

无损量子计算通过减少量子比特开销以实现高效的算术运算

Omid Faizy^{1,2,3,4}, Norbert Wehn³, Paul Lukowicz^{4,5}, and Maximilian Kiefer-Emmanouilidis^{4,5}

¹ Laboratoire de Chimie de la Matière Condensée de Paris, UMR CNRS 7574, Sorbonne Université, 4, place Jussieu, 75252 Paris, France.

² Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville, Université du Littoral Côte d'Opale, 50 rue Ferdinand Buisson, CS 80699, 62228 Calais, France.

³ Microelectronic Systems Design (EMS), RPTU Kaiserslautern-Landau, Germany

⁴ Department of Computer Science and Research Initiative QC-AI, RPTU Kaiserslautern-Landau, Kaiserslautern, Germany.

⁵ German Research Center for Artificial Intelligence (DFKI), Kaiserslautern, Germany.

摘要 量子算术计算需要大量的暂存量子位以保持可逆性。这些操作所需的量子位和门资源等同于输入或输出寄存器中较大的那个,这是由于状态编码造成的。量子哈密顿计算(QHC)通过在单个旋转量子门内对逻辑运算的输入进行编码而引入了一种新方法。这一创新将所需量子位寄存器 N 减少到输出状态 O 的大小,其中 $N = \log_2 O$ 。利用 QHC 原理,我们展示了可逆半加法和全加法器电路,这些电路压缩了标准 Toffoli+CNOT 布局 [Vedral 等人,《物理评论 A》, 54, 11, (1996)] 从量子半加法器电路的三量子位和四量子位格式以及使用五个量子位的五级 Fredkin 门 [Moutinho 等人,《PRX 能源》2, 033002 (2023)] 全加法器电路;将其压缩到两量子位, 4×4 希尔伯特空间。这里呈现的方案针对在量子硬件上评估的经典逻辑进行了优化,由于么正演化可以一定程度上绕过经典 CMOS 能限。虽然我们在本文中避免了输入和输出状态的叠加,但这原则上仍然是可行的。我们看到 QHC 的最佳应用是在寻找评估任何真值表所需的最小量子位和门资源方面,利用集成量子电路或光子学推进 FPGA 能力。

Keywords: 量子算术 · 量子哈密顿计算 · 加法器。

1 介绍

最小且最高效的算术运算符问题正接近原子极限。每晶体管少于数百个原子时,泄漏和能量耗散至少为每比特 $kT \ln 2$, 变得难以接受 [1–3]。可逆量子逻辑可以在一定程度上绕过这些限制 [2–4]。遵循这一原则,早期的量子加法器 [4, 5] 使用 Toffoli 和 CNOT 门实现了二进制加法,但需要额外的辅助量子比特以实现可逆性和状态嵌入。在这篇手稿中,我们将任何不需要用于编码输出的量子比特视为辅助量子比特。这使我们的方法区别于其他无需辅助量子比特的方法,在转译为通用门时不需要任何额外量子比特,如三量子比特半加器和四量子比特全加器。在这里,输入嵌入所需的量子比特不被视为辅助量子比特。为

了强调这一区别，我们将用于嵌入的量子比特称为临时量子比特或临时寄存器，作为一种形式上的辅助量子比特。

例如，标准的可逆半加器和全加器电路 [6] 分别需要三个和四个量子比特来生成求和输出和进位输出而不擦除输入。即使输入是经典的，使得输入和输出都是乘积态，因此是可分离态，这一点仍然成立。这种“临时”量子比特开销不仅增加了希尔伯特空间的维度（对于三个量子比特为 8 维，对于四个量子比特为 16 维），而且还添加了大量门来取消中间结果，使实际实现变得更加复杂。最近的设计减少了 T 计数或辅助计数——有时减少到一甚至零 [7–9]，其中额外的辅助指的是半加器输入嵌入之外和全加器四个量子比特所需的必要量子比特。

量子哈密顿计算 (QHC) 将布尔输入编码在哈密顿矩阵元素中，而不是基态种群中，从而最小化逻辑门的状态计数 [10–13]。之前在单分子平台上的 QHC 研究实现了不需要量子比特并依赖内在不可逆动力学的四状态半加器和八状态全加器；后来的研究引入了多能量读出方案以进一步压缩有效哈密顿量 [12, 13]。

理论研究表明，可以通过使用双硝基功能化的纳米石墨烯分子并由石墨烯电极桥接的 QHC 电路将经典数据编码为旋转角度，其中硝基团的旋转作为二进制输入共同实现半加器布尔操作 [14]。将这些想法适应于量子计算就是要找到一个依赖于二进制输入制定给定真值表所需逻辑输出的幺正矩阵 $U(\vec{\theta}) = \exp(-iH(\vec{\theta})t)$ ，针对给定输入 $\vec{\theta}$ 。从这个角度来看，我们认为可以制定一种量子表示（以量子门的形式），仅使用 $N = \log_2(O)$ 个量子比特就能得到给定输出（遵循相应的真值表），其中 O 是可能输出的数量。

使用 QHC 范式，我们展示了仅用两个量子比特构建的可逆半加器和全加器电路。这与传统设计相比，在所需资源方面有显著减少。我们的半加器和全加器都在 4×4 希尔伯特空间（两个量子比特）内运行，而不是以前方法所需的 8×8 （三个量子比特），或 16×16 （四个量子比特）或更大的空间。目前，这些电路仅限于经典的布尔输入，无法处理输入的量子叠加态。

2 电路设计

如图 1(a) 所示，该设备使用两个制备在 $|\psi(t=0)\rangle = |00\rangle$ 态的量子比特。一个 4×4 单位矩阵 $U(\alpha, \beta)$ 将动态限制在一个受保护的子流形内，并将角度 $(\alpha, \beta) \in \{0, 1\}^2$ 编码为逻辑输入。 $U(\alpha, \beta)$ 过滤并映射结果振幅到最终量子比特上，然后在计算基中测量这些量子比特以获得 SUM（异或）和 CARRY（与）输出。

$$U(\alpha, \beta) = \begin{pmatrix} A & B - F & B + F & 0 \\ B + F & A & B - F & 0 \\ B - F & B + F & A & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad (1)$$

其中

$$\begin{aligned} A &= \frac{1}{3} \left(2 \cos \left(\frac{2}{3} \pi (\alpha + \beta) \right) + 1 \right), \\ B &= \frac{1}{3} \left(1 - \cos \left(\frac{2}{3} \pi (\alpha + \beta) \right) \right), \\ F &= \frac{\sin \left(\frac{2}{3} \pi (\alpha + \beta) \right)}{\sqrt{3}}. \end{aligned} \quad (2)$$

对应的半加器哈密顿量是

$$H_{\text{ha}}(\alpha, \beta) = \frac{2i\pi(\alpha + \beta)}{3\sqrt{3}} h_{\text{ha}} = \frac{2i\pi(\alpha + \beta)}{3\sqrt{3}} \begin{pmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (3)$$

该哈密顿量的时演化 $U(\alpha, \beta) = \exp(-ih_{\text{ha}} t_{\text{eff}}(\alpha, \beta))$ 表明, 可以在由 $t_{\text{eff}}(\alpha, \beta) = \frac{2i\pi(\alpha + \beta)}{3\sqrt{3}}$ 给出的时间点上提取出半加器的解。在整个工作中, 我们采用约化普朗克常数为 $\hbar = 1$ 的单位系统。

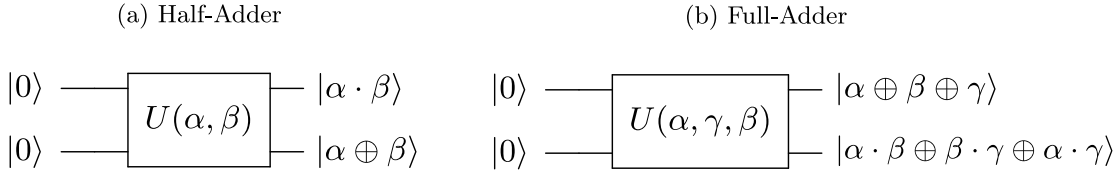


图 1: (a) 具有经典二进制输入 α 和 β 的两量子比特 QHC-半加器电路直接在电路内部实现。
(b) 具有经典二进制输入 α 、 γ 和 β 的两量子比特 QHC-全加器电路直接在电路内部实现。

给定初始状态 $|00\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}^T$ 我们可以完成半加器的真值表和响应如下:

$$\begin{aligned} U(0, 0) |00\rangle &= |00\rangle \\ U(0, 1) |00\rangle &= |01\rangle \\ U(1, 0) |00\rangle &= |01\rangle \\ U(1, 1) |00\rangle &= |10\rangle \end{aligned} \quad (4)$$

我们现在可以将图 1(b) 中所示的全加器协议进行一般化。再次, 该设备使用两个处于 $|\psi(t=0)\rangle = |00\rangle$ 态的量子比特。一个 4×4 幺正矩阵 $U(\alpha, \gamma, \beta)$ 将动力学限制在一个受保护的子流形内, 并编码角度 $(\alpha, \gamma, \beta) \in \{0, 1\}^2$ 作为逻辑输入。矩阵 $U(\alpha, \gamma, \beta)$ 过滤并将结果

振幅映射到最终的量子比特上，然后在计算基中测量这些量子比特以得到 SUM（异或）和 CARRY 输出。

相应的矩阵具有以下形式：

$$U(\alpha, \gamma, \beta) = \frac{1}{4} \begin{pmatrix} l+2m+1 & -2n-p-iq+1 & l-2m+1 & 2n-p-iq+1 \\ 2n-p-iq+1 & l+2m+1 & -2n-p-iq+1 & l-2m+1 \\ l-2m+1 & 2n-p-iq+1 & l+2m+1 & -2n-p-iq+1 \\ -2n-p-iq+1 & l-2m+1 & 2n-p-iq+1 & l+2m+1 \end{pmatrix}, \quad (5)$$

其中

$$\begin{aligned} l &= e^{i\pi(\alpha+\beta+\gamma)}, \\ m &= \cos\left(\frac{1}{2}\pi(\alpha+\beta+\gamma)\right), \\ n &= \sin\left(\frac{1}{2}\pi(\alpha+\beta+\gamma)\right), \\ p &= \cos(\pi(\alpha+\beta+\gamma)), \\ q &= \sin(\pi(\alpha+\beta+\gamma)). \end{aligned} \quad (6)$$

参见第 4 节附录以获得方程 (5) 的推导步骤。

相应的全加器哈密顿量为

$$H_{fa} = \frac{1}{4}\pi(\alpha+\beta+\gamma)h_{fa} = \frac{1}{4}\pi(\alpha+\beta+\gamma) \begin{pmatrix} -1 & 1-i & -1 & 1+i \\ 1+i & -1 & 1-i & -1 \\ -1 & 1+i & -1 & 1-i \\ 1-i & -1 & 1+i & -1 \end{pmatrix}. \quad (7)$$

该哈密顿量的随时间演化 $U(\alpha, \beta) = \exp(-ih_{fa}t_{\text{eff}}(\alpha, \beta, \gamma))$ 表明，在 $t_{\text{eff}}(\alpha, \beta, \gamma) = \frac{1}{4}\pi(\alpha + \beta + \gamma)$ 给定的时间点可以提取出全加器的解。

应用全加器门我们得到相应的真值表

$$\begin{aligned} U(0, 0, 0) |00\rangle &= |00\rangle & U(0, 0, 1) |00\rangle &= |01\rangle \\ U(0, 1, 0) |00\rangle &= |01\rangle & U(0, 1, 1) |00\rangle &= |10\rangle \\ U(1, 0, 0) |00\rangle &= |01\rangle & U(1, 0, 1) |00\rangle &= |10\rangle \\ U(1, 1, 0) |00\rangle &= |10\rangle & U(1, 1, 1) |00\rangle &= |11\rangle. \end{aligned} \quad (8)$$

3 结论

在本研究中，我们介绍了量子哈密顿计算作为执行量子算术运算的方法，该方法通过将经典输入编码在一个量子门内减少了量子比特的负担。我们的两量子比特半加器和全加器电路在 $4\mathbb{E}4$ 希尔伯特空间中需要比传统教科书上的可逆设计（由 Toffoli 门加上清理门构成）更少的资源 [4, 5, 15, 16]。利用幺正演化使我们能够绕过经典 CMOS 的能量限制，并以更少的量子比特和门实现可逆逻辑，其中量子比特的数量仅与可能的输出状态呈对数依赖关系。此外，QHC 幺正可以在一个模拟脉冲中实现完整的真值表，只要该门可以在相应的量子硬件上实施。虽然当前的设计目标是经典逻辑而没有利用输入和输出态的叠加，但应该清楚的是，在原则上这是可能的，并且可以简单地将输入从二进制转换为实数值来实现这一点。然而，找到的幺正并不是完全表达式的，只能映射希尔伯特空间中的一个子流形。消除这种限制会导致再次需要擦除量子比特，因此对之前的实施没有好处 [4]。然而，可以优化该子流形以评估电路中预期最突出的叠加态，而无需引入额外的量子比特。

QHC 框架通过利用量子架构来最小化能耗，有望推动 FPGA 设计的进步。这种方法在量子电路、集成量子光子学和其他新兴技术中具有潜在应用，特别是在集成量子光子设备的操作速度可以超过经典计算机 [17] 的情况下。

致谢

我们感谢研究计划“量子计算用于人工智能”（QC-AI）的支持。

4 附录：全加器幺正矩阵 $U(\alpha, \gamma, \beta)$ 的构造

令两个量子比特的计算基按如下顺序排列： $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ 。我们可以固定列向量（即控制或特征向量）为：

$$V = |00\rangle, \quad (\text{A.1})$$

以及三个实参数 $\alpha, \gamma, \beta \in \mathbb{R}$ 。任务是构建一个 4×4 幺正矩阵 $U(\alpha, \gamma, \beta)$ ，使得当每个参数被限制在布尔集 $\{0, 1\}$ 中时，八个输入三元组映射为

(α, γ, β)	$U(\alpha, \gamma, \beta) V$
$(0, 0, 0)$	$ 00\rangle$
$(0, 0, 1)$	$ 01\rangle$
$(0, 1, 0)$	$ 01\rangle$
$(0, 1, 1)$	$ 10\rangle$
$(1, 0, 0)$	$ 01\rangle$
$(1, 0, 1)$	$ 10\rangle$
$(1, 1, 0)$	$ 10\rangle$
$(1, 1, 1)$	$ 11\rangle$

我们现在定义一个 4-循环置换矩阵 $\mathcal{R}$ 作为

$$\mathcal{R} = |01\rangle\langle 00| + |10\rangle\langle 01| + |11\rangle\langle 10| + |00\rangle\langle 11|. \quad (\text{A.2})$$

方程 (A.2) 循环排列基底 $|00\rangle \rightarrow |01\rangle \rightarrow |10\rangle \rightarrow |11\rangle \rightarrow |00\rangle$; 因此 $\mathcal{R}^4 = I_4$ 。写成矩阵形式,

$$\mathcal{R} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \mathcal{R}^\dagger \mathcal{R} = I_4.$$

因为 $\mathcal{R}$ 是么正的, 主矩阵对数

$$\mathcal{R} = e^{-iH}, \quad H = i \log \mathcal{R}, \quad H^\dagger = H, \quad (\text{A.3})$$

是 Hermitian 的。($\mathcal{R}$ 的本征值是单位 $\{1, i, -1, -i\}$ 的四次根。)

三参数族可以定义为

$$U(\alpha, \gamma, \beta) = \exp[-i(\alpha + \gamma + \beta)H] \quad (\text{A.4})$$

一些代数运算导出了方程 (5)。

参考文献

1. R. Landauer, “Irreversibility and heat generation in the computing process,” *IBM Journal of Research and Development*, vol. 5, no. 3, pp. 183–191, 1961.
2. C. H. Bennett, “Logical reversibility of computation,” *IBM journal of Research and Development*, vol. 17, no. 6, pp. 525–532, 1973.
3. G. Chiribella, Y. Yang, and R. Renner, “Fundamental energy requirement of reversible quantum operations,” *Phys. Rev. X*, vol. 11, p. 021014, Apr 2021.
4. V. Vedral, A. Barenco, and A. Ekert, “Quantum networks for elementary arithmetic operations,” *Physical Review A*, vol. 54, no. 1, p. 147, 1996.
5. S. A. Cuccaro, T. G. Draper, S. A. Kutin, and D. P. Moulton, “A new quantum ripple-carry addition circuit,” *arXiv preprint quant-ph/0410184*, 2004.
6. J. a. P. Moutinho, M. Pezzutto, S. S. Pratapsi, F. F. da Silva, S. De Franceschi, S. Bose, A. T. Costa, and Y. Omar, “Quantum dynamics for energetic advantage in a charge-based classical full adder,” *PRX Energy*, vol. 2, p. 033002, Jul 2023.
7. C. Gidney, “Halving the cost of quantum addition,” *Quantum*, vol. 2, p. 74, 2018.
8. M. Remaud and V. Vandaele, “Ancilla-free quantum adder with sublinear depth,” in *Reversible Computation* (R. Glück and R. Kaarsgaard, eds.), (Cham), pp. 137–154, Springer Nature Switzerland, 2025.

9. M. Remaud, “Optimizing t and cnot gates in quantum ripple-carry adders and comparators,” in *Proceedings of Recent Advances in Quantum Computing and Technology*, ReAQCT ’24, (New York, NY, USA), p. 56 – 61, Association for Computing Machinery, 2024.
10. G. Dridi, R. Julien, M. Hliwa, and C. Joachim, “The mathematics of a quantum hamiltonian computing half adder boolean logic gate,” *Nanotechnology*, vol. 26, p. 344003, aug 2015.
11. F. Ample, O. Faizy, H. Kawai, and C. Joachim, “The design of a surface atomic scale logic gate with molecular latch inputs,” in *On-Surface Atomic Wires and Logic Gates* (M. Kolmer and C. Joachim, eds.), (Cham), pp. 139–155, Springer International Publishing, 2017.
12. G. Dridi, O. F. Namarvar, and C. Joachim, “Qubits and quantum hamiltonian computing performances for operating a digital boolean 1/2-adder,” *Quantum Science and Technology*, vol. 3, no. 2, p. 025005, 2018.
13. O. F. Namarvar, O. Giraud, B. Georgeot, and C. Joachim, “Quantum hamiltonian computing protocols for molecular electronics boolean logic gates,” *Quantum Science and Technology*, vol. 4, no. 3, p. 035009, 2019.
14. S. Srivastava, H. Kino, and C. Joachim, “Quantum half-adder boolean logic gate with a nano-graphene molecule and graphene nano-electrodes,” *Chemical Physics Letters*, vol. 667, pp. 301–306, 2017.
15. M. Amy, D. Maslov, M. Mosca, and M. Roetteler, “A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 32, no. 6, pp. 818–830, 2013.
16. P. Selinger, “Quantum circuits of t -depth one,” *Phys. Rev. A*, vol. 87, p. 042302, Apr 2013.
17. L. Labonté, O. Alibart, V. D’Auria, F. Dautre, J. Etesse, G. Sauder, A. Martin, E. Picholle, and S. Tanzilli, “Integrated photonics for quantum communications and metrology,” *PRX Quantum*, vol. 5, p. 010101, Feb 2024.