arXiv:2601.02435v1 [quant-ph] 5 Jan 2026

Grover 算法的形式化建模与验证

HONGXIA SUN [a]、ZHIPING SHI [b]、SHANYAN CHEN [c]、GUOHUI WANG [a]、XIMENG LI [b]、YONG GUAN [d]、QIANYING ZHANG [a] 和 ZHENZHOU SHAO [a]

[a]首都师范大学信息工程学院，北京电子邮件地址：hxsun@cnu.edu.cn；ghwang@cnu.edu.cn；qyzhang@cnu.edu.cn；zshao@cnu.edu.cn

[b]首都师范大学北京电子系统可靠性技术重点实验室，北京电子邮件地址：shizp@cnu.edu.cn；lixm@cnu.edu.cn

[c]首都师范大学数学科学学院，北京电子邮件地址：sychen@cnu.edu.cn

[d]首都师范大学电子系统可靠性与数学交叉国际科技合作基地，北京电子邮件地址：guanyong@cnu.edu.cn

摘要。Grover 算法利用量子力学中的叠加和干涉，在搜索无序数据库等特定任务中比经典计算更高效。由于量子力学复杂度很高，难以通过传统模拟方法保证量子算法的正确性。相比之下，Grover 算法的基本概念和数学结构可以形式化为逻辑表达式，并通过高阶逻辑推理进行验证。本文在 HOL Light 定理证明器中对 Grover 算法进行形式化建模与验证。我们重点证明其预言机和扩散算子的幺正性、成功概率随迭代次数变化的单调性，以及最优迭代次数的精确表达式。通过分析整数分解中的一个具体应用，我们展示了这项工作的实用性和发展前景。

引言

量子计算作为一种变革性范式，在特定问题上展现出远超经典计算的处理能力 [MJB+17, ZWC+20, PAB+23]。以 Grover 算法为代表的量子搜索技术，是量子计算领域的一项里程碑 [JZCM22, CLCH20]，，它将无序数据库搜索的时间复杂度从经典的 $O(N)$ 降至 $O(\sqrt{N})$ [Gro96]。凭借这种优越的复杂度，Grover 算法具有重要的理论意义。此外，它

关键词和短语：Grover 算法、定理证明器、量子算法、形式化验证。SUN 和 SHI 为共同第一作者，贡献相同。WANG 为通讯作者。

© H.Sun,Z.Shi,S.Chen,G.Wang,X.Li,Y.Guan,Q.Zhang,andZ.Shao 知识共享

在组合优化 [ZWL+24, LQW+25]、密码分析 [SJK+22, YHK+23]和数据库检索 [SW24,AB20]等多个实际领域也展现出广阔的应用前景。

然而，随着量子算法逐渐走向工程化实现，如何确保其正确性已成为制约量子计算可靠性与发展的主要瓶颈 [LSZ23]。叠加、测量坍缩和概率性输出等量子固有特性，使传统测试方法难以覆盖所有可能的执行路径 [CLV+23]。与此同时，手动进行数学推导和验证的方法缺乏可扩展性，且极易出错 [RH20]。

在此背景下，基于高阶逻辑定理证明器的形式化验证方法展现出独特价值。这种方法能够在严格的数学公理框架内，以机器辅助且完全可靠的方式验证算法性质与功能。通过严谨的数学推理，形式化验证能够从算法设计层面根本性地识别并消除系统漏洞和安全风险 [HT15], ，从而为量子算法的正确性提供可靠保障。近年来，许多研究人员利用定理证明工具，在量子计算领域取得了显著进展。Liu 等人 [LZW+19] 在 Isabelle/HOL 中形式化了量子程序的语法和语义，写出了量子霍尔逻辑的规则，并验证了量子程序部分正确性演绎系统的可靠性和完备性。Lin 等人 [LWC+24]提出了一种利用纠缠和量子隐形传态的并行分布式量子 SAT 求解器。通过引入辅助纠缠量子比特，他们将每次 Grover 迭代的时间复杂度从 $O(N)$ 降至$O(1)$。Bordg 等人 [BLH21] 在 Isabelle/HOL 中对多种量子算法进行了形式化验证，包括量子隐形传态和 Deutsch 算法。Hietala 等人 [HRH+21]独立地使用 SQIR 语言验证了量子相位估计算法。Shi 等人 [SCD+21]使用 Coq 对 Deutsch-Jozsa 算法和量子隐形传态进行了符号验证。这些成果证明了形式化验证在量子算法中的适用性，并为本文对 Grover 算法进行形式化验证提供了重要参考和实践基础。

此外，Chareton 等人 [CBB21]提出了 QBRICKS 验证框架，该框架采用参数化路径和电路描述，以函数式编程风格有效地表示量子电路。然而，这种表示是无测量的。另一方面，Shi 等人 [SCD24]在 Coq 中形式化了一种经典量子混合语言，并验证了 Grover 算法的最终态正确性。不过，他们的工作仅限于双量子比特情形，未涉及最优迭代次数的推导，也未分析成功概率（即找到正确解的概率）分布与迭代次数之间的关系。

克服了测量语义和验证规模方面的上述局限后，我们的工作得以对 Grover 算法进行更深入、更全面的形式化验证。本文在 HOL Light[1],中，从量子态和算子的代数定义出发，对 Grover 算法的每个步骤进行了形式化验证。我们通过归纳证明，证明了该算法对任意数量的量子比特均正确。此外，本文还通过整数分解案例研究，展示了 Grover 算法的实际应用价值。我们的主要贡献包括

[1]代码可在 https://github.com/shx-02/Grover-algorithm 获取

- 为 Grover 算法构建完整的形式化模型，其中包含对其量子态、预言机和扩散算子的形式化定义。
- 验证关键算法性质，包括成功概率的单调性以及最优迭代次数公式。

- 通过将该框架应用于整数分解，展示其实际可行性。

论文结构。 第 1 节对 Grover 算法的基础理论进行形式化。第 2 节构建从初始量子态到最终测量的量子演化形式模型。第 3 节介绍核心性质的验证，例如最优迭代次数。第 4 节通过一个整数分解简要案例进行说明。最后，我们在第 5 节总结全文。

1. 基础理论的形式化

Grover 算法的数学描述基于线性代数和量子力学原理。本节系统回顾所需理论，为后续的形式化验证和深入应用奠定坚实基础。

1.1. 线性代数。 量子力学的数学框架建立在复向量空间之上。该空间中的向量（量子态）采用狄拉克符号表示：右矢 $|\varphi\rangle$ 表示一个列向量，左矢 $\langle\varphi|$ 表示其对偶向量（共轭转置）。该复向量空间上的内积 V 是一个映射

$$\langle\cdot|\cdot\rangle : V \times V \to \mathbb{C} \tag{1.1}$$

它必须满足共轭对称性、线性和正定性。

复矩阵是复向量空间上的线性变换。其中，具有特定结构和性质的矩阵，例如单位矩阵和对角矩阵，可以显著简化量子门的酉性的验证。表 1 展示了这两类矩阵的关键性质。

表 1：矩阵的关键性质

性质	公式	伪代码
自伴性	$I = I^\dagger$	id_复矩阵 = 厄米_矩阵 id _复矩阵
对角性	$I = diag(1, \cdots, 1)$	对角_复矩阵单位元_复矩阵
左乘性的单位元	$IA = A, \quad Iq = q$	单位元_复矩阵 ** A = A, id_复矩阵 ** q =q
右乘单位元	$AI = A$	A ** id_复矩阵 = A
对称性	$D = D^T$	对角_复矩阵 A ⟹A = ctransp A
对角矩阵乘法	$A = \text{diag}(a_1, \ldots, a_n) \ \wedge B = \text{对角矩阵}(b_1, \ldots, b_n) \implies AB = \text{diag}(a_1 b_1, \ldots, a_n b_n)$	对角_复矩阵 A ∧ 对角_复矩阵 B ⟹A ** B = λij. $A_{ij}B_{ij}$

定义 1.1。 厄米共轭

复矩阵 A 的共轭转置运算称为厄米共轭，记作 $A^\dagger$，即 $A^\dagger = (A^*)^T$。

设厄米_矩阵 =新_定义
‘（厄米_矩阵：$\mathbb{C}^{2^N \times 2^M} \to \mathbb{C}^{2^M \times 2^N}$）A=λij.cnj(A$_{ji}$)‘

此处， A^* 表示 A中各元素的复共轭。

该运算是定义酉矩阵的基础，也是验证量子态演化合法性的关键。接下来，我们使用厄米共轭来定义酉矩阵。

定义 1.2. 酉矩阵

酉矩阵是一个复方阵，其共轭转置恰好是它的逆矩阵，如方程 1.2 所示。

$$U^\dagger U = UU^\dagger = I \tag{1.2}$$

令酉_矩阵 =新_定义
‘酉_矩阵(U:$\mathbb{C}^{2^N \times 2^N}$) $\iff$
厄米_矩阵 U ** U = id_复矩阵 ∧ U ** 厄米_矩阵 U = id_复矩阵‘

为便于验证状态演化过程中的概率守恒，我们进一步推导出，酉矩阵的列（或行）向量彼此正交且已归一化。

定理 1.3. 酉矩阵的正交性与归一化

若 U是酉矩阵，则其列向量 u_1， u_2，……， u_n满足以下性质：（i）归一化：若 $i = j$，则 $u_i^\dagger u_j = 1$；（ii）正交性：若 $i \neq j$，则$u_i^\dagger u_j = 0$。使用克罗内克δ函数 δ 表示的相应表达式见公式1.3。

$$\sum_{i=1}^{n} U_{ix}\overline{U_{iy}} = \delta_{xy} = \begin{cases} 1, & \text{if } x = y, \\ 0, & \text{otherwise.} \end{cases} \tag{1.3}$$

∀A:$\mathbb{C}^{2^N \times 2^N}$. 酉_矩阵 A $\implies$(∀x y. 1 ≤x ∧x ≤2^N∧ 1 ≤y ∧y ≤2^N) $\implies$vsum(1..2^N)
(λi. A$_{ix}$ * cnj(A$_{iy}$)) = 若 x = y，则 Cx(&1)，否则 Cx(&0))

这里，vsum 用于对向量的元素求和，对应于公式1.3中的 Σ 。Cx(&1) 表示将实数 1 转换为复数。

定理1.4. 酉矩阵乘法封闭性

两个酉矩阵的乘积也是酉矩阵。

∀A B:$\mathbb{C}^{2^N \times 2^N}$. 酉矩阵_矩阵 A ∧酉矩阵_矩阵 B $\implies$ 酉矩阵_矩阵 (A ** B)

张量积是一种将向量空间组合在一起以形成更大空间的方法。在量子计算中，我们经常需要计算多个单量子比特量子门（即二维酉矩阵）的张量积，以构造多量子比特门。因此，本文正式定义了一个函数，用于计算任意数量的二维矩阵的张量积。

定义 1.5. 矩阵张量积

设 A_1，A_2，……，A_k为 2×2复矩阵。它们的张量积 $A_1\otimes A_2\otimes\cdots\otimes A_k$是由以下方式定义的 $2^k\times 2^k$ 矩阵：

$$(A_1\otimes\cdots\otimes A_k)_{ij}=\prod_{l=0}^{k-1}(A_{k-l})_{p_l,q_l}$$

其中，对于 $l=0,\ldots,k-1$：

$$p_l=\left\lfloor\frac{i-1}{2^l}\right\rfloor \bmod 2+1,\quad q_l=\left\lfloor\frac{j-1}{2^l}\right\rfloor \bmod 2+1$$

其中，$\lfloor x\rfloor$ 表示下取整函数，而 $(A_{k-l})_{p_lq_l}$ 表示矩阵 A_{k-l}中第 p_l行、第 q_l列的元素。

令张量 _n2 = 新_定义
‘∀m:(ℂ^(2×2)) 列表。tensor_n2 m = λi j。cproduct (0.. LENGTH m - 1) (λk. EL k (REVERSE m)(⌊(i−1)/2^k⌋模 2+1)(⌊(j−1)/2^k⌋模 2+1))‘

定义 1.6. 矩阵列表生成器

长度为 n 的矩阵列表是一个有限序列 $(A_0,\ A_1,\ \ldots\ldots,\ A_{n-1})$，其中每个 A_i 都是一个复矩阵。
let 复矩阵_列表 = 新_定义
‘∀n:ℕ f:ℕ → ℂ^(2×2). (复矩阵_列表 f n):(ℂ^(2×2)) 列表 = MAP f (list_of_seq (λk. k) n)‘
这支持生成由任意组合的 2×2 个矩阵组成的列表，其中 f 是矩阵生成函数，n 是矩阵的数量。

1.2. **量子力学基础**。 量子力学的四大基石——状态、量子门、演化和测量——共同构成了量子计算的形式语言。量子态编码信息，量子门实现信息的酉变换，酉演化确保概率守恒，而测量则实现从量子信息到经典信息的转换。下面将依次考察各个组成部分，以建立一套精简且可运行的基本规则。

在量子力学中，纯态必须满足归一化条件。因此，我们引入一般谓词 is_qstate，用于断言复向量的平方范数为 1，并以此谓词定义一种新的量子态类型。

定义 1.7. 量子态

An n量子比特纯态是一个 2^n 维复向量 $|\varphi\rangle$，满足 $\langle\varphi|\varphi\rangle=$ 1.
let is_量子态 = new_definition ‘is_qstate (q:ℂ^M) ⇔
cnorm2 q = &1‘ let 量子态_tybij = prove let th =
prove (‘∃q:ℂ^(2^N). is_量子态 q‘) in new_type_definition "
量子态" ("mk_qstate","dest_qstate") th

此处，cnorm2 表示复向量 $\|\cdot\|^2$ 的平方范数。函数 mk_qstate 将复向量映射为量子态，而 dest_qstate 则从量子态中提取原始复向量。

量子系统的演化通过量子门所描述的线性变换来实现。根据作用的量子比特数量，量子门可分为单量子比特门和多量子比特门。在各种单量子比特门中，Hadamard 门（哈达玛门）具有基础性作用，是实现量子并行性和量子干涉现象的关键组成部分。其定义和酉性验证如下。

定义 1.8. Hadamard 门

单量子比特 Hadamard 门是一个 2×2 酉矩阵，表示为：

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

```
令 hadamard = new_definition
  ‘哈达玛: ℂ^(2×2) = λi j.
     若 i = 1 ∧ j = 1 ，则 Cx(&1 / sqrt(&2))；否则，若 i = 1 ∧ j
      = 2 ，则 Cx(&1 / sqrt(&2))；否则，若 i = 2 ∧ j = 1 ，则 Cx(&
     1 / sqrt(&2))；否则，若 i = 2 ∧ j = 2 ，则 –Cx(&1 / sqrt(&2));
     否则 Cx(&0)‘
```

定理 1.9. *Hadamard* 门的幺正性

Hadamard 门是酉的。

```
酉_矩阵 Hadamard
```

定义 1.10. 态演化

封闭量子系统的演化由酉矩阵 U 描述。系统在初始时刻的状态记为 $|\varphi\rangle$，演化后的状态记为$|\varphi'\rangle$，二者之间的关系为 $|\varphi'\rangle = U|\varphi\rangle$。

```
令 复矩阵_量子态_乘 = 新_定义 ‘∀q:(N)状态 A:ℂ^(2^N×2^M). A ** q  =mk_量子态 (λi.
vsum (1..2^N) (λj. A_ij * (dest_量子态 q)_j))‘
```

定理 1.11. 概率守恒

设 $|\psi\rangle$ 是满足 $\langle\psi|\psi\rangle = 1$的归一化量子态，且 U 是酉矩阵。那么，演化态 $|\psi'\rangle = U|\psi\rangle$ 满足 $\langle\psi'|\psi'\rangle = 1$。

```
∀A:ℂ^(2^N×2^N) q:(N)量子态。酉_矩阵 A  ⟹
  cnorm2((λi. vsum (1..2^N)(λj. A_ij * (dest_量子态 q)_j)):ℂ^(2^N) )  =&1
```

酉演化完整描述了量子系统的确定性动力学。然而，它无法直接解释实验观测中固有的概率性事件。为形式化地描述此类事件及其概率，我们引入投影算符，作为测量公设的数学体现。

定义 1.12. 投影算子

投影测量由一组投影算符 $\{P_m\}$表征，满足 $P_m = |m\rangle\langle m|$，其中每个基向量 $|m\rangle$ 对应一个测量结果m。

设 project = new_definition
‘(project:(N)量子态 $\to \mathbb{C}^{2^N \times 2^N}$) v = 量子外积 v v‘

这里，量子外积生成 $|v\rangle$ 的外积。

Th这些投影算符满足自伴性、幂等性和完备性 :

定理 1.13。 自伴性

投影算子 P 是自伴的： $P = P^\dagger$。

投影 (v:(N)量子态) = 厄米_矩阵 (投影 v)

定理 1.14. 幂等性

投影算子 P 是幂等的： $P = P^2$

(投影 (v:(N)量子态)) ** (投影 v) = 投影 v

定理 1.15. 完备性

对于投影算符集合 $\{P_m\}$，完备关系始终成立$\sum_m P_m = I$。

cmat_sum (1..2^N) (λi. project (qbasis i:(N)qstate)) =id_复矩阵:$\mathbb{C}^{2^N \times}$ $^{2^N}$

这里，cmat_sum 将范围$1 \cdots 2^N$内的所有投影算符 project (qbasis i) 相加，其中 i in，得到单位矩阵。

定义 1.16. 测量

当待测量的状态为 $|\varphi\rangle$ 时，获得测量结果 m 的概率为$p(m) = \langle\varphi|P_m|\varphi\rangle$。

定义新的测量 = new_
‘∀x y:(N)qstate. 测量 x y = cnorm2(apply_复矩阵 (project x) y)‘

这里，apply_复矩阵将投影算子 $|x\rangle\langle x|$ 作用于量子态 $|y\rangle$，得到一个新的复向量，其平方范数给出获得测量结果 x的概率。

2. Grover 算法的形式化建模

该算法描述如下。在一个大小为 $N = 2^n$的无序数据库中，只有一个目标项 x'满足 $f(x') = 1$，而其他所有项均满足 $f(x) = 0$。任务是以尽可能少的量子查询识别x' 。

该算法首先对零态应用哈达玛门（H），生成均匀叠加。随后将该均匀叠加输入过程 G，该过程执行 $k = O(\sqrt{N})$ 次连续迭代，逐步放大目标态的振幅。最后，对目标态进行测量以获得搜索结果。这里， $N = 2^n$，其中n 表示量子比特的数量。

根据 Grover 算法的原理，求解过程可分为三个模块：初始化模块、Grover 迭代模块和测量模块。Grover 迭代模块本身由预言机模块（U_f）和扩散算子模块（D）组成。图 1 展示了 Grover 算法的量子电路图。()

1 量子态初始化

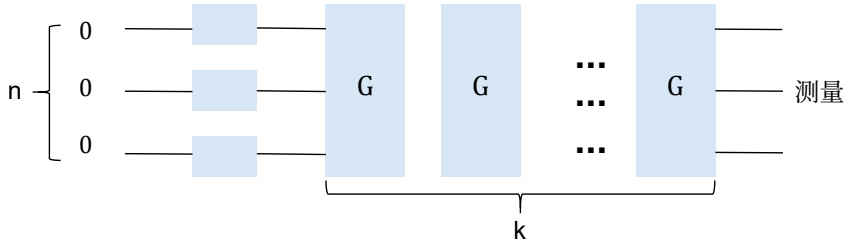


图 1：Grover 算法的量子电路图

将 n 个量子比特初始化为 $|0\rangle^{\otimes n}$，如公式 2.1 所示。

$$|0\rangle^{\otimes n} = \underbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}_{n \text{ times}} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{C}^{2^n} \tag{2.1}$$

公式 2.1 可以形式化地表述为定义 2.1。

定义 2.1. 初始状态

```
令零_量子态 = 新_定义‘零_量子态:(N)量子态 = mk_量子态 (λi.if i = 1 then Cx(&
1) else Cx(&0))‘
```

(2) H⊗n 的应用

分别对每个 n 量子比特应用 H门，这等价于执行复合门 $H^{\otimes n}$。使用定义 1.5 中形式化的函数 tensor_n2，可以精确地构造这个门。

```
令 n_阿达马 = 新_定义 n_阿达马 (n:ℕ) = 张量_n2 (复矩阵_列表 (λk. 阿达马)
n)
```

这里，cmatrix_list 会生成一个包含 n 个 H 门的列表，而 tensor_n2 则计算它们的张量积。此操作会将初始状态 $|0\rangle^{\otimes n}$ 转换为均匀叠加。

$$|\varphi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \tag{2.2}$$

```
令零_h =新_定义
 ‘零_h = 复矩阵_量子态_乘 (阿达马_n:ℂ^(2^N × 2^N)) (零_量子态:(N)量子态)‘
```

（3）预言机模块的构建 U_f

要将目标项与其他所有项区分开来，需要一个预言机算子。该算子的作用是翻转目标项的相位，即施加 π 相位偏移（通过添加负号）。

$$U_f|x\rangle = \begin{cases} |x\rangle, & \text{if } x \neq \tau \\ -|x\rangle, & \text{if } x = \tau \end{cases}$$

这里，状态 τ 是该函数的解态；这种相位变换可以通过酉矩阵实现：$U_f = I - 2|\tau\rangle\langle\tau|$。

令 U =新_定义
‘(U:ℕ → ℂ^(2^N × 2^N)) k =id_复矩阵 - Cx(&2) %* project (tau k)‘

相位翻转算子会标记目标态。这一操作是分析 Grover迭代的关键。我们将其形式化为定理 2.2。

定理 2.2. 相位翻转

预言机算子 U_f 对目标态 $|\tau\rangle$执行相位翻转，并满足对于任意系数 $a, b \in \mathbb{C}$: $U_f($ $a|\tau\rangle + b|\tau^{\perp}\rangle)$ $= b|\tau^{\perp}\rangle - a|\tau\rangle$。

∀k:ℕ a b:ℝ. 1 ≤k ∧k ≤ 2^N ⟹(U k:ℂ^(2^N × 2^N)) ** (mk_量子态 (Cx(a) %%% (tau k:(N) qstate) + Cx(b) %%% (tau_perp k:(N)qstate))):(N)qstate = mk_量子态(Cx(b) %%% (tau_perp k:(N)qstate) - Cx(a) %%% (tau k:(N)qstate))
这里，%%% 表示复数与量子态的乘法。

（4）扩散算子的构造 D

扩散算子 D 对振幅执行关于平均值的反演，从而增大目标态的概率振幅。它定义为 $D = 2|\varphi_0\rangle\langle\varphi_0| - I$，相应的矩阵表示如下。

$$D = \begin{pmatrix} \frac{1}{2^{n-1}} - 1 & \cdots & \frac{1}{2^{n-1}} \\ \vdots & \ddots & \vdots \\ \frac{1}{2^{n-1}} & \cdots & \frac{1}{2^{n-1}} - 1 \end{pmatrix}$$

由于量子计算中的所有演化操作都必须是酉的，因此有必要验证算子 D 是一个酉矩阵。

（5）Grover迭代算子的构造

算子 G 由预言机和扩散算子组成： $G = DU_f$ =(2|φ₀⟩⟨φ₀| − I)(I − 2|τ⟩⟨τ|)。由于已验证 D和 U_f是酉矩阵，根据定理1.4（酉矩阵乘法封闭性），它们的乘积也是酉矩阵。

算子 G 会被反复作用于初始叠加态 $|\varphi_0\rangle$，每次作用称为一次迭代。为简化分析，将 $|\varphi_0\rangle$分解为目标态 $|\tau\rangle$和非目标态 $|\tau^{\perp}\rangle$。通过构造一组正交基，可将整个量子态限制在一个二维子空间内。在该子空间中，初始状态可表示为 $|\varphi_0\rangle = \sqrt{\frac{N-1}{N}}|\tau\rangle + \sqrt{\frac{1}{N}}|\tau^{\perp}\rangle$。其中，$|\tau^{\perp}\rangle = \sqrt{\frac{1}{N-1}}\sum_{x\neq x_0}^{N-1}|x\rangle$ 表示所有非目标态的归一化叠加， N 为状态总数。为进一步简化表达式，引入三角函数来表示这些系数：

$$|\varphi_0\rangle = cos(\theta)|\tau^{\perp}\rangle + sin(\theta)|\tau\rangle \tag{2.3}$$

其中 $\theta = arcsin(\sqrt{\frac{1}{N}})$。

Grover 算法的第一次迭代从 $|U\rangle$ （初始叠加态）开始。通过对 $|B\rangle$（基态）进行反射，我们得到 O_x， $\pm|U\rangle$；随后通过对 $|U\rangle$进行反射，我们得到 $g|U\rangle$，并逐渐接近目标态 $|G\rangle$。这一变换在图 2 中以几何方式表示。

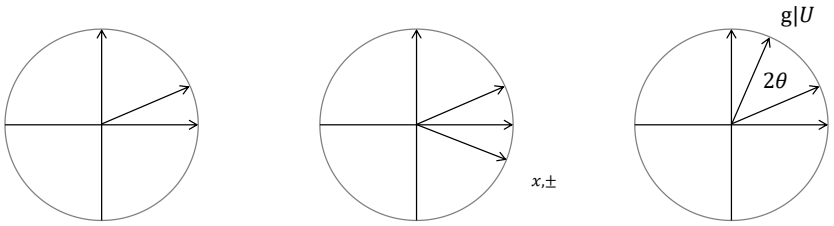


图 2：G 算子迭代示意图

经过 t 次迭代后，状态变为：

$$|\varphi_t\rangle = G^t|\varphi_0\rangle = \cos\big((2t+1)\theta\big)|\tau^\perp\rangle + \sin\big((2t+1)\theta\big)|\tau\rangle \tag{2.4}$$

方程 2.4 可通过以下定理得到形式化验证：

定理 2.3. *Grover* 迭代下的演化

∀k t:num. 1 ≤k ∧k ≤2^N ⟹((G k:$\mathbb{C}^{2^N\times 2^N}$) 复矩阵_pow t) ** zero_h:(N)量子态= mk_量子态 (Cx(sin((&2 * &t + &1) * asn(&1 /sqrt(&2^N)))) %%% ((tau k):(N)量子态)+ Cx(cos((&2 * &t + &1) * asn(&1 / sqrt(&2^N))))%%% ((tau_perp k):(N)量子态))

方程 2.4 给出了经过 t 次迭代后的量子态 $|\varphi_t\rangle$ 的显式表达式。为兼顾直观性与严谨性，我们采用两种互补的归纳方法证明定理 2.3：代数方法和几何方法。代数方法适用于整个 2^N 维希尔伯特空间，从而保证了普遍性。几何方法利用动力学受限于二维子空间这一性质，使证明得以简化。两种方法相互验证结果，并从多维视角阐明 Grover 迭代机制。

- **代数归纳**

我们用数学归纳法证明，对于所有 t，恒等式 $G^t|\varphi_0\rangle = \cos\big((2t+1)\theta\big)|\tau^\perp\rangle + \sin\big((2t+1)\theta\big)|\tau\rangle$ 成立。

对于基础情形 $t=0$，恒等式变为

$$G^0|\varphi_0\rangle = cos(\theta)|\tau^\perp\rangle + sin(\theta)|\tau\rangle$$

由于 $G^0 = I$，且恒等算子使任意态矢量保持不变，因此我们有$|\varphi_0\rangle = cos(\theta)|\tau^\perp\rangle + sin(\theta)|\tau\rangle$。根据方程 2.3，这个等式成立。

对于归纳步骤，假设方程对于某个 t 成立，并证明它对于 $t+1$ 也成立。

A1: $G^t|\varphi_0\rangle =$余弦$\big((2t+1)\theta\big)|\tau^\perp\rangle +$正弦$\big((2t+1)\theta\big)|\tau\rangle$

G1: $\implies G^{t+1}|\varphi_0\rangle =$余弦$\big((2(t+1)+1)\theta\big)|\tau^\perp\rangle +$正弦$\big((2(t+1)+1)\theta\big)|\tau\rangle$

证明分为四个关键阶段：作用分解、相位翻转简化、扩散算子展开和三角恒等式变换。下面将详细阐述各个阶段。

步骤 1：作用分解

首先，根据矩阵幂运算的定义，我们将 $G^{t+1}|\varphi_0\rangle$ 表示为 $(G\cdot G^t)|\varphi_0\rangle$。直接代入归纳假设 A1 后，G1 方程的左边变为：

$$G\left(\cos((2t+1)\theta)|\tau^\perp\rangle + \sin((2t+1)\theta)|\tau\rangle\right)$$

然后，利用 $G = DU_f$，我们将算子 G的一次作用分解开来。该作用由预言机算子 U_f 和算子 D依次作用构成。现在，左边变为：

$$D\left(U_f\left(\cos((2t+1)\theta)|\tau^{\perp}\rangle + \sin((2t+1)\theta)|\tau\rangle\right)\right) \tag{2.5}$$

步骤 2：相位翻转化简

根据定理 2.2（相位翻转），方程 2.5 可简化为：

$$D\left(\cos((2t+1)\theta)|\tau^{\perp}\rangle - \sin((2t+1)\theta)|\tau\rangle\right) \tag{2.6}$$

步骤 3：扩散算子展开

将算子 $D = 2|\varphi_0\rangle\langle\varphi_0| - I$ 代入方程 2.6，得到：

$$(2|\varphi_0\rangle\langle\varphi_0| - I)\left(\cos\big((2t+1)\theta\big)|\tau^{\perp}\rangle - \sin\big((2t+1)\theta\big)|\tau\rangle\right) \tag{2.7}$$

利用正交归一化条件 $\langle\tau^{\perp}|\tau\rangle = \langle\tau|\tau^{\perp}\rangle = 0$和 $\langle\tau|\tau\rangle = \langle\tau^{\perp}|\tau^{\perp}\rangle = 1$，计算内积：

$$\langle\varphi_0|\tau\rangle = \cos\theta\langle\tau^{\perp}|\tau\rangle + \sin\theta\langle\tau|\tau\rangle = \sin\theta \tag{2.8}$$

$$\langle\varphi_0|\tau^{\perp}\rangle = \cos\theta\langle\tau^{\perp}|\tau^{\perp}\rangle + \sin\theta\langle\tau|\tau^{\perp}\rangle = \cos\theta \tag{2.9}$$

将公式 2.8 和公式 2.9 代入公式 2.7，并利用分配律展开，得到

$$\begin{aligned}&2\cos\big((2t+1)\theta\big)\cos\theta\left(\cos\theta|\tau^{\perp}\rangle + \sin\theta|\tau\rangle\right) - 2\sin\big((2t+1)\theta\big)\sin\theta\left(\cos\theta|\tau^{\perp}\rangle + \sin\theta|\tau\rangle\right)\\ &-\cos\big((2t+1)\theta\big)|\tau^{\perp}\rangle + \sin\big((2t+1)\theta\big)|\tau\rangle\end{aligned} \tag{2.10}$$

步骤 4：三角恒等式变换

我们分别合并 $|\tau^{\perp}\rangle$和 $|\tau\rangle$的系数，得到以下结果：

$$\begin{aligned}&\Big(2\cos\big((2t+1)\theta\big)\cos^2\theta - 2\sin\big((2t+1)\theta\big)\sin\theta\cos\theta - \cos\big((2t+1)\theta\big)\Big)|\tau^{\perp}\rangle\\ &+\Big(2\cos\big((2t+1)\theta\big)\cos\theta\sin\theta - 2\sin\big((2t+1)\theta\big)\sin^2\theta + \sin\big((2t+1)\theta\big)\Big)|\tau\rangle\end{aligned} \tag{2.11}$$

然后，利用倍角公式和积化和差三角恒等式，可将公式 2.11 简化为：

$$\cos\big((2(t+1)+1)\theta\big)|\tau^{\perp}\rangle + \sin\big((2(t+1)+1)\theta\big)|\tau\rangle \tag{2.12}$$

至此，G1 的左边和右边完全相同，证明完成。

- **几何归纳法**

代数归纳已验证 Grover 算法迭代后的振幅演化公式。事实上，也可以从二维旋转的角度推导出这一结果。在由目标态 $|\tau\rangle$ 和非目标态 $|\tau^{\perp}\rangle$张成的二维空间中，$\{|\tau^{\perp}\rangle, |\tau\rangle\}$ 基下的 G算符的矩阵形式为 $\begin{bmatrix}\cos(2\theta) & -\sin(2\theta)\\ \sin(2\theta) & \cos(2\theta)\end{bmatrix}$。

初始叠加态 $|\varphi_0\rangle = \cos\theta|\tau^{\perp}\rangle + \sin\theta|\tau\rangle$在 $\{|\tau^{\perp}\rangle, |\tau\rangle\}$基下的向量表示如下：

$$|\varphi_0\rangle = \begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix} \tag{2.13}$$

经过 t 次 G 算子迭代后，状态 $G^t|\varphi_0\rangle = \cos\big((2t+1)\theta\big)|\tau^\perp\rangle + \sin\big((2t+1)\theta\big)|\tau\rangle$在$\{|\tau^\perp\rangle, |\tau\rangle\}$基下的向量形式为：

$$G^t|\varphi_0\rangle = \begin{pmatrix} \cos\big((2t+1)\theta\big) \\ \sin\big((2t+1)\theta\big) \end{pmatrix} \tag{2.14}$$

为验证公式 2.14，我们应用归纳策略，将目标拆分为两个子目标：对于基础情形 $t=0$，我们验证 $G^0|\varphi_0\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$。

由于 $G^0 = I$，且恒等算子使任意态矢量保持不变，因此我们有$|\varphi_0\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$。根据公式 2.13，这个等式成立。

对于归纳步骤，假设该方程对某个 t 成立，并证明它对$t+1$也成立。

A1：$G^t|\varphi_0\rangle = \begin{pmatrix} \cos\big((2t+1)\theta\big) \\ \sin\big((2t+1)\theta\big) \end{pmatrix}$ G1：

$\Longrightarrow G^{t+1}|\varphi_0\rangle = \begin{pmatrix} \cos\big((2(t+1)+1)\theta\big) \\ \sin\big((2(t+1)+1)\theta\big) \end{pmatrix}$

证明由三个步骤组成：归纳步骤、矩阵乘法和三角恒等式变换。下面将详细介绍这些步骤。步骤 1：归纳步骤

首先，我们将 $G^{t+1}|\varphi_0\rangle$ 表示为 $(G\cdot G^t)|\varphi_0\rangle$。然后，通过代入归纳假设 A1 以及 G 算子的旋转矩阵形式，目标 G1 的左侧变为：

$$\begin{bmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{bmatrix} \begin{pmatrix} \cos\big((2t+1)\theta\big) \\ \sin\big((2t+1)\theta\big) \end{pmatrix} \tag{2.15}$$

步骤 2：矩阵乘法

执行矩阵与向量的乘法后，公式 2.15 变为：

$$\begin{pmatrix} \cos(2\theta)\cos\big((2t+1)\theta\big) - \sin(2\theta)\sin\big((2t+1)\theta\big) \\ \sin(2\theta)\cos\big((2t+1)\theta\big) + \cos(2\theta)\sin\big((2t+1)\theta\big) \end{pmatrix} \tag{2.16}$$

步骤 3：三角恒等式变换

利用三角函数和角公式，公式 2.16 可简化为：

$$\begin{pmatrix} \cos\big((2t+3)\theta\big) \\ \sin\big((2t+3)\theta\big) \end{pmatrix} \tag{2.17}$$

至此，目标得证。

两种证明策略相辅相成。代数归纳仅依赖矩阵乘法和内积等基本代数运算，不诉诸任何特定的几何直觉，从而在最一般的情形下验证了结果的普适性。相比之下，几何归纳法揭示了 Grover 迭代固有的二维旋转结构。它表明，指数级加速源于有效子空间中动力学的几何简化。这些方法相结合，不仅交叉验证了定理 2.3，还将算法的代数形式与其几何本质统一起来。

(6) 测量

经过 t 次迭代后，目标态 $|\tau\rangle$ 的概率振幅达到最大值。此时，我们对量子态 $|\varphi_t\rangle$ 进行投影测量，

使用投影算子 $P_\tau = |\tau\rangle\langle\tau|$。因此，测量后观测到 $|\tau\rangle$ 的概率为

$$p_t = \sin^2\big((2t+1)\theta\big) \tag{2.18}$$

3. Grover 算法的形式化验证

如上一节所述，算法最后会进行投影测量，以较高的概率获得目标解。该概率并非固定不变，而是随 Grover 迭代次数 t 变化。为确保效率，我们将对成功概率 P_t 如何随 t变化进行形式化分析。具体而言，我们将依次验证其周期性、最优性和单调性。

成功概率 $p_t = \sin^2((2t+1)\theta)$（式 2.18）呈现出明显的周期性振荡。性能分析必须限定在一个周期内。这意味着算法的性能分析必须限制在一个完整周期内。它决定最优迭代次数，并防止因迭代过多而导致性能下降。因此，我们首先对这一性质进行形式化验证。

定理 3.1. 概率的周期性

Grover 算法的成功概率 p_t 是一个周期为 π 的周期函数。也就是说，

$$\sin^2\big((2t+1)\theta+\pi\big) = \sin^2\big((2t+1)\theta\big) \tag{3.1}$$

∀x. sin(x +pi) 的幂 2 = sin(x) 的幂 2

成功概率的周期性 p_t 意味着，可以将算法的分析限制在单个周期内。在此区间内，严格单调增加直至达到峰值，保证每个 Grover 步骤都能系统地放大解的振幅。验证这种放大效应可确保搜索过程确定性地收敛，而不是随机游走。

定理 3.2。 概率单调增加

对于所有满足 $0 < t \wedge t+1 \le \frac{\pi}{4\theta} - \frac{1}{2}$ 的迭代次数 t，我们有 $0 < p_{t+1} - p_t$，其位于相位区间 $[0, \frac{\pi}{2}]$ 内。 −

∀t:ℕ。 1 ≤ k ∧ k ≤ 2^N ∧ &0 < &t ∧ &(t+1) ≤ pi / (&4 * asn (&1/sqrt(&2^N))) - &1 / &2 ⟹ & 0 < 测量 (tau k:(N) 量子态)(状态_在_giter k (t + 1):(N) 量子态之后) - 测量 (tau k:(N)量子态) (状态_在_giter k t:(N)量子态之后)

在定理 3.2 中，state_after_giter 表示经过 t 次迭代后， G 算子的量子态。我们将证明分为两步。S

tep 1: $\mathrm{S}_{\mathrm{quare}}\ \mathrm{d}$-difference to pro duct

代入成功概率公式可得 $0 < \sin^2\big((2t+3)\theta\big) - \sin^2\big((2t+1)\theta\big)$。利用单位元 $\sin^2 a - \sin^2 b = \sin(a+b)\,\sin(a-b)$，得到 $0 < \sin\big((4t+4)\theta\big)\,\sin(2\theta)$。第二步：因子的符号

已知 $\theta =$反正弦$(1/\sqrt{N})$ 和 $0 < t \wedge t+1 \le \frac{\pi}{4\theta} - \frac{1}{2}$，我们有 $0 < \theta < \frac{\pi}{2}$ and $0 < (4t+4)\theta < \pi$。因此，$\sin(2\theta) > 0$ 且 $\sin\big((4t+4)\theta\big) > 0$。两个正因子的乘积给出 $0 < \sin\big((4t+4)\theta\big)\sin(2\theta)$，证明完毕。

在讨论概率放大效应之后，我们现在来考察其对称的一面：概率衰减。概率的单调下降意味着，一旦超过最优迭代次数，

性能就会如预期般下降。因此，这为及时停止迭代、避免计算资源浪费提供了理论依据。

定理 3.3. 概率单调递减

在相位区间 $[\frac{\pi}{2},\pi]$ 内，对于满足 $\frac{\pi}{4\theta}-\frac{1}{2}\le t\wedge t\le\frac{\pi}{2\theta}-\frac{3}{2}$ 的任意迭代次数 t，有 $0<p_t-p_{t+1}$。该证明与定理 4.2 的证明思路相同，因此略去。

∀t:ℕ. 1 ≤k ∧k ≤ 2^N∧pi / (&4 * asn (&1 / sqrt(&2^N)) - &1 / &2 ≤&t ∧&t ≤ pi / (&2 * asn (&1 / sqrt(&2^N))) - &3 / &2 ⟹ &0 < 测量 (tau k:(N) 量子态)(状态_在_giter k t:(N)量子态之后) - 测量 (tau k:(N) 量子态)(状态_在_giter k (t+1):(N)量子态之后)

上述性质为 p_t 建立了单峰曲线：在 $[0,\pi/2]$ 上单调增加，并在 $[\pi/2,\pi]$ 上单调减少。当 $(2t+1)\theta$ 最接近 $\pi/2$ 时，性能达到峰值。因此，需要一个严格且可验证的停止准则。该准则将理论最优值映射为可执行的迭代次数。它能够保证峰值性能，并消除迭代不足或过度迭代造成的资源浪费。

定理 3.4。 最优迭代次数

在区间 $[0,\pi]$ 内，为使 $p_t=\sin^2\big((2t+1)\theta\big)$ 最大，相位角必须满足$t=\frac{\pi}{4}$反正弦($1/\sqrt{N}$)$-\frac{1}{2}$。由于 t 表示迭代次数且必须为非负整数，因此只有两个实际可行的值：向下取整值 $t_{\text{floor}}=\left\lfloor\frac{\pi}{4}\text{反正弦}(1/\sqrt{N})-\frac{1}{2}\right\rfloor$ 和向上取整值 $t_{\text{ceil}}=\left\lceil\frac{\pi}{4}\text{反正弦}(1/\sqrt{N})-\frac{1}{2}\right\rceil$，即 $\forall t',\ 0\le(2t'+1)\theta\le\pi\implies p_{t'}\le p_t\vee p_{t'}\le p_{t+1}$。单调增加（定理 3.2 ）和单调减少（定理 3.3）有助于确定这一最优迭代次数。

∀k t':ℕ. 1 ≤k ∧k ≤ 2^N∧(&2 * &t' +&1) * asn (&1 / sqrt(&2^N)) ≤pi ⟹测量(tau k:(N)量子态)(状态_之后_giter k t':(N)量子态) ≤测量(tau k:(N)量子态)(状态_之后_giter k (num_of_real(pi / (&4 * asn (&1 / sqrt(&2^N))) - &1 / &2)):(N)量子态) ∨ 测量(tau k:(N)量子态)(状态_之后_giter k t':(N)量子态) ≤测量(tau k:(N)量子态)(状态_之后_giter k (num_of_real (pi / (&4 * asn (&1 / sqrt(&2^N))) - &1 / &2) + 1):(N)量子态)

本节基于第 2 节的状态演化模型，对 Grover 算法的概率演化进行形式化验证，从而揭示其完整的动力学特征。研究结果表明，算法效率在很大程度上取决于精确的迭代控制。在由周期性界定的有限相位区间内（定理 3.1），成功概率随迭代次数呈现单峰特征：先单调递增（定理 3.2），随后单调递减（定理 3.3）。离散最优解确定方法（定理 3.4）实现了理论最优值与实际迭代策略之间的有效衔接。这些性质共同构成了 Grover 算法参数优化与效率评估的严谨理论基础，为其在实际应用中的可靠性和鲁棒性提供了根本保障。

4. 应用

在经典计算中，整数分解是一项极具挑战性的问题，其计算复杂度会随位数增加而呈指数级增长。Grover 算法可以通过在范围$[2, \sqrt{N}]$内搜索潜在因子，以加速这一搜索过程，从而找到 N的一个非平凡因子。

以 $143 = 11 \times 13$ 的分解为例，只需找出其中一个因子（11 或 13），因为另一个因子可以通过经典除法得到。由于$\sqrt{143} < 12$，我们取最接近的 2 的幂，并使用 4 个量子比特。因此，搜索空间大小为 $N = 2^4 = 16$。接下来，我们将重点分析该情形下的最优迭代次数和概率单调性。

1) 整数分解的最优迭代次数

对于 $N = 16$ 的分解实例，在区间 $[0, \pi]$ 内，没有任何成功概率超过理论最优值的下取整或上取整。也就是说：

$$\forall t.\ (2t+1) \cdot \arcsin\left(\frac{1}{\sqrt{16}}\right) \le \pi \implies p(t) \le p\left(\left\lfloor \frac{\pi}{4 \arcsin\left(1/\sqrt{16}\right)} - \frac{1}{2} \right\rfloor\right)$$

$$\vee\, p(t) \le p\left(\left\lfloor \frac{\pi}{4 \arcsin\left(1/\sqrt{16}\right)} - \frac{1}{2} \right\rfloor + 1\right)$$

此处，$\lfloor \cdot \rfloor$ 表示下取整函数。

$\forall t : \mathbb{N}$.(&2 * &t + &1) * asn(&1 / sqrt(&2^4)) $\le$ pi $\implies$ 测量(tau 11:(4)量子态) (状态_之后_giter 11 t:(4)量子态)$\le$ 测量(tau 11:(4)量子态 (状态_之后_giter 11(num_of_real (pi / (&4 * asn (&1 / sqrt(&2^4))) - &1 / &2)):(4)量子态) $\vee$测量(tau 11:(4)量子态)(状态_之后_giter 11 t:(4)量子态) $\le$ 测量(tau 11:(N)量子态)(状态_之后_giter 11(num_of_real (pi / (&4 * asn (&1 / sqrt(&2^4))) - &1 / &2) + 1):(4)量子态)

这一结论可由定理 3.4（最优迭代次数）验证。

2) 单 整数分解中概率函数的单调性分析

在一个周期内（即满足 $(2t+1) \cdot$反正弦 $\left(\frac{1}{\sqrt{16}}\right) \le \pi$），迭代次数的有效范围为 $t \le 5$。在此范围内，成功概率 $p(t)$ 随着迭代次数呈现先增后减的趋势，如图 3 所示。

我们验证最优迭代之前的递增性质，即 $p(0) < p(1)$ 和$p(1) < p(2)$。这表明，在初始阶段，成功概率随着迭代次数单调递增。这两个不等式的证明过程相似。下面以 $p(0) < p(1)$ 为例，详细说明证明过程。步骤 1：不等式变形

将 $p(0) < p(1)$ 变形为 $0 < p(1) - p(0)$，使其符合定理 3.2 的形式。步骤 2：证明充分条件

给定定理 $P \implies Q$，为了证明目标 Q，我们使用策略 MATCH_ MP_TAC，将目标替换为 P。因此，应用定理 3.2 后，目标变为证明：

$$1 \le \frac{\pi}{4 \arcsin\left(1/4\right)} - \frac{1}{2}.$$

步骤 3：三角不等式缩放

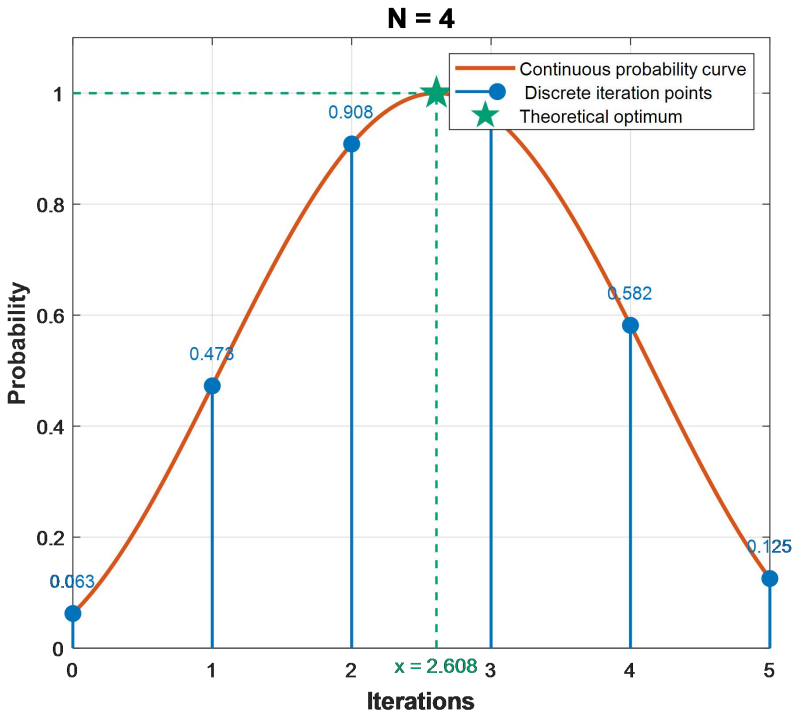


图 3：Grover 算法中的非单调成功概率

将目标不等式变形为：

$$\arcsin\left(\frac{1}{4}\right) < \frac{\pi}{6},$$

然后，利用反三角函数在该区间上的单调性，将其转化为证明：

$$\frac{1}{4} < \sin\left(\frac{\pi}{6}\right).$$

接下来，我们验证在达到最优迭代次数后，成功概率会随着迭代次数的增加而单调递减，即 $p(3) > p(4)$ 和 $p(4) > p(5)$。证明过程与递增性质的证明类似，不同之处在于推导依赖于定理 3.3。

这一验证的结论超越了简单的仿真观察。它从数学上排除了在达到峰值之前成功概率曲线出现波动或平台期的可能性，确认了其严格单调性。这意味着，任何遵循 Grover 方法的量子电路，都会随着迭代次数增加而不可避免且确定性地提升其性能（直至达到最优值）。我们的证明将算法“有效性”和“可靠性”这一传统的定性概念转化为定量的、机器验证的保证。

5. 结论

本文提出了一个使用 HOL Light 定理证明器构建和验证 Grover 算法的形式化模型。具体而言，我们通过形式化定义量子态、量子门、酉变换和量子测量等核心概念，建立了一个新颖的量子框架，为量子计算的形式化验证奠定了基础。在该框架内，我们验证了 Grover 算法的若干关键性质，并以整数分解为例，展示了其在解决基于搜索的问题中的潜在应用。这项工作不仅拓展了量子算法的形式化分析，也为量子计算中的其他应用场景（如量子通信和量子密码学）提供了形式化验证基础。未来的工作将重点拓展所提出的框架，包括探索更多量子算法，并进一步研究其在更复杂场景中的应用，同时结合量子纠错码和高维量子系统开展深入验证。

致谢

本研究部分得到了国家自然科学基金（62372312、62272323、62272322、62372311）的资助。

参考文献

[AB20] Anthony E Armenakas 和 Oliver K Baker。将量子搜索算法应用于大型强子对撞机的高能物理数据。*arXiv* 预印本 *arXiv:2010.00649*，2020。doi:10.48550/arXiv.2010.00649。[BLH21] Anthony Bordg、Hanna Lachnitt 和 Yijun He。使用 Isabelle/HOL 进行经认证的量子计算。*J. Autom. Reason.*，65(5):691–709，2021。doi:10.1007/s10817-020-09584-7。[CBB21] Christophe Chareton、Sébastien Bardin、François、Perrelle、Valentin、Benoît Valiron 和 Benoît Bobot。面向电路构建型量子程序的自动化演绎验证框架。载于第*30*届欧洲编程研讨会（*ESOP*）论文集，第148–177页。Springer International Publishing，2021。doi:10.1007/978-3-030-72019-3_6。[CLCH20] Ching-Ray Chang、Yeu-Chung Lin、Kuei-Lin Chiu 和 Tsung-Wei Huang。量子计算机与第二次量子革命。*AAPPS Bull.*，30(1)，2020。doi:10.22661/AAPPSBL.2020. 30.1.09。[CLV+23] Christophe Chareton、Dongho Lee、Benoit Valiron、Renault Vilmart、Sébastien Bardin 和 Zhaowei Xu。量子算法的形式化方法。载于形式化分析、验证与密码学手册，第319–422页。CRC Press，2023。doi:10.1201/9781003090052-7。[Gro96] Lov K Grover。一种用于数据库搜索的快速量子力学算法。载于第*28*届*ACM*计算理论年会（*STOC*）论文集，第212–219页，1996。doi:10.1145/237814.237866。[HRH+21] Kesha Hietala、Robert Rand、Shih-Han Hung、Liyi Li 和 Michael Hicks。证明量子程序正确。载于第*12*届国际交互式定理证明会议（*ITP*）论文集，2021。doi:10.4230/LIPIcs.ITP.2021.21。[HT15] Osman Hasan 和 Sofiene Tahar。形式化验证方法。载于信息科学与技术百科全书（第*3*版），第7162–7170页。IGI global，2015。doi:10.4018/978-1-4666-5888-2.ch705。[JZCM22] Yaoyao Jiang、Wenbin Zhang、Pengcheng Chu 和 Hongyang Ma。基于置换群的环上多粒子量子行走反馈搜索算法。*Acta Phys. Sin.*，71(3)，2022。doi:10.7498/aps.71.20211000。[LQW+25] Lu Liu、Ling Qian、Xingyu Wu、Chenrui Fan、Lufan Zhang、Dunbo Cai、Huijun Lu、Tiejun Wang 和 Chuan Wang。使用 Grover自适应搜索算法求解车辆路径问题。*IEEE Trans. Intell. Transp. Syst.*，2025。doi:10.1109/TITS.2025.3562860。

[LSZ23] Marco Lewis、Sadegh Soudjani 和 Paolo Zuliani。量子程序的形式化验证：理论、工具与挑战。《ACM量子计算汇刊》，5(1):1–35，2023。doi:10.1145/ 3624483。[LWC+24] Shang-Wei Lin、Tzu-Fan Wang、Yean-Ru Chen、Zhe Hou、David Sanán 和 Yon Shin Teo。一种基于纠缠和量子隐形传态的并行分布式量子 SAT 求解器。载于TACAS论文集，第363–382页。Springer，2024。doi:10.1007/978-3-031-57249-4_18。[LZW+19] Junyi Liu、Bohua Zhan、Shuling Wang、Shenggang Ying、Tao Liu、Yangjia Li、Mingsheng Ying 和 Naijun Zhan。使用量子霍尔逻辑对量子算法进行形式化验证。载于第31届国际计算机辅助验证会议（CAV）论文集，第187–207页。Springer，2019。doi:10.1007/978-3-030-25543-5_12。[MJB+17] Saptarshi Mitra、Bappaditya Jana、Supratim Bhattacharya、Prashnatita Pal 和 Jayanta Poray。量子密码学：概述、安全问题与未来挑战。载于第4届国际光电子应用会议（OPTRONIX）论文集，第1–7页，2017。doi:10.1109/OPTRONIX.2017. 8350006。[PAB+23] Alexey Pyrkov、Alex Aliper、Dmitry Bezrukov、Yen-Chu Lin、Daniil Polykovskiy、Petrina Kamya、Feng Ren 和 Alex Zhavoronkov。面向生成化学与药物发现近期应用的量子计算。《今日药物发现》，28(8):103675，2023。doi:10.1016/j.drudis. 2023.103675。[RH20] Adnan Rashid 和 Osman Hasan。使用 HOL Light 对最多4自由度的机器人细胞注射系统进行形式化验证。Form. Asp. Comput.，32(2):1–22，2020。doi:10.1007/s00165-020-00514-3。[SCD+21] Wenjun Shi、Qinxiang Cao、Yuxin Deng、Hanru Jiang 和 Yuan Feng。在 Coq 中对量子电路进行符号推理。J. Comput. Sci. Technol.，36:1291–1306，2021。doi:10.1007/ s11390-021-1637-9。[SCD24] Wenjun Shi、Qinxiang Cao 和 Yuxin Deng。在 Coq 中形式化经典—量子命令式语言的语义。J. Circuits Syst. Comput.，33(06):2450112，2024。doi:10.1142/ S0218126624501123。[SJK+22] Gyeongju Song、Kyoungbae Jang、Hyunjun Kim、Siwoo Eum、Minjoo Sim、Hyunji Kim、Waikong Lee 和 Hwajeong Seo。适用于 Grover 算法的快速量子电路。Appl. Sci.，12 6870，2022 14 10 3390 12146870 ( ): . doi: . /app . [SW24] Yifan Sun 和 Lian-Ao Wu。加权数据库上的量子搜索算法。Sci. Rep.，14(1):30169，2024。doi:10.1038/s41598-024-81701-7。[YHK+23] Chun Seok Yoon、Chang Ho Hong、Min Sung Kang、Ji-Woong Choi 和 Hyung Jin Yang。使用 Grover 迭代的量子非对称密钥密码方案。Sci. Rep.，13(1):3810，2023。doi:10.1038/s41598-023-30860-0。[ZWC+20] Leo Zhou、Sheng-Tao Wang、Soonwon Choi、Hannes Pichler 和 Mikhail D Lukin。量子近似优化算法：性能、机制及其在近期量子设备上的实现。Phys. Rev. X，10(2):021067，2020。doi:10.1103/PhysRevX.10.021067。[ZWL+24] Haoying Zhang、Shaoxuan Wang、Xinjian Liu、Yingtong Shen 和 Yukun Wang。通过电路设计求解最小支配集问题的量子算法。Chin. Phys. B，33 020310，2024 2 10 1088 1674 1056 02 5 ( ): . doi: . / - /ad e 。

本作品采用知识共享署名许可协议授权。要查看该许可协议副本，请访问 https://creativecommons.org/licenses/by/4.0/，或致函美国加利福尼亚州旧金山第二街171号300室，邮编94105；或德国柏林艾森纳赫街2号，邮编10777