用于验证量子傅里叶变换电路的旋转抽象

1st Arun Govindankutty电气与计算机工程系，北达科他州立大学美国法戈 arun.g@ndsu.edu2nd Sudarshan K. Srinivasan电气与计算机工程系，北达科他州立大学美国法戈 sudarshan.srinivasan@ndsu.edu3rd Nimish Mathure 电气与计算机工程系，北达科他州立大学美国法戈 nimish.mathure@ndsu.edu

arXiv:2301.00737v1 [quant-ph] 2 Jan 2023

摘要—**随着大规模量子计算机研发竞赛的展开，以及人们努力利用量子算法高效解决科学和工程学科中的问题，高效且可扩展的验证方法至关重要。我们提出了一种针对量子傅里叶变换（QFT）电路的新型形式化验证方法。量子傅里叶变换是一种基础量子算法，也是许多量子计算应用的基础。该验证方法对量子傅里叶变换中使用的量子门进行抽象，从而将验证问题从希尔伯特空间简化为位向量无量词逻辑。现已有非常高效的判定过程可用于位向量推理。因此，我们的方法能够扩展至验证含有 10,000 个量子比特和 5,000 万个量子门的量子傅里叶变换电路，在迄今采用形式化验证方法验证过的量子傅里叶变换电路规模方面取得了飞跃式进展。**

索引词—**形式化验证、量子算法、量子计算、量子傅里叶变换、量子电路验证。**

[1]

I. 引言

建造拥有 1,000 个及更多量子比特的大规模量子计算机的竞赛正如火如荼地进行 [1] [2]。预计 IBM Condor 量子计算机将于 2023 [3] 发布，拥有 1,000 个量子比特。继 Condor 之后，IBM 计划使用芯片间耦合器构建更大规模的量子计算系统 [4], , 目标是打造一台拥有 100 万个量子比特的系统 [5]。Google 的路线图也计划在不久的将来建造一台拥有 100 万个量子比特的量子计算机 [6]。此外，Xanadu、Rigetti、IonQ 和 D-Wave 等公司也在开发众多其他量子计算机。Intel 展示的低温控制电路开发（Horse Ridge 芯片） [7], 也在加速推进，以实现量子计算和通信应用 [8]。

量子算法动物园网站跟踪该领域的算法，目前列出了 430 篇关于各种量子算法的引文 [9]。

80/20 设计规则在计算领域广为人知，即设计周期中只有 20% 的时间用于实际设计，而 80% 的时间用于验证。若缺乏可扩展的验证技术，大规模量子系统的实际部署将受到严重阻碍。因此，开发量子电路的验证方法至关重要，这也是本研究的重点。形式化验证凭借其提供正确性保证和发现难以查找的边界情况错误的能力，已成为半导体行业的标准。已有多种针对量子电路的形式化验证方法 [10]。

然而，例如，据文献报道，已验证的最大量子傅里叶变换（QFT）电路仅包含 31 个量子比特 [11]。因此，开发可扩展的验证方法已刻不容缓。

贡献： 实现形式化验证可扩展性的方法之一，是开发特定领域的方法。本研究针对一种基础量子算法——量子傅里叶变换（QFT）。在计算和工程领域，变换在问题求解和分析中发挥着重要作用。量子计算利用 QFT 解决各种问题。QFT 是众多量子算法不可或缺的一部分，包括 Shor 因数分解算法、量子相位估计算法以及离散对数计算等 [12] [13]。QFT 的现实应用包括计算金融中的投资组合优化 [14],金融衍生品的蒙特卡洛定价 [15], 用于构建干涉仪的量子气象学 [16], 材料检测与分析 [17], 医学应用中的图像数据分析 [18]以及风险分析 [19]等。

我们开发了一种形式化验证方法，可以

[1]本文是已提交至 IET Quantum Computing 的论文预印本。若论文被接收，正式版本将在 IET Digital Library 上发布。

用于高效验证多达 *10,000* 个量子比特、包含 *5,000* 万个量子门的量子傅里叶变换（*QFT*）电路。我们的具体贡献如下：

1）哈达玛（H）门和受控旋转门（R_n）的抽象，该抽象利用这些量子门对输入量子比特产生的旋转影响。2）一种正确性框架，利用上述抽象，将验证问题从希尔伯特空间（复向量空间）归约为位向量无量词逻辑（QFBV）。3）带有证明的定理，用于证明这些抽象是可靠的，即如果抽象量子傅里叶变换电路被验证为正确，则可保证待验证的量子傅里叶变换电路的正确性

尽管我们以量子傅里叶变换为目标开发了该方法，但抽象中所采用的关键思想可以应用于更广泛的量子电路，这正是我们计划在未来开展的工作。

本文其余部分的组织如下。第二节介绍量子电路和量子傅里叶变换电路的背景。第三节概述了用于验证量子电路的形式化方法相关工作。第四节介绍所提出工作的主要贡献，包括量子门抽象和正确性框架。第五节讨论这些抽象及整体方法的正确性。第六节给出并讨论实验结果。第七节概述结论和未来工作。

II. 背景

本节将回顾量子比特、量子门和量子傅里叶变换电路的相关背景。 [12]中提供了对这些主题的详细介绍。量子计算领域中的信息由量子比特表示。量子比特是信息的基本单位，类似于经典计算中的比特。一般而言，量子比特表示为正交归一（正交且归一化）向量 $|0\rangle$ 和 $|1\rangle$的线性组合。这些向量线性无关，也就是说，我们无法将其中一个表示为另一个的线性组合。如下所示为这些线性无关的向量。

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, and \;\; |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

上述正交归一向量可通过向量加法和缩放（线性组合）来表示向量空间中的任意向量，因此称为基向量。如下所示为量子比特 $|q\rangle$ 的标准表示，其中，α 和 β 是复数，且满足 $\alpha^2 + \beta^2 = 1$。

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle$$

量子门是作用于量子比特并产生所需输出的酉算子。量子算法是一种利用量子力学性质解决特定问题的分步过程。量子算法运行于量子计算的计算模型之上，而本研究基于量子电路模型，这是目前应用最广泛的方法 [20]。

量子傅里叶变换类似于经典领域中的离散傅里叶变换（DFT），能够高效地执行量子力学模型中的傅里叶变换。量子傅里叶变换作用于输入量子比特状态（正交归一基向量 $|0\rangle$，.....，$|N-1\rangle$），并将其转换为相应的输出状态。如下所示为该变换 [12]。

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle$$

在上述内容中，$|j\rangle$，N，i，和 k 分别表示输入量子比特、量子傅里叶变换点数、虚数（$\sqrt{-1}$）和迭代变量。这里 $N = 2^n$，其中 n 是量子傅里叶变换中的量子比特数。

在变换域中，这个变换后的状态（变换后的$|j\rangle$）可表示为若干独立分量之和，这些分量的频率是 $\frac{2\pi}{N}$ 的整数倍。同一方程可以重新整理，从而得到每个量子比特独立发生的等效变换，这正是我们在本研究中加以利用的性质。

量子傅里叶变换电路可以通过一系列级联的哈达玛（H）门和受控旋转（R_n）门来实现。H 门和 R_n 门定义如下。

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & e^{\pi i}\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

$$\mathrm{R}_n = \begin{bmatrix}1 & 0\\ 0 & e^{2\pi i/2^n}\end{bmatrix}$$

H门会使该量子比特的输入基向量形成等权叠加态。 R_n 门负责产生频率谐波。构建量子傅里叶变换电路时，首先对所有量子比特施加 H 门。对于一个包含 m 个量子比特的量子傅里叶变换电路，量子比特 1 上应作用 R_2, ...、R_m 门，其控制输入分别取自量子比特 2 至量子比特 m，且这些控制量子比特在施加 H 门之前取值。量子比特 2 上应作用 R_2,...、R_{m-1} 门，其控制输入分别取自量子比特 3 至量子比特 m，且这些控制量子比特在施加 H 门之前取值，依此类推。图 1(a) 展示了在一个含 3 个量子比特的系统上执行量子傅里叶变换时发生的变换。

III. 相关工作

量子算法和电路的形式化验证一直是一个活跃的研究领域。本节将概述这些相关工作，并说明它们与我们的方法有何不同。主要结论是，这些方法尚未展现出我们已实现的效率和可扩展性。从这个意义上说，就迄今已验证的量子电路规模而言，我们的方法取得了飞跃式进展。

Yamashita 和 Markov [22]提出了一种用于量子电路的等价性检查方法。在等价性检查中，需要将待验证的电路与参考

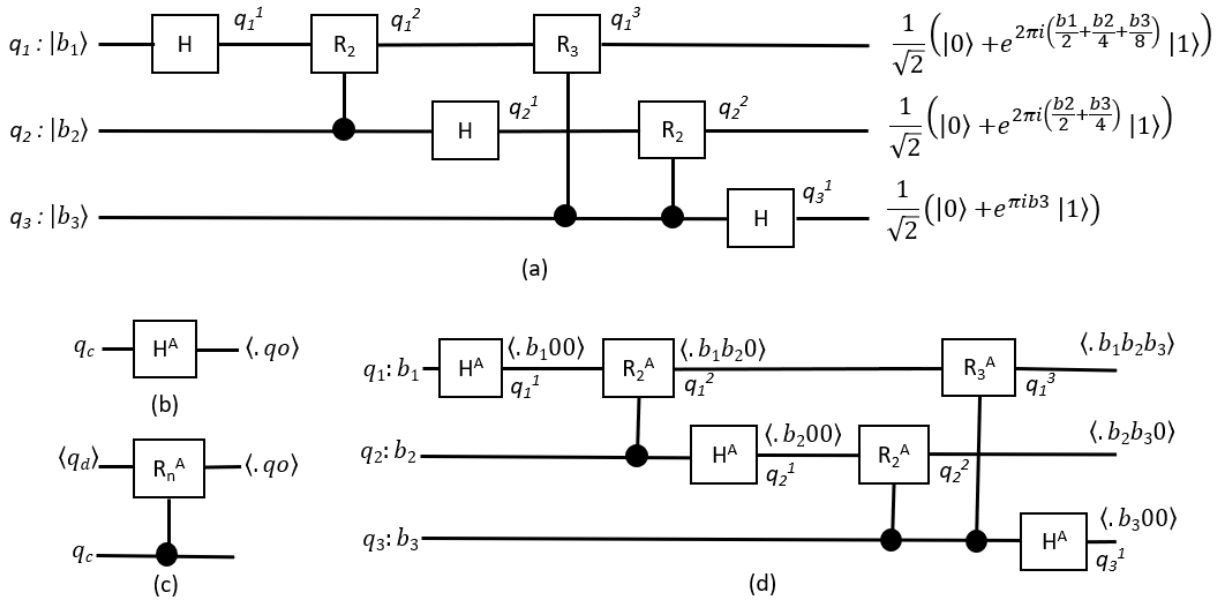


图 1。（a）3 量子比特量子傅里叶变换电路 [21]。（b）抽象 Hadamard 门。（c）抽象旋转门。（d）3 量子比特量子傅里叶变换抽象电路表示。

电路进行比较。这种方法与我们的方法有两点显著区别。第一点区别与一般的等价性检查有关：它需要一个黄金电路（已验证且可信）作为参考电路。例如，要验证一个包含 10,000 个量子比特和 5,000 万个量子门的量子傅里叶变换电路，就需要一个规模相同且可信的量子傅里叶变换电路。因此，要实现等价性检查，必须有能够验证给定电路功能正确性的方法。这正是我们要解决的缺口。等价性检查在综合优化中很有用。我们的方法基于属性，无需规模相同的参考电路即可进行验证。如果一个包含 10,000 个量子比特和 5,000 万个量子门的量子傅里叶变换电路满足我们提出的正确性属性，就能保证该电路正确。第二点区别是，如果他们无法将问题归约到布尔空间，就会采用混合方法 [23], , 在希尔伯特空间中求解验证问题。我们采用旋转抽象，将问题完全归约到布尔空间；针对布尔空间的求解器效率高出几个数量级，且可扩展性更强。我们还利用了我们的方法专用于量子傅里叶变换电路验证这一特点。对方验证的最大电路包含 5,000 个量子门，耗时约 59 秒。相比之下，我们能够在 0.04 秒内验证包含 8,000 个量子门的电路，在约 60 秒内验证包含 500 万个量子门的电路，并在 2,380 秒内验证包含 5,000 万个量子门的电路。

Amy [11] 使用复数路径和对量子门进行建模，以实现验证。他们对所得电路执行化简，这些化简通过重写规则实现。这些化简使用 Haskell 定理证明器执行。重写规则保证将电路化简为范式，随后利用该范式检查正确性。他们验证了一个 16 量子比特和一个 31 量子比特的量子傅里叶变换，分别对无错误电路耗时 1.250 秒和 16.020 秒。相比之下，我们的方法对 16 量子比特和 32 量子比特的量子傅里叶变换电路分别耗时 0.02 秒和 0.03 秒，分别如此。他们采用二进制有理数算术技术，但当前实现会在量子比特数大于 31 的量子傅里叶变换电路中导致整数溢出。因此，使用当前实现时，他们无法处理量子比特数大于 31 的量子傅里叶变换电路。我们能够处理最多 10,000 个量子比特。

Liu 等人 [24]在 Isabelle/HOL 定理证明器中形式化了量子霍尔逻辑，并用其证明了 Grover 搜索算法在无限大小输入下的正确性。他们报告称，该证明耗费了 5 人月的工作量。他们没有说明如何使用该证明来验证给定的 Grover 算法量子电路。相比之下，我们的方法可全自动验证任意量子傅里叶变换电路。他们没有研究量子傅里叶变换验证。

Feng 等人 [25] 开发了一种模型检测算法，可检查量子马尔可夫链上的量子计算树逻辑（QCTL）性质。该方法用于检查 BB84 协议在 n=1 时的正确性；其对应电路包含 8 个量子比特和 24 个量子门。他们也没有研究量子傅里叶变换验证。

IV. 旋转抽象

在为哈达玛（H）门和受控旋转（R_n）门开发抽象时，有三个关键思想。

第一个关键思想与基向量有关。如果量子傅里叶变换电路在输入量子比特为基向量 $|0\rangle$ 或 $|1\rangle$ 时能够正确工作，那么可以保证该电路对于任意量子比特输入 [26] 都能正确工作。因此，出于验证目的，我们只考虑输入量子比特为 $|0\rangle$ 或 $|1\rangle$ 的情况。

第二个关键想法涉及量子门，内容如下：如果输入量子比特仅限于基向量，那么 H门和 R_n 门都可以建模为使基向量发生旋转的量子门。H门只有一个输入。我们称之为控制输入 q_c，如图1(b)所示，

因为如果输入是 $|1\rangle$，那么 H门的功能可以表示为在 $|1\rangle$上进行旋转。如果该控制输入是 $|0\rangle$，则不进行旋转。R_n 门有两个输入（控制输入和数据输入）以及一个输出，我们称控制输入为 q_c，数据输入为 q_d，输出为 q_o （如图1(c)所示）。如果 q_c 是$|1\rangle$，那么 R_n 会在 q_d上进行旋转。否则，如果 q_c 是 $|0\rangle$，则不进行旋转。

第三个关键思想涉及量子门对数据输入量子比特施加的旋转量，以及由此产生的输出量子比特状态，具体如下：H门会对 $|1\rangle$ 施加 π (2π/2) 旋转，而不会旋转 $|0\rangle$。R_n 门会对 $|1\rangle$ 施加 $2\pi/2^n$ ($\pi/2^{n-1}$) 旋转，而不会旋转 $|0\rangle$。例如，R_4 会施加 $\pi/8$ 的旋转。因此，量子门对 $|1\rangle$ 施加的旋转是相对于 2π 的 2 的负次幂。

量子傅里叶变换电路的结构使得量子门的控制输入始终是初始量子比特状态，并且仅用于决定是否进行旋转。

因此，我们可以用布尔值 0 和 1 表示基向量输入值 $|0\rangle$ 和$|1\rangle$。

经过这些旋转变换后的量子比特将作为下一个量子门的输入，最终形成电路的输出状态。

如果将指数中的 $2\pi i$ 项提取出来，每个量子比特变换后的最终输出状态便可用分数位向量进行抽象表示，这些向量实质上记录了量子比特所经历的旋转量。分数位向量 $\langle .b_1b_2b_3\rangle$ 对应的旋转值为 $2\pi * (b_1 * 2^{-1} + b_2 * 2^{-2} + b_3 * 2^{-3})$。例如，位向量 $\langle .101\rangle$ 对应的旋转值为 2π（1/2+0+1/8）。通过定义 H门和 R_n 门对分数位向量的旋转影响，可以得到它们的抽象形式，并利用这些抽象门构造抽象量子傅里叶变换电路。在包含 m 个量子比特的量子傅里叶变换电路中，最小旋转量为 $2\pi/2^m$。因此，用于表示抽象量子傅里叶变换电路中量子比特的分数位向量必须包含 m 位。

抽象 H 门定义如下，它有一个输入量子比特 q_c，其类型为布尔类型。输出量子比特 q_o 是一个位向量，其大小等于 m，即量子比特的数量。

定义 1. *(抽象 Hadamard 门)* 若 q_c=1，则 $q_o \leftarrow \langle .100...0\rangle^m$；否则 $q_o \leftarrow \langle .000...0\rangle^m$.

抽象 R_n 量子门定义如下，它有两个输入量子比特 q_c 和 q_d。控制输入 q_c 的类型为布尔型，数据输入 q_d 和输出量子比特 q_o 均为大小为 m 的分数位向量，其中 m 为量子比特的数量。

定义 2. *(抽象 R_n 量子门)* 若 q_c=1，则 $q_o \leftarrow q_d +_m \langle .00..01_{m-n}0...0\rangle^m$；否则 $q_o \leftarrow q_d$。

在上述内容中，$+_m$ 表示关于 m的定点模加法。抽象量子傅里叶变换电路是通过将原始电路中的 H 门和 R_n 门替换为抽象门得到的。输入量子比特声明为布尔型，所有其他量子比特声明为大小为 m 的位向量类型。含 3 个量子比特的抽象量子傅里叶变换电路如图 1(d) 所示。当应用抽象H门时，图 1(d) 中量子傅里叶变换电路的 H 门输出端的量子比特将具有以下值：

$$q_1^1 \leftarrow \langle .b_100\rangle$$
$$q_2^1 \leftarrow \langle .b_200\rangle$$
$$q_3^1 \leftarrow \langle .b_300\rangle$$

接下来给出量子傅里叶变换正确性。令 QFT- $Abs_i(b_1, b_2, ..., b_m)$ 表示量子傅里叶变换电路抽象版本中第 i^{th} 个量子比特的输出状态，其中 m 为量子比特的数量，b_1、b_2、...、b_m 为布尔变量。

性质1. （量子傅里叶变换正确性属性）如果对于所有 $1 \le i \le m$，i 都是整数，且 $QFT\text{-}Abs_i(b_1, b_2, ..., b_m) = \langle .b_ib_{i+1}...b_m0...0\rangle^m$，那么量子傅里叶变换电路在功能上是正确的。

根据上述正确性属性，要使图1(a)中的量子傅里叶变换电路正确，输出处量子比特的状态应如下所示：

$$q_1^3 = \langle .b_1b_2b_3\rangle$$
$$q_2^3 = \langle .b_2b_30\rangle$$
$$q_3^3 = \langle .b_300\rangle$$

抽象门、抽象量子傅里叶变换电路和性质1均可用位向量无量词逻辑（QF BV）表示。已有多种 SMT 求解器能够非常高效地检查该逻辑中的属性。因此，可以通过使用 SMT-LIB 语言将抽象电路和正确性属性编码为该逻辑中的表达式，从而验证给定的量子傅里叶变换电路。SMT 求解器将自动检查该属性，并指出该属性是否成立。如果该属性成立，则可以保证量子傅里叶变换电路正确（下一节将对此加以证明）。如果该属性不成立，该工具将生成一个反例，可用于追查电路中的错误。

V. 抽象正确性

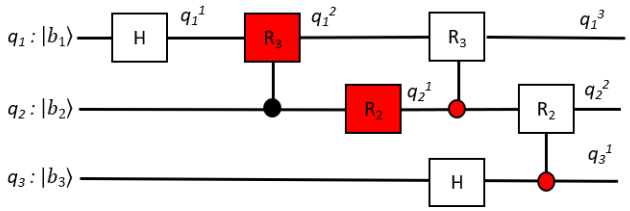


图 2. 展示错误情形的量子傅里叶变换电路。

本节将证明我们的验证方法的正确性。总体思路是遍历量子傅里叶变换电路中所有可能的错误类别，并说明验证方法如何标记每一类错误。错误类别如图 2 所示。我们也将位向量值称为数据值。

表 I 验证结果

QFT 基准测试		正确电路 无错误		错误门错误 错误深度 门-2		错误门错误 错误深度 门-n		错误控制错误 错误深度 门-2		错误控制错误 错误深度 门-n	
		验证统计数据		验证统计数据		验证统计数据		验证统计数据		验证统计数据	
量子比特(n)	量子门	M(MB)	T(s)	M(MB)	T(s)	M(MB)	T(s)	M(MB)	T(s)	M(MB)	T(s)
16	136	19.0	0.02	27.2	0.04	27.3	0.02	19.0	0.01	27.2	0.02
32	528	19.0	0.03	27.2	0.02	27.5	0.02	19.0	0.02	19.0	0.01
64	2,080	19.0	0.03	27.3	0.03	27.6	0.02	19.1	0.02	19.1	0.03
128	8,256	19.3	0.04	27.4	0.07	27.9	0.04	19.3	0.03	19.3	0.02
256	32,896	20.1	0.19	27.7	0.06	28.6	0.06	20.0	0.08	20.0	0.08
512	131,328	22.1	0.26	28.3	0.29	29.8	0.2	22.2	0.29	22.2	0.2
1,024	524,800	29.1	1.37	29.5	0.77	32.2	0.92	29.5	1.46	29.5	1.29
2,048	2,098,176	56.1	9.85	56.9	5.52	73.7	5.87	56.9	9.66	56.9	9.47
4,096	8,390,656	169.3	95.75	169.6	51.78	203.3	53.57	169.6	73.65	169.6	79.68
8,192	33,558,528	592.1	1,109.0	593.6	640.53	596.2	643.9	593.6	641.03	593.6	639.57
10,000	50,005,000	888.7	2,379.88	890.7	1,523.99	894.5	1,568.79	890.6	1,571.29	890.6	1,524.65

引理 1. 如果量子傅里叶变换电路存在错误，即向 H门输入了错误的输入，那么对该量子傅里叶变换电路抽象版本的验证要么会产生类型错误，要么无法满足性质1。

如果输入到抽象H门的是位向量输入，则会被标记为类型错误，因为H门期望的是布尔输入。如果量子比特 q_j 应接收布尔输入量子比特 b_j ，却输入了 b_k ，那么 q_j 的性质1左侧将为 $\langle .b_k ... \rangle$，右侧将为 $\langle .b_j ... \rangle$。因此，性质1将不成立。

引理 2. 如果量子傅里叶变换电路存在错误，即向R_n 门输入了错误的输入，那么对量子傅里叶变换电路抽象版本的验证要么会产生类型错误，要么无法满足性质*1*。

如果将控制值输入到R_n 门的数据输入端，或将数据值输入到R_n 门的控制输入端，则会产生类型错误。如果 R_n 门作用于量子比特 q_j时，其控制输入应为 b_j ，但实际输入了 b_k，那么 q_j 的性质1左侧将为 $\langle ....b_k ... \rangle$ ，右侧将为 $\langle ....b_j ... \rangle$。因此，性质1将不成立。如果向$R_n$ 门输入了错误的数据值，就会导致某个量子比特上缺少一个R_n 门；这种情况将在下文中讨论。

上面的错误如图 2 所示。输入为 q_1^2 的 R_3 门应将 b_3 作为其控制输入。实际上， b_2 被错误地用作控制输入。

引理 3. 如果量子傅里叶变换电路存在错误，例如某个量子比特缺少 H 门，或有多个 H 门作用于同一个量子比特，那么对该量子傅里叶变换电路的抽象版本进行验证时将产生类型错误。

在量子傅里叶变换电路的抽象版本中，H 门的输入是控制值，输出是数据值。因此，如果有多个 H 门作用于同一个量子比特，第一个 H 门之后的 H 门将接收数据输入，从而导致类型错误。如果没有 H 门作用于某个量子比特，后续的 R_n 门将无法在其数据输入端获得数据值，这同样会导致类型错误。

图 2 展示了一个缺失 H门导致的量子门错误示例。 q_2 上的 H门缺失。

引理 4. 如果量子傅里叶变换电路存在错误，即错误的一组 R_n 量子门作用于某个量子比特上，也就是说，所需的 R_n 量子门缺失，或出现了额外的 R_n 量子门，或两者兼有，那么对量子傅里叶变换电路的抽象版本进行验证将不满足性质*1*。

对于含有 m 个量子比特的量子傅里叶变换电路，量子比特 1 上应作用有 R_2，.....、R_m 。量子比特 2 上应作用有 R_2，.....、R_{m-1} ，依此类推。因此，每个量子比特只需作用一个具有特定 n 值的 R_n 门。如果缺少所需的 R_n 门，那么在性质1中将无法观察到该门对抽象该量子比特的分数位向量值产生的旋转影响。如果某个量子比特上还作用有额外的错误 R_n 门，那么该量子比特所需的旋转将不正确，并反映在该量子比特最终的分数位向量值上。上述两种情况下，性质1均不成立。请注意，一个 R_n 门可以替换为两个控制输入相同的 R_{n-1} 门。例如，R_2 可以替换为两个 R_3 门。如果一系列 R_n 门产生的总旋转影响符合预期，即使其不符合上述 R_n 门序列，性质1仍将成立，因为分数位向量抽象能够准确地捕捉这些旋转。

图 2 展示了一个错误的 R_n 门示例，其中 q_1^1 上的量子门应为 R_2 ，而不是 R_3。

引理5。 如果量子傅里叶变换电路包含引理*1*至*4*所述错误类别中的多种错误，则对量子傅里叶变换电路的抽象版本进行验证将产生类型错误，或不满足性质*1*。

由引理1至4可知，标记每个错误类别的效应是互不相交的，即对于类型错误或性质1而言，这些效应之间不存在重叠。因此，多种错误的组合也会被标记为类型错误，或不满足性质1。

定理1。 （量子傅里叶变换旋转抽象正确性）如果量子傅里叶变换电路存在错误，则对量子傅里叶变换电路的抽象版本进行验证将产生类型错误，或不满足性质*1*。

量子傅里叶变换电路只有两种类型的量子门：H门和 R_n 门。因此，可能的错误只有四类：

H门的输入不正确、R_n 门的输入不正确、电路中缺少或多出 H 门，以及作用于量子比特的一组 R_n 门不正确。错误的量子傅里叶变换电路的第五种情况是上述错误的任意组合。根据引理1-5，我们可以看到，在上述所有情况下，对量子傅里叶变换电路的抽象版本进行验证都会产生类型错误，或者不满足性质1。

VI. 结果与讨论

表 I 给出了验证结果。验证基准测试是通过将量子傅里叶变换电路中的量子比特数量从 16 个变至 10,000 个而生成的。该表还给出了每个量子傅里叶变换基准测试电路中的量子门数量（第 2 列：量子门）。验证实验在配备 32 GB RAM、运行 Ubuntu 64 位操作系统的 Intel(R) Core(TM) i9 - 12900K CPU @ 3.2 GHz 上进行。所有基准测试均使用 z3 版本 4.8.12 SMT 求解器 [27]检查性质1。

表中，“T(s)”表示以秒为单位的验证时间，即 z3 的运行时间。“M(MB)”表示 z3 运行时的内存消耗量，单位为 MB。“正确电路”给出了无错误量子傅里叶变换电路的验证统计结果。对于这些电路，已证明性质1成立。性质1允许独立验证每个量子比特的输出。因此，电路中所有量子比特输出的验证均并行完成，所报告的内存和时间对应于最坏情况。

“错误门错误”是包含量子门错误的电路，具体描述如下。这里的 Gate-2错误表示 R_3 量子门错误地作用于量子比特 1，而不是 R_2。这里的 Gate-n错误表示 R_{n-1} 量子门错误地作用于量子比特 1，而不是 R_n。“错误控制错误”是指 R_n 量子门的控制输入不正确的电路。这里的 Gate-2错误表示量子比特 1 上的 R_2 量子门错误地由量子比特 3 控制，而不是由量子比特 2 控制。这里的 Gate-n错误表示量子比特 1 上的 R_n 量子门错误地由量子比特 n-1 控制，而不是由量子比特 n 控制。对于存在错误的电路，验证性质1会生成一个反例。报告的时间和内存对应于验证第一个导致生成反例的量子比特输出所用的时间和内存。

图3和图4分别绘制了表 I 中的验证时间和内存随量子门数量的变化情况。在这些图中，x 轴和 y 轴均采用对数刻度。从图中可以看出，随着量子门数量增加，对于正确电路和存在错误的电路，内存和验证时间都呈线性增长。最复杂的电路包含 10,000 个量子比特和 5,000 万个量子门，仅需约 37 分钟即可完成验证。这表明我们的方法具有很高的效率和可扩展性。验证存在错误的电路所需的时间少于验证正确电路所需的时间。然而，这种时间并未像形式化验证中常见的情况那样减少一个数量级。

图 5 展示了在含有 10,000 个量子比特的量子傅里叶变换电路中，将量子门错误的位置从量子比特 1 移至量子比特 10,000 时，验证时间和内存的变化。x 轴为线性刻度，y 轴为对数刻度。该图显示了时间和内存随错误垂直位置的变化情况。可以看到，当错误从量子比特 1 移至量子比特 10,000 时，时间和内存均呈指数级下降。

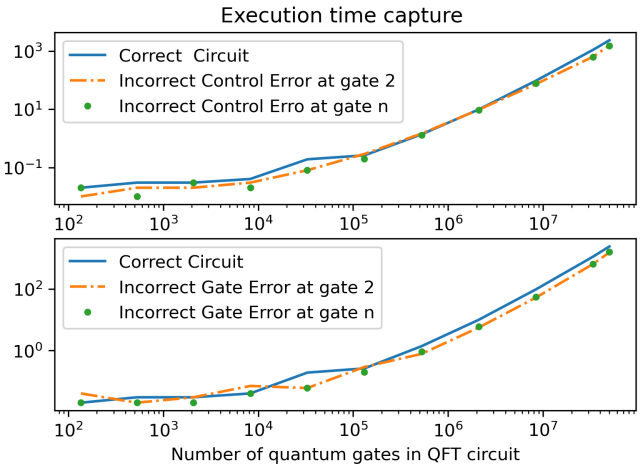


图 3. 量子傅里叶变换验证所需执行时间与量子门数量的关系。图中捕获了正确电路、控制输入错误和数值错误在量子比特位置 2 和 10000 处的情况，以供说明。

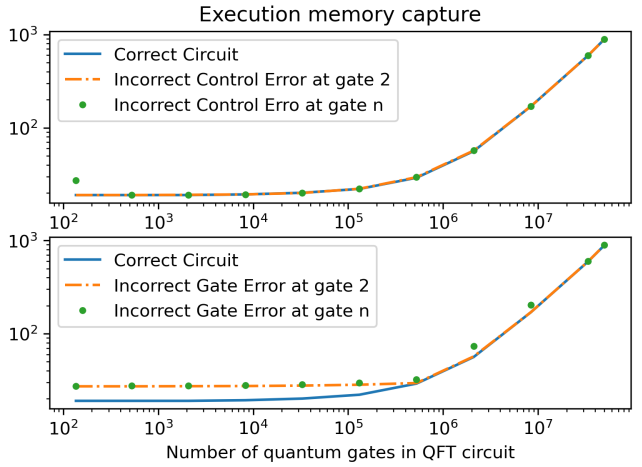


图 4. 量子傅里叶变换验证所需执行内存与量子门数量的关系。图中捕获了正确电路、控制输入错误和数值错误在量子比特位置 2 和 10000 处的情况，以供说明。

VII. 结论与未来工作

我们提出的量子傅里叶变换（QFT）电路验证方法，使迄今为止已验证的量子电路在效率和可扩展性方面取得了飞跃式进展。我们已能在约 37 分钟内验证一个包含 10,000 个量子比特和超过 5,000 万个量子门的量子傅里叶变换电路。我们利用了该方法专用于量子傅里叶变换验证这一特点。这是实现形式化验证可扩展性的一种常见思路。例如，有大量专门用于验证乘法器的形式化验证技术。我们还利用了量子门所执行的旋转均为 2 的负整数次幂这一特点

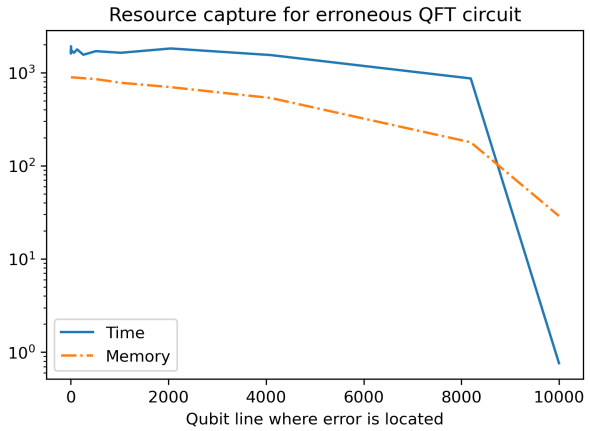


图 5. 错误的量子傅里叶变换电路的资源利用率（时间和内存）随量子比特数量变化的图。

因此可以将其编码为分数位向量，从而将验证义务的范围从希尔伯特空间缩小到布尔空间。未来，我们的目标是将这些思路推广到其他量子算法，以提升形式化验证的效率和可扩展性，从而应对近期量子硬件路线图所规划的规模与复杂性。

参考文献

[1] D. Gottesman 和 I. L. Chuang，“利用量子隐形传态和单量子比特操作展示通用量子计算的可行性”，《自然》，第 402 卷，第 390–393 页，1999 年 11 月。[2] F. A. 等，“利用可编程超导处理器实现量子霸权”，《自然》，第 574 卷，第 505–510 页，2019 年 10 月。[3] G. Jay、F. Ismael 和 W. Karl。（2021 年 2 月）IBM 构建开放量子软件生态系统的路线图。 [在线]。网址：https://research.ibm.com/blog/quantum-development-roadmap [4] K. Krewell 和 T. Research。（2022 年 6 月）新一代 IBM 量子计算机。[在线]。网址：https://www.forbes.com/sites/tiriasresearch/2022/06/22/the-next-generation-of-ibm-quantum-computers/?sh=5083d463266f [5] J. Gambetta。（2022 年 5 月）扩展 IBM 量子路线图，迎接量子中心超级计算的未来。 [在线]。网址：https://research.ibm.com/blog/ibm-quantum-roadmap-2025 [6] 2021， 5 J. Porter。（）Google 希望在 2029年 前造出一台实用的量子计算机。[在线]。网址：https://www.theverge.com/2021/5/19/22443453/google-quantum-computer-2029-decade-commercial-useful-qubits-quantum-tra

[7] J.-S. Park, S. Subramanian, L. Lampert, T. Mladenov, I. Klotchkov, D. J. Kurian, E. Juarez-Hernandez, B. Perez-Esparza, S. R. Kale, K. T. Asma Beevi, S. Premaratne, T. Watson, S. Suzuki, M. Rahman, J. B. Timbadiya, S. Soni, 和 S. Pellerano，“13.1 一种完全集成的低温 CMOS 片上系统，用于控制量子计算机中的量子比特，能够在英特尔 22纳米 FFL FinFET 技术中实现自旋量子比特的量子态操控、读出和高速栅极脉冲”，收录于 2021 IEEE 国际固态电路会议（ISSCC），第 64 卷，2021 年，第 208–210 页。[8] G. Arun 和 V. Mishra，“量子计算与通信综述”，收录于 2014 年第 2 届新兴电子、通信与网络技术趋势国际会议，2014 年，第 1–5 页。[9] S. Jordan。（2021 年，第 2 期）量子算法动物园。 [在线]。网址：https://quantumalgorithmzoo.org [10] M. Lewis、S. Soudjani 和 P. Zuliani，“量子程序的形式化验证：理论、工具与挑战”，CoRR，第 abs/2110 01320，卷。在线。网址：2021 [ ] 2110 https://arxiv.org/abs/ 。 01320 [11] M. Amy，“迈向通用量子电路的大规模功能验证”，《理论计算机科学电子论文集》，第 287 卷，第 1–21 页，2019 年 1 月。[12] M. A. Nielsen 和 I. L. Chuang，《量子计算与量子信息：十周年纪念版》，第 10 版。美国：剑桥大学出版社，2011 年。

[13] E. Sakk，《量子傅里叶算子及其应用》。IntechOpen，2021 年 7 月。[14] P. Rebentrost 和 S. Lloyd，“量子计算金融：用于投资组合优化的量子算法”，2018 年 11 月。[15] P. Rebentrost、B. Gupt 和 T. R. Bromley，“量子计算金融：金融衍生品的蒙特卡洛定价”，Physical Review A，第 98 卷，第 022321 页，2018 年 8 月。[16] Z.-E. Su、Y. Li、P. P. Rohde、H.-L. Huang、X.-L. Wang、L. Li、N.-L. Liu、J. P. Dowling、C.-Y. Lu 和 J.-W. Pan，“量子傅里叶变换电路中的多光子干涉及其在量子计量学中的应用”，Physical Review Letters，第 119 卷，第 080502 页，2017 年 8 月。[17] H. Grimm-Strele 和 M. Kabel，“基于 FFT 的混合均匀边界条件均匀化”，International Journal for Numerical Methods in Engineering，第 122 卷，第 7241–7265 页，2021 年 12 月。[18] A. Geng、A. Moghiseh、C. Redenbach 和 K. Schladitz，“超导处理器上改进的 FRQI 及其在 NISQ 时代的局限性”，2021 年 10 月。[19] S. Woerner 和 D. J. Egger，“量子风险分析”，npj Quantum Information，第 5 卷，第 15 页，2019 年 12 月。[20] A. Barenco、C. H. Bennett、R. Cleve、D. P. DiVincenzo、N. Margolus、P. Shor、T. Sleator、J. A. Smolin 和 H. Weinfurter，“量子计算的基本门”，Phys. Rev. A，第 52 卷，第 3457–3467 页，1995 年 11 月。 [在线]。网址：https://link.aps.org/doi/10.1103/PhysRevA. 52.3457 [21] R. Muradian。（2011 年，第 3 期）量子傅里叶变换电路。[在线]。网址：https://demonstrations.wolfram.com/ QuantumFourierTransformCircuit [22] S. Yamashita 和 I. L. Markov，“量子电路的快速等价性检查”，2009 [ ] 0909 4119 。在线。网址：[23] https://arxiv.org/abs/ 。G. F. Viamontes、I. L. Markov 和 J. P. Hayes，“量子电路与量子态的等价性检查”，2007 年。 [在线]。网址：https://arxiv.org/abs/0705 0017 。J. Liu、B. Zhan、S. Wang、S. Ying、T. Liu、Y. [24] Li、M. Ying 和 N. Zhan，“使用量子霍尔逻辑对量子算法进行形式化验证”，收录于 Computer Aided Verification，I. Dillig 和 S. Tasiran 编。Cham：Springer International Publishing，2019 年，第 187–207 页。[25] Y. Feng、N. Yu 和 M. Ying，“量子马尔可夫链模型检测”，Journal of Computer and System Sciences，第 79 卷，第 7 期，第 1181–1198 页，2013 年。 [在线]。网址：https://www.sciencedirect.com/science/article/pii/S0022000013000780 [26] F. X. Lin，“Shor 算法与量子傅里叶变换”，麦吉尔大学，2014 年。[27] L. De Moura 和 N. Bjørner，“Z3：一种高效的 SMT 求解器”，收录于 Theory and Practice of Software，第 14 届 International Conference on Tools and Algorithms for the Construction and Analysis of Systems 论文集，丛书 TACAS’08/ETAPS’08。柏林、海德堡：Springer-Verlag，2008 年，第 337–340 页。

nsistor