arXiv:2305.01674v2 [quant-ph] 2 Jun 2023

使用 SAT 求解器对 Clifford 电路进行深度最优综合

Tom Peham*
设计自动化教席
慕尼黑工业大学
德国
tom.peham@tum.de

Nina Brandl*
集成电路研究所
林茨约翰内斯·开普勒大学
奥地利
nina.brandl@jku.at

Richard Kueng
集成电路研究所
林茨约翰内斯·开普勒大学
奥地利
richard.kueng@jku.at

Robert Wille
设计自动化教席
慕尼黑工业大学
德国
Software Competence Center Hagenberg GmbH
奥地利
robert.wille@tum.de

Lukas Burgholzer
集成电路研究所
林茨约翰内斯·开普勒大学
奥地利
lukas.burgholzer@jku.at

* 两位作者对本研究的贡献相同。

摘要—量子电路综合是将给定的逻辑功能分解为一系列基本门的过程。若无法用更短的量子电路实现所需功能，则称其为（深度）最优。最优综合是量子和经典硬件设计中的核心问题，但也受到复杂性理论障碍的困扰。受容错量子计算的推动，我们研究合成 Clifford 酉算子块这一特殊情形。借助纠缠输入刺激和稳定子形式体系，我们能够将 Clifford综合问题归约为一族多项式规模的可满足性（SAT）问题——每个目标电路深度对应一个问题。从概念上看，我们的结果表明，Clifford综合问题属于多项式层次的第一级（NP），而已知逻辑电路的经典综合问题是多项式层次第二级的完全问题（Σ_2^P）。基于这一理论归约，我们为深度最优 Clifford 合成构造了 SAT 编码。随后，我们使用 SAT 求解器确定一个满足赋值，或证明不存在这样的赋值。由此既可以得到仍可实现综合的最短深度（最优性），也可以获得实际的量子电路（综合）。实证评估表明，对于随机克利福德电路以及用于 Grover 搜索的 Clifford+T 电路，最优综合方法能够显著降低深度。

I. 引言

量子计算是一种计算范式，对于某些问题，它可能比经典算法具有计算优势。最先进水平的量子计算硬件在规模上仍然受到限制，其量子比特数量相对较少，且容易出现错误。尽管为这些含噪中等规模量子（NISQ）计算机寻找短期应用是一个持续且充满活力的研究领域 [1]，但它们仍无法用于整数因数分解（Shor； [2]）、无结构搜索（Grover； [3]）、求解线性方程组（HHL； [4]）或凸优化 [5]–[7] 等高级应用。

要将量子计算扩展到包含多个量子比特的更长计算，必须采用容错 计算方案，以保护量子比特的信息免受错误影响，并允许以较低错误率应用量子门，参见例如 [8]–[10]。一种实现方式是使用量子纠错码，并在 Clifford+T 门集 [11]中执行所有计算。限制门集的好处是，每个门都能在适当的编码上以容错方式实现。

容错量子电路可能会变得相当庞大，这是因为需要将每次量子计算分解为这个受限门集中的量子门，并执行错误综合征提取和纠错步骤。对于近期应用，通常会对其进行优化，以使双量子比特门数量达到最小，因为这类量子门往往具有最高的错误率。对于容错计算而言，合适的性能指标是电路深度，因为它与计算的运行时间直接相关。

在容错场景下，综合最优电路的问题通常采用整体或部分的方式来处理：前者试图最小化整个量子电路，后者则仅减少 T 门数量，参见例如 [13]–[16]。一般综合问题事实证明非常困难。与其最小化整个 Clifford+T 量子电路，不如只考虑 Clifford 部分，以尝试降低一般综合问题的难度。

在这项工作中，我们证明，深度最优 Clifford 电路的综合问题实际上至多与布尔可满足性（SAT）一样难。我们通过考虑一个更大型电路的综合问题来实现这一点，该电路以一对最大纠缠态作为输入。尽管理论上这会增大问题规模，但利用最大纠缠态可以将综合问题分解为关于稳定子的问题（Gottesman-Knill）。

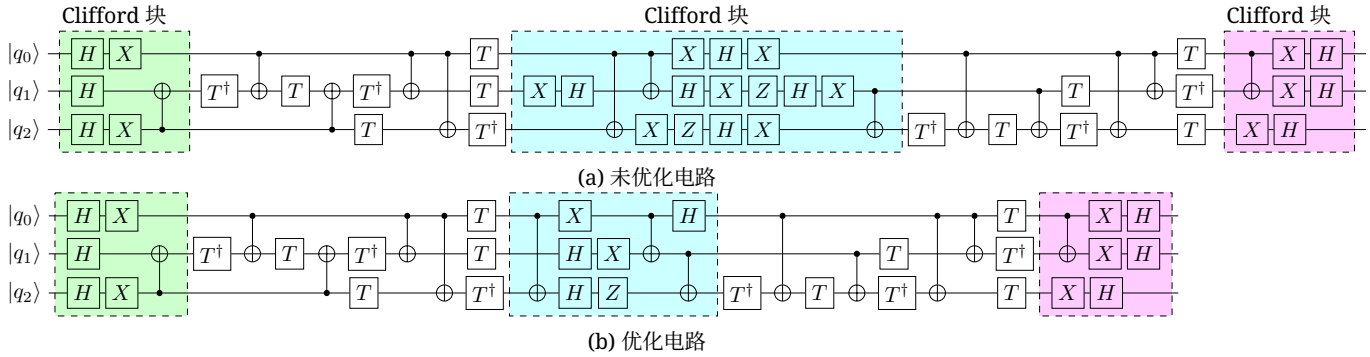


图 1. 用于 *3* 量子比特 *Grover* 搜索的两个 *Clifford+T* 电路：预言机对应于一个含有 3 个变量和 5 个子句的随机 3-SAT 公式。**(上图)** 将一个 Grover 块分解为 Clifford+T 门；实际综合是使用 Qiskit 的 Grover 类和一个 PhaseOracle [12]实现的。**(下图)** 使用本文的方法对所有（非平凡）Clifford 块进行深度优化综合。我们的 SAT 方法证明，绿色和紫色块已经达到深度最优。而中央的蓝绿色块并非如此，我们的方法在此处带来了显著改进（深度从 9 降至 5）。

基于这一视角，我们构建了一种 SAT 编码，用于合成和优化最大深度为 $d_{\max}$ 的 n 量子比特 Clifford 电路，包含 $O(n^2 d_{\max})$ 个变量和 $O(n^4 d_{\max})$ 个约束。对于更大的电路，我们进一步开发了基于最优 SAT 编码的启发式优化流程，以分治方法降低 Clifford 电路的深度。

我们实现了所提出的方法，并将其与最先进且公开可用的 Clifford 合成技术进行了比较。结果表明，尽管最优综合仅能扩展到 5 个量子比特，但最先进水平与最优深度平均相差两个数量级。启发式方法也取得了优于最先进水平的结果，并且比最优方法具有更好的可扩展性。通过展示如何优化 Clifford+T 电路中的 Clifford 子电路来降低其深度，说明了这些方法对容错量子计算的有效性。所有实现均可通过量子电路编译工具 QMAP [17],获得，该工具是慕尼黑量子工具包 （MQT）的一部分，可访问 https://github.com/cda-tum/qmap。

本文其余部分的结构如下：第 II 节阐述了进行深度最优 Clifford 电路综合的必要性，并介绍经典电路综合问题的背景。随后，第 III 节简要回顾量子电路综合方面的既有工作，尤其是 Clifford 情形下的相关工作。在第 IV 节中，我们介绍本文的主要构造，并将 Clifford 合成归约为 SAT，然后在第V节中详细说明 SAT 编码。在此基础上，我们在第 VI 节中推导出一种启发式优化流程。本文所介绍方法的评估结果见第VII节。最后，第 VIII 节对本文进行总结。

II. 背景与动机

为使本文内容完整自洽，以下各节将回顾容错量子计算和量子电路综合的核心概念，这些概念在本文其余部分都会用到。

A. 容错量子计算

量子计算容易受到多种来源的错误影响，例如退相干、信息泄漏或其他类型的噪声。为了保护量子信息，人们引入了 量子纠错码 （量子纠错码）。本质上，单个逻辑量子比特 的信息被编码到多个物理量子比特 中，目前已发现多种不同的编码方案。

在逻辑量子比特上执行量子门已不再是件简单的事，因为如何将物理门的功能扩展到逻辑层面，并非显而易见。此外，对逻辑量子比特施加量子门时，应能以容错 方式进行，使得施加量子门所引入的错误能够以任意高的概率得到纠正。

Clifford 门集 是一组可以横向地 作用于许多量子纠错码的量子门；也就是说，对逻辑量子比特施加 Clifford 操作，可以通过分别对每个物理量子比特执行相应的 Clifford 门来实现。因此，如果施加量子门时在某个物理量子比特上引入了错误，该错误就不会在编码量子比特中传播，因而更容易纠正。任意 Clifford 酉变换都可以由一系列*Hadamard* 门、相位门 和 *CNOT* 门 构成。值得注意的是，Pauli X 门、Y 门和 Z 门也属于 Clifford 群。

仅使用 Clifford 门不足以实现通用量子计算，而且可以在多项式时间内进行经典模拟 [11]，[18]。然而，加入 T 门 $T = |0\rangle\langle 0| + e^{i\frac{\pi}{8}}|1\rangle\langle 1|$ 即可实现通用性。通过魔态蒸馏协议 [19]和门传送，可以以容错方式实现 T 门。

因此，可以通过交替使用 Clifford 门模块和 T 门模块来实现容错量子计算，并在整个计算过程中检测和纠正错误症状。 图 1 展示了使用逻辑量子比特上的 Clifford+T 门集实现的 3 量子比特 Grover 搜索量子电路 $|q_0\rangle$， $|q_1\rangle$ 和 $|q_2\rangle$。

在这种容错机制中，最重要的性能指标是电路深度。假设不同量子比特上的量子门可以并行执行，深度直接决定了.....

决定计算的运行时间。由于量子计算机所采用的技术不同，周期时间可能会有很大差异，因此降低量子电路的深度可以大幅降低计算成本。

示例 1。 图 *1a* 中的量子电路包含 *3* 个值得关注的 *Clifford* 块。 图 *1b* 展示了同一个量子电路，其中每个块都经过综合，以实现最小深度。可以看出，最外侧的两个块在原始电路中已经达到深度最优。尽管从直觉上看这似乎成立，但仍然需要某种形式的证明。然而，中间的 *Clifford* 块深度为 9 （第一个 *Hadamard* 门和 *CNOT* 门可以并行执行），并且可以优化至深度 5。在使用最先进水平的量子计算综合工具对电路进行综合时，经常会出现此类深度较大的 *Clifford* 块[1]。

寻找这类 Clifford 电路的深度最优实现，将是本工作的主要动机，因为这类电路的受限特性非常适合采用经典设计自动化方法，例如*SAT* 和 *SMT* 求解器。

B. 从经典综合到量子综合

在深入探讨我们的量子协议细节之前，值得先简要回顾逻辑电路（或函数）的经典等价性检查，以及经典电路综合。这将为我们提供指导，也能说明我们为何使用 SAT 求解器进行量子电路综合。

1）经典等价性检查与 *SAT*： 设 C, C'为两个含有 n 个输入位的量子电路。当且仅当它们对每个可能的输入都产生相同的输出时，我们称这两个电路等价（$C \simeq C'$）。用公式表示为：$\forall x \in \{0,1\}^n \ Cx = C'x$。取其逆否命题可得

$$C \not\simeq C' \quad \Leftrightarrow \quad \exists x \in \{0,1\}^n \text{ s.t. } Cx \neq C'x.$$

逻辑不等式 $Cx \neq C'x$ 可以轻易转换为一个输入为 x的布尔函数 $\phi_{C,C'}(x)$。这凸显了（取反后的）电路等价性与可满足性问题（SAT）之间有趣的一一对应关系。从理论上说，SAT 是一个困难问题，属于 NP 完全问题。然而，大量启发式 SAT 求解器 [20] 在实践中表现出色。

2）经典最优综合与量化布尔公式： 电路综合旨在找到一个逻辑电路，用尽可能少的基本门实现所需的 n 位目标功能。这里，我们将着重关注电路深度（即量子门层数）。这一优化问题的判定版本如下：

$$\exists C_d, \mathrm{depth}(C_d) \leq d_{\max} \ \forall x \in \{0,1\}^n \ C_d x = Cx, \qquad (1)$$

其中， C_d 是另一个逻辑电路的占位符。换言之，当且仅当可以用另一个满足 $\mathrm{depth}(C_d) \leq d_{\max}$ 的逻辑电路 C_d，精确复现电路 C 的功能时，该公式才求值为 true。通过对该逻辑函数使用不同的 $d_{\max}$ 值进行多次查询，我们可以确定任意电路综合的最优深度，例如通过二分搜索来实现。

[1]此处的量子电路由 Qiskit 0.42.1 生成

我们也可以将Eq.(1)改写为量化布尔公式（QBF）。首先，请注意，我们可以用长度至多为 C_d 的二进制编码 y 来表示任意逻辑电路$\mathrm{poly}(nd_{\max})$。不同的比特串 y 会产生不同的电路 C_d ，反之亦然。有了这种二进制编码，我们就可以将等价性检查的布尔函数改写应用到当前情形： $\phi_C(y, x) = 1$ 当且仅当$Cx = C_d x$ ，且 C_d 是由 y编码的电路时成立。否则，该公式求值为0。综上，我们得到逻辑电路综合的如下 QBF 改写：

$$\exists y \in \{0,1\}^{\mathrm{poly}(nd_{\max})} \ \forall x \in \{0,1\}^n \ \phi_C(y,x) \overset{!}{=} 1. \qquad (2)$$

存在量词（$\exists$）遍历所有深度至多为 $d_{\max}$ （$C_d \leftrightarrow y$）的可能逻辑电路编码，而全称量词（$\forall$）遍历所有 2^n 可能的输入位串。

这类量化布尔公式通常比仅含一种量词的 SAT 问题难处理得多。事实上，重新表述后的电路综合问题 式（2）对于问题类 Σ_2^p 是完备的——它是多项式层次第二层的一个分支 [21]。除非多项式层次坍缩到第一层（人们普遍认为这种情况不会发生），否则这些问题比 SAT 难得多，进而也比等价性检查难得多。

量化布尔公式确实会在各种情境中自然出现 [22]。现有求解器，例如 [23]–[25] ，通常依赖反例引导的归纳综合（CEGIS）原理 [26]，而该原理源于抽象精化（CEGAR）[27]–[28]。例如，在程序综合中，采用 CEGIS 方法的求解器会交替执行生成候选程序和检查其中是否存在反例。

3）进入量子领域：电路等价性与综合：我们刚才讨论的两个经典挑战在量子领域都有自然的经典对应物。作用于 n 量子比特的量子电路同样由基本的（量子）量子门组成，但其功能却截然不同。我们称两个这样的电路 U, V 当且仅当它们等价 时

$$U \simeq V \quad \Leftrightarrow \quad \forall |\psi\rangle \in \mathbb{C}^{2^n} \ U|\psi\rangle = \mathrm{e}^{i\phi} V|\psi\rangle,$$

其中 $\phi \in [0, 2\pi)$ 是一个复相位。与（经典）逻辑电路不同，存在无穷多个可能的输入态$|\psi\rangle$ 需要检查。[2] 一致性及相互关系使我们能够将这个数量压缩为（至多） 4^n 个互不相交的输入态 [30]–[34]。然而，这一数量相对于量子比特总数而言仍然呈指数增长。众所周知，（取否定的）酉等价问题是 QMA 完全问题 [35] （QMA 是经典问题类 NP 的恰当量子推广）。因此，乍看之下，量子电路等价问题似乎比其经典对应物更加困难。

假设给定一个目标酉算子 U，例如以高级量子电路的形式表示，并且我们希望将其分解为尽可能少的门层（即电路深度）。每当我们想要执行一个

[2]这正是我们与先前工作的出发点不同之处，尤其是与 [29]的不同之处。在那项工作中，部分作者提出了一个相关但更简单的问题，这个问题仅需考虑 $|\psi\rangle = |0, \ldots, 0\rangle$（即固定一个输入态）即可。

高级酉算子（例如量子算法）时，这个实际问题就会出现；我们希望在一台实际的 n 量子比特量子计算机上执行它。这一综合问题的具体内容取决于基本门集的类型，但始终会形成一个双重量化问题

$$\exists U_d, \mathrm{depth}(U_d) \leq d_{\max}\ \forall |\psi\rangle\ U_d|\psi\rangle = \mathrm{e}^{i\phi}U|\psi\rangle,$$

与……相似公式（1），其中包含非二元量子态和复相位 $\phi \in [0, 2\pi)$。该问题至少与逻辑门综合一样困难，因为它将后者的（可逆）编码作为一种特殊情况包含在内。量子电路的可逆性使我们能够对这一表示稍作简化：

$$\exists U_d, \mathrm{depth}(U_d) \leq d_{\max}\ \forall |\psi\rangle\ UU_d^\dagger|\psi\rangle = \mathrm{e}^{i\phi}|\psi\rangle, \quad (3)$$

其中 $U_d^\dagger$ 是 U_d 的伴随或逆向电路。

对于 Clifford 电路等特殊情况，我们可以将式（3）重写为逻辑布尔公式，其固有难度与逻辑电路等价性或 SAT 相当，如第 IV 节所示。其难度远低于一般的经典电路综合。基于这一严谨的理论洞见，我们随后采用最先进的 SAT 求解器来解决完整的 Clifford 综合问题。

III. 相关工作

由通用门集构成的量子电路具有通用性，因为它们能够近似 每一种酉演化。量子门综合可以被视为对这一问题的定量研究：实现给定酉演化（例如量子计算）的最佳方式是什么？

著名的 Solovay-Kitaev 定理 [8], [36] 可视为一种非常通用的综合方案，适用于任意单量子比特酉算子（$n = 1$）以及任意通用门集。扩展到 n 量子比特的情形，可以通过将单量子比特门综合与特定的多量子比特纠缠门相结合来实现，也可以直接将 Solayev-Kitaev 算法推广到 $d = 2^n$维酉算子 [36]。尽管已有实现，例如参见 [37], ，但这种综合算法通常对于实际应用来说过于缓慢。因此，学界已不再采用这种严格的元算法，转而使用更具可扩展性的启发式方法。其中许多方法针对由 Clifford+T 门组成的通用门集，例如参见 [13]–[16]。

Clifford 电路（不含 T 门）在此背景下是一个有趣的特例。从数学角度来说，它们构成了一个带有额外结构的有限辛群 [38]–[40]的表示。例如，众所周知，每个 Clifford 酉变换都可以分解为一个深度至多为 $O(n)$ [41] 的 Clifford 电路。这些见解表明，Clifford 电路不可能过于复杂——这一特点也延伸到了 Clifford 合成。对于 $n = 6$ 量子比特这一特殊情形， [42]提出了具有竞争力的 Clifford 综合协议。对于一般的 n，Koenig 和 Smolin 的算法可用于将给定的 Clifford 电路与 Clifford 群中的唯一一个元素关联起来。随后，他们的算法还可用于综合这一群元素。最近，Robert Calderbank 团队开发了 Clifford 综合算法，甚至能够在逻辑层面（即基于纠错稳定子码）运行 [43], 而 Bravyi 等人发现，在允许使用 Ising 型全局纠缠操作的假设下，任意 Clifford 电路都存在常数深度表示 [44]。

虽然上述方法确实能将 Clifford 电路分解为基本的（Clifford）量子门，并且可以证明分解正确，但其规模和深度是否（接近）最优尚不明确。此时，采用 SAT/QBF 对问题进行重新表述便能带来显著改变。它们将门综合问题重新表述为一组量化布尔公式（QBF），每个公式对应我们允许的一个最大电路深度 $d_{\max}$。当且仅当存在深度不超过 $d_{\max}$ 的精确电路表示时，相应的 QBF 才会求值为真，并返回该表示的具体形式；否则，求值为假。尝试求解不同深度对应的这些 QBF，有望找到实现给定功能的最佳电路表示。因此，基于 SAT/QBF 的综合方法长期以来一直是经典设计自动化的重要手段 [45]。事实上，将基于 SAT 的综合与 Clifford 电路相结合的想法并非全新。文献 [29], 中的部分作者针对最优稳定子态制备提出了这一想法：寻找最短的 Clifford 电路，以 $|0\rangle$、……、$|0\rangle$ 为输入，并输出已知的目标稳定子态。本文提出的思路可视为将这些早期想法扩展到完整的 Clifford 电路综合。此外，我们还提供了严谨的正确性证明，并补充了相关背景和上下文。

IV. 主要结果与理论基础

我们的主要概念性结果是，Clifford 合成与布尔可满足性（SAT）之间存在一一对应关系。主要结果见定理 1，它源自对原始综合问题的两项真正具有量子特色的改造：（i）最大纠缠输入激励；（ii）Gottesman-Knill 定理。该结果为使用 SAT 进行最优 Clifford 电路综合奠定了严谨的基础，这也是下文第 V 节的主题。

A. 量子改造 1：最大纠缠输入态

我们理论论证的第一步有许多名称，包括 Choi-Jamiolkowski 同构 [46],[47], 纠缠辅助过程层析 [48] 以及张量分析中的展平操作 [49], [50]。从概念上说，我们取两个作用于 n 个量子比特的量子电路 U 和 V。我们不再测试所有可能的输入态，而是构造一个普遍有效的输入态来检验它们是否等价。首先，我们设想一个规模扩大一倍的测试电路，在上方的 n 个量子比特上施加 U，并在其余的 n 个量子比特上施加 V 中每个门的逆门。将 U 的第 k 个输入量子比特与 V 的第 k 个输入量子比特纠缠起来，我们便得到一个大小为 $2n$ 的新态 $|\omega_{2n}\rangle$。由于 U 和 V 作用于纠缠量子比特，只有当两个电路的功能相同（至多相差一个全局相位）时，第一个电路施加的所有变化才会被第二个电路完全还原。若它们的酉算子在任何一点上不同，那么得到的态就不会再次等于 $|\omega_{2n}\rangle$。即使让 U 和 $V^\dagger$ 都作用于

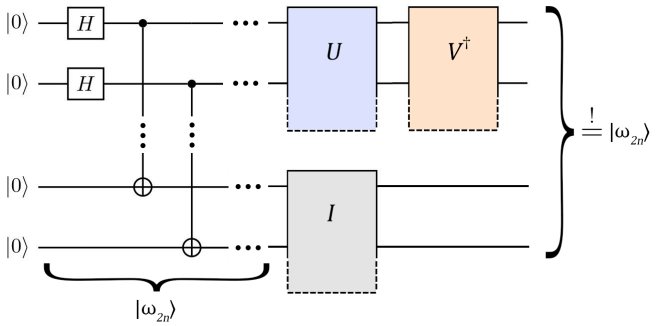


图 2. 纠缠辅助等价性检查示意图：当且仅当上方的量子电路产生两两最大纠缠态 $|\omega_{2n}\rangle$ 时，两个 n 量子比特电路 U，V 的功能（相差一个全局相位）等价。这里，$V^\dagger$ 是 V 的逆向电路（伴随），而 I 是单位元。

同一组 n 量子比特上，也就是说，作用于成对纠缠中的控制量子比特上。对于其余的目标量子比特，我们施加单位元，如图2所示。

引理 1。设 U、V 是两个 n 量子比特量子电路，$I^{\otimes n}$ 是 n 量子比特上的恒等操作。那么，$U \simeq V$ 当且仅当

$$(UV^\dagger)\otimes I^{\otimes n}|\omega_{2n}\rangle\langle\omega_{2n}|(UV^\dagger)^\dagger\otimes I^{\otimes n}=|\omega_{2n}\rangle\langle\omega_{2n}|. \quad (4)$$

这里，$|\omega_{2n}\rangle$ 是 n 2 个量子比特贝尔态的张量积，这些贝尔态将第 k 个量子比特与第 $n+k$ 个量子比特纠缠起来，对所有 $k\in[n]$ 均如此。

证明。注意，贝尔态与向量化单位矩阵成比例，即 $|\omega_{2n}\rangle\sqrt{2^n}=\mathrm{vec}(I^{\otimes n})$。算子—向量对应关系（参见例如 [49, Eq. (1.132)], ）进而断言 $UV^\dagger\otimes I_n|\omega_{2n}\rangle=\mathrm{vec}(UV^\dagger)/\sqrt{2^n}$。这确保了 $UV^\dagger=\mathrm{e}^{i\phi}I_n$（作为矩阵值等式）当且仅当

$$UV^\dagger\otimes I|\omega_{2n}\rangle=\tfrac{1}{\sqrt{2^n}}\mathrm{vec}(UV^\dagger)\overset{!}{=}\tfrac{\mathrm{e}^{i\phi}}{\sqrt{2^n}}\mathrm{vec}(I^{\otimes n})=\mathrm{e}^{i\phi}|\omega_{2n}\rangle.$$

式 (4) 对这个向量值方程取外积，以吸收剩余的全局相位（混态形式主义）。

□

将引理 1 应用于量子电路综 合公式式（3），可消去复相位和对所有可能输入态的全称量词：

$$\exists U_d,\mathrm{depth}(U_d)\le d_{\max}\ (UU_d^\dagger)\otimes I\Omega(UU_d^\dagger)^\dagger\otimes I=\Omega, \quad (5)$$

其中我们使用了 Ω 作为 $|\omega_{2n}\rangle\langle\omega_{2n}|$的简写符号。不过，对于整个全称量词的消除，我们必须采用混态形式主义，并将涉及的量子比特数量从 n 增加到 $2n$，见 图 2。

B. 量子转折二：*Gottesman-Knill* 定理

乍一看，式 (5) 似乎远没有式 (3)甚至它的经典对应物式 (1)那么令人望而生畏。这是因为纠缠使我们只需用一个输入态（引理 1）就能检查等价性，而不必针对指数多种可能性进行全称量化（∀）。

为了利用这种重新表述，后续大致有两种途径：(i) 使用真正的量子计算机来通过实验检验式 (5)中唯一剩余的等价关系。例如，量子辅助量子编译 [51]就采用了这种途径。(ii) 使用（强）量子电路经典模拟，检验这两个 $2n$量子比特态在式 (5) 中是否确实等价。我们可以想到四种主要的模拟方法：基于数组 [52],基于稳定子 [18], 张量网络 [53] 和决策图 [54], [55]。

这里，我们沿用第二条路径，采用基于稳定子态的模拟。主要原因是 Ω $=|\omega_{2n}\rangle\langle\omega_{2n}|$，即负责实现所有这些简化的 $2n$ 量子比特态，本身就是一种结构非常理想的稳定子态。

事实1。 $2n$量子比特态$\Omega=|\omega_{2n}\rangle\langle\omega_{2n}|$ 是一个稳定子态，其生成元为 $\langle(X\ I^{\otimes(n-1)})^{\otimes 2}、(Z\ I^{\otimes(n-1)})^{\otimes 2}\rangle$，其中圆括号() 表示循环置换。

众所周知，2量子比特贝尔态是一个稳定子态，其生成元为 $\langle XX, ZZ\rangle$ [10]。 事实1 可通过在适当的量子比特位置上对这些生成元取 n重张量积得到。例如，对于 n=2 ，这意味着$\langle XIXI, ZIZI, IXIX, IZIZ\rangle$或者对于 n=3$\langle XIIXII, ZIIZII, IXIIXI, IZIIZI, IIXIIX, IIZIIZ\rangle$，等等。不过，每隔 k个量子比特就会与第 $(n+k)$个量子比特纠缠。

根据 Gottesman-Knill 定理 [56]，我们可以在经典计算机上以多项式时间高效地模拟稳定子电路（Clifford 电路是其中的一类）。为了模拟量子电路对 $2n$量子比特稳定子态 Ω 的作用，我们根据量子门对稳定子进行逻辑映射，从而再次得到一个稳定子态。通过比较输入生成元与输出生成元是否相等，我们可以判断所应用的电路是否实现了单位元。

事实2 (Gottesman-Knill)。假设 U 和 U_d 都是 n 量子比特 *Clifford* 电路。那么，可以高效地进行检查。

$$(UU_d^\dagger)\otimes I\Omega(UU_d^\dagger)^\dagger\otimes I=\Omega. \quad (6)$$

这也可以从纠缠输入的概念得到：如果 U 和 U_d 具有相同的功能，$U_d^\dagger$ 就会逆转由 U完成的稳定子映射，从而完全不改变输入稳定子。注意，输入生成元和输出生成元必须完全匹配。由于该 $2n$量子电路的下半部分应用了单位元，因此不会改变最后 n 个量子比特上的生成元。因此，我们还可以将需要检查的生成元数量减半，从而消除 $^{\otimes 2}$ 操作（见 事实1）。

更准确地说，我们可以构造一个布尔函数$\phi_{U,\ \Omega}(U_d)$：当输入量子电路 U_d 满足式（6）时，该函数的值为 1，否则为 0。我们将在下文的第V节 给出这种显式构造。此处重要的是，我们可以用一个比特串 $y\in\{0,1\}^l$ 表示任意深度至多为 $d_{\max}$ 的 Clifford 酉变换 U_d，该比特串包含至多 $l(n,\ d_{\max})$ 个布尔变量。而且，我们实际上可以将$\phi_{U,\ \Omega}(y)$表示为一个子句长度为常数的合取范式，其中包含 $O\left(n^4d_{\max}\right)$ 个子句。综上，我们可以将克利福德电路综合问题改写为

$$\exists y\in\{0,1\}^{l(n,d_{\max})}\ \phi_{U,\Omega}(y)\overset{!}{=}1. \quad (7)$$

C. 主要结果与概述

最终导出式（7）的这些见解值得醒目地呈现，并补充一些背景信息。

定理 1 (Clifford综合的SAT重构)。 设U 为一个 n量子比特 *Clifford* 酉变换（目标），并固定最大深度 $d_{\max} \in \mathbb{N}$。那么，判定问题“能否用（至多） $d_{\max}$ 个 *Clifford* 层精确复现 U？”可以改写为一个 *SAT* 实例，其中包含 $O(n^2 d_{\max})$ 个变量和 $O(n^4 d_{\max})$个子句，且每个子句的大小均为常数。

这一见解在概念和实践层面均有重要意义，尤其要注意到 $d_{\max} \leq O(n)$ 对任意 Clifford 电路 [41]均成立。因此，二分搜索可以通过求解至多 U 个不同试探电路深度的 $\lceil \log_2(n) \rceil + O(1)$ SAT 重构问题 $d_{\max}$，精确确定给定 Clifford 酉变换的最小电路深度 U。此外，式（7）中布尔公式的满足赋值，是实际 Clifford 电路的位编码；这些电路能够精确复现U，且深度至多为 $d_{\max}$ （综合）。

从概念上来说，这种方法将最优 Clifford 综合问题多项式时间归约为（对数多个实例的）SAT 问题。这凸显出，这个特殊情形要容易得多，比起一般的量子电路综合问题（经典和量子）要容易得多。具体而言：最优 Clifford 综合至多与经典电路等价性检查一样难。

从实践层面来看，定理 1 为采用最先进水平的 SAT 求解器，严谨地解决 Clifford 综合问题，提供了严谨且针对具体情境的依据。本文余下部分将逐步介绍这种编码，并给出基准测试。

V. 使用 SAT 进行最优 Clifford 电路综合

Clifford 电路能够高效模拟，基于对稳定子态的稳定子表格编码，参见例如 [10]及其中的参考文献。这种量子态的多项式规模表示，是为所研究的综合问题推导多项式规模 SAT 编码的关键。因此，在详细讨论编码本身之前，我们先简要回顾如何使用稳定子表格。

A. 稳定子态的稳定子表格表示

一个 n 量子比特稳定子态可以用一个 $(2n+1) \times n$ 二进制矩阵表示，称为稳定子表格。其基本思想是，状态的每个稳定子生成元都可以用 $2n+1$ 位信息表示。在稳定子表格的标准记法 [18] 中，分别用二进制变量表示 Pauli X 型和 Z 型稳定子 $x_{i,\,j}$、$z_{i,\,j}$，并用 i，$j \in \{0, 1, ..n-1\}$ 表示相位；如果第 i 个稳定子具有负相位，则$r_i = 1$：

$$\left[\begin{array}{ccc|ccc|c} x_{0,0} & \cdots & x_{0,n-1} & z_{0,0} & \cdots & z_{0,n-1} & r_0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{n-1,0} & \cdots & x_{n-1,n-1} & z_{n-1,0} & \cdots & z_{n-1,n-1} & r_{n-1} \end{array}\right]$$

对于位置 i，j 处的 Pauli-Y 型稳定子，$x_{i,\,j}$ 和 $z_{i,\,j}$在对应位置都必须设为 1。此格式的稳定子态可以通过常见的 Clifford 门及以下更新规则进行变换，其中 $\oplus$ 表示按位异或运算：

- 在量子比特 j 上施加 H 门：交换第 j 个 X 型列与第 j 个 Z 型列，并且 $r \oplus= x_j z_j$。这可由变换 $HXH^\dagger = Z$、$HZH^\dagger = X$ 和 $HYH^\dagger = -Y$ 得出，因此它会交换 $x_{i,\,j} \leftrightarrow z_{i,\,j}\ \forall i$，并且仅在 Pauli-$Y$ 稳定子的情况下翻转相位；
- 在量子比特 j上应用 S 门：即将 j类型列的第 XOR 列按位X到 j类型列的第 Z列 $z_j \oplus= x_j$，并再次使用 $r \oplus= x_j z_j$；
- 在控制量子比特 c 和目标量子比特 t上应用 *CNOT* 门：即将 X类型列的第 c列与X类型列的第 t列进行按位异或 $x_t \oplus= x_c$，反之对 Z类型$z_c \oplus= z_t$ 同样适用 $r \oplus= x_c z_t (x_t \oplus z_c \oplus 1)$。

任何其他 Clifford 门的进一步更新规则都可以从这些基本规则推导出来。

通过将其反稳定子 [18]纳入其中，可以在稳定子表格中编码有关稳定子态的更多信息。这些是 Pauli 字符串，与稳定子一起生成整个 Pauli 群。在更新稳定子表格时，它们与稳定子生成元的处理方式完全相同。

B. 表格与门变量

下文中，令 Q 表示量子电路作用的量子比特集合，d_{max} 表示该电路的最大深度。

虽然所有 Clifford 酉算子都只需由 H、S 和 $CNOT$ 量子门生成，但为方便起见，用于编译的目标门集也可以包含其他量子门，例如 Pauli X、Y 和 Z 操作，或 CZ 门等双量子比特门。为体现编码中的这种灵活性，我们定义两个集合$SQGs$ 和 $TQGs$，分别表示单量子比特门集合和双量子比特门集合，使其能够用于实现任意 Clifford 电路。

在量子电路的每一层，都可以选择是否应用某个量子门。因此，我们引入以下变量

$$\begin{aligned} Svars &= \{g_q^d \quad | \, g \in SQGs,\ q \in Q,\ 0 \leq d < d_{max}\} \\ Tvars &= \{g_{q_0,\,q_1}^d | \, g \in TQGs,\ q_0 \in Q,\ q_1 \in Q \setminus \{q_0\}, \\ &\qquad 0 \leq d < d_{max}\} \end{aligned}$$

表示在深度 d 处对特定量子比特（或量子比特对）应用某个量子门。

根据定义，可以直接编码可能的稳定子表格。表格的 Z 部分、X 部分和 R 部分使用以下变量

$$\begin{aligned} Xvars &= \{z_q^d \mid q \in Q,\ 0 \leq d < d_{max}\}, \\ Zvars &= \{x_q^d \mid q \in Q,\ 0 \leq d < d_{max}\}, \\ Rvars &= \{r^d \mid 0 \leq d < d_{max}\}, \end{aligned}$$

其中，集合 $Zvars$、$Xvars$ 和 $Rvars$ 中的每个元素都是位向量。这些位向量编码了所有稳定子对特定量子比特的 Z、X、R 部分的作用方式。

<escape>根据引理 1中的构造，为了保证由这些变量合成的所有电路具有相同的酉算子，该编码需要 $2n$ 个量子比特。但是
</escape>

拥有这些 n 额外量子比特会产生不良副作用：合成电路应当在该量子电路的较低位 n 量子比特上实现单位元。这会不必要地扩大搜索空间，因为单位元可以通过多种方式实现。我们可以对这些量子比特施加约束，但这会不必要地增加编码的规模。我们可以通过仅考虑上方的 n 量子比特，并将纠缠输入态的稳定子切换为以下事实所述的 $|0\rangle^{\otimes n}$ 态的稳定子和反稳定子，来避免这一复杂问题。

事实 3。对于 *Clifford* 酉变换 U，$(U\otimes I^{\otimes n})|\omega_{2n}\rangle$ 在前 n 个量子比特上的稳定子，与 $U|0\rangle^{\otimes n}$ 的稳定子和反稳定子相同。

结合 事实1，引理 1 告诉我们，对于 Clifford 电路 U，其 $2n$ 稳定子 $U\otimes I_n|\omega_{2n}\rangle$ 唯一确定该量子电路的酉算子。给定 U，我们可以通过将 Ω 的生成元 Ω 经过$U\otimes I$ 传播并忽略较低位的 n 量子比特，显式计算这些稳定子。这归结为只分析 $2n$量子比特态 Ω中每个稳定子生成元的前半部分。结果是每个给定 $2n(n+1)$ 对应的表格U。初始表格的对角线元素值为 1，并且与 $|0\rangle^{\otimes n}$ 输入态（Z型）稳定子和相应反稳定子（X型）相结合。

因此，我们可以仅使用 $|Q| = n$个量子比特来编码问题，而每个表格变量的位向量大小为 $2n$，因为还必须包含有关反稳定子的信息。

C. 转移关系

定义变量后，我们现在可以按照V-A 小节中的描述，对量子门如何作用于稳定子表格进行编码。自然地，表格之间的转移将成为类似于以下形式的约束：

$$g_q^d \Rightarrow (UpdateZ(g,q,d)\wedge UpdateX(g,q,d)\wedge UpdateR(g,q,d)),$$

其中，右侧的更新公式编码了量子门在特定深度作用于某个量子比特的过程。对于 Hadamard 门，这意味着

$$\begin{aligned} UpdateZ(H,q,d) &= (z_q^{d+1} \Leftrightarrow x_q^d)\\ UpdateX(H,q,d) &= (x_q^{d+1} \Leftrightarrow z_q^d)\\ UpdateR(H,q,d) &= (r^{d+1} \Leftrightarrow (r^d \oplus x_q^d \wedge z_q^d)) \end{aligned}$$

虽然这种编码是正确的，但它也是浪费的，因为对于每个量子比特和深度，它都会产生 $|SQG| + |TQG|$ 数量的此类蕴含式。注意到许多量子门对稳定子表格的不同部分执行相同的操作后，可以大幅减少这一数量（量子计算具有局部性）。例如，Pauli 门对表格的 Z-部分和 X-部分执行单位元操作，仅在如何改变 R-部分方面有所不同。

由于我们已知门集，因此可以预先收集表格各个部分的所有可能变换。令 $Z\text{–}updates(q,\ d)$ 表示在深度 d 时，对量子比特 q 上稳定子表格的 Z-部分进行的所有可能更新的集合。这些集合的元素是关于表格变量的逻辑公式。随后，我们可以定义映射 $Z\text{–}impliedby(q,d)$:$Z\text{–}updates(q,d) \rightarrow \mathcal{P}(Svars)$，将每个更新公式映射到一组单量子比特门变量，这些变量对应于按照该更新规则作用于稳定子表格的门。

对 Z 部分的单量子比特变化随后通过为每个量子比特 q、深度 $0 \le d < d_{max} - 1$ 以及 $Z\text{–}update \in Z\text{–}updates\ (q,d)$ 引入以下约束来编码：

$$\bigvee_{g_q^d \in Z\text{–}impliedby(Z\text{–}update)} \Longrightarrow (z_q^{d+1} \Leftrightarrow Z\text{–}update).$$

显然，对于表格的 X 部分和 R 部分，以及双量子比特门，也可以用类似的方法完成。

虽然此时的约束编码了所有可能的稳定子表格，但有些变量赋值会导致无效电路，例如同一深度下一个量子比特被两个量子门作用。因此，我们需要为每个深度 d 和量子比特 q 引入另一组约束，以确保所得解的一致性。

$$ExactlyOne\begin{pmatrix} \{g_q^d & | g\in SQGs\} & \cup \\ \{g_{q,\ q_1}^d & | q_1\in Q, g\in TQGs\} & \cup \\ \{g_{q_0,\ q}^d & | q_0\in Q, g\in TQGs\} & \end{pmatrix}$$

D. 对称性破缺

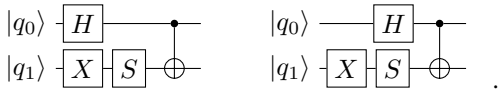
对称性破缺 [57] 是 SAT 求解领域中广泛使用的一种技术。它会向现有的合取范式公式添加额外约束，以避免在搜索空间的对称部分中进行搜索。我们可以通过分析公式的自同构，自动生成所谓的“对称性破缺约束”。自动执行这一过程的缺点是，我们无法清楚知道找到了哪些对称性，也无法确定推导出的约束究竟会让 SAT 实例更容易求解，还是反而更难。对于上述 SAT 公式，我们可以利用 Clifford 合成特有的知识，手动生成对称性破缺约束。

我们可以通过排除那些能够以更简单方式表示的有效解，向 SAT 求解器添加额外约束。例如，Hadamard 门是自逆的。因此，我们可以添加约束

$$H_q^d \Longrightarrow \neg H_q^{d+1}$$

适用于 $q \in Q$ 和 $0 \le d < d_{max} - 1$。这会排除所有将两个连续 Hadamard 门序列建模出来的门变量赋值。

另一种对称性涉及门排序中可能存在的自由度，以下等价电路最能说明这一点：



第一个量子比特上的 Hadamard 门可以与第二个量子比特上的 X 门或 S 门并行。我们可以通过规定单量子比特恒等门之后不能接单量子比特非恒等门来打破这种对称性。否则，在不改变 Clifford 酉变换的情况下，可以将非恒等门移到左侧

。更正式地说，对于$q \in Q$、 $0 \le d < d_{max} - 1$，我们规定

$$I_q^d \implies \bigwedge_{g \in SQGs \setminus \{I\}} \neg g_q^{d+1},$$

其中 I 是恒等门。

可以对双量子比特门施加类似的约束。如果对一对量子比特施加单位元，则在这些单位元之后不能再有双量子比特门。同样，我们添加约束

$$(I_{q_0}^d \wedge I_{q_1}^d) \implies \bigwedge_{g \in TQGs} \neg g_{q_0,\, q_1}^{d+1}.$$

对于 $q_0 \in Q$、 $q_1 \in Q \setminus \{q_0\}$、 $0 \le d < d_{max} - 1$。

编码中还有许多其他对称性可以破缺。原则上，任何 Clifford 门恒等式都可以用来推导对称性破缺约束。不过，需要在约束数量与解空间大小之间做出权衡。

E. 优化电路深度

上述编码可用于合成深度至多为 $d_{\max}$ 的量子电路，但不一定能合成深度最优电路。只有当$d_{\max}$ 恰好等于最优深度时，才能保证这一点，而最优深度必须预先确定。

一种方法是先为d_{max} 设定一个初始猜测值，然后逐步减小该值，直到对应的 SAT 实例存在解，而针对 $d_{max} - 1$的 SAT 实例则无解。实现这一目标的一种（理论上）高效的方法是二分搜索。可以将原始电路的深度作为上界。然而，如果该上界与最优值相差较大，就可能导致生成难以求解的实例。

相反，可以动态确定上界。对于一个相关问题（量子态制备电路），文献 [29] 探索了二分搜索，并提出以几何级数增加搜索解的深度范围。不幸的是，经过几次迭代后，SAT 调用的成本会相当高；只有当求解 SAT 实例的运行时间呈次指数增长时，这种方法才有望加速整个优化过程。在指数增长的情况下，直接进行线性搜索或按等差数列搜索反而更快。

另一种估算初始深度的方法是依据经验知识。如果已知 SAT 方法生成的解平均而言比另一种优化流程输出的量子电路浅 20%，我们就可以直接尝试运行该方法，并以预期深度作为初始猜测。然后可以从这个初始猜测出发，采用线性探测或二次探测来寻找最优解。

VI. 通过电路分解实现启发式方法

上文中，我们已经看到如何将 Clifford 合成重新表述为 SAT问题。然而，该问题的搜索空间会随最大量子电路深度 $d_{\max}$ 和量子比特数量 n呈指数级增长。根据所使用的具体 SAT 求解器，这种精确综合方法很快就会变得成本高得令人难以承受。缓解这些扩展性问题的一种方法是将大型 Clifford 电路拆分成一组可以并行合成的子电路。这种拆分既可以水平进行（以减少量子比特数量），也可以垂直进行（以降低电路深度），从而显著缩小 SAT 搜索空间。其结果是一种通用的启发式方法（无法保证拆分得到的子电路是最优的），可应用于更大的 Clifford 电路。

更准确地说，设 G 是一个作用于 n 个量子比特、最大深度为 $d_{\max}$ 的目标 Clifford 电路。那么，相应的 SAT 编码包含长度为 $l = O\left(n^2 d_{\max}\right)$ 的比特串，这对应于大小为 $2^l = 2^{O(n^2 d_{\max})}$ 的搜索空间。现在，我们可以将 $U = L_1 L_2$ 垂直拆分，其中每个 L_i 的深度为 $d' \approx d_{\max}/2$，并对每个 Clifford 块分别应用 Clifford 合成。这样得到两个并行的 SAT 实例，每个实例的比特串长度均为 $l' \approx l/2$ 。相应地，搜索空间的大小仅为 $2^{l'} \approx \sqrt{2^l}$。搜索空间大小的这一二次改进，是以将电路（可能）非最优地分解为两个块为代价的。

这一总体思路可以扩展到两个以上的垂直块。设 $G = L_1 \cdots L_m$ 是一个包含 m 层的 Clifford 电路，即由量子比特块 $L_i = g_i^1 \cdots g_i^{k_i}$组成，并且所有 $g_i^{k_i}$均作用于不同的量子比特上，因此可以并行运行。给定一个拆分大小 s，我们可以将该电路划分为 $\frac{m}{s}$ 个子电路$G_i = L_{i \cdot s} \cdots L_{(i+1) \cdot s}$，其中 $0 \le i < m$（此处假设 m 可被 s 整除，但对论证进行扩展是直接的）。然后，我们只需计算这些子电路各自的目标稳定子表格。对于 G_i，可以通过模拟电路直至 $L_{i \cdot s}$来完成。接着，我们可以对每个子电路分别使用 第 V 节提出的 SAT 重构方法。拆分大小 s 还可以为每个独立电路的编码所需最大深度提供一个较好的初始估计。

由于各个实例之间无需共享数据，因此可以并行运行所有 SAT 实例，以获得优化后的子电路 G_i' 然后将这些子电路串联起来，得到最终结果，即 $G' = G_1' \cdots G_m'$。需要注意的是，这种划分^s 方法能够保证生成正确的 Clifford 门分解。这是因为对所涉及的每个子块应用定理 1 即可得出这一结论。然而，这种方法未必能实现最优电路深度。毕竟，这种分治启发式方法将目标量子电路的不同块完全独立地处理，其规模随初始量子电路的深度和量子比特数量而变化。可以通过减小划分规模来缓解扩展性问题，但最终会达到收益递减点，此时划分规模的减小会对目标指标产生显著的负面影响。

由于可以使用 SAT 方法优化任意子电路，且不改变量子电路的功能，因此我们可以进一步采用分治方法。给定最大量子比特数 n_{max}，可以将量子电路分解为子电路 $G = G_1 \cdots G_m$，使每个电路中的量子比特数不超过 n_{max} ，并且任意两个子电路之间都没有双量子比特门，从而可以并行优化。

表 I 随机克利福德电路的实验结果。

	最优			垂直启发式			水平启发式			Bravyi 等人		
n	d	$\|G\|$	t [s]	d	$\|G\|$	t [s]	d	$\|G\|$	t [s]	d	$\|G\|$	t [s]
3	5.70	11.40	0.33	8.30	18.90	0.69	-	-	-	11.70	16.10	0.18
4	6.60	16.70	4.10	13.30	23.70	2.03	-	-	-	16.00	23.50	0.16
5	7.60	25.00	381.95	18.90	38.60	7.72	7.80	25.50	603.08	22.90	37.30	0.18
6	-	-	-	24.60	55.40	27.27	17.00	51.10	180.77	29.40	55.10	0.20
7	-	-	-	31.40	69.40	43.51	25.10	75.80	97.16	37.00	70.20	0.17
8	-	-	-	37.40	88.50	153.96	32.00	97.20	186.42	42.10	86.30	0.20
9	-	-	-	41.20	102.40	313.82	39.70	121.30	219.32	53.50	108.80	0.28
10	-	-	-	50.80	131.30	547.93	53.00	155.20	106.66	59.90	128.70	0.28
11	-	-	-	58.80	152.90	838.91	60.70	180.90	133.97	72.20	157.30	0.25
12	-	-	-	66.70	174.50	1464.46	75.80	217.40	117.73	78.90	170.10	0.26
13	-	-	-	75.50	206.50	2423.24	86.10	250.00	283.31	91.40	207.10	0.34
14	-	-	-	83.00	237.10	4412.97	99.80	305.70	111.89	100.30	235.20	0.33

n：量子比特数 d：平均深度 $|G|$：平均门数　t：平均运行时间

这两种拆分技术可以结合使用，使该方法尽可能具备可扩展性。给定深度阈值d_{thr}、拆分大小 $s < d_{trh}$ 和最大量子比特数n_{max}，可以将量子电路拆分为至多包含 n_{max}个量子比特的子电路。如果这些子电路中有任何一个的深度超过 d_{thr}，则可以进一步将其水平拆分为深度为s的电路块。随后，这些电路块可以彼此独立地（并行）进行优化。

VII. 评估

第V 节和VI 节中提出的方法已使用 C++，并借助公开可用的 SMT 求解器 Z3 [58]实现。这一实现已集成到量子电路编译工具 QMAP [17]，中，该工具是慕尼黑量子工具包（MQT）的一部分，可通过以下网址获取：
https://github.com/cda-tum/qmap。

为了了解所提出的方法在实践中的表现，我们考虑了两类基准测试：

(i) 随机 *Clifford* 电路 （受随机基准测试 [59]–[61] 启发）：这些电路是通过采样随机稳定子表格（包括反稳定子信息）得到的。由于我们的 SAT 编码基于稳定子表格，因此这种格式本身就是我们方法的有效输入格式，无需显式生成电路。对于每个量子比特数 n，我们生成了 10 个随机稳定子表格，并对所有运行结果取平均值。我们将所提出的方法与 Bravyi 等人 [62] 提出的最先进水平的贪心 Clifford 合成器进行比较。超时时间设为 3 小时。

(ii) *Clifford+T* 实现的 *Grover* 搜索 （受容错量子计算 [3], [8], [63] 启发）：我们使用随机布尔函数作为预言机，为 Grover 搜索算法生成了量子电路。对于每个量子比特数 n，均以这种方式生成了 10 个量子电路。由于这些量子电路包含 T 个量子门，因此将量子电路划分为 Clifford 块和 T 块，并分别对每个（非平凡）Clifford 块进行优化。

所有评估均在一台运行 Ubuntu 20.04 的 3.6GHz Intel Xeon W-1370P 机器上完成，该机器配备 128GiB 主内存和 16 个硬件线程。在电路的生成与综合以及贪心优化器的实现中，均使用了 IBM 开发的量子计算软件开发工具包 Qiskit [12]（版本 0.42.1）。

合成随机 Clifford 电路的实验结果见 表 I。

“最优 ”列展示了采用所提出的最优 SAT 方法得到的结果。遗憾的是，变量数量的增加以及编码随量子比特数扩展的情况在这里显得尤为明显。在给定的时间限制内，只能合成最多包含 5 个量子比特的随机 Clifford 电路。尽管如此，我们可以看到，其他方法，尤其是最先进水平的方法，合成的 n量子比特电路远非深度最优，其深度平均分别增加了 105.26%（$n = 3$）、142.42%（$n = 4$）和 201.32%（$n = 5$）。

“垂直启发式”列展示了采用所提出的启发式方法所得的结果，其中电路沿垂直方向进行划分，即所得的子电路均与原始电路具有相同数量的量子比特。与垂直拆分启发式方法相比，当前最先进的方法生成的电路平均仍深.92 %。

“水平启发式”列展示了采用所提出的启发式方法所得的结果，其中电路被划分为每个包含五个量子比特的子电路。在这一取值下，最优方法仍能在可接受的时间内得出结果（因此没有针对三个和四个量子比特的条目）。这种分解方式在量子比特数较少时能带来更好的结果，但当量子比特数超过九个后，结果最终会比垂直分解更差——这部分是分解方案本身造成的。电路不一定总能被完美地拆分为包含五个量子比特的子电路，而且原始电路中可能并行执行的量子门在优化后也可能无法再并行执行。另一个原因是，对于随机克利福德电路而言，量子比特之间的相互作用很快就会涉及五个以上的量子比特，因此越来越难找到仅包含五个量子比特的深层子电路

。这种综合方法的一大优势是运行时间。由于综合五量子比特电路的运行时间是可预测的，因此综合所有这些子电路所需的时间也同样可预测。

总而言之，表 I中的结果表明，通过更复杂的电路分解技术，可以改进启发式方法。目前最先进水平所生成的电路远非最优，因此仍有相当大的改进空间。

为分析实际容错量子电路深度可能得到的改进，我们选择了 Grover 搜索基准测试。根据 randomClifford 基准测试的结果，我们考察了针对 3 至 5 个量子比特的 Grover 电路。所提出的优化方案使电路的平均长度分别缩短了 13。38%、21。71% 和 16。72% 。Grover 基准测试已在以下网址公开：https://github.com/cda-tum/qmap。

VIII. 结论与展望

一方面，经典电路综合；另一方面，量化布尔公式（QBF）——这两个问题看似迥异，却彼此相关。这种对应关系可以建立一一映射，并构成若干最先进的最优（逻辑）电路综合方法的基础：QBF 求解器用于确定实现所需逻辑功能的最短电路表示。

在这项工作中，我们将这一通用思路拓展到量子领域，研究如何将 n 量子比特 Clifford 电路分解为尽可能少的基本门。随后，我们证明，判断能否用至多 $d_{\max}$ 个 Clifford 层来表示给定的 Clifford 功能，可以重新表述为一个涉及 $O(n^2 d_{\max})$ 个布尔变量的可满足性（SAT）问题。该归约既使用了最大纠缠输入激励，也运用了 Gottesman-Knill 定理。这表明，Clifford 合成属于 NP（多项式层次的第一层），比一般的逻辑电路综合更容易；后者是 Σ_2^p 完全问题（属于多项式层次的第二层）。

在电子设计自动化领域，SAT 求解器已成功应用于解决经典综合问题。我们证明了类似的方法也适用于量子计算，并且有很大潜力复制解决经典综合问题的成功经验。尽管最优综合方法在量子比特数量增加时扩展性较差，但它表明最优解与最先进水平之间存在巨大差距。据我们所知，这些是首批 (i) 经证明正确且 (ii) 附有最优性证书的 Clifford 综合协议。此外，所有提出的方法都已公开提供，集成在慕尼黑量子工具包 (MQT) 中，并作为开源量子电路编译工具 QMAP 的一部分（https://github.com/cda-tum/qmap）。QMAP 已原生支持 IBM 的 Qiskit；与量子软件开发工具包的进一步紧密集成则留待未来实现。

这些初步发现令人鼓舞，也为多个有趣的后续项目打开了大门，例如改进所提出的数值求解器。这需要调整稳定子编码以进一步提升性能，同时尝试不同的 SAT 求解器和新的预处理技术，以便为最大电路深度确定更精确的初始界。可配置的门集 也在我们的待办清单上。目前，我们只使用 H、S、$S^\dagger$、$CNOT$，以及 Pauli 门。未来，这一方案可以扩展为纳入更多单量子比特门（例如完整的单量子比特 Clifford 群）和双量子比特门（例如 $SWAP$、CZ、 CY，.....）。请注意，更多“基本”量子门会直接导致编码更复杂，从而扩大逻辑搜索空间（变量更多）。另一方面，每个时间步表达能力的提升必然会降低电路深度，因此最终会得到更短的 SAT 公式（逻辑子句更少）。这种权衡很可能是值得的。

所提出的编码过程足够灵活，能够支持面向架构的 Clifford 电路综合。一些量子架构仅支持量子比特之间的特定相互作用，这通常由耦合映射定义。在所提出的 SAT 编码中，我们只允许使用具体架构原生支持的 Clifford 门，从而遵循这一耦合映射。

几乎所有这些未来研究方向也都适用于改进所提出的启发式求解器，以实现近最优 Clifford 综合。我们打算探索不同的分治策略（分解为子电路），并研究如何以最优（或近最优）的方式综合这些电路块。

最后但同样重要的是，研究人员现在开始提出并探索利用量子计算机解决量子综合中具有挑战性的子程序。量子辅助量子编译 [51]就属于这一类。对于这项工作，我们有意将研究范围限制在 Clifford 电路上，因此目前还无需考虑这些思路；Gottesman-Knill 定理确保了整个过程中的经典模拟仍然易于处理。不过，将量子辅助量子编译的理念与传统的 SAT 求解技术有效结合，是一个值得未来研究的方向。这种协同作用留待未来探索。

致谢

作者感谢 Armin Biere、David Gross 和 Martina Seidl 提供启发性的讨论和宝贵的反馈。

T.P.、R.W. 和 L.B. 感谢欧洲研究委员会（ERC）通过欧盟地平线 2020 研究与创新计划（资助协议编号：101001318）提供的资助，以及慕尼黑量子谷提供的资金支持。慕尼黑量子谷由巴伐利亚州政府使用巴伐利亚高科技议程 Plus 的资金予以支持。所有作者均获得德国联邦经济和气候保护部（BMWK）的支持。该资助依据德国联邦议院的决议，通过 ProvideQ 和 QuaST 项目、QuantumReady 项目（FFG 896217）以及上奥地利州在 COMET 计划框架内提供；该计划由奥地利研究促进署（FFG）管理。

参考文献

[1] John Preskill, 《NISQ 时代及之后的量子计算》，第 2 卷，第 79 页，2018年。[2] Peter W. Shor, 《量子计算机上用于素因数分解和离散对数的多项式时间算法》，《SIAM计算杂志》，1997年。[3] Lov K. Grover, 《用于数据库搜索的快速量子力学算法》，ACM 会议论文集，第 212–219 页，1996年。[4] Aram W. Harrow、Avinatan Hassidim 和 Seth Lloyd, 《用于求解线性方程组的量子算法》，《物理评论快报》，第 103 卷，第 15 期，2009年。[5] Fernando G.S.L. Brandao 和 Krysta M. Svore, 《求解半定规划的量子加速》，载于 2017年 IEEE 第 58 届计算机科学基础年度研讨会（FOCS），2017年，第 415–426 页。DOI：10.1109/FOCS.2017.45。[6] Joran van Apeldoorn 等, 《量子半定规划求解器：更优的上界和下界》，第 4 卷，第 230 页，2020年。DOI：10.22331/q-2020-02-14-230。[7] Fernando G. S. L. Brandão、Richard Kueng 和 Daniel Stilck França, 《用于二次二元优化的更快速量子与经典半定规划近似》，第 6 卷，第 625 页，2022年。DOI：10.22331/q-2022-01-20-625。[8] Alexei Kitaev, 《量子计算：算法与纠错》，《俄罗斯数学调查》，第 52 卷，第 6 期，第 1191–1249 页，1997年。[9] Peter W. Shor, 《容错量子计算》，载于第 37 届计算机科学基础会议论文集，1996年，第 56–65 页。DOI：10 . 1109 / SFCS.1996.548464。[10] Michael A. Nielsen 和 Isaac L. Chuang, 《量子计算与量子信息》。剑桥大学出版社，2010年。[11] Daniel Gottesman, 《稳定子码与量子纠错》，1997年。[12] Abraham Asfaw 等, 《使用 Qiskit 学习量子计算》。（2020年）。[13] Vadym Kliuchnikov, 《Clifford+T 电路的酉算子综合》。arXiv：1306 . 3200 [quant-ph]。（2013年），预印本。[14] Matthew Amy 等, 《用于快速综合深度最优量子电路的中间相遇算法》，《IEEE集成电路与系统计算机辅助设计汇刊》，第 32 卷，第 6 期，第 818–830 页，2013年。DOI：10.1109/TCAD. 2013.2244643。[15] Olivia Di Matteo 和 Michele Mosca, 《量子电路综合的并行化》，《量子科学与技术》，第 1 卷，第 1 期，第 015 003 页，2016年。DOI：10 . 1088 / 2058 - 9565/1/1/015003。arXiv：1606。07413 [quant-ph]。[16] Philipp Niemann、Robert Wille 和 Rolf Drechsler, 《Clifford+T 电路的高级精确综合》，《量子信息处理》，第 19 卷，第 9 期，第 317 页，2020年。DOI：10.1007/s11128-020-02816-0。[17] Robert Wille 和 Lukas Burgholzer, 《MQT QMAP：高效量子电路映射》，载于《国际物理设计研讨会》，2023年。[18] Scott Aaronson 和 Daniel Gottesman, 《改进稳定子电路的模拟》，《物理评论 A》，第 70 卷第 5 期，页码 052 328，2004年。DOI：10.1103/PhysRevA.70. 052328。[19] Sergey Bravyi 和 Alexei Kitaev, 《利用理想 Clifford 门和含噪辅助量子比特实现通用量子计算》，《物理评论 A》，第 71 卷第 2 期，页码 022 316，2005年。DOI：10.1103/PhysRevA.71.022316。[20] Sahel Alouneh 等, 《SAT 求解器的综合研究与分析：进展、用途和成果》，《人工智能评论》，第 52 卷第 4 期，页码 2575–2601，2019年。DOI：10.1007/s10462-018-9628-0。[21] Sanjeev Arora 和 Boaz Barak, 《计算复杂性：现代方法》。剑桥大学出版社，2009年。DOI：10.1017/CBO9780511804090。[22] Ankit Shukla 等, 《量化布尔公式应用综述》，载于《国际人工智能工具会议》，2019年，页码 78–84。DOI：10.1109/ICTAI.2019.00020。[23] Markus N. Rabe 和 Sanjit A. Seshia, 《增量确定化》，载于《可满足性测试理论与应用会议》，第 9710 卷，2016年，页码 375–392。[24] Florian Lonsing 和 Uwe Egly, 《DepQBF 6.0：超越传统 QCDCL 的基于搜索的 QBF 求解器》，载于《国际自动演绎会议》，第 10395 卷，2017年，页码 371–384。[25] Markus N. Rabe 和 Leander Tentrup, 《CAQE：一个可验证的 QBF 求解器》，载于《CAD 中的形式化方法国际会议》，2015年，页码 136–143。DOI：10.1109/FMCAD. 2015.7542263。[26] Armando Solar-Lezama 等, 《有限程序的组合式草图设计》，载于《编程语言与操作系统架构支持国际会议》，2006年，页码 404–415。DOI：10 .1145/1168857. 1168907。[27] Edmund Clarke 等, 《反例引导的抽象精化》，载于《计算机辅助验证》，第 1855 卷，2000年，页码 154–169。[28] Susmit Jha 和 Sanjit A. Seshia, 《通过归纳学习实现形式化综合的理论》，《计算机学报》，第 54 卷第 7 期，页码 693–726，2017年。DOI：10.1007/s00236- 017-0294-5。[29] Sarah Schneider、Lukas Burgholzer 和 Robert Wille, 《用于最优 Clifford 电路综合的 SAT 编码》，载于《亚洲及南太平洋设计自动化会议》，2023年。[30] David Gross 等, 《通过压缩感知进行量子态层析》，《物理评论快报》，第 105 卷第 15 期，页码 150 401，2010年。DOI：10 . 1103 / PhysRevLett . 105 . 150401。

[31] Martin Kliesch 等，《通过少量测量保证恢复量子过程》，第 3 卷，页码 171，2019年。DOI：10.22331/q-2019-08-12-171。[32] Ingo Roth 等，《根据少量平均门保真度恢复量子门》，《物理评论快报》，第 121 卷第 17 期，页码 170 502，2018年。DOI：10.1103/PhysRevLett. 121.170502。[33] Lukas Burgholzer、Richard Kueng 和 Robert Wille，《用于量子电路验证的随机激励生成》，载于《亚洲及南太平洋设计自动化会议》，2021年。[34] Madalin Gu¸t˘a 等，《利用最优误差界实现快速量子态层析》，《物理学杂志 A：数学与理论》，第 53 卷第 20 期，页码 204 001，2020年。DOI：10 . 1088 /1751 - 8121 / ab8111。[35] Dominik Janzing、Pawel Wocjan 和 Thomas Beth，《“非恒等性检验”是 QMA 完全问题》，《国际量子信息学杂志》，第 03 卷第 03 期，页码 463–473，2005年。[36] Christopher M. Dawson 和 Michael A. Nielsen，《Solovay-Kitaev 算法》，《量子信息与计算》，第 6 卷第 1 期，页码 81–95，2006 年。[37] Tien Trung Pham 、Rodney Van Meter 和 Clare Horsman，《Solovay-Kitaev 算法的优化》，《物理评论 A》，第 87 卷第 5 期，页码 052 332，2013年。DOI：10.1103/PhysRevA.87.052332。[38] Jeroen Dehaene 和 Bart De Moor，《Clifford 群、稳定子态以及 GF(2) 上的线性与二次运算》，《物理评论 A》，第 68 卷第 4 期，页码 042 318，2003年。DOI：10.1103/PhysRevA.68.042318。[39] David Gross，《有限维量子系统的 Hudson 定理》，《数学物理学杂志》，第 47 卷第 12 期，页码 122 107，2006 年。DOI：10.1063/1.2393152。[40] Huangjun Zhu 等，《Clifford 群并非平滑地偏离酉 4-设计》。arXiv：1609 . 08172[量子物理]。（2016年），预印本。[41] D. Maslov，《有限邻接量子架构中无辅助量子比特的线性深度稳定子电路与量子傅里叶变换电路》，《物理评论 A》，第 76 卷第 5 期，页码 052 310，2007年。DOI：10.1103/PhysRevA.76.052310。arXiv：quant-ph/0703211。[42] Sergey Bravyi、Joseph A. Latone 和 Dmitri Maslov，《6 量子比特最优 Clifford 电路》。arXiv：2012.06074。（2020年），预印本。[43] Narayanan Rengaswamy 等，《稳定子码的逻辑 Clifford 综合》，《IEEE 量子工程汇刊》，第 1 卷，页码 1–17，2020年。DOI：10.1109/TQE.2020.3023419。[44] Sergey Bravyi、Dmitri Maslov 和 Yunseong Nam，《利用全局相互作用实现 Clifford 运算和多重受控门的恒定成本实现》，《物理评论快报》，第 129 卷第 23 期，页码 230 501，2022年。DOI：10.1103/PhysRevLett.129.230501。[45] Roderick Bloem 等，《用于电路综合的基于 SAT 的方法》。arXiv：1408.2333 [cs]。（2014年），预印本。[46] Man-Duen Choi，《复矩阵上的完全正线性映射》，《线性代数及其应用》，第10卷，第3期，第285–290页，1975年。DOI：10.1016/0024- 3795(75)90075-0.[47] Andrzej Jamiołkowski，《保持算符的迹和半正定性的线性变换》，《数学物理报告》，第3卷，第4期，第275–278页，1972年。DOI：10.1016/0034-4877(72)90011-0。[48] Joseph B. Altepeter 等人，《辅助量子过程层析》，《物理评论快报》，第90卷，第19期，第193 601页，2003年。DOI：10.1103/PhysRevLett.90.193601。[49] John Watrous，《量子信息理论》。剑桥大学出版社，2018年，共590页。[50] Richard Kueng。《ACM 270：基于张量的量子与经典信息处理》。（2019年）。[51] Sumeet Khatri 等人，《量子辅助量子编译》，第3卷，第140页，2019年。[52] Hans De Raedt 等人，《大规模并行量子计算机模拟器：十一年后》，《计算机物理通讯》，第237卷，第47–61页，2019年。DOI：10.1016/j.cpc.2018.11.005。[53] Jacob C. Bridgeman 和 Christopher T. Chubb，《徒手阐释与诠释性舞蹈：张量网络入门课程》，《物理学杂志 A：数学与理论》，2017年。[54] Stefan Hillmich、Igor L. Markov 和 Robert Wille，《如同真实量子计算机一般：量子计算的快速弱模拟》，发表于《设计自动化会议》，2020年。[55] Philipp Niemann 等人，《量子多决策图：高效的量子函数表示与操作》，《IEEE集成电路与系统计算机辅助设计汇刊》，2016年。[56] Daniel Gottesman。《量子计算机的海森堡表象》。arXiv：quant-ph/9807006。（1998年），预印本。[57] Armin Biere 等人，《可满足性手册》。IOS出版社，2009年。[58] Leonardo de Moura 和 Nikolaj Bjørner，《Z3：一种高效的 SMT 求解器》，发表于《系统构造与分析工具和算法》，2008年，第337–340页。[59] Emanuel Knill 等人，《量子门的随机基准测试》，《物理评论 A》，第77卷，第1期，第012307页，2008年。DOI：10.1103/PhysRevA.77.012307。[60] Easwar Magesan 等人，《通过交错随机基准测试高效测量量子门误差》，《物理评论快报》，第109卷，第8期，第080505页，2012年。DOI：10.1103/PhysRevLett.109.080505。[61] Richard Kueng 等人，《将实验结果与容错阈值进行比较》，《物理评论快报》，第117卷，第17期，第170 502页，2016年。[62] Sergey Bravyi 等人，《利用模板和符号化泡利门优化 Clifford 电路》，第5卷，第580页，2021年。DOI：10.22331/q-2021-11-16-580。arXiv：2105.02291。[63] Daniel Gottesman，《容错量子计算理论》，《物理评论 A》，第57卷，第1期，第127–137页，1998年。DOI：10.1103/PhysRevA.57.127。