# 基于 Quantum Shannon Decomposition 的通用量子门分解算法 (草稿)

## 1 摘要

本文实现了一种基于 Quantum Shannon Decomposition 的任意量子门分解算法. 算法利用了量子信息理论中的 Shannon 分解定理, 将任意量子门分解成一系列基本量子门的组合. 该算法在 NISQ (Noisy Intermediate-Scale Quantum) 阶段具有较高的效率和精度. 此外, 本文还基于该算法结合 Gram–Schmidt Process 实现了任意量子态制备. 该算法的实现对于 NISQ 阶段的量子计算机有着积极的作用.

## 2 引言与背景介绍

随着量子计算技术的不断发展, 量子计算机已经成为了备受关注的研究领域. 在量子计算机中, 量子门是实现量子计算的基本操作. 然而, 由于量子门的复杂性, 设计和现任意量子门是一个非常具挑战性的问题.

在 NISQ (Noisy Intermediate-Scale Quantum) 阶段, 量子计算机的规模和精度都受到了限制. 因此, 如何在这个阶段实现任意量子门成为了一个重要的问题. 门分解法是一解决这个问题的方法, 它可以将任意量子门分解成一系基本量子门的组合. 这种方法可以在 NISQ 阶段的量子计算机上实现任意量子门, 从而推动量子计算机的发展.

在门分解算法中, Shannon 分解定理是一种常用的方法. 该定理可以将任意量子门分解成一系列基本量子门的组合, 从而实现任意量子门.

## 3 主要结果介绍

本文基于 Quantum Shannon Decomposition 实现了一种通用量子门分解算法, 该算法可以将任意量子酉门分解为仅包含 $R_y$, $R_z$ 以及相邻 $CNOT$ 的量子线路. 该算法优点是时间复杂度低, 并且对于相同比特数的量子门其分解出的线路区别仅在于 $R_y$, $R_z$ 门的参数, 因此可进行离线预处理, 进一步降低运行时线路分解的时间复杂度. 附录 A 中展示了 3-qubit 任意酉门的分解结果.

此外, 本文也实现了一种基于 Gram–Schmidt Process 和 Quantum Shannon Decomposition 制备任意量子态的方法. 该方法使用 Gram–Schmidt Process 构造量子门 $U$, 使得 $U|0\rangle = |\psi\rangle$, $|\psi\rangle$ 为目标量子态. 再通过 Quantum Shannon Decomposition 对量子门 $U$ 进行分解从而得到仅包含 $R_y$, $R_z$ 及 $CNOT$ 的量子线路. 执行分解后的线路即可得到待制备的量子态.

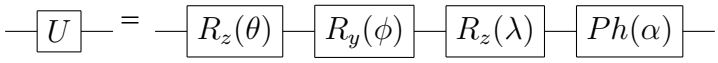
# 4 主要方法与原理

## 4.1 ZYZ Decomposition

ZYZ 分解是一种用于将任意酉门分解为 Rz, Ry 门的方法 [1]，分解过程中会产生一个全局相位 $\alpha$. 用公式可表示为:

$$U = e^{i\alpha} Rz(\theta) Ry(\phi) Rz(\lambda) \tag{4.1}$$

对应的量子线路为:




为求出 $\theta$, $\phi$, $\lambda$ 和全局相位 $e^{i\alpha}$ 的具体值, 我们将公式 4.1 等号右边的乘积用矩阵表示, 则有:

$$U = e^{i\alpha} \begin{bmatrix} e^{i(\frac{\lambda}{2}+\frac{\theta}{2})}\cos(\frac{\phi}{2}) & -e^{-i(\frac{-\lambda}{2}+\frac{\theta}{2})}\sin(\frac{\phi}{2}) \\ e^{i(\frac{\lambda}{2}-\frac{\theta}{2})}\sin(\frac{\phi}{2}) & e^{-i(\frac{\lambda}{2}+\frac{\theta}{2})}\cos(\frac{\phi}{2}) \end{bmatrix} \tag{4.2}$$

推导得:

$$\phi = \begin{cases} 2\arccos(|U_{00}|), |U_{00}| \geq |U_{01}| \\ 2\arcsin(|U_{01}|), |U_{00}||U_{01}| \end{cases} \tag{4.3}$$

$$\theta + \lambda = 2\arctan 2(\mathrm{Im}(\frac{|U_{11}|}{\cos(\frac{\phi}{2})}), \mathrm{Re}(\frac{|U_{11}|}{\cos(\frac{\phi}{2})})) \tag{4.4}$$

$$\theta - \lambda = 2\arctan 2(\mathrm{Im}(\frac{|U_{10}|}{\sin(\frac{\phi}{2})}), \mathrm{Re}(\frac{|U_{10}|}{\sin(\frac{\phi}{2})})) \tag{4.5}$$

其中全局相位参数 $\alpha$ 为待分解门 $U$ 转化为 $SU(2)$ 矩阵时的产生的相位差.

## 4.2 Kronecker Decomposition

Kronecker Decomposition [2] 常用于将 4x4 的酉矩阵分解为两个 2x2 的酉矩阵的张量积的形式, 如:

$$U = A \otimes B \tag{4.6}$$

$$= \begin{bmatrix} A_{11}B_{11} & A_{12}B_{12} & A_{12}B_{11} & A_{12}B_{12} \\ A_{11}B_{21} & A_{11}B_{22} & A_{12}B_{21} & A_{12}B_{22} \\ A_{21}B_{11} & A_{21}B_{12} & A_{22}B_{11} & A_{22}B_{12} \\ A_{21}B_{21} & A_{21}B_{22} & A_{22}B_{21} & A_{22}B_{22} \end{bmatrix} \tag{4.7}$$

我们可以使用 Pitsianis-Van Loan 算法 [3] 通过 $U$ 反向求解 $A$ 和 $B$, 可以保证求解出的 $A \otimes B$ 在 Frobenius norm 下是最接近与原始矩阵 $U$ 的一组张量积. 该算法将待分解矩阵 $U$ 看成一个 2x2x2x2 的张量, 则 $U$ 为 $A$ 与 $B$ 的外积第二维与第三维的转置: e

$$U_{mpnq} = A_{mn} \otimes B_{pq} = (A_{mn} \circ B_{pq})^{T_{n,p}} \tag{4.8}$$

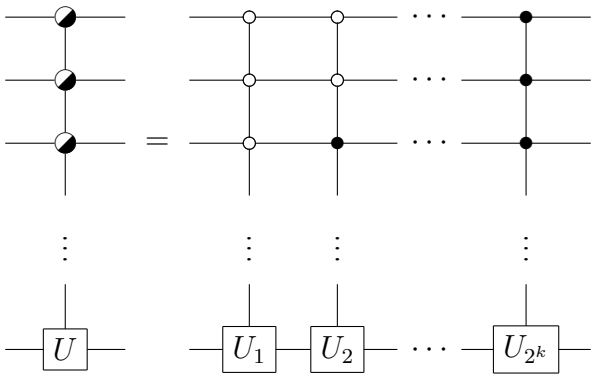
这时 $A, B$ 就可以用奇异值分解 (Singular Value Decompostion) 进行求解.

## 4.3 Uniformly Controlled Gate (Multiplexed Gate)

Uniformly Controlled Gate 是一种在量子门线路中较为常用的结构, Bergholm 等在其文章中使用 $F_t^k(U(2))$ 表示一个 k-fold controlled one-qubit gate [4], 即一个有 k 个控制比特和一个目标比特的 uniformly controlled gate. 其中 $t$ 为目标比特, $k$ 为控制比特数, $U(2)$ 代表构成该门的基础门都是 2x2 的酉矩阵. 该 uniformly controlled gate 可被定义为:

$$F_t^k(U(2)) = \bigoplus_{i=0}^{2^k} U_i(2) = \begin{pmatrix} u_1 & & & \\ & u_2 & & \\ & & \ddots & \\ & & & u_{2^k} \end{pmatrix} \tag{4.9}$$

对应的量子线路为:




对单目标比特 Uniformly Controlled Gate 进行推广可以等到多目标比特 Uniformly Controlled Gate:

$$F_T^n(U(2^t)) = \bigoplus_{i=0}^{2^n} U_i(2^t) = \begin{pmatrix} u_1 & & & \\ & u_2 & & \\ & & \ddots & \\ & & & u_{2^n} \end{pmatrix} \tag{4.10}$$

该门作用于量子态 $|\phi\rangle|\psi\rangle$ 可表示为:

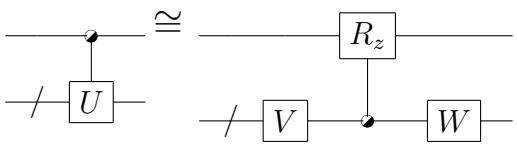
$$F_T^n(U(2^t))|\phi\rangle|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |c_{i1}c_{i2}\dots c_{in}\rangle \otimes U_i(2^t)|\psi\rangle \tag{4.11}$$

此外, 一个 Uniformly Controlled Gate 可以表示为 $U = (I\otimes V)(D\oplus D^\dagger)(I\otimes W)$. 使用子矩阵可表示为:

$$\begin{pmatrix} U_1 & \\ & U_2 \end{pmatrix} = \begin{pmatrix} V & \\ & V \end{pmatrix} \begin{pmatrix} D & \\ & D^\dagger \end{pmatrix} \begin{pmatrix} W & \\ & W \end{pmatrix} \tag{4.12}$$

其中 $U_1, U_2, V, W$ 为酉矩阵, $D, D^\dagger$ 为对角酉矩阵.

Shende 等人的文章 [5] 中给出了一种基于上式将一个 $n$ 比特 Uniformly Controlled Gate 分解成两个 $n-1$ 比特酉门和一个 Uniformly Controlled Rz Gate 的方法, 其线路表示如下:



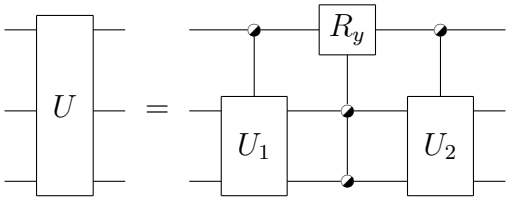

该算法可被用于 Quantum Shannon Decomposition 中 Cosine-Sine Decomposition 产生的 Uniformly Controlled Gate 的分解.

## 4.4 Cosine-Sine Decomposition

Cosine-Sine Decomposition 是一种可以将任意偶数维酉矩阵 $U \in \mathbb{C}^{l\times l}$ 分解为 $\frac{l}{2}$ 维酉矩阵 $A_1, B_1, A_2, B_2$ 及实数对角阵 $C$ 和 $S$ ($C^2 + S^2 = I_{\frac{l}{2}}$) 的方法.

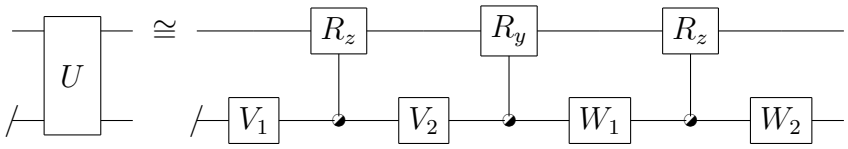
$$U = \begin{pmatrix} A_1 & \\ & B_1 \end{pmatrix} \begin{pmatrix} C & -S \\ S & C \end{pmatrix} \begin{pmatrix} A_2 & \\ & B_2 \end{pmatrix} \tag{4.13}$$

上式中等号右边的矩阵 $A_1 \oplus B_1$ 和 $A_1 \oplus B_1$ 在量子线路中可以表示为 Uniformly Controlled Gate. 而中间由实对角阵 $C, S$ 构成的矩阵则可以表示为一个 Uniformly Controlled Ry Gate.



## 4.5 Quantum Shannon Decomposition

Quantum Shannon Decomposition 是一种基于 Shannon 分解定理结合了 Cosine-Sine Decomposition 和 Uniformly Controlled Gate Decompostion 的门分解算法, 其线路表示如下:




## 4.6 Gram-Schmidt Process

Gram-Schmidt 过程是一种将线性无关的向量组转化为正交向量组的方法. 具体来说, 对于一个线性无关的向量组 $v_1, v_2, ..., v_n$, 我们可以通过以下公式将它们转化为正交向量组 $u_1, u_2, ..., u$:

$$u_1 = v_1 \tag{4.14}$$

$$u_2 = v_2 - \frac{\langle v_2, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 \tag{4.15}$$

$$u_3 = v_3 - \frac{\langle v_3, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 - \frac{\langle v_3, u_2 \rangle}{\langle u_2, u_2 \rangle} u_2 \tag{4.16}$$

$$\vdots \tag{4.17}$$

$$u_n = v_n - \sum_{i=1}^{n-1} \frac{\langle v_n, u_i \rangle}{\langle u_i, u_i \rangle} u_i \tag{4.18}$$

其中, $\langle \cdot, \cdot \rangle$ 表示向量的内积, 即 $\langle x, y \rangle = x^T y$. 这个公式的意义是, 我们首先将第一个向量 $v_1$ 作为正交向量组的第一个向量 $u_1$, 然后对于后面的每个向量 $v_i$, 我们将它减去它在前面所有向量 $u_1, u_2, \ldots, u_{i-1}$ 上的投影, 得到一个与前面所有向量都正交的向量 $u_i$. 接着, 我们可以将这些正交量组归一化, 得到单位向量组:

$$\hat{u}_i = \frac{u_i}{|u_i|} \tag{4.19}$$

向量组 $\hat{u}_1, \hat{u}_2..., \hat{u}_n$ 满足以下两个条件:

- 它们是正交的, 即 $\langle \hat{u}_i, \hat{u}_j \rangle = 0$, 其中 $i \neq j$.
- 它们是单位向量, 即 $|\hat{u}_i| = 1$.

将这些单位向量按列排列成一个矩阵 $U = [\hat{u}_1 \hat{u}_2 ... \hat{u}_n]$. 因为其列向量 $\{\hat{u}_i\}$ 满足正交性, 并且 $|\hat{u}_i| = 1$, 进一步推导易得 $|\det(U)| = 1$, 所以 $U$ 满足酉矩阵的性质, 是一个酉矩阵.

## 4.7 任意量子态酉矩阵构造

对于任意量子态 $|\psi\rangle$, 需要构造一个酉矩阵 $U$ 使得 $U|0\rangle = |\psi\rangle$. 易知 $U$ 的第一列为向量 $|0\rangle$, 因此需要构造 $U$ 除第 2 到第 n 列使该矩阵为一个酉矩阵. 根据上文中 0.4.6 对 Gram-Schmidt Process 的介绍, 不难看出 Gram-Schmidt Process 可以将一个线性无关向量组 $\{v_i\}$ 转化为用于构成酉矩阵的单位正交向量组 $\{\hat{u}_i\}$, 同时保证 $\hat{u}_1 = \frac{v_1}{|v_1|}$. 因此, 只需构造向量组 $|\psi\rangle, v_2, \ldots, v_n$ 其中 $v_2, \ldots, v_n$ 为随机向量, 再执行 Gram-Schmidt Process 就可以得到满足 $U|0\rangle = |\psi\rangle$ 的酉矩阵 $U$.

该过程具体代码如下:

```python
def generate_unitary(psi):
    dim = len(psi)  # Dimension of the state psi

    # Normalize the state vector
    psi_normalized = psi / np.linalg.norm(psi)

    # Create the unitary matrix
    U = np.zeros((dim, dim), dtype=complex)
    # Set the first column of U as the normalized state vector
    U[:, 0] = psi_normalized

    # Fill the remaining columns with
    #   arbitrary orthonormal vectors
    for i in range(1, dim):
        # Generate a random vector
        v = np.abs(np.random.randn(dim)).astype(complex)
        # Orthogonalize with respect to the previous columns
        v -= np.dot(U[:, :i], np.conj(U[:, :i]).T.dot(v))
        v /= np.linalg.norm(v)  # Normalize the vector
        U[:, i] = v

    return U.astype(complex)
```

# 5 结论与展望

本文实现了一种基于 Quantum Shannon Decomposition 的任意量子门分解算法. 该算法利用了量子信息理论中的 Shannon 分解定理, 将任意量子门分解成一

系列基本量子门的组合. 我们还对该算法进行了实验验证, 结果表明，该算法在 NISQ 阶段具有较高的效率和精度.

根据 Shende 等人的文章 [6], 任意 n-qubit 酉门分解后线路中 CNOT 门数量的理论下界为:

$$\frac{1}{4}(4^n - 3n - 1) \tag{5.20}$$

而优化过后的 Quantum Shannon Decomposition 的实现 CNOT 门数量下界能达到:

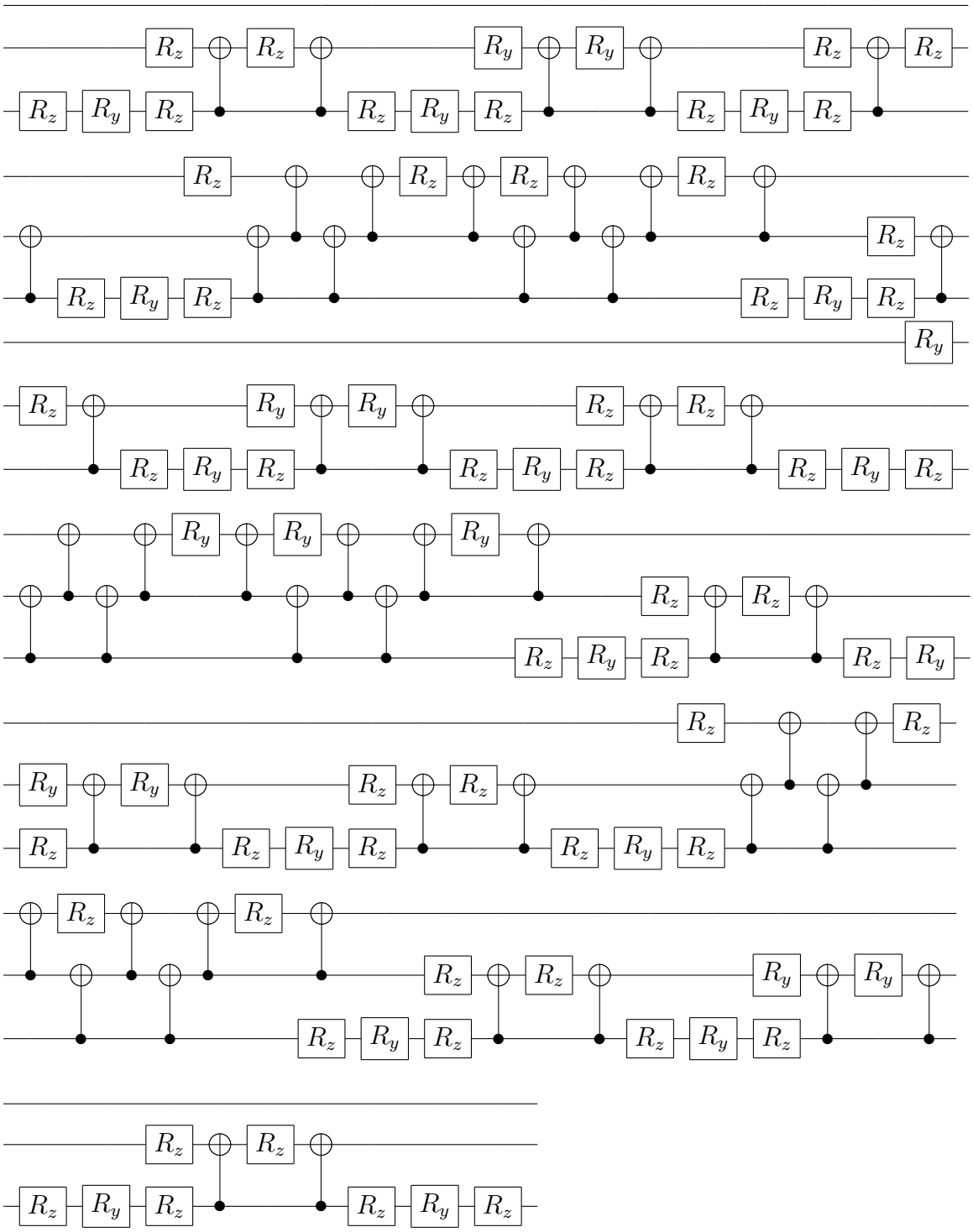
$$\frac{23}{48}4^n - \frac{3}{2}2^n + \frac{4}{2} \tag{5.21}$$

我们对 Quantum Shannon Decomposition 的实现在深度方面仍有一定的优化空间.

除此之外, 在未来的量子计算机发展中, 我们仍然需要在多个方面对该实现进行进一步改进和优化. 具体来说, 我们可以考虑以下几个方面:

- 实现该算法的离线版本, 最大化该算法的性能优势
- 改进算法的精度和效率, 使其在更大规模的量子计算机上运行更加高效
- 探索新的量子门分解算法, 以进一步优化门分解算法的性能, 线路深度和精度
- 研究该算法在量子计算相关细分领域的应用

# 6 附录: 3-qubit 酉门分解线路



# 参考文献


[1] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Phys. Rev. A*, vol. 52, pp. 3457–3467, Nov 1995. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.52.3457

[2] C. F. Loan, "The ubiquitous kronecker product," *Journal of Computational and Applied Mathematics*, vol. 123, no. 1, pp. 85–100, 2000, numerical Analysis 2000. Vol. III: Linear Algebra. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0377042700003939

[3] C. F. Van Loan and N. Pitsianis, *Approximation with Kronecker Products*. Dordrecht: Springer Netherlands, 1993, pp. 293–314. [Online]. Available: https://doi.org/10.1007/978-94-015-8196-7_17

[4] V. Bergholm, J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, "Quantum circuits with uniformly controlled one-qubit gates," *Physical Review A*, vol. 71, no. 5, may 2005. [Online]. Available: https://doi.org/10.1103%2Fphysreva.71.052330

[5] B. Drury and P. Love, "Constructive quantum shannon decomposition from cartan involutions," *Journal of Physics A: Mathematical and Theoretical*, vol. 41, no. 39, p. 395305, sep 2008. [Online]. Available: https://doi.org/10.1088%2F1751-8113%2F41%2F39%2F395305

[6] V. Shende, I. Markov, and S. Bullock, "Smaller two-qubit circuits for quantum communication and computation," in *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, vol. 2, 2004, pp. 980–985 Vol.2.