi'\colon\ n+k \to m$，使得 $\pi' \circ \mathrm{II}_1 = f$ 但 $\pi \neq \pi'$。由于 $\pi' \circ \mathrm{II}_1 = f = \pi \circ \mathrm{II}_1$，对所有 $a \leq n$可得

$$\pi(a) = \pi(\mathrm{II}_1(a)) = f(a) = \pi'(\mathrm{II}_1(a)) = \pi'(a)$$

因此 π 和 π' 只能在 a 的取值上不一致，其中 $n \leq a \leq n+k$，而这无论如何都必须落入像 $m \setminus \mathrm{im}(f)$的子集中。现在考虑双射$\pi'^{-1} \circ \pi\colon\ n+k \to n+k$。根据上述论证，当 $a \leq n$时$(\pi'^{-1} \circ \pi)(a) = a$，而当 $a \geq n$时$(\pi'^{-1} \circ \pi)(a) \geq n$。定义 $\psi'(a) = (\pi'^{-1} \circ \pi)(a+n) - n$，我们看到当 $a \leq n$时，

$$(\mathrm{id}_n \oplus \psi')(a) = \mathrm{id}_n(a) = a = (\pi'^{-1} \circ \pi)(a)$$

并且当 $a > n$ 时，我们有

$$(\mathrm{id}_n \oplus \psi')(a) = n + \psi'(a-n) = n + (\pi'^{-1} \circ \pi)((a-n)+n) - n = (\pi'^{-1} \circ \pi)(a)$$

因此，$\mathrm{id} \oplus \psi' = \pi'^{-1} \circ \pi$。但随后，应用于 k 的双射所给出的唯一性可由

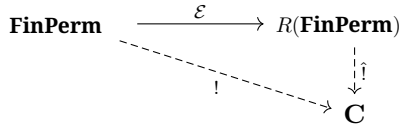
$$\pi' \circ (\mathrm{id}_n \oplus \psi') = \pi' \circ (\pi'^{-1} \circ \pi) = (\pi' \circ \pi'^{-1}) \circ \pi = \pi$$

ˆ 这反过来意味着 F 也是忠实的。 □

当任意对象 A都恰有一个从加法单位元 O出发的态射时，幺半环范畴称为余仿射 。

定理 24。 若$\mathbf{C}$ 是余仿射幺半环范畴，则存在唯一的 *rig* 函子$\mathbf{FinInj} \to \mathbf{C}$。

证明。 由于$\mathbf{FinPerm}$ 是初始幺半环范畴，因此存在唯一的 rig 函子$\mathbf{FinPerm} \to \mathbf{C}$。由于$\mathbf{C}$是余仿射的，根据$R$-构造的泛性质，这个唯一函子可唯一地分解为



这就证明了存在性。对于唯一性，假设还存在另一个 rig 函子 $F\colon R(\mathbf{FinPerm}) \to \mathbf{C}$。注意到，根据 rig 函子唯一性

!: **FinPerm** $\to \mathbf{C}$，我们也必须有 $! = F \circ \mathcal{E}$。根据 Expansion-Raw 态射分解，R**(FinPerm)** 中的每个态射都可分解为典范单射 $\amalg_1 \colon n \to n+k$，后接双射 $\pi \colon n+k \to m$。由 $! = F \circ \mathcal{E}$, F 可知，! 和 必须在所有双射上相同，因此它们唯一可能不同之处，就是将典范单射 $\amalg_i$ 映射到何处。由于 F 和 ! 是 rig 函子，它们必须保持始对象，因为始对象在 R**(FinPerm)** 和**C** 中都是加法单位元：因此，它们也必须保持始映射 $0 \to A$，因为这些映射在 R**(FinPerm)** 和 **C** 中都是唯一的。但这样一来，它们就必须保持 $\amalg_1$，因为 $\amalg_1 =$ (id $\oplus$!) $\circ \rho_{\oplus}^{-1}$，其中 $\rho_{\oplus} \colon O \oplus A \to A$ 是相干同构，而 F 和 ! 保持其中涉及的所有映射；所以 $F =$!

由于 R**(FinPerm)** 与 **FinInj** 由引理 23 半环同构，因此**FinInj** 满足相同的泛性质。□

上述定理的另一种表述是，**FinInj**是自由余仿射 rig 范畴。若图表由 rig 相干同构和始映射 $0 \to A$组成，则称其为余仿射图表。

推论 25. 在**FinInj**中交换的余仿射图表，在任何其他余仿射 *rig* 范畴中也交换。

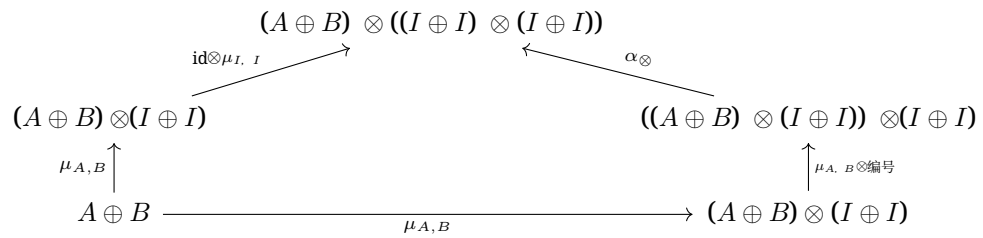
Classical control

在验证所需公理之前，我们最后要做的准备是证明 Split(LR(C)) 具有经典控制；更确切地说，证明 $\oplus$是余积。其主要思路是，在像 Split(LR(C)) 这样的余仿射 rig 范畴中，我们可以如下记录对象 $I \oplus I$ 中的测量结-果。

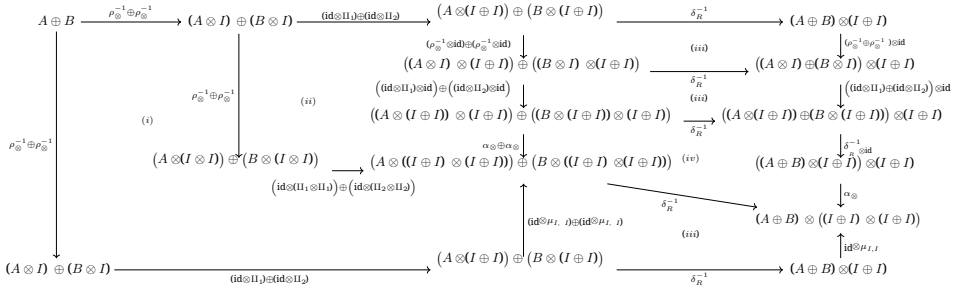
定义 26. 在余仿射幺半环范畴中，定义如下态射的自然族$\mu_{A,B}$:

$$\begin{array}{ccc} A \oplus B & \xrightarrow{\quad\mu_{A,B}\quad} & (A \oplus B) \otimes (I \oplus I) \\ {\scriptstyle \rho_{\otimes}^{-1} \oplus \rho_{\otimes}^{-1}}\downarrow & & \uparrow{\scriptstyle \delta_R^{-1}} \\ (A \otimes I) \oplus (B \otimes I) & \xrightarrow[(\mathrm{id} \otimes \amalg_1) \oplus (\mathrm{id} \otimes \amalg_2)]{} & (A \otimes (I \oplus I)) \oplus (B \otimes (I \oplus I)) \end{array}$$

引理 27. 下方的五边形在任意余仿射幺半环范畴中都可交换。



证明。 由下方图表的交换性。



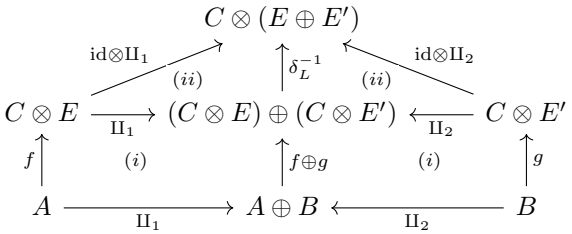
此处，(i) 由推论 25 交换，(ii) 由 $\otimes$ 的双函子性与相干性交换，(iii) 由 δ_R^{-1} 的自然性交换，(iv) 由相干性交换。□

推论 28. 当$\mathbf{C}$ 是一个余仿射幺半环范畴时，$\mu_{A,B}$ 在 $L(\mathbf{C})$中是幂等的。

证明。根据上述引理，$\mu_{I,\ I}$ 在 $\mu_{A,\ B}$ 与 $\mu_{A,\ B}\circ\mu_{A,\ B}$之间起中介作用。 □

此处的直观理解是，$\mu_{A,\ B}$ 测量该状态是否处于子空间 A 或 B 中，从而得到一比特信息。这一比特可由 $\mu_{I,\ I}$中介，意味着我们可以再次执行相同的测量（得到相同的结果），或者通过测量它来复制该（经典）测量结果。

引理 29。下方图表在任意余仿射 *rig* 范畴中交换。



证明。(i) 由单射的自然性交换，(ii) 由定理 25 交换。 □

对象 $A+B$ 是 A 与 B 的余积，当它具有单射 $A\to A+B\leftarrow B$，并且态射对 $A\to C\leftarrow B$ 经由这些单射通过唯一态射 $A+B\to C$ 分解。这以范畴的方式刻画了经典控制 [25]。

命题 30. 分裂(LR(**C**)) 有余积。

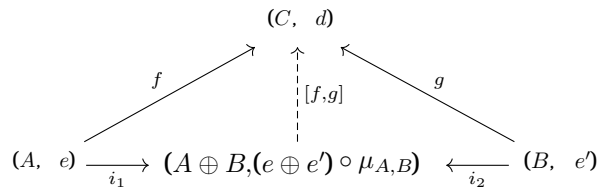
证明。 对于 Split(LR(C)) 中的对象 (A,e) 和 (B,e')，我们看到这些图表

$$\begin{array}{ccccc} A & \xrightarrow{\amalg_1} & A\oplus B & \xleftarrow{\amalg_2} & B \\ {\scriptstyle\rho_\otimes^{-1}}\downarrow & & \downarrow{\scriptstyle\mu_{A,B}} & & \downarrow{\scriptstyle\rho_\otimes^{-1}} \\ A\otimes I & \xrightarrow[\amalg_1\otimes\amalg_1]{} & (A\oplus B)\otimes(I\oplus I) & \xleftarrow[\amalg_2\otimes\amalg_2]{} & B\otimes I \end{array}$$

根据推论 25，在 R(C) 中交换，因此 $\mu_{A,B}\circ\amalg_1=\amalg_1$和 $\mu_{A,B}\circ\amalg_2=\amalg_2$属于 LR(C)；分别将它们在 LR(C) 中的等价类记为 i_1 和 i_2。进一步注意到，根据 $\mu_{A,B}$ 的自然性，$(e\oplus e')\circ\mu_{A,\ B}=\mu_{A,B}\circ(e\oplus e')$，所以当 e 和 e' 为幂等时，$(e\oplus e')\circ\mu_{A,B}$ 也是幂等，因为

$$(e\oplus e')\circ\mu_{A,\ B}\circ(e\oplus e')\circ\mu_{A,\ B}=(e\oplus e')\circ(e\oplus e')\circ\mu_{A,\ B}\circ\mu_{A,\ B}=(e\oplus e')\circ\mu_{A,\ B}$$

因此，由 $\amalg_1$ 与 $\amalg_2$ 的自然性可知，$(e \oplus e') \circ \amalg_1$ 与$(e \oplus e') \circ \amalg_2$分别是从$(A, e)$与$(B, e')$到$(A \oplus B, (e \oplus e') \circ \mu_{A,B})$的态射。给定态射 $f\colon (A, e) \to (C, d)$以及 $g\colon (B, e') \to (C, d)$，并选取 $[f, g]$ 为 LR(C) 中 $\delta_L^{-1} \circ (f \oplus g) \circ \mu_{A,B}$ 的等价类，我们便看到余积三角的交换性



由引理 29 以及上文确立的 $\amalg_1 = \amalg_1 \circ \mu_{A,\ B}$ 和 $\amalg_2 = \amalg_2 \circ \mu_{A,\ B}$ 可得。注意，$[f, g]$ 尊重这些幂等元，因为

$$\begin{aligned}
&d \circ [f, g] \circ (e \oplus e') \circ \mu_{A,B} \\
&\quad = d \circ \delta_L^{-1} \circ (f \oplus g) \circ \mu_{A,B} \circ (e \oplus e') \circ \mu_{A,B} \\
&\quad = d \circ \delta_L^{-1} \circ (f \oplus g) \circ (e \oplus e') \circ \mu_{A,B} \circ \mu_{A,B} \\
&\quad = \delta_L^{-1} \circ (d \oplus d) \circ (f \oplus g) \circ (e \oplus e') \circ \mu_{A,B} \circ \mu_{A,B} \\
&\quad = \delta_L^{-1} \circ ((d \circ f \circ e) \oplus (d \circ g \circ e')) \circ \mu_{A,B} \circ \mu_{A,B} \\
&\quad = \delta_L^{-1} \circ (f \oplus g) \circ \mu_{A,B} \circ \mu_{A,B} \\
&\quad = \delta_L^{-1} \circ (f \oplus g) \circ \mu_{A,B} \\
&\quad = [f, g]
\end{aligned}$$

在 LR(C) 中，由于 δ_L^{-1} 的自然性、$\mu_{A,\ B}$、$\mu_{A,\ B}$ 的幂等性，以及$d \circ f \circ e = f$和 $d \circ g \circ e'$ 是态射这一假设（$A,\ e$）$\to (C,\ d)$ 和（$B,\ e'$）$\to (C,\ d)$，它们属于 Split(LR(C))，因此这确实是 Split(LR(C)) 中所述对象之间的一个态射。这就证明了存在性。

要证明 $[f, g]$ 也是唯一这样的态射，假设 h 是另一个使余积三角可交换的态射（$A \oplus B,\ (e \oplus e') \circ \mu_{A,\ B}$）$\to (C,\ d)$。由于 h 是从 $(A \oplus B,\ (e \oplus e') \circ \mu_{A,\ B})$ 出发的态射，我们知道 h 分别尊重 $\mu_{A,\ B}$ 和 $(e \oplus e')$，因为

$$\begin{aligned}
h \circ \mu_{A,B} = h \circ (e \oplus e') \circ \mu_{A,B} \circ \mu_{A,B} = h \circ (e \oplus e') \circ \mu_{A,B} = h \\
h \circ (e \oplus e') = h \circ (e \oplus e') \circ \mu_{A,B} \circ (e \oplus e') = h \circ (e \oplus e') \circ (e \oplus e') \circ \mu_{A,B} \\
= h \circ (e \oplus e') \circ \mu_{A,B} = h
\end{aligned}$$

在 LR(C) 中。但随后

$$\begin{aligned}
h &= h \circ \mu_{A,B} \\
&= h \circ \mu_{A,B} \circ \mu_{A,B} \\
&= h \circ \delta_R^{-1} \circ ((\mathrm{id} \otimes \amalg_1) \oplus (\mathrm{id} \otimes \amalg_2)) \circ \rho_\otimes^{-1} \oplus \rho_\otimes^{-1} \circ \mu_{A,B} \\
&= h \circ \delta_L^{-1} \circ ((\amalg_1 \otimes \mathrm{id}) \oplus (\amalg_2 \otimes \mathrm{id})) \circ (\rho_\otimes^{-1} \oplus \rho_\otimes^{-1}) \circ \mu_{A,B} \\
&= \delta_L^{-1} \circ ((h \otimes \mathrm{id}) \oplus (h \otimes \mathrm{id})) \circ ((\amalg_1 \otimes \mathrm{id}) \oplus (\amalg_2 \otimes \mathrm{id})) \circ (\rho_\otimes^{-1} \oplus \rho_\otimes^{-1}) \circ \mu_{A,B} \\
&= \delta_L^{-1} \circ (((h \circ \amalg_1) \otimes \mathrm{id}) \oplus ((h \circ \amalg_2) \otimes \mathrm{id})) \circ (\rho_\otimes^{-1} \oplus \rho_\otimes^{-1}) \circ \mu_{A,B} \\
&= \delta_L^{-1} \circ ((f \otimes \mathrm{id}) \oplus (g \otimes \mathrm{id})) \circ (\rho_\otimes^{-1} \oplus \rho_\otimes^{-1}) \circ \mu_{A,B}
\end{aligned}$$

$$= \delta_L^{-1} \circ (\alpha_\otimes \oplus \alpha_\otimes) \circ (\rho_\otimes^{-1} \oplus \rho_\otimes^{-1}) \circ (f \oplus g) \circ \mu_{A,B}$$
$$= (\mathrm{id} \otimes \rho_\otimes^{-1}) \circ \delta_L^{-1} \circ (f \oplus g) \circ \mu_{A,B}$$
$$= (\mathrm{id} \otimes \rho_\otimes^{-1}) \circ [f, g]$$

在 R(C) 中，因此 h 和 $[f, g]$ 在 LR(C) 中属于同一个等价类。 □

Completeness

我们现在已准备好证明主文中定理 5 所述的分裂(LR(Π_k))的完备性。我们将通过验证它是满足量子计算代数理论的某一签名的模型来完成这一证明。关于这些公理，请参阅 [51]以及下文定理 31 和定理 33 的证明。

命题 31. 在分裂(LR(C))中，在 $I \oplus I$ 对 $\otimes$的指数作用下，对象 I 是量子计算代数理论 [51]之签名的一个结构（限于C的酉算子）。

证明. 由于当**D**为对称幺半时，分裂(D)也是对称幺半的，因此分裂(LR(C))同样是对称幺半的（因为 LR(C)是对称幺半的），从而由引理 21，它容许与 $I \oplus I$ 的指数作用。对于运算新建：$0 \to 1$、测量：$1 \to (0, 0)$以及应用$_U$：$n \to n$，我们关联如下态射

$$[\![\mathsf{new}]\!] = \Pi_1 \colon I \to I \oplus I$$
$$[\![\mathsf{measure}]\!] = \mu_{I,I} \colon I \oplus I \to I + I$$
$$[\![\mathsf{apply}_U]\!] = F(U) \colon (I \oplus I)^{\otimes n} \to (I \oplus I)^{\otimes n}$$

其中 F 是对称幺半函子 $\mathbf{C} \to$Split(LR(C))。这些运算与签名相符，因为在 $I \oplus I$ 的指数作用中，$m \bullet I = (I \oplus I)^{\otimes m}$（相差一个典范相干同构）。□

定义 32. [51] 带线性参数的代数理论模型，是指其签名的一种结构，并且对于每条公理 $x_1 \colon m_1, \ldots, x_k \colon m_k \mid a_1, \ldots, a_p \vdash t = u$，解释 $[\![t]\!], [\![u]\!] \colon p \bullet X \to (m_1 \bullet X) + \cdots + (m_k \bullet X)$ 相等。

定理 33. 在 $\mathrm{Split}(\mathrm{LR}(\mathbf{C}))$ 中，令 $I \oplus I$ 在 $\otimes$上具有指数作用，则对象 I 构成量子计算代数理论 [51]的一个模型。

证明. 我们验证所需的公理 (A)-(L) [51]。将对象 $1 + 1$记作 2，将 δ^{l} 和 δ^{r} 记作相干同构 $A \otimes (B \oplus C) \to (A \otimes B) \oplus (A \otimes C)$ 和 $(A \oplus B) \otimes C \to (A \otimes C) \oplus (B \otimes C)$，并将相干同构$I \otimes A \to A$记作 λ_A。

第一组公理涉及余仿射图表。直接计算可知，这些公理在**FinInj** 中成立，因此根据定理 25，它们在 Split(LR(C))中也成立：

(A) [\![测量]\!] $\circ X = \mu_{1,1} \circ \sigma^+ =$ ($\sigma^+ \times \sigma^+$)$\circ \mu_{1,1} = X \circ$ [\![测量]\!]; (D) 测量 $\circ$ 新建 $=$ 新建; (J) $(\delta^{\mathrm{r}} + \delta^{\mathrm{r}}) \circ \big($(测量 $\otimes$ id) $+$(测量 $\otimes$ id)$\big) \circ \delta^{\mathrm{l}} \circ$ (id $\otimes$ 测量)= (id $+ \sigma +$ id) $\circ(\delta^{\mathrm{l}} + \delta^{\mathrm{l}}) \circ \delta^{\mathrm{r}} \circ$ (id $\otimes$ 测量) $\circ$ (测量 $\otimes$ id); (K) ([\![新建]\!] $\otimes \mathrm{id}_2$) $\circ (\mathrm{id}_2 \otimes$ [\![新建]\!]) $= (\mathrm{id}_2 \otimes$ [\![新建]\!]) $\circ$ ([\![新建]\!] $\otimes \mathrm{id}_2$); (L) ($\mathrm{id}_2 \otimes$测量) $\circ$(新建 $\otimes \mathrm{id}_2) \circ \lambda_2^{-1} =$ (新建 $\otimes \mathrm{id}_2) \circ \lambda_2^{-1} \circ$测量。

例如，自然变换 $\mu_{A,B}\colon A+B\to(A+B)\times(1+1)$ 由 $,\amalg_1(*)$ 和 $B\ni b\mapsto(b,\amalg_2(*))$ 在 **FinInj** 中给出。记作

$$D(u,v)=(\delta^{\mathrm{r}})^{-1}\circ(u\oplus v)\circ\delta^{\mathrm{r}}\colon 2^{\otimes n+1}\to 2^{\otimes n+1}$$

对于 LR(**C**) 中的映射，该映射对 $n+1$ 量子比特上的计算进行建模，其中第一个量子比特控制是否将 u 或 v 应用于最后的 n 量子比特。下面的两个公理利用自然性，通过上述定理 25 得到证明。

(B) $D(u,\ v)\circ(\text{测量}\otimes\mathrm{id}_{2^{\otimes n}})=(\text{测量}\otimes\mathrm{id}_{2^{\otimes n}})\circ D(u,\ v)$；(E) $D(u,\ v)\circ(\text{新建}\otimes\mathrm{id}_{2^{\otimes n}}\otimes\mathrm{id}_{2^{\otimes n}})=\text{新建}\otimes u$。

下面这组公理成立，因为嵌入 $F\colon\mathbf{C}\to\text{Split(LR(}\mathbf{C}\text{))}$ 按照构造是一个对称幺半函子：

(F) $F(\sigma^{\otimes}_{2^{\otimes m},\ 2^{\otimes n}})=\sigma^{\otimes}_{2^{\otimes m},\ 2^{\otimes n}}$；(G) $F(\mathrm{id}_{2^{\otimes n}})=\mathrm{id}_{2^{\otimes n}}$；

(H) $F(v\circ u)=F(v)\circ F(u)$；

(I) $F(u\otimes v)=F(u)\otimes F(v)$；

最后一条公理源于 Split(LR(**C**)) 构造的本质：

(C) 由 I 是 Split(LR(**C**)) 中的终对象这一事实可知，对于 **C** 中任意的 $u\colon\ 2^{\otimes n}\to 2^{\otimes n}$ 和 $d\colon\ 2^{\otimes n}\to I$，都有 $d\circ u=d$；因此，特别地，对于由 **C** 中的 $\lambda^{-1}\colon\ 2^{\otimes n}\to I\otimes 2^{\otimes n}$ 提升而来的、Split(LR(**C**)) 中的丢弃映射 $d\colon\ 2^{\otimes n}\to 1$，也成立。□

令 **QChannel** 表示有限维 C^*-代数与量子信道（完全正保迹线性映射）的范畴。以下这条定理 33 的推论确立了主文中定理 5 的第一部分。

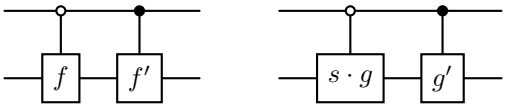
推论 34. 诱导函子 $[\![-]\!]\colon$ 分裂(LR(Π_k)) $\to$ **QChannel** 是忠实的。

证明. 在 [51] 中已经证明，量子信道的每一个等式都可以借助定理 33 所表明在分裂(LR(Π_k))中成立的那组离散公理来确立。□

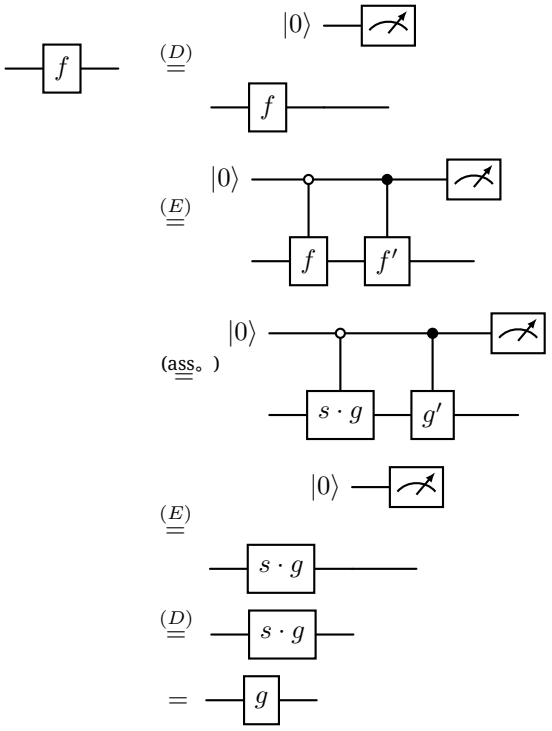
最后，我们得出结论：分裂(LR(Π_k))对于酉算子是完备的，从而确立了主文中定理 5 的最后一部分。

定理 35. Π_k 中的平行态射 f 与 g 在被纳入分裂(LR(Π_k)) 后相等，当且仅当对某个标量 s有 $f\approx_k s\cdot g$。

证明。假设 $f\approx_k s\cdot g$属于 Π_k，即存在 f'和 g'，使得 $f\oplus f'=(s\cdot g)\oplus g'$。注意，$f\oplus f'$ 和 $(s\cdot g)\ \oplus g'$ 恰好是这些电路的解释



但随后，$f=g$ 在 Split(LR(Π_k)) 中可由下式推出



□

其中，最后一步成立是因为 Split(LR(Π_k)) 中所有标量都被视为相同（因为 I 是终对象），所以 $s \cdot g = \mathrm{id} \cdot g = g$。

反过来，当 f 和 g 是 Π_k 中的酉算子，且将 $f = g$ 包含在 Split(LR(Π_k)) 中时，由 $[\![-]\!]$的函子性可得：Split(LR(Π_k)) $\to$**QChannel**，于是 $[\![f]\!] = [\![g]\!]$。由于 f 和 g 是从 Π_k 中包含的，这些量子信道实际上只是通过 f 和 g的底层酉算子进行附加。由于通过 f 和 g 的底层酉算子进行附加会得到相同的量子信道，根据其 Choi态的酉自由度 [44, 定理 2。6]，可知它们的底层酉算子相差一个全局相位。随后应用定理 20，即可在 Π_k中确立 $f \approx_k s \cdot g$。

Asymptotic scaling with k

我们研究近似目标酉算子所需的 Π_k 项大小如何取决于精度级别 k。给定算子范数下的总体近似误差 ε，对于不同类别的酉算子，最小的 Π_k 项大小如何随 k 变化？两个典型情形展现了行为范围：一般酉变换和量子傅里叶变换。

一般酉变换。考虑由单量子比特旋转门和 CNOT门构成的电路。当且仅当 $R_a(\phi)$的元素属于 $\mathbb{D}[\zeta_k]$ [33]时，旋转 $R_a(\phi)$才能用 Π_k 中的一项精确表示；其他所有旋转都必须近似。对于这类一般旋转，任何 ε近似都需要 $O(\log(1/\varepsilon))$个基本项，并且可以高效地构造出达到这一下界的近似 [46]。如果电路中有固定比例的旋转属于一般旋转，那么相应 Π_k 项的总规模对于任意固定的 k都按 $O(\log(1/\varepsilon))$增长，其中

增大 k 可能只能改善隐藏的常数因子。因此，无论 k取何有限值，都无法消除对 ε的对数依赖，只能改善其常数因子。

量子傅里叶变换。 n量子比特量子傅里叶变换（QFT_n）包含 n 个哈达玛门和 $\binom{n}{2}$ 个受控相位门。相位门中出现的角度形式为 $2\pi/2^d$，其中 d 的取值范围从 2 到 n。在精度级别k下，所有满足 $d \leq k$ 的旋转门都是 Π_k 的原生门，因此无需近似。因此，当 $n \leq k$时，完全不需要近似，并且 $O(n^2)$ 个 Π_k项就足以精确表示 QFT_n 。当 $n > k$时，

$$\binom{(n-k)+1}{2}$$

受控相位门无法在 Π_k 中精确表示，因此必须进行近似。例如，当 $k = n - 1$时，一个门就需要近似；当 $k = n - 2$时，三个门需要近似，以此类推。总体而言，假设总误差预算 ε 在所有需要近似的门之间平均分配，标准方法 [46] 因此将产生大小为 O的 Π_k 项，即$((n^2 - (n-k)^2) + (n-k)^2 \log_2((n-k)^2/\varepsilon))$。因此，对于量子傅里叶变换，提高 k 可以完全消除对 ε 的依赖：随着 k 增加，剩余成本会下降，直到 $k = n$，此后所有旋转门都是原生门，规模稳定在$O(n^2)$。

McMaster University, Department of Computing and Software, Canada
Email address: carette@mcmaster.ca

University of Edinburgh, School of Informatics, United Kingdom
Email address: chris.heunen@ed.ac.uk

University of Southern Denmark, Department of Mathematics and Computer Sci-ence, Centre for Quantum Mathematics, Centre for Formal Methods and Future Com-puting, Denmark
Email address: kaarsgaard@imada.sdu.dk

Dalhousie University, Department of Mathematics and Statistics, Canada
Email address: neil.jr.ross@dal.ca

Indiana University, Department of Computer Science, United States of America
Email address: sabry@iu.edu