

# 带振幅放大的对偶量子算法 及其应用

(申请清华大学理学博士学位论文)

培养单位: 物理系

学 科: 物理学

研究 生: 朱 垣 眥

指 导 教 师: 龙 桂 鲁 教 授

二〇二二年九月



# **Duality quantum algorithm with amplitude amplification and its application**

Dissertation Submitted to

**Tsinghua University**

in partial fulfillment of the requirement

for the degree of

**Doctor of Philosophy**

in

**Physics**

by

**Zhu Yuanye**

Dissertation Supervisor: Professor Long Guilu

**September, 2022**



## 学位论文指导小组、公开评阅人和答辩委员会名单

### 公开评阅人名单

无（全隐名评阅）

### 答辩委员会名单

主席	范衍	研究员	中国科学院物理研究所
委员	何珂	教授	清华大学物理系
	龙桂鲁	教授	清华大学物理系
	李桂琴	副教授	清华大学物理系
	高健存	副教授	清华大学物理系
	何琼毅	教授	北京大学物理学院
	尹璋琦	教授	北京理工大学物理学院
秘书	皮竟辉	助理研究员	清华大学物理系



## 关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：

清华大学拥有在著作权法规定范围内学位论文的使用权，其中包括：（1）已获学位的研究生必须按学校规定提交学位论文，学校可以采用影印、缩印或其他复制手段保存研究生上交的学位论文；（2）为教学和科研目的，学校可以将公开的学位论文作为资料在图书馆、资料室等场所供校内师生阅读，或在校园网上供校内师生浏览部分内容；（3）根据《中华人民共和国学位条例暂行实施办法》及上级教育主管部门具体要求，向国家图书馆报送相应的学位论文。

本人保证遵守上述规定。

作者签名： 朱垣华

导师签名： 柳晓

日期： 2022.09.14

日期： 2022.09.14



## 摘要

量子信息科学是信息科学与量子力学的交叉学科，包括量子计算，量子通信与量子精密测量三个主要方向。量子计算运用量子并行性等量子力学独有的性质进行计算，相比于传统计算机在算力方面有大幅度的提升。然而传统的量子算法都是运用量子逻辑门的乘积去模拟量子态的酉演化。而近年来提出的量子计算的对偶模式可运用量子逻辑门的线性组合去模拟量子态的非酉演化。该算法丰富了量子算法的工具，为量子算法的研究提供了新的思路。然而每次通过量子计算对偶模式实现非酉算符都需要在量子线路结尾进行投影测量，因此得到有用计算结果是概率性的。这种概率性影响了量子计算的效率，因而需要使用带有振幅放大的对偶量子算法，即在对偶模式的结尾通过量子搜索算法来进行振幅放大以提高整体算法的成功概率。

本文首先研究了对初值不确定度具有高鲁棒性的搜索算法。这种搜索算法特别适合对偶量子计算。本文研究了带有振幅放大的对偶量子算法及其应用，研究成果主要包括以下三方面内容：

(1) 研究了 Grover-Long 量子搜索算法的成功概率，提出了对于数据库占比  $\lambda$  的不确定度具有高鲁棒性的量子搜索算法。该算法克服了 Grover-Long 算法须知道确切占比值  $\lambda$  才能进行量子搜索的问题。该算法在极端条件下，即对数据库占比值一无所知的情况下，面对量子计数算法引入的误差仍能达到较高成功率。而该算法作为基本量子算法，用于对偶量子算法的振幅放大算法。该部分成果对应于本文的第 3 章内容。

(2) 将带有振幅放大的对偶量子算法，应用于量子模拟领域提出了范畴化量子模拟算法，它不再基于群的结构而是基于张量范畴的结构进行模拟。这种方式使得之前部分不能被有效量子模拟的系统变得可能。范畴化量子模拟算法采用演生论编码，相比于还原论的量子编码方式更加节省量子比特资源。关于范畴化量子模拟这部分成果对应于本文的第 4 章内容。

(3) 将带有振幅放大的对偶量子算法应用于波动方程的求解问题，展示了求解偏微分方程的一种新的量子算法。该算法每次迭代与经典算法相比具有二次加速的特性。该部分成果对应于本文的 5 章内容。

**关键词：**量子计算；量子算法；张量范畴；非酉演化；量子模拟算法

## Abstract

Quantum information science is the intersection of information science and quantum mechanics, including quantum computing, quantum communication and quantum precision measurement. Quantum computing uses the unique properties of quantum mechanics, such as quantum parallelism, to perform calculations, which has a significant increase in arithmetic power compared to traditional computers. However, traditional quantum algorithms use the product of quantum logic gates to simulate the unitary evolution of quantum states. In recent years, the proposed duality model of quantum computing can use linear combinations of quantum logic gates to simulate the non-unitary evolution of quantum states. This algorithm has enriched the tools of quantum algorithms and provided new ideas for the research of quantum algorithms. However, each time the non-unitary operator is implemented by quantum computation in duality mode, a projection measurement at the end of the quantum line is required, and the useful computational results are probabilistic. This probabilistic nature affects the efficiency of quantum computation and thus requires the use of duality quantum algorithms with amplitude amplification, i.e., amplification is performed at the end of the duality mode by a quantum search algorithm to improve the overall success probability of the algorithm.

In this paper, we first investigate search algorithms with high robustness to initial value uncertainty. This search algorithm is particularly suitable for duality quantum computing. In this paper, the duality quantum algorithm with amplitude amplification and its applications are studied, and the research results include the following three main aspects.

(1) The success probability of the Grover-Long quantum search algorithm is studied, and a quantum search algorithm with high robustness to the uncertainty of the database occupancy ratio  $\lambda$  is proposed. The algorithm overcomes the problem that the Grover-Long algorithm must know the exact occupancy value  $\lambda$  in order to perform quantum search. The algorithm achieves a high success rate under extreme conditions, i.e., without knowledge of the database occupation value, in the face of the errors introduced by the quantum counting algorithm. The algorithm is used as a basic quantum algorithm for the amplitude amplification of the duality quantum algorithm. This part of the results corresponds to Chapter 3 of this paper.

(2) The duality quantum algorithm with amplitude amplification is applied to the

---

## Abstract

---

field of quantum simulation to propose a categorical quantum simulation algorithm, which is not based on the structure of the group but on the structure of the tensor category. This approach makes it possible to simulate systems that were previously partially unavailable for effective quantum simulation. The categorical quantum simulation uses emergenism coding, which is more economical in terms of quantum bits than reductionism coding. This part of the results on categorical quantum simulation corresponds to Chapter 4 of this paper.

(3) A new quantum algorithm for solving partial differential equations is demonstrated by applying the duality quantum algorithm with amplitude amplification to the solution of the wave equation. The algorithm has the property of quadratic acceleration in each iteration compared to the classical algorithm. This part of the results corresponds to Chapter 5 of this paper.

**Keywords:** Quantum computation; Quantum algorithm; Tensor category; Non-unitary evolution; Quantum simulation algorithm

## 目 录

摘 要 .....	I
Abstract .....	II
目 录 .....	IV
符号和缩略语说明 .....	VII
<b>第 1 章 绪论 .....</b>	<b>1</b>
1.1 量子计算与信息科学 .....	1
1.2 量子比特 .....	4
1.3 直积态与纠缠态 .....	7
1.4 量子不可克隆定理 .....	9
1.5 量子线路与量子计算的直乘模式 .....	9
1.6 非酉演化与量子计算的对偶模式 .....	15
1.7 开放量子系统与量子噪声 .....	18
1.8 量子纠错码 .....	20
1.9 Toric Code .....	22
1.10 范畴论与拓扑序 .....	25
1.11 本章小结 .....	28
<b>第 2 章 量子算法 .....</b>	<b>30</b>
2.1 量子傅里叶变换算法 .....	30
2.2 量子相位估计算法 .....	34
2.3 Shor 算法 .....	37
2.3.1 大数分解问题转化为求阶问题 .....	37
2.3.2 求阶问题的量子算法 .....	39
2.4 线性方程组求解的量子算法 .....	40
2.5 量子搜索算法 .....	42
2.5.1 Grover 搜索算法 .....	42
2.5.2 Grover-Long 算法 .....	45
2.5.3 定点搜索算法 .....	45
2.5.4 Yoder-Low-Chuang 搜索算法 .....	46

## 目 录

---

2.6 全量子本征求解器 .....	47
2.7 本章小结 .....	49
<b>第 3 章 高鲁棒量子搜索算法 .....</b>	<b>50</b>
3.1 背景介绍 .....	50
3.2 Grover-Long 算法的几何描述 .....	51
3.3 Grover-Long 算法的成功率与搜索迭代次数的关系 .....	53
3.4 对目标数量高鲁棒的量子搜索算法 .....	55
3.5 讨论 .....	59
3.6 本章小结 .....	61
<b>第 4 章 范畴化量子模拟的对偶量子算法 .....</b>	<b>62</b>
4.1 背景介绍 .....	62
4.2 量子线路的范畴结构 .....	64
4.3 不同学科的范畴论表述 .....	65
4.4 范畴化量子模拟的定义 .....	65
4.5 拓扑量子场论 .....	67
4.6 $SU(3)$ 杨-米尔斯理论的范畴化量子模拟算法 .....	70
4.7 讨论 .....	83
4.8 本章小结 .....	85
<b>第 5 章 波动方程行波解的对偶量子求解算法 .....</b>	<b>86</b>
5.1 背景介绍 .....	86
5.2 一阶波动方程求解的对偶量子算法 .....	88
5.3 行波耗散问题求解的对偶量子算法 .....	91
5.4 行波色散问题求解的对偶量子算法 .....	96
5.5 讨论 .....	101
5.6 本章小结 .....	103
<b>第 6 章 总结与展望 .....</b>	<b>104</b>
<b>参考文献 .....</b>	<b>106</b>
<b>附录 A 张量范畴基础知识简要 .....</b>	<b>116</b>
<b>致 谢 .....</b>	<b>121</b>
<b>声 明 .....</b>	<b>122</b>
<b>个人简历、在学期间完成的相关学术成果 .....</b>	<b>123</b>

## 目 录

---

指导教师学术评语 .....	124
答辩委员会决议书 .....	125

## 符号和缩略语说明

BQP	有界误差量子多项式时间 (Bounded error quantum polynomial time)
$\mathbb{C}$	复数
CPTP	正定保迹 (Completely positive trace-preserving)
FFT	快速傅里叶变换 (Fast Fourier transform)
FQH	分数量子霍尔效应 (Fractional quantum Hall effect)
MFC	多融合范畴 (Multi-fusion category)
NP	不确定多项式时间 (Non-deterministic polynomial time)
P	多项式时间 (Polynomial time)
PSPACE	多项式空间 (Polynomial space)
SET	对称性富化拓扑序 (Symmetry enriched topological order)
SL	特殊线性群 (Special linear group)
SPT	对称保护拓扑态 (Symmetry protected topological phase)
UFC	融合酉范畴 (Unitary fusion category)
UMTC	酉模张量范畴 (Unitary modular tensor category)
USFC	球状融合酉范畴 (Unitary spherical fusion category)



# 第 1 章 绪论

## 1.1 量子计算与信息科学

人类文明的发展始终伴随着信息记录与处理手段的提高。原始人在没有数的概念以前还谈不上算术运算。大概在公元前 3000-前 2500 年的古埃及出现了象形数字。在我国出土的距今约 4000 年前的甲骨文中出现了十进制的数字符号。直到上世纪 40 年代，随着电子计算机的出现，人类对于信息处理的能力大幅提升。这直接使得人类进入了信息时代。随着物理学与半导体工业的发展，人类运用晶体管取代了电子管，这使得计算机变得便携。这进一步增强了人类的信息处理能力。随着市场需求与半导体物理学的发展，人类不断地挑战技术的极限。不断地减小晶体管的尺寸。近些年来晶体管的发展经历了从最开始的平面场效应管到 25nm 制程以下的鳍式场效应管，到如今已经向 5nm 制程以下的闸极全环晶体管进行攻坚克难。摩尔定律<sup>[1]</sup>大致描述了半导体工业的发展规律。该定律由英特尔公司创始人戈登·摩尔提出，其内容为：在价格不变的前提下，集成电路上的晶体管数目每隔 18 个月翻一番，其运算性能也提升一倍。计算机处理器晶体管的数量如下图 6.1 所示。

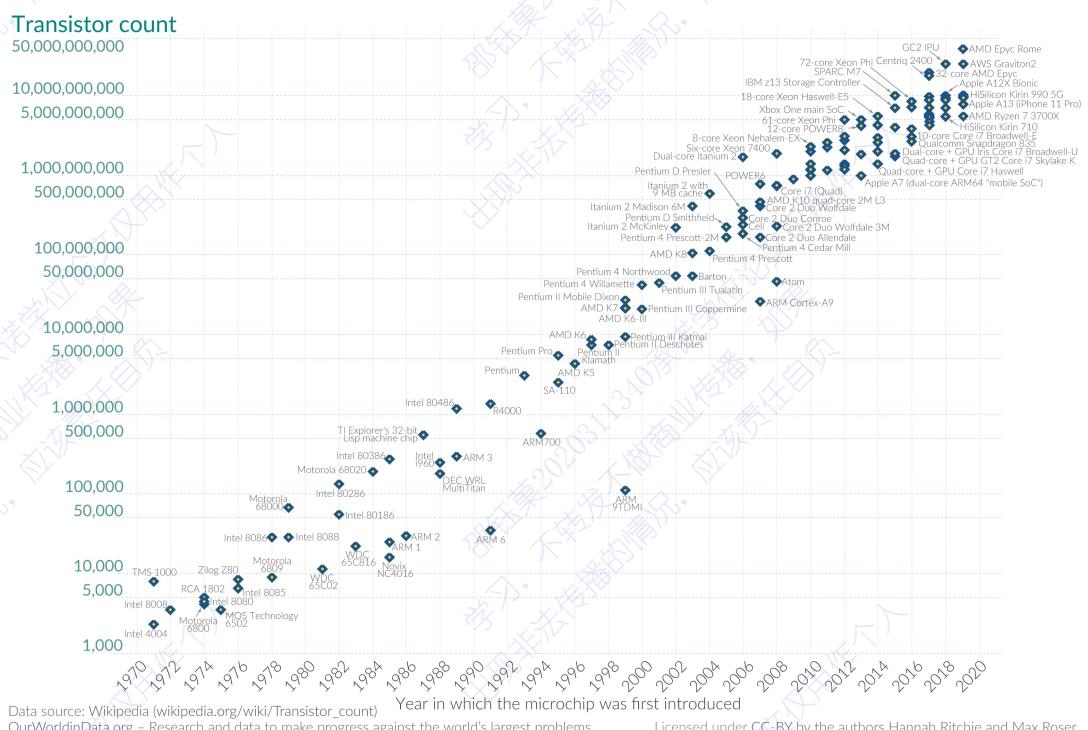
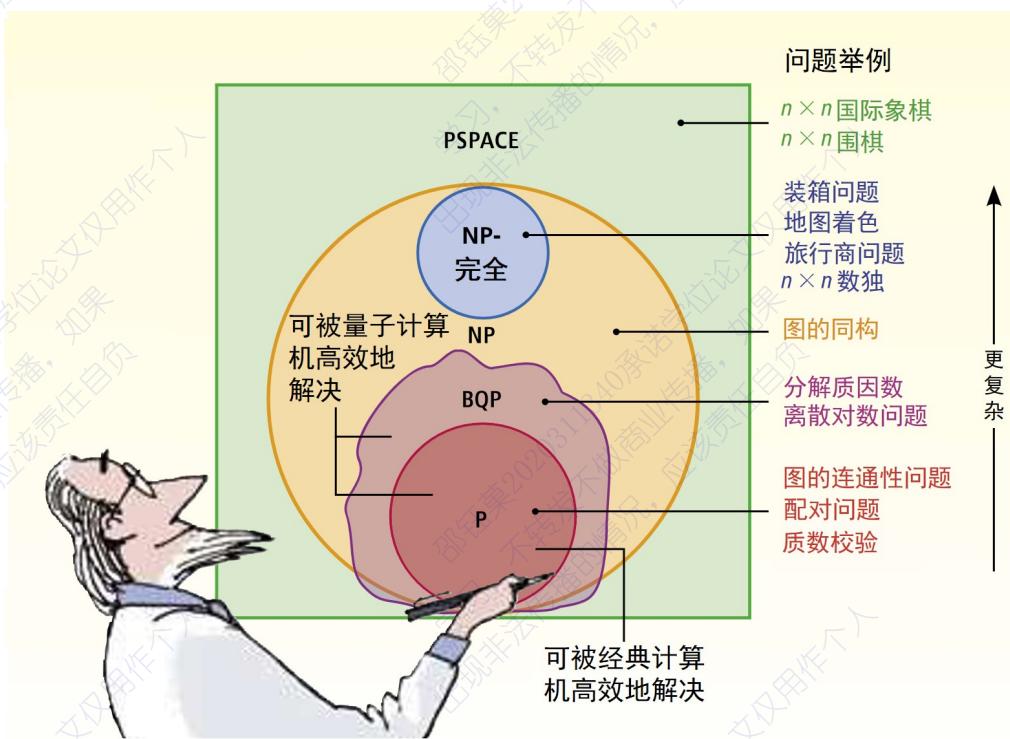


图 1.1 1970-2020 年计算机处理器晶体管的数量<sup>[2]</sup>

虽然摩尔定律时代运用的是等效制程的概念，但整体的趋势就是制程不断被减小。而不幸的是这个尺寸不可能无限制的小下去。因为当制程小到一定程度，材料的量子性质就会表现出来。其中最致命的就是量子隧穿效应。这会影响晶体管对电子的控制从而导致晶体管失效。另外一个无法逾越的瓶颈就是能量耗散问题。Landauer 定律指出，每不可逆地擦除单比特的信息量就要向环境至少释放  $kT \ln 2$  焦耳的热量<sup>[3-4]</sup>。而经典计算机的初始化以及运算过程都存在着不可逆过程，这使得计算机必须要向环境释放热量。这两点都制约半导体工业未来的发展，最终将导致摩尔定律的失效。有研究表明目前人类社会每年产生的数据量是阿伏伽德罗常数 ( $6 \times 10^{23}$ ) 量级<sup>[5]</sup>，而人类对于更高算力的追求是不会改变的。幸运的是，量子计算机可以克服经典计算机的瓶颈。首先量子计算机是基于量子力学原理的，不会因为量子效应而变得不可控制。其次量子计算机基于酉演化，这是可逆的，因此整个计算过程理论上不会产生热耗散。除此之外，量子计算机运用量子力学的基本特性——量子相干性，这令量子计算机拥有量子并行性，这使得量子算法相较于经典算法可以实现指数加速的特性。例如目前常见的 RSA 加密算法<sup>[6]</sup>，其加密的安全性来自于分解大数的时间复杂度。运用目前现有的超级计算机对一个几百位的大数进行分解需要数百年的时间才能完成。如果在实用化的量子计算机上使用 Shor 算法<sup>[7]</sup>则几分钟即可完成分解。因此一旦实用化量子计算机研制成功，此加密方式将变得不再安全。从这个例子可以看出量子计算机可以高效解决的问题要比经典计算机更加广泛。图 1.2 中的 BQP 区域描绘了量子计算机可高效解决的问题类别。BQP 即所有能用量子计算机在多项式时间内解决的问题。这里包括所有的 P 问题(在多项式时间内可给出答案的问题，即经典计算机可高效解决的问题类别)以及部分 NP 问题(经典计算机可在多项式时间内验证答案的问题类别)，例如因式分解，离散对数问题。此外 BQP 可能会超出 NP 达到 PSPACE 问题(不关注解决问题的时间，通过合理的内存可以解决的问题)，这意味着量子计算机在解决某些特定问题比经典计算机要快，甚至可以快速验证求解的答案。

量子计算机的发展经历了一些重要的阶段。美国物理学家 Benioff 在 1980 年运用量子力学语言描述了图灵机<sup>[9]</sup>。但这并不是真正意义上的量子图灵机。真正意义上的量子图灵机<sup>[10]</sup>是由 David Deutsch 于 1985 年提出，它完全建立在量子力学基本原理上，其中的量子寄存器可以储存由本征态所构成的叠加态，具有极好的并行性。物理学家 Richard Feynman 在 1982 年指出，运用经典计算机模拟量子系统会有很大的复杂度，甚至无法有效模拟常见大小的量子系统。如果用可控制的量子体系来模拟量子系统，其复杂度仅仅是多项式的形式而非指数形式<sup>[11]</sup>。1985 年他提出了运用可逆逻辑门作为基本单元来实现量子计算的模型机<sup>[12]</sup>。1989

图 1.2 量子计算机可解决的问题类别<sup>[8]</sup>

年 David Deutsch 提出了三比特量子逻辑门，以及量子计算机网络的概念<sup>[13]</sup>。1992 年，Berthiaume 和 Brassard 对于量子图灵机的速度快于经典图灵机的事实给出了严格的数学证明<sup>[14-15]</sup>。1994 年 Peter Shor 提出了质因数分解算法<sup>[7,16]</sup>。1997 年 Grover 提出了量子搜索算法<sup>[17]</sup>，这是对无序数据库的搜索，经典搜索算法需要  $O(N)$  次，而量子搜索算法只需要  $O(\sqrt{N})$  次。2012 年 John Preskill 提出了量子优越性的概念<sup>[18]</sup>即对于一个可编程的量子设备是否可以解决一个经典计算机无法解决的问题。在 2019 年谷歌公司声称实现了量子优越性<sup>[19]</sup>，他们通过控制 53 个超导量子比特仅仅 200 秒的时间就完成了经典计算机需要花费一万年完成的任务<sup>[20]</sup>。在量子纠错方面 Shor 与 Steane 等人提出了量子纠错理论<sup>[21-22]</sup>，Kitaev 则提出能够抵抗量子噪声的拓扑量子计算模型<sup>[23]</sup>。在量子计算机的实验层面，DiVincenzo 首先提出了构建量子计算机硬件的五条准则<sup>[24]</sup>。现在量子计算的硬件研究已经取得了不小的进展。高校，科研院所以及谷歌，IBM 等一大批科技公司都加入到了研究之中<sup>[25-26]</sup>。量子计算机比特数以及保真度的记录正不断地被刷新<sup>[20,27-30]</sup>。人们已经在超导系统<sup>[31-33]</sup>，离子阱系统<sup>[34-36]</sup>，半导体量子点系统<sup>[37-38]</sup>，以及核磁共振系统<sup>[39-41]</sup>实现了基本算法的演示。尽管目前几乎所有的体系都存在着尚未解决的问题。但通过科研工作者的努力，作者相信终究有一天这些问题会被科研工作者攻破，最终通用量子计算机会实现量产。

## 1.2 量子比特

虽然我们的世界并不是二元论的，但运用二进制来编码或者描述这个世界是最简洁的一种方式。正如《周易·系辞上》所云“易有太极，是生两仪，两仪生四象，四象生八卦，八卦定吉凶，吉凶生大业。”太极即亦阴亦阳，这是对万物最为宏观的描述。正是因为太极的描述如此宏伟且包罗万象，所以太极这个描述是宇宙万物整体的性质，个体的特征在这里被抹去。因此要描述具体的事物需要从第二个层次即两仪开始。由此来演生或者说描述万物。

在经典计算机中的二元论即二进制编码。它的每一位由 0 或 1 构成，这个二进制位称之为比特是二进制编码的最小信息单元。现实中任何由两种状态的实体都可以作为比特的物理载体。比如早期计算机运用晶体管的通断来作为比特的物理载体。随着半导体工业的发展，人们运用场效应管来替代原来的晶体管。现在则运用场效应管的高低电位，来作为计算机比特的物理载体。

在量子计算机中，量子比特是经典比特概念的推广。与经典比特不同的是，量子比特不仅仅只有 0 和 1 这两种状态。事实上每一位量子比特都是一个 2 维的希尔伯特空间。因此量子比特还可以处在 0 和 1 这两个状态的线性叠加态。即

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1.1)$$

其中  $|\alpha|^2 + |\beta|^2 = 1$ 。从式 (1.1) 可知，物理实现量子比特的系统需要具有正交的两个态，即  $|0\rangle$  和  $|1\rangle$  态。且该系统要存在满足量子力学基本原理的量子叠加态。即在不经过破坏性测量的前提下无法区分系统处在哪个状态。下面列举 3 个可作为量子比特物理实现的系统：

(1) 单光子可以作为量子比特的物理实现。量子化的光场是由一个个光子构成的。单个光子的能量  $E$  和动量  $\vec{P}$  满足普朗克-德布罗意方程组。

$$E = \hbar\omega, \quad \vec{P} = \hbar\vec{k} \quad (1.2)$$

其中  $\omega$  为光子的频率， $\vec{k}$  为光的波矢。虽然光子的自旋为 1，但是由于光子的质量为零，因此单光子的自旋角动量沿波矢方向只有两个取向，其大小为  $\pm\hbar$ 。这分别对应着光子左旋和右旋两种偏振态。在这里将这两种偏振态记为  $|L\rangle$  和  $|R\rangle$ ，通过光学器件可制备光子的叠加态，例如：

$$|x\rangle = \frac{1}{\sqrt{2}}(|R\rangle - |L\rangle), \quad i|y\rangle = \frac{1}{\sqrt{2}}(|R\rangle + |L\rangle) \quad (1.3)$$

这两个状态代表光子沿着  $x$  和  $y$  轴的线偏振状态。

(2) 恒定磁场  $\vec{B}$  中自旋为  $1/2$  的粒子（例如电子或者核自旋等）。其自旋在磁场方向（即  $z$  轴方向上）的投影有向上或者向下两个线性独立的状态，这两个状

态可以编码为  $|0\rangle$  和  $|1\rangle$  态。其能量大小为：

$$E = -\vec{\mu}_s \cdot \vec{B} = \pm \frac{e\hbar}{2m} B_z \quad (1.4)$$

其中， $\vec{\mu}$  为粒子的自旋磁矩， $m$  为粒子的质量。通过对系统施加共振频率的电磁波脉冲，并精准控制时长和功率即可实现对系统的控制。

(3) 利用原子或离子的基态  $E_0$  和第一激发态  $E_1$  也可实现一个量子比特。在这里选择基态  $E_0$  为 0 态，第一激发态  $E_1$  为 1 态。在稳态下原子或者离子处于基态。如果运用频率为  $\frac{E_1-E_0}{\hbar}$  的光来照射原子或者离子，通过严格控制照射脉冲的时长。系统可以被制备到任意的叠加态上：

$$\alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1 \quad (1.5)$$

一般情况下单量子比特可以表示为

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad (1.6)$$

考虑到归一化条件  $|a|^2 + |b|^2 = 1$ ，因此可以运用三个参数  $\gamma, \theta, \varphi$  把式 (1.6) 表示为

$$|\psi\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right) \quad (1.7)$$

对于单个量子比特全局相位没有可观测效应，因此一个量子位通常只用两个参数  $\theta, \varphi$  来表示

$$|\psi\rangle = \left( \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right) \quad (1.8)$$

众所周知，描述量子态的波函数是复数而非实数，这不同于经典力学。因此描述量子比特的波函数看起来并没有那么直观。式 (1.8) 是  $SU(2)$  群表示空间内的矢量。这是复空间中的向量。而我们熟悉的几何大多为实空间。因此可以把式 (1.8) 映射到我们熟悉的实空间旋转群（即  $SO(3)$  群）的表示空间上。这种映射即是式 (1.8) 对于泡利矩阵  $\sigma_x, \sigma_y, \sigma_z$  的测量值。在这种映射下描述量子态的向量变为  $(\langle \psi | \sigma_x | \psi \rangle, \langle \psi | \sigma_y | \psi \rangle, \langle \psi | \sigma_z | \psi \rangle)$  即  $(\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$ 。这个矢量叫做 Bloch 矢量，这种直观的表示则称作单比特的 Bloch 球表示<sup>[42]</sup>（如图 1.3）。Bloch 球为一个单位球，球面上的点由两个方位角参数  $\theta, \varphi$  确定。每一个球面上的点都对应式 (1.8) 的一种状态。这些球面上的点代表量子比特的纯态。

此外，Bloch 球还可以表示量子比特的混态。量子态的混态一般采用密度矩阵  $\rho$  来表示。对于单量子比特其密度矩阵  $\rho$  是一个二阶厄米矩阵，可以在泡利算子基下展开

$$\rho = \frac{1}{2} (I + \vec{p} \cdot \vec{\sigma}) \quad (1.9)$$

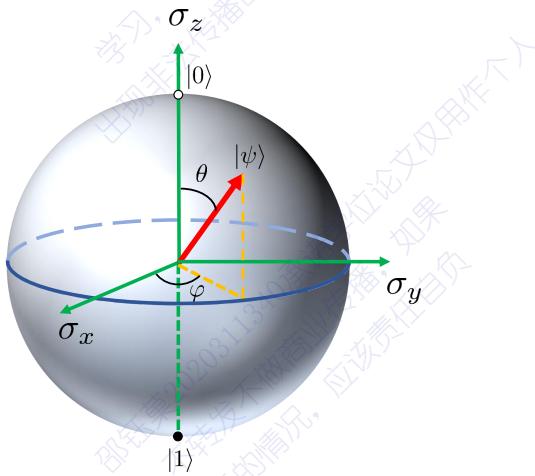


图 1.3 单量子比特的 Bloch 球表示

其中  $\vec{p}$  是一个 3 维向量，称为 Bloch 矢量。其模长可度量一个量子态的纯度。当  $|\vec{p}| = 1$  时  $\rho^2 = \rho$  对应于单量子比特的纯态。可以证明，当  $|\vec{p}| \leq 1$  时对应量子态的混态。因此直观地说，在图 1.3 中球面上的点对应纯态，而球内的点则对应混态。

介绍完了单量子比特，下面介绍多量子比特。由多个单量子比特组成的系统叫做量子存储器。对于一个  $n$  量子比特的量子存储器来说，它是由  $n$  个单量子比特直积构成的。该量子存储器拥有  $2^n$  个相互独立且正交的运算基底  $\{|i\rangle\}$ ，这些基底张成一个  $2^n$  维的希尔伯特空间。这个空间中任意的量子态  $|\psi\rangle$  可表示为这组基底的线性组合

$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle \quad (1.10)$$

其中  $c_i$  是线性叠加系数，代表不同基底的概率幅。对于一个  $n$  位的经典存储器来说每次只能储存 0 到  $n-1$  这  $n$  个数字其中之一。而对于一个  $n$  位的量子存储器来说一次可以同时存储 0 到  $2^{n-1}$  这所有的  $2^n$  个数字。例如  $n = 500$ ，只需要 500 个量子比特即可存储 0 到  $2^{500}$  所有的数字，而  $2^{500}$  比宇宙中全部的粒子数量还要多。因此经典计算机每次运算只能针对经典存储器上的一个数据进行运算操作，而量子计算机每次则可针对量子存储器上这  $n$  个数据同时进行操作。因此量子计算机的并行性与存储能力都远超于经典计算机。而量子计算机的这种能力则来源于量子叠加态与量子纠缠。在下一节 1.3 将介绍这部分的内容。

### 1.3 直积态与纠缠态

一个量子多体系统的子系统之间一般都存在着关联。式(1.11)给出了多体量子态的一般化描述

$$|\psi\rangle = \sum_{j_1 j_2 \cdots j_N} C_{j_1 j_2 \cdots j_N} |j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_N\rangle \quad (1.11)$$

其中  $\{|j_1\rangle, |j_2\rangle, \dots |j_N\rangle\}$  为  $N$  个子系统希尔伯特空间的基底,  $C_{j_1 j_2 \cdots j_N}$  为一个  $N$  阶张量。如果这个张量可以写成  $N$  个一阶张量的直积(如式(1.12)), 那么这个多体系统对应的量子态叫做直积态。或者称为可分离态。

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_N\rangle \quad (1.12)$$

其中每一项  $|\psi_n\rangle$  为

$$|\psi_n\rangle = \sum_{j_n} C_{j_n}^{(n)} |j_n\rangle \quad (1.13)$$

如果该量子多体系统对应的量子态  $|\psi\rangle$  不能分离成式(1.12)的形式则称该量子态为纠缠态。量子纠缠有着很多新奇的现象。其中最著名的则是 EPR 佯谬。1935 年 Einstein, Podolsky 和 Rosen 发表论文<sup>[43]</sup>, 以佯谬的形式对量子力学的哥本哈根诠释提出质疑, 并希望通过理想实验来证明量子力学是否是不完备的。文中对于 A, B 两粒子纠缠体系的波函数定义为

$$\Psi(x_A, x_B) = \int_{-\infty}^{\infty} dp e^{\frac{2\pi i}{\hbar}(x_A - x_B + x_0)p} = 2\pi\hbar\delta(x_A - x_B + x_0) \quad (1.14)$$

对于两个自旋  $1/2$  粒子的体系, Bohm 给出其纠缠态的简化表达式<sup>[44]</sup>

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B) \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B) \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) \end{aligned} \quad (1.15)$$

这些态称之为贝尔态。贝尔态也是一组正交完备的基底。即空间中任何量子态都可以在这组正交完备基底下展开。后来物理学家贝尔为了解决对于量子力学是否完备这个问题的争论提出了著名的贝尔不等式<sup>[45-46]</sup>, 并证明任何定域隐变量理论都必须满足贝尔不等式(式(1.16))

$$|P(\vec{m}, \vec{n}) - P(\vec{m}, \vec{l})| \leq 1 + P(\vec{n}, \vec{l}) \quad (1.16)$$

其中  $\vec{n}, \vec{l}, \vec{m}$  代表三个测量的方向。以  $P(\vec{m}, \vec{n})$  为例,  $P(-, -)$  的表达式为

$$P(\vec{m}, \vec{n}) = \int d\lambda \rho(\lambda) A(\vec{m}, \lambda) B(\vec{n}, \lambda) \quad (1.17)$$

该式描述的是粒子  $A$  在  $\vec{m}$  方向上观测量与粒子  $B$  在  $\vec{n}$  方向上观测量的关联函数。其中  $\lambda$  为隐变量,  $\rho(\lambda)$  为一个未知的概率分布。关于贝尔不等式证明过程如下:

$$\begin{aligned} P(\vec{m}, \vec{n}) - P(\vec{m}, \vec{n}') &= \int d\lambda \rho(\lambda) [A(\vec{m}, \lambda) B(\vec{n}, \lambda) - A(\vec{m}, \lambda) B(\vec{n}', \lambda)] \\ &= \int d\lambda \rho(\lambda) \{A(\vec{m}, \lambda) B(\vec{n}, \lambda) [1 \pm A(\vec{m}', \lambda) B(\vec{n}', \lambda)]\} \quad (1.18) \\ &\quad - \int d\lambda \rho(\lambda) \{A(\vec{m}, \lambda) B(\vec{n}', \lambda) [1 \pm A(\vec{m}', \lambda) B(\vec{n}, \lambda)]\} \end{aligned}$$

由于  $A(-, \lambda)$  与  $B(-, \lambda)$  的值域为  $[-1, 1]$ , 因此可得

$$\begin{aligned} |P(\vec{m}, \vec{n}) - P(\vec{m}, \vec{n}')| &\leq \int d\lambda \rho(\lambda) [1 \pm A(\vec{m}', \lambda) B(\vec{n}', \lambda)] \\ &\quad + \int d\lambda \rho(\lambda) [1 \pm A(\vec{m}', \lambda) B(\vec{n}, \lambda)] \quad (1.19) \\ &= 2 \pm [P(\vec{m}', \vec{n}') + P(\vec{m}', \vec{n})] \end{aligned}$$

令  $\vec{m}' = \vec{n}' = \vec{l}'$ , 同时设定 AB 在相同方向的测量结果相反, 比如 AB 量子态为  $|\phi^-\rangle$ , 即  $P(\vec{l}, \vec{l}) = -1$ , 可以推导得出  $P(\vec{l}, \vec{n}) = P(\vec{n}, \vec{l})$ , 则

$$|P(\vec{m}, \vec{n}) - P(\vec{m}, \vec{n}')| \leq 2 \pm [-1 + P(\vec{n}, \vec{l})] \quad (1.20)$$

由于  $-1 + P(\vec{m}, \vec{l}) < 0$ , 则可以得到贝尔不等式。

$$|P(\vec{m}, \vec{n}) - P(\vec{m}, \vec{n}')| \leq 1 + P(\vec{n}, \vec{l}) \quad (1.21)$$

如果抛开 AB 在相同方向测量结果相反这一假设, 由公式 (1.19) 可以直接推导出更一般的 CHSH 不等式<sup>[47]</sup>

$$P(\vec{m}, \vec{n}) - P(\vec{m}, \vec{n}') + P(\vec{m}', \vec{n}') + P(\vec{m}', \vec{n}) \leq 2 \quad (1.22)$$

这是贝尔不等式的推广。

在贝尔不等式提出后关于其验证实验不胜枚举<sup>[48-52]</sup>, 但这些实验都因存在着漏洞而饱受争议。关于贝尔不等式最有说服力的实验验证是在 2015 年完成的<sup>[53]</sup>, 该工作证实了贝尔不等式是不成立的。至此结束了物理学家对于量子力学是否是完备的这一问题的旷世争论, 量子纠缠这种新奇的现象终于被人们所认可。

## 1.4 量子不可克隆定理

量子不可克隆定理<sup>[54]</sup>是量子力学中的重要推论，具体表述为：不可能对于任意未知的量子态进行复制。这里做一个简单的证明。假设存在一个系统，其中的算符  $U$  可以对未知的量子态进行克隆。则对于任意的两个量子态  $|\phi_1\rangle$  和  $|\phi_2\rangle$

$$\begin{aligned} U(|\phi_1\rangle \otimes |k\rangle) &= |\phi_1\rangle \otimes |\phi_1\rangle \\ U(|\phi_2\rangle \otimes |k\rangle) &= |\phi_2\rangle \otimes |\phi_2\rangle \end{aligned} \quad (1.23)$$

可以看出式 (1.23) 是经过算符  $U$  把初态  $|k\rangle$  克隆为未知的量子态  $|\phi_1\rangle$  或  $|\phi_2\rangle$ 。由于此系统是封闭系统，因此算符  $U$  必定是酉操作，即

$$U^\dagger U = UU^\dagger = I \quad (1.24)$$

由式 (1.23) 和式 (1.24) 可得

$$(\langle k| \otimes \langle \phi_1|) U^\dagger U (|\phi_2\rangle \otimes |k\rangle) = (\langle \phi_1| \otimes \langle \phi_1|) (|\phi_2\rangle \otimes |\phi_2\rangle) \quad (1.25)$$

经过化简可得

$$\langle \phi_1 | \phi_2 \rangle = |\langle \phi_1 | \phi_2 \rangle|^2 \quad (1.26)$$

$\langle \phi_1 | \phi_2 \rangle$  只可能是 0 或 1。即  $|\phi_1\rangle$  与  $|\phi_2\rangle$  必定相同或正交。这与假设的  $|\phi_1\rangle$  与  $|\phi_2\rangle$  是两个任意量子态相矛盾。则假设的反面也就是量子不可克隆定理成立。正是由于此定理的成立，任何人无法在不破坏量子态的情况下得到该量子态的全部信息。

## 1.5 量子线路与量子计算的直乘模式

经典计算机程序的运行是基于包含导线和逻辑门的电子线路，与此类似，量子计算机算法的运行则基于包含量子比特 [图 1.4 (a), (b)]，量子逻辑门 [图 1.4 (c), (f), (g)] 以及量子测量 [图 1.4 (e)] 的量子线路。与经典电子线路类比，在量子线路中一根导线代表一个量子比特。

量子线路与经典电路不同的是。第一，量子计算机进行的是可逆运算，因此量子线路中没有扇入操作。第二，由于量子不可克隆定理的存在，量子线路中也没有扇出操作。第三，在量子线路中按照时序从左到右依次执行线路中的操作。因此在量子线路中是不存在回路的，所以是不存在反馈电路的。第四，量子线路的结尾可以存在测量操作，这个操作是非酉的，在完成测量后量子比特退化为经典比特 [图 1.4 (d)]。第五，量子计算机是以量子态为载体携带信息的，因此这里的量子逻辑门操作要满足量子力学的演化规律。而量子力学指出若要保证量子信息不丢失（即量子态保持相干性）则施加的操作必须是酉变换。因此量子逻辑门必

须是酉的。量子逻辑门包括单比特门 [图 1.4 (c)]，两比特门 [图 1.4 (f)] 和多比特门 [图 1.4 (g)]。下面将逐一介绍。

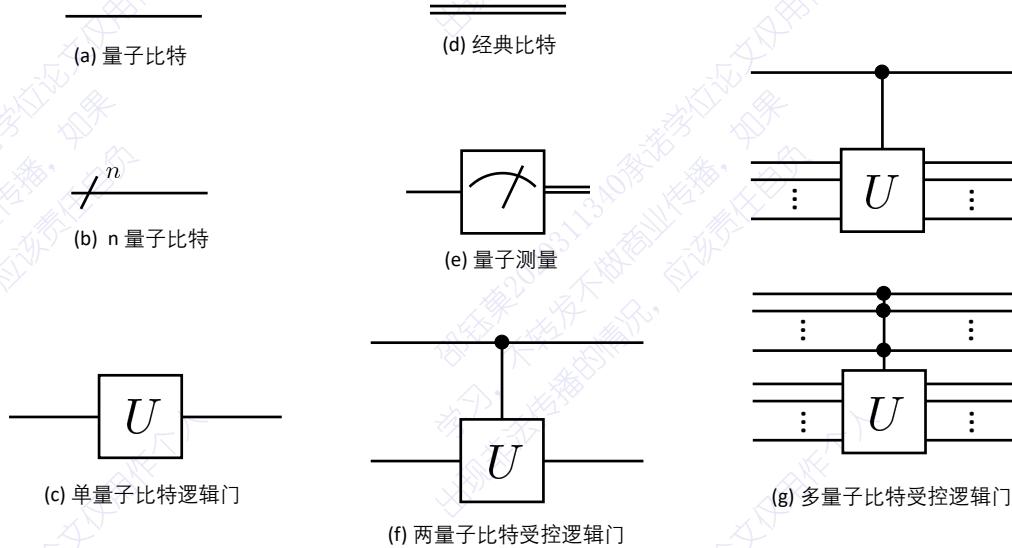


图 1.4 量子逻辑门

在量子力学中，封闭系统量子态的演化满足薛定谔方程

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = H|\psi(t)\rangle \quad (1.27)$$

其中  $H$  代表系统的哈密顿量算符。只要给定初态  $|\psi(0)\rangle$ ，通过方程即可求解出末态

$$|\psi(T)\rangle = U(T)|\psi(0)\rangle \quad (1.28)$$

其中演化算符  $U(T)$  的具体形式由下式给出

$$U(T) = \mathcal{T} \exp \left[ -\frac{i}{\hbar} \int_{t=0}^T H(t) dt \right] \quad (1.29)$$

其中  $\mathcal{T}$  为编时算符，因为在量子态演化的过程中不同时刻的哈密顿量一般都是非对易的，所以这里运用编时算符来强调积分运算时要按照时序进行，不可以调换积分的次序。在量子计算机中我们习惯于把系统简化为封闭系统模型来讨论，即系统与环境之间既不存在物质交换也不存在能量交换。在这种情况下  $U(T)$  为酉算符，即满足性质

$$U^\dagger U = UU^\dagger = I \quad (1.30)$$

量子计算就是对于量子态施加一系列设计好的量子逻辑门操作的过程，而量子逻

辑门操作就是一系列的酉演化。对于单量子比特的操作称为单量子比特逻辑门，所有的单量子比特逻辑门构成  $SU(2)$  李群。该群所对应的李代数的生成元为泡利算子

$$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (1.31)$$

由于  $SU(2)$  群与  $SO(3)$  群存在群同态的关系，因此可以用 Bloch 球（图 1.3）形象地表示量子态的演化。绕着 Bloch 球 3 个坐标轴旋转任意角度的量子逻辑门对应如下

$$\begin{aligned} R_x(\theta) &= e^{-i\theta\sigma_x/2} = \begin{bmatrix} \cos(\theta/2) & -i \sin(\theta/2) \\ -i \sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \\ R_y(\theta) &= e^{-i\theta\sigma_y/2} = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \\ R_z(\theta) &= e^{-i\theta\sigma_z/2} = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix} \end{aligned} \quad (1.32)$$

一个绕任意轴  $\vec{n}$  的三维旋转操作  $R_n(\theta)$  可表示为绕着两个不平行的定轴转动。这里选取这两个定轴为  $y$  轴与  $z$  轴。在这种情况下，任意三维旋转操作的算符如下

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos(\gamma/2) & -e^{i(\alpha-\beta/2+\delta/2)} \sin(\gamma/2) \\ e^{i(\alpha+\beta/2-\delta/2)} \sin(\gamma/2) & e^{i(\alpha+\beta/2+\delta/2)} \cos(\gamma/2) \end{bmatrix} \quad (1.33)$$

其中  $e^{i\alpha}$  为全局相位因子。

介绍完一般的情况，下面将介绍常用的单比特逻辑门。常用的单量子比特逻辑门包括量子非门，沃尔什-哈达玛门，以及量子相位门。量子非门与经典非门的作用类似，它的作用是把  $|0\rangle$  变换为  $|1\rangle$ ， $|1\rangle$  变换为  $|0\rangle$ 。量子非门具体的作用效果如图 1.5。

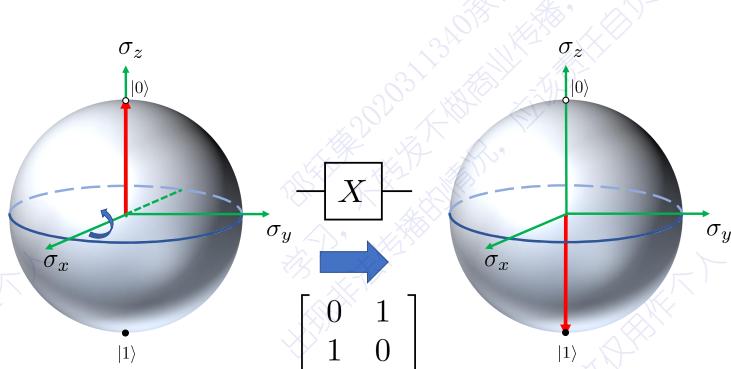


图 1.5 量子非门

沃尔什-哈达玛门也是一种极为常见的单量子比特门，它的作用是把  $|0\rangle$  变换为  $|0\rangle$  和  $|1\rangle$  的均匀叠加态  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ，将  $|1\rangle$  变换为另一均匀叠加态  $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ ，沃尔什-哈达玛门具体的作用效果如图 1.6。

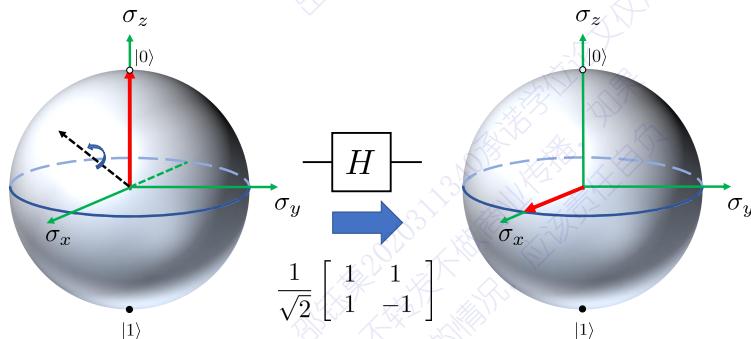


图 1.6 沃尔什-哈达玛门

量子相位门则是使量子态绕着  $z$  轴旋转相应的角度，其中  $T$  门 ( $\frac{\pi}{8}$  相位门) 代表绕着  $z$  轴旋转  $\frac{\pi}{4}$ ， $S$  门 ( $\frac{\pi}{4}$  相位门) 代表绕着  $z$  轴旋转  $\frac{\pi}{2}$ ， $Z$  门 ( $\frac{\pi}{2}$  相位门) 代表绕着  $z$  轴旋转  $\pi$ 。量子相位门具体的作用形式如图 1.7。

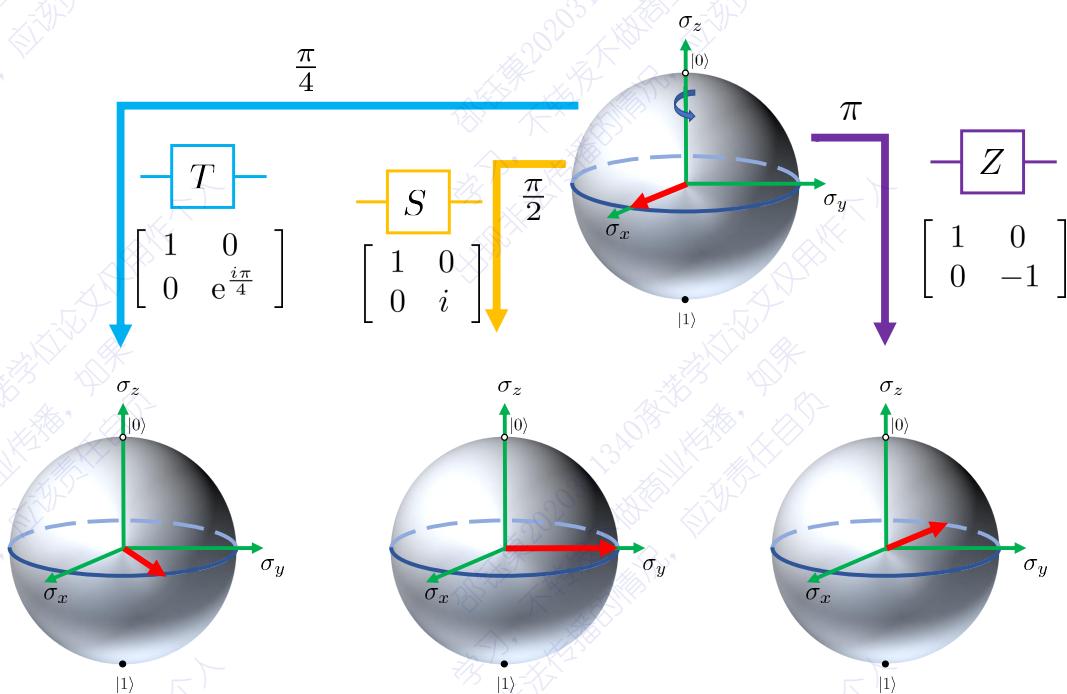


图 1.7 量子相位门

介绍完了单量子比特门，下面开始介绍两量子比特门。两量子比特张起了一个 4 维希尔伯特空间，其态空间的酉变换由  $4 \times 4$  的酉矩阵表示。两个单量子比特

门的直积是两量子比特门。但是这种两量子比特门过于平凡。要实现量子运算，则需要比特之间进行交流，进而实现逻辑运算。这种逻辑运算是通过 $4 \times 4$ 酉变换的一个重要子集——受控  $U$  门操作  $C(U)$  来实现的。受控  $U$  门操作如图 1.4-(f)，其算符表达形式如下

$$C(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U \quad (1.34)$$

上式表示只有当第一量子比特处在  $|1\rangle$  态时，才对第二量子比特施加  $U$  操作。其中第一量子比特称为控制位，第二量子比特称为目标位。最常见的受控  $U$  门为 CNOT 门（或者称为受控非门），其矩阵表示为：

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (1.35)$$

其作用规则为，当控制位处于  $|0\rangle$  态时不对目标位做任何操作，当控制位处于  $|1\rangle$  态时，对目标位做  $\sigma_x$  操作，具体的作用效果如图 1.8。

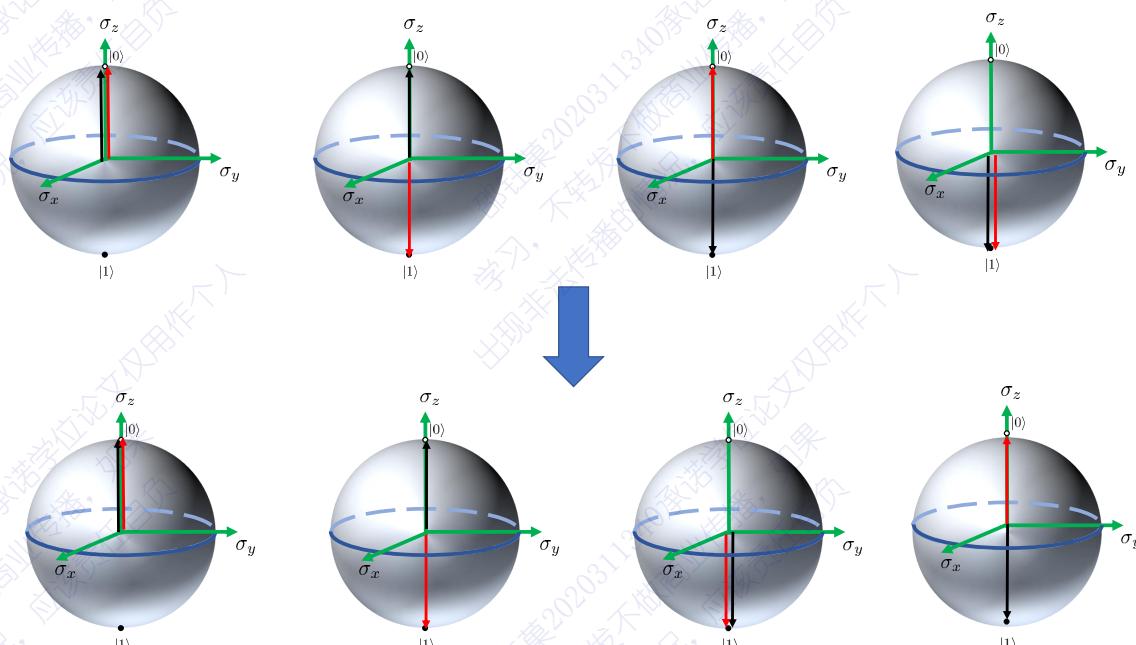


图 1.8 两量子比特受控非门

对于受控  $U$  门并不局限于控制位为单量子比特，可以推广到有  $n$  个控制位的受控门  $C^n(U)$ ，其作用效果如下

$$C^n(U)|x_1x_2 \cdots x_n\rangle|\psi\rangle = |x_1x_2 \cdots x_n\rangle U^{x_1x_2 \cdots x_n}|\psi\rangle \quad (1.36)$$

其中  $U$  的指数  $x_1x_2 \cdots x_n$  代表  $x_1, x_2, \dots, x_n$  的乘积，当且仅当  $x_1, x_2, \dots, x_n$  均为 1 时才对控制位施加  $U$  操作。对于两量子比特以上的操作称为多量子门，但并不是所有的多量子门都可以拆解成单量子门的直积形式。Barenco 等给出证明：任意多量子门可以拆解成单量子门和两量子受控非门的组合<sup>[55-56]</sup>。例如 Toffoli 门的拆解如图 1.9。提到量子门的拆解，大家关心的一定是通用量子逻辑门集合是否存在。下面将介绍通用量子逻辑门。

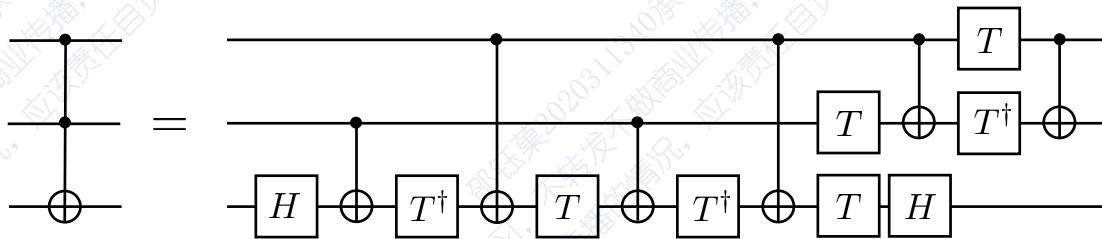


图 1.9 Toffoli 门的拆解

对于经典计算机来说，只需要实现或非门操作，即可通过或非门操作的组合来实现所有的逻辑门操作。但是对于量子计算机来说，由于量子比特是存在纠缠的，且一个  $n$  量子比特系统若要实现全局控制，则要求所有的门操作要构成  $SU(2^n)$  群，这是一个李群，没有办法通过有限个生成元来生成这个群。但是如果给定允许的误差  $\epsilon$ ，还是可以通过有限个元素（基本量子逻辑门）的组合来近似地逼近任意量子逻辑门。例如，量子门  $U$  可以通过  $t$  个基本量子逻辑门去实现

$$\|U - U_t \cdots U_2 U_1\| \leq \epsilon \quad (1.37)$$

其中范数  $\|\cdot\|$  对于任意矩阵  $A$  的定义为

$$\|A\| = \max_{|\psi\rangle} \frac{\langle \psi | A^\dagger A | \psi \rangle}{\langle \psi | \psi \rangle} \quad (1.38)$$

事实上，对于任意的单量子门在给定误差的情况下，通过施加有限个沃尔什-哈达玛门和  $T$  门 ( $\frac{\pi}{8}$  相位门) 即可实现。因此  $\{H, T, \text{CNOT}\}$  构成一组通用量子门集合。通用量子门集合并不唯一，比如  $\{H, S, \text{CNOT}, \text{Toffoli}\}$  也可以构成一组通用量子逻辑门。Solovay-Kitaev 定理<sup>[57-58]</sup>指出：需要施加  $t$  个量子门的量子线路，在给定误差  $\epsilon$ ，如果运用通用量子逻辑门集合来实现这些操作时，则运用通用量子逻辑门的数量为  $t \cdot \text{poly}(\log(t/\epsilon))$ 。由此可以看出使用通用量子逻辑门集合并不会过多增加量子线路的复杂度。此外还可以得出推论：并不存在某一种通用量子逻辑门集合相比其他的通用量子逻辑门集合存在绝对优势。如果某一个量子体系能够实现某一组通用量子逻辑门集合，则这种量子体系可实现通用量子计算。通用量

子计算是无法被经典计算机有效模拟的。因为 Gottesman-Knill 定理<sup>[59-60]</sup>指出：只有当量子线路仅包含 Cifford 群（生成元为： $\langle H, S, \text{CNOT}, \text{C}(Z) \rangle$ ）的群元时，才可以被经典计算机有效模拟。但事实上 Cifford 群加上  $T$  门才构成一组通用量子逻辑门集合。

本节介绍了基本量子逻辑门与量子线路，传统的量子算法都是通过量子逻辑门的乘积来模拟酉演化的过程。这种传统的模式叫做量子计算的直乘模式。然而这种模式是存在局限性的，因为并不是所有的数学算符都具有酉的性质。如果要扩大量子计算机的适用范围，则需要突破量子计算机的直乘模式，找到可以运用量子逻辑门模拟非酉演化的模式，而这种模式叫做量子计算的对偶模式。下一节将介绍这部分内容。

## 1.6 非酉演化与量子计算的对偶模式

在 20 世纪末期对于量子算法的研究主要集中在这几个方面，以 Shor 算法<sup>[7,16]</sup>为基础的解决含隐子群问题的算法，以 Grover 算法为代表的量子搜索算法<sup>[17,61]</sup>等，除此之外，几乎没有具有框架性质的量子算法产生。但令人欣慰的是在 21 世纪初期量子算法取得了一些突破性进展。比如，以求解线性方程组算法<sup>[62]</sup>为基础的一类量子机器学习算法，还有就是由清华大学龙桂鲁教授课题组提出的量子计算的对偶模式<sup>[63-65]</sup>。在该框架下，量子计算机可以实现非酉量子门。通过将非酉算符拆解成酉算符线性组合的形式，再通过投影测量即可实现非酉量子门操作。量子计算机对偶模式的数学原理由 Gudder 给出<sup>[66]</sup>。对偶量子计算通过对辅助比特空间进行投影测量进而实现非酉演化操作。因此该算法是存在失败概率的。但毫无疑问量子计算机的对偶模式为量子算法的研究提供了新的思路，可以解决之前无法解决的问题。而且该算法可以带来相较于经典算法加速的效果<sup>[67-69]</sup>。其中的投影测量可以运用第 3 章提出的搜索算法进行概率幅放大来等效地实现。

量子计算机的对偶模式是指在一台比特数为  $n$  的量子计算机中通过增加一个维度为  $d$  的辅助比特希尔伯特空间，使其可以模拟具有  $d$  条非对称路径的  $n$  比特对偶量子计算机。在这种模式下量子计算机可以实现形式为  $\sum_{i=0}^{d-1} p_i U_i$  的非酉量子门操作。其中  $p_i$  是模长小于 1 的复数。 $\sum_i p_i$  是模长小于等于 1 的复数。形象地说，量子计算机的对偶模式可以看作一个具有  $d$  条狭缝的量子干涉仪，在每条路径上施加不同的酉量子门操作。最后在接收端对某条狭缝输出的量子态进行测量，得到计算结果。其过程如图 1.10 所示

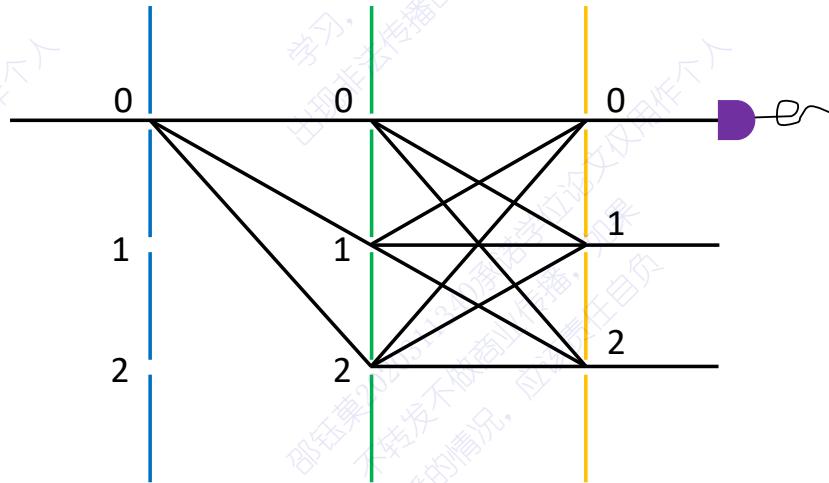


图 1.10 对偶量子计算机的理想工作模式示意图

其中第一个过程为波函数经过狭缝的过程，这个过程用分波算符  $D_m$  来表示

$$D_m \psi = \bigoplus_{i=0}^{d-1} (p_i \psi) \quad (1.39)$$

该算符的作用是将量子态从原本的希尔伯特空间  $\mathcal{H}$  映射到高维度希尔伯特空间  $\mathcal{H}^{\oplus d}$ ，其中  $\sum_{i=0}^{d-1} |p_i|^2 = 1$ 。接下来在每一个子空间内进行量子逻辑门操作。最后进行干涉，这个过程用合波算符  $C_m$  来表示：

$$C_m (\psi_0 \oplus \psi_1 \oplus \dots \oplus \psi_{d-1}) = \sum_{i=0}^{d-1} q_i \psi_i \quad (1.40)$$

其中  $\sum_{i=0}^{d-1} |q_i|^2 = 1$ 。经过合波算符作用的量子态从高维度的希尔伯特空间  $\mathcal{H}^{\oplus d}$  又映射回原本的希尔伯特空间  $\mathcal{H}$ 。

在实际的量子线路中则需要通过增加辅助比特来实现对偶量子计算。在此框架下可以实现非酉量子门操作。易证任何有界非酉线性算子都可以表示成酉算符的线性组合。通过对偶量子计算实现的非酉量子门具有的一般形式为

$$L_c = \sum_{i=0}^{d-1} c_i U_i \quad (1.41)$$

其中  $U_i$  是酉算符， $c_i$  为复数，满足

$$\sum_{i=1}^{d-1} |c_i| \leq 1 \quad (1.42)$$

众所周知，对于封闭量子系统其时间演化算符是酉的。但是对于开放系统其时间演化算符是非酉的，通过 Naimark 扩张<sup>[70-72]</sup>，提升希尔伯特空间的维度可以将低维非酉演化变为高维度的酉演化。对于量子线路来说，Naimark 扩张可以通过增加辅助比特的方法来实现非酉的量子演化。在实际量子线路中对偶量子计算的线路图如图 1.11 所示。

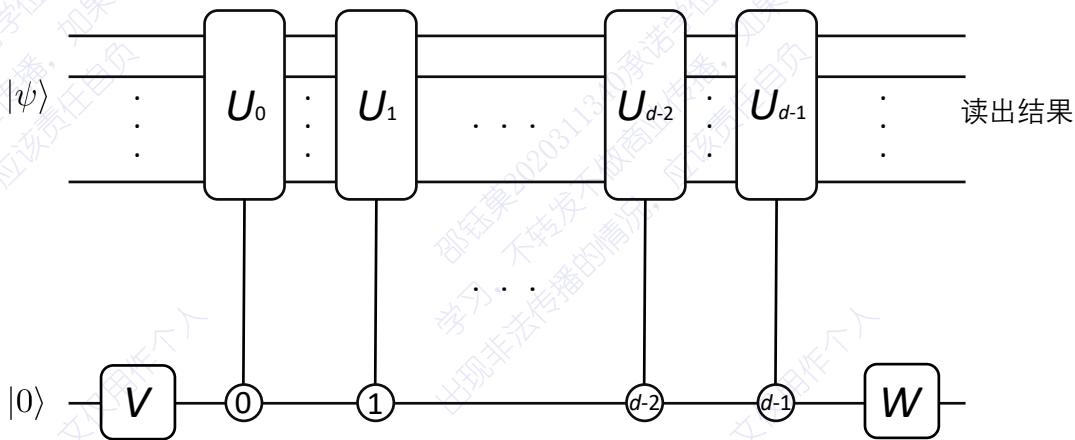


图 1.11 对偶量子计算框架实现的线路图

在量子线路图（图 1.11）中首先制备量子计算的初态  $|\psi\rangle$ ，并且引入  $\lceil \log_2 d \rceil$  个辅助比特作为辅助空间。并且在辅助空间上作用算符  $V$ ，其作用类似于前面提到的分波算符。通过此算符开启量子计算的对偶量子计算模式。作用效果如下：

$$(I \otimes V) |\psi\rangle |0\rangle \rightarrow \sum_{i=0}^{d-1} V_{i0} |\psi\rangle |i\rangle = |\psi_1\rangle \quad (1.43)$$

其中  $V_{i0}$  是一个复数，且满足归一化条件  $\sum_{i=0}^{d-1} |V_{i0}|^2 = 1$ 。紧接着对工作比特实施  $d$  个受控操作。对整个希尔伯特空间来说则是实施  $U$  操作，具体的定义如下

$$U = \sum_{i=0}^{d-1} U_i \otimes |i\rangle\langle i| \quad (1.44)$$

当且仅当控制位的值为  $0, 1, \dots, d - 1$  时，才对相应的工作比特施加  $d$  个受控操作  $U_0, U_1, \dots, U_{d-1}$ 。这一过程对应量子干涉仪在  $d$  条路径上分别进行不同的酉操作，此时状态变为

$$U |\psi_1\rangle \rightarrow \sum_{i=0}^{d-1} V_{i0} U_i |\psi\rangle |i\rangle = |\psi_2\rangle \quad (1.45)$$

再对辅助比特位施加合波算符  $W$  来关闭对偶量子计算模式。其对应的量子态为：

$$(I \otimes W) |\psi_2\rangle \rightarrow \sum_{i=0}^{d-1} W_{0i} V_{i0} U_i |\psi\rangle |0\rangle + \sum_{i=0}^{d-1} \sum_{j=1}^{d-1} W_{ji} V_{i0} U_i |\psi\rangle |j\rangle \quad (1.46)$$

最后只对路径编号为 0 的波函数进行测量，即只测量  $d$  维辅助比特均为 0 时的工作比特的量子态。

$$|\psi_f\rangle = \frac{\sum_{i=0}^{d-1} W_{0i} V_{i0} U_i |\psi\rangle}{\left\| \sum_{i=0}^{d-1} W_{0i} V_{i0} U_i |\psi\rangle \right\|} \quad (1.47)$$

通过对算符  $W$  与  $V$  的设计，使其满足

$$c_i = W_{0i} V_{i0} \quad (1.48)$$

进而实现式 (1.41)，来模拟工作比特上非酉量子门的演化。各个  $c_i$  之和为

$$\left| \sum_{i=0}^{d-1} c_i \right| = \left| \sum_{i=0}^{d-1} W_{0i} V_{i0} \right| = |(WV)_{00}| \leq 1 \quad (1.49)$$

此结果即满足约束条件式 (1.42)。因此通过量子计算的对偶模式最终可实现一般的非酉逻辑门操作

$$|\psi_f\rangle = \frac{\sum_{i=0}^{d-1} W_{0i} V_{i0} U_i |\psi\rangle}{\left\| \sum_{i=0}^{d-1} W_{0i} V_{i0} U_i |\psi\rangle \right\|} = \frac{L_c |\psi\rangle}{\|L_c |\psi\rangle\|} \quad (1.50)$$

可以看到量子计算的对偶模式是存在成功率的，其成功的概率为

$$P_s = \|L_c |\psi\rangle\| \quad (1.51)$$

理论上平均经过  $O(1/P_s)$  次实验即可获得成功，事实上可以在测量之前运用量子搜索算法进行概率幅放大，即对于辅助比特均为 0 的态进行概率幅扩增，使其接近 100%。如果在量子算法中需要将对偶量子线路作为子线路，则每完成一个子线路需要进行投影测量，实际执行过程中考虑到运用通用量子门集合实现量子门存在误差，以及量子门实际操作的误差的积累。则需要运用本文第 3 章提出的对于误差高鲁棒性的量子搜索算法来完成对概率幅的扩增。

## 1.7 开放量子系统与量子噪声

量子计算机与环境之间是存在相互耦合作用的，事实上，量子计算机与环境的相互作用是无法避免的，也就是量子计算机在演化的过程中会将编码的信息散布到环境当中，同样环境的“信息”也会流入量子计算机中，进而导致量子计算机失去相干性。最终随时间退化为经典的热平衡态，这个过程称为退相干过程。而

环境对于量子计算机的干扰称之为量子噪声。在这个过程中单看量子计算机系统，由于与环境存在着相互作用，因此量子计算机系统不再是封闭系统，而是开放系统。开放系统中量子态的演化不再是酉的，其演化方程可通过第一性原理得到。即量子系统  $\rho_{\text{rel}}(0)$  与环境  $\rho_{\text{env}}(0)$  组成的复合系统  $\rho$  经过酉演化，再取  $\hat{P}$  投影，可得到描述开放量子系统  $\rho_{\text{rel}}$  演化的 Nakajima-Zwanzig 方程<sup>[73-74]</sup>：

$$\partial_t \rho_{\text{rel}} = \hat{P} \hat{L} \rho_{\text{rel}} + \int_0^t dt' \mathcal{K}(t') \rho_{\text{rel}}(t-t') \quad (1.52)$$

其中  $\hat{P}$  和  $\hat{Q}$  为投影算符，其作用为

$$\begin{aligned} \hat{P}\rho &= (\text{Tr}_{\text{env}} \rho) \otimes \rho_{\text{env}}(0) = \rho_{\text{rel}} \\ \hat{Q}\rho &= (\hat{I} - \hat{P})\rho \end{aligned} \quad (1.53)$$

$\hat{L}$  为 Liouville 算子，其作用为

$$\hat{L} = \frac{i}{\hbar} [-, \hat{H}] \quad (1.54)$$

积分核  $\mathcal{K}$  的表达式如下：

$$\mathcal{K}(t) = \hat{P} \hat{L} e^{\hat{Q} \hat{L} t} \hat{Q} \hat{L} \hat{P} \quad (1.55)$$

积分核  $\mathcal{K}$  是量子系统  $\rho_{\text{rel}}$  马尔可夫性的度量。可以看到 Nakajima-Zwanzig 方程中对于  $\mathcal{K}$  是存在积分操作的，这表明系统在  $t+dt$  时刻的演化规律是由  $t$  时刻之前系统所经历的历史决定的，而不仅仅是由  $t$  时刻决定的。也就是说系统是存在记忆的。这样的系统被称作非马尔可夫系统。反之当  $\mathcal{K} = 0$ ，则系统是没有记忆的， $t$  时刻演化的规律与  $t$  时刻之前系统所经历的历史是无关的。这样的系统称为马尔可夫系统。与马尔可夫量子噪声相比非马尔可夫量子噪声对系统的影响是更大的，但对于这方面的研究目前还较少<sup>[75]</sup>。在马尔可夫近似条件下<sup>[76]</sup>，即  $\mathcal{K} = 0$  时，Nakajima-Zwanzig 方程退化成为 Lindblad 方程<sup>[77]</sup>

$$\frac{d\rho(t)}{dt} = -\frac{i}{\hbar} [H, \rho(t)] + L_D(\rho(t)) \quad (1.56)$$

其中：

$$L_D(\rho(t)) = \sum_{n>0} \hat{L}_n^\dagger \rho(t) \hat{L}_n - \frac{1}{2} \sum_{n>0} \hat{L}_n^\dagger \hat{L}_n \rho(t) - \frac{1}{2} \rho(t) \sum_{n>0} \hat{L}_n^\dagger \hat{L}_n \quad (1.57)$$

式 (1.57) 中  $\hat{L}_n$  称为 Lindblad 算子<sup>[78]</sup>或者跃迁算子，即每个  $\hat{L}_n^\dagger \rho(t) \hat{L}_n$  代表一种可能的量子跃迁。式 (1.57) 中的后两项是为了保证归一化。为了清晰地给出开放量子系统的演化算符，定义如下算符

$$\hat{M}_n(dt) = \sqrt{dt} \hat{L}_n, \quad n = 1, 2, \dots \quad (1.58)$$

为 Kraus 算子<sup>[79]</sup>。Kraus 算子满足完备条件  $\sum_n \hat{M}_n^\dagger \hat{M}_n = I$ 。在马尔可夫近似下，量子系统的动力学演化过程可由超算符  $\Lambda$  给出

$$\Lambda(\rho) = \sum_n \hat{M}_n \rho(0) \hat{M}_n^\dagger \quad (1.59)$$

可以证明超算符  $\Lambda$  是一个正定保迹映射。

在进行量子计算时，量子系统会受到环境量子噪声的影响而产生退相干。量子噪声包括比特翻转，相位反转，退极化，振幅阻尼等<sup>[80-82]</sup>。这些退相干过程可以通过式 (1.59) 中的量子信道  $\{\hat{M}_n\}$  进行描述。例如相位反转噪声对应的 Kraus 算子为

$$\hat{M}_0 = \sqrt{p} \sigma_0 = \sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \hat{M}_1 = \sqrt{1-p} \sigma_z = \sqrt{1-p} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (1.60)$$

对应的量子信道为  $\Lambda(\rho) = p\rho + (1-p)\sigma_z \rho \sigma_z$ 。即量子态经过此信道有  $p$  概率不改变，有  $1-p$  概率发生相位反转。退极化噪声对应的量子信道为：

$$\hat{M}_0 = \sqrt{1-p} \sigma_0, \quad \hat{M}_1 = \sqrt{\frac{p}{3}} \sigma_x, \quad \hat{M}_2 = \sqrt{\frac{p}{3}} \sigma_y, \quad \hat{M}_3 = \sqrt{\frac{p}{3}} \sigma_z \quad (1.61)$$

量子态经过此过程演化为  $\Lambda(\rho(t_0)) = \frac{1}{2} \left( 1 + \vec{P}(t) \cdot \vec{\sigma} \right)$  其中演化后的自旋极化矢量为：

$$\vec{P}(t) = \left( 1 - \frac{4p}{3} \right) \vec{P}(t_0) \quad (1.62)$$

即如果每种情况等概率地出现则整个量子位出错的概率为  $p = 0.75$ 。此时  $\vec{P}(t) = 0$ ，即演化后的密度矩阵变为了单位矩阵的 0.5 倍，这表示演化后的末态是一个纯混态。

在开放量子系统中由于量子噪声而产生的退相干过程会影响量子计算的保真度以及相干时间，为了克服量子噪声的影响科学家们提出了量子纠错码。下一节将介绍这部分的内容。

## 1.8 量子纠错码

1995 年——1997 年，Galderbank, Shor, Steane, Gottesman 和 Calderbank 等在经典纠错码的基础上逐步建立了量子纠错码的群结构理论<sup>[83-90]</sup>。本小节将简要阐述该理论的思想。经过 1.7 节的分析，对于单比特开放量子系统的演化，可以用 Kraus 算子来描述。由于泡利算子构成一组完备基，因此单比特 Kraus 算子都可以用泡利算子群  $G_1 = \{\pm i\sigma_0, \pm\sigma_0, \pm i\sigma_x, \pm\sigma_x, \pm i\sigma_y, \pm\sigma_y, \pm i\sigma_z, \pm\sigma_z\}$  的群元来表示。对于  $n$  量子比特系统，在独立相互作用的模型下，Kraus 算子可运用泡利算子直积构成的  $n$

量子位泡利算子群  $G_n = \{P_1 \otimes P_2 \otimes \cdots \otimes P_n \mid P_j \in G_1\}$  来构建。泡利算子群具有以下优秀的性质：

1.  $G_n$  中的群元素都是酉的。
2. 对于任意  $g \in G_n$ , 若  $\sigma_y$  在  $g$  中出现奇数次,  $g$  是反厄米的, 否则  $g$  是厄米的。
3. 对于任意  $g_1, g_2 \in G_n$ ,  $g_1, g_2$  要么对易, 要么反对易。
4.  $G_n$  中相互对易且为厄米的群元构成  $G_n$  的一个阿贝尔子群。

下面将阐述量子纠错码的构建过程。经过此过程构建的量子纠错码可纠正的错误集合为  $\mathcal{E} = \{g_1, g_2, \dots, g_{n-k}, E_1, E_2, \dots, E_m \mid g_i, E_j \in G_n\}$ 。

首先, 在错误集合  $\mathcal{E}$  选取  $n - k$  个相互独立的且不包含  $-I$  的稳定子  $g_i$  构成  $G_n$  子群  $S_0$  的生成元集合  $\langle S_0 \rangle = \langle g_1, g_2, \dots, g_{n-k} \rangle$ 。要求被选取的稳定子要两两对易。

第二步, 在集合  $Z(S_0|G_n) - S_0$  中选取  $k$  个相互独立的元素  $\bar{Z}_j$  加入集合  $\langle S_0 \rangle$  构成最大算子集  $S = \langle g_1, g_2, \dots, g_{n-k}; \bar{Z}_1, \bar{Z}_2, \dots, \bar{Z}_k \rangle$ , 并保证最大算子集  $S$  中的元素依然两两对易。其中  $Z(S_0|G_n)$  表示集合  $S_0$  在  $G_n$  中的中心子, 即

$$Z(S_0|G_n) = \{g : gMg^{-1} = M, \forall M \in S_0, g \in G_n\} \quad (1.63)$$

事实上, 引入的  $\bar{Z}_j$  为逻辑比特  $j$  的量子逻辑门  $Z$  操作。挑选对于集合  $\langle S_0 \rangle$  中所有元素本征值都为 +1 的本征态, 同时还是  $k$  个算符  $\bar{Z}_j$  本征态的量子态构成基本码字空间  $V$  如图 1.12。在这个基本码字空间中选择对于  $k$  个算符  $\bar{Z}_j$  本征值为 +1 的量子态。这些量子态张成的空间为  $V_S$  即为逻辑比特的  $|00 \cdots 0\rangle$ (共  $k$  个 0 态(如图 1.12 中标注  $V_S$  的部分))。基本码字空间中对于  $\bar{Z}_1$  的本征值为 -1, 对于其他  $k - 1$  个算符  $\bar{Z}_j$  本征值为 +1 的量子态张成的空间即为逻辑比特  $|00 \cdots 1\rangle$ (共  $k$  位); 基本码字空间中对于  $\bar{Z}_1, \bar{Z}_2$  的本征值为 -1, 对于其他  $k - 2$  个算符  $\bar{Z}_j$  本征值为 +1 的量子态张成的空间即为逻辑比特  $|00 \cdots 11\rangle$ (共  $k$  位)等。按照此方式可以得到所有的逻辑比特。这些逻辑比特对应图 1.12 中的橙色部分。

分析该纠错码, 可以发现对于发生的错误在稳定子集合  $S_0$  内是不会改变逻辑比特状态的。因为即使错误发生, 改变后物理比特的状态仍然在逻辑比特所标定的空间内, 并不会改变逻辑比特的状态。

对于不在稳定子集合  $S_0$  中的错误来说分为以下两种情况:

1. 与  $S_0$  对易, 则这些元素在  $Z(S_0|G_n) - S_0$  中。这些错误是无法纠正的。因为这些算子正是对于逻辑比特的逻辑操作算符。经这些算子的作用将子空间  $V_S$  变换到其他的逻辑比特空间, 例如  $U_1 V_S, U_2 V_S$  等(如图 1.12 中的橙色部分)。商空间  $V/V_S$  可以标记逻辑比特的编码空间。
2. 另一种情况的错误类型为  $E_i = G_n - Z(S_0|G_n)$  (错误发生后将图 1.12 中  $V$  变

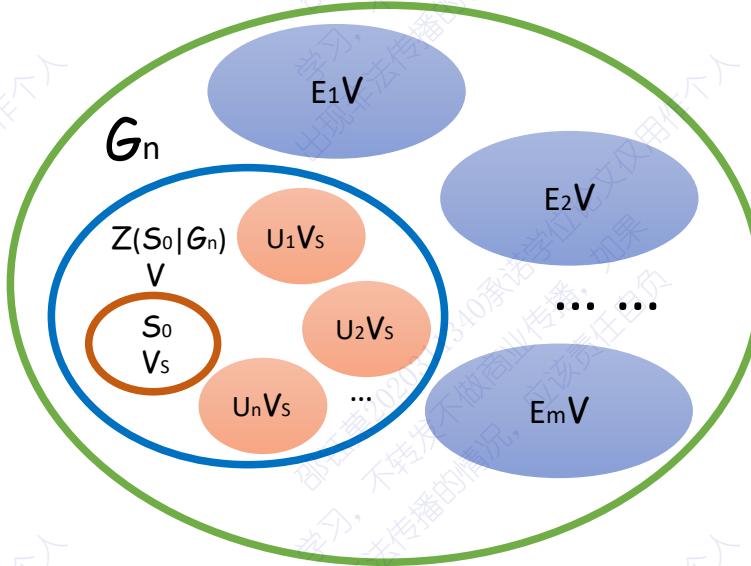


图 1.12 量子纠错码代数结构图解

换到与其相正交的空间中，例如  $E_1V, E_2V$ ）， $E_i$  与  $S_0$  中至少一个元素反对易，可以运用  $S_0$  中的元素作为指错子。如果对于指错子的本征值测量结果均为 +1 则说明没有错误出现。如果对于某位指错子测量结果出现本征值 -1，则代表出现了与指错子反对易算子产生的错误，并可以施加逆操作来更正这种错误。

本小节给出了稳定子码  $[n, k]$  的构造方式，即可将  $n$  个物理比特编码为  $k$  个逻辑比特。这样的稳定子码可以纠错的条件为：对于属于泡利算子群的噪声  $\{E_i\}$ ，其任意两个算符满足  $E_j^\dagger E_k \notin Z(S_0|G_n) - S_0$ ，那么该噪声就是可纠错的。

## 1.9 Toric Code

在 1.8 中介绍了对于  $n$  物理比特， $n - k$  个稳定子生成元的系统可以用其来编码  $k$  个逻辑比特。本节将基于此介绍一种特殊的量子纠错码——Toric Code<sup>[23]</sup>。在 2 维空间考虑一个拥有周期性边界条件的  $r \times r$  的格点，且每两个格点之间都存在自旋 1/2 的粒子（如图 1.13）。则这个系统拥有  $2r^2$  个量子比特。在系统中定义两类稳定子：

$$A_s = \prod_{j \in \text{star}(s)} \sigma_x^j, \quad B_p = \prod_{j \in \text{plaquette}(p)} \sigma_z^j \quad (1.64)$$

其中  $\sigma_x, \sigma_z$  为泡利矩阵。根据 1.8 的讨论 Toric code 模型中逻辑比特对应的希尔伯特空间的维数为  $2^{2r^2-(2r^2-2)} = 2^2$ 。这个模型是用  $2r^2$  个物理比特编码 2 个逻辑比特。对于逻辑比特的逻辑操作定义如下（如图 1.13 中 4 条贯穿的直线）

$$\bar{Z}_1 = \prod_{j \in red_v} \sigma_z^j, \quad \bar{X}_1 = \prod_{j \in red_h} \sigma_x^j \quad (1.65)$$

$$\bar{Z}_2 = \prod_{j \in blue_h} \sigma_z^j, \quad \bar{X}_2 = \prod_{j \in blue_v} \sigma_x^j \quad (1.66)$$

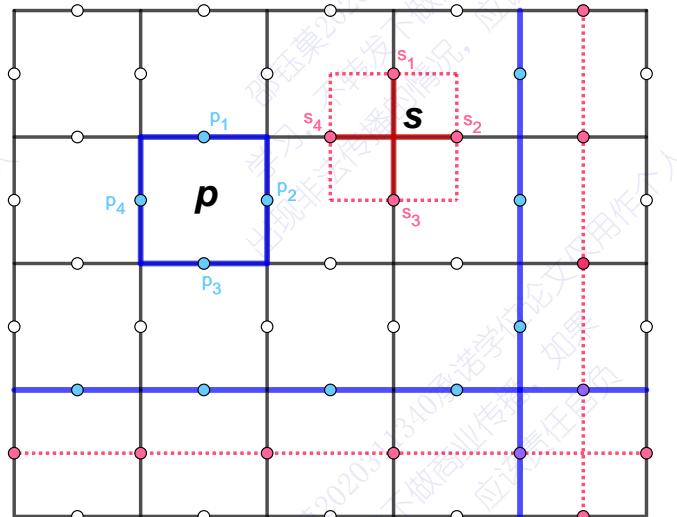


图 1.13 Toric code 模型

根据纠错码的规则，该系统的逻辑 0 态即为稳定子与逻辑算符本征值为 +1 的态。或者说逻辑 0 态是  $\sum_{i=1}^{n-k} g_i$ （其中  $g_i$  为稳定子算符）的本征态。可以运用投影算符来给出

$$|0_L\rangle = \frac{1}{2^n} \prod_{i=1}^{n-k} \prod_{j=1}^k (I + g_i) (I + \bar{Z}_j) |0\rangle \quad (1.67)$$

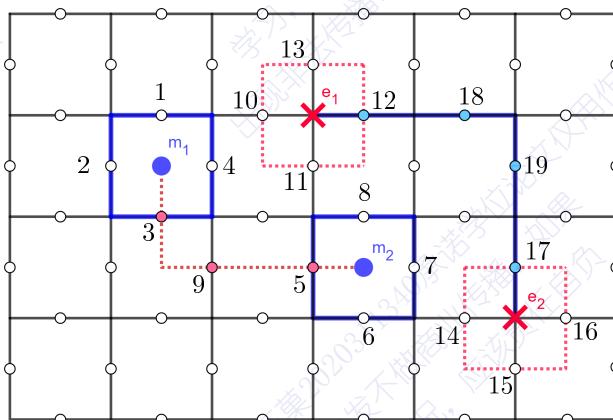
在凝聚态物理的观点下，基态就是哈密顿量最低的本征态，因此可以定义格点模型的哈密顿量为  $H = -\sum_{i=1}^{n-k} g_i = -\sum_s A_s - \sum_p B_p$ 。此模型是最简单的量子对模型<sup>[91]</sup>，同时也是最简单的拓扑序—— $\mathbb{Z}_2$  拓扑序<sup>[92-93]</sup>。

在  $\mathbb{Z}_2$  拓扑序中有 3 种低能有效准粒子激发。这种准粒子称之为任意子。任意子的存在与否可以通过  $A_s$  与  $B_p$  算符来检测。如果在某一个区域对于  $A_s$  或者  $B_p$  算符进行测量发现本征值为 -1，则代表其对应类型的任意子被激发。任意子可以被

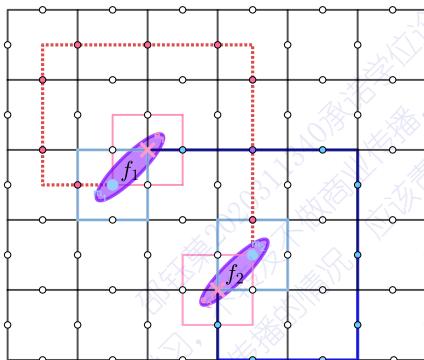
## 弦算符

$$S^x(t) = \prod_{j \in t} \sigma_x^j, \quad S^z(t') = \prod_{j \in t'} \sigma_z^j \quad (1.68)$$

激发产生。在  $\mathbb{Z}_2$  拓扑序的基态  $|\epsilon\rangle$  上作用  $Z$ -型弦算符  $S^z(t')$  即可在弦算符的两端激发出一对  $e$  任意子。例如图 1.14 中  $|e_1, e_2\rangle = \sigma_z^{12}\sigma_z^{18}\sigma_z^{19}\sigma_z^{17}|\epsilon\rangle$  可以验证  $|e_1, e_2\rangle$  态对于  $A_s$  算符即  $\sigma_x^{10}\sigma_x^{11}\sigma_x^{12}\sigma_x^{13}$  与  $\sigma_x^{14}\sigma_x^{15}\sigma_x^{16}\sigma_x^{17}$  的本征值为 -1，因此在  $Z$ -型弦算符两端出现了一对任意子  $e_1, e_2$ 。在基态  $|\epsilon\rangle$  上作用  $X$ -型弦算符  $S^x(t')$  即可在弦算符的两端激发出一对  $m$  任意子。例如图 1.14 中  $|m_1, m_2\rrangle = \sigma_x^3\sigma_x^9\sigma_x^5|\epsilon\rangle$  可以验证  $|m_1, m_2\rangle$  态对于  $B_p$  算符即  $\sigma_z^1\sigma_z^2\sigma_z^3\sigma_z^4$  与  $\sigma_z^5\sigma_z^6\sigma_z^7\sigma_z^8$  的本征值为 -1，因此在  $X$ -型弦算符两端出现了一对任意子  $m_1, m_2$ 。

图 1.14 任意子  $e, m$  的激发

如果当  $e, m$  任意子靠近的时候可以融合为  $f$  任意子(如图 1.15)。

图 1.15 任意子  $f$  的激发

通过上面的介绍可以得到  $\mathbb{Z}_2$  拓扑序其任意子的融合规则

$$e \times e = m \times m = f \times f = \mathbf{1}, \quad e \times m = m \times e = f, \quad f \times e = m, \quad f \times m = e \quad (1.69)$$

关于任意子的自旋与统计性质则可通过弦算符激发产生一对任意子  $a, b$ , 将这一对任意子中的一个通过施加弦算符使其绕着第三个任意子  $c$  旋转一周形成, 最后  $a, b$  湮灭的过程得出。通过此操作可以得到所有任意子的统计性质。这里不展开介绍。最终可得到  $\mathbb{Z}_2$  拓扑序任意子的自旋为:

$$\theta_1 = 1, \quad \theta_m = 1, \quad \theta_e = 1, \quad \theta_f = 1/2 \quad (1.70)$$

可以看到, 只有在弦算符, 即非局域算符作用下才能激发出任意子, 而局域操作是无法对该模型产生任何作用的。这就是拓扑学的基本思想, 即局部是无序的但是整体是有序的。拓扑序是物体整体的形态。是无法通过能带理论描述的。

因为在这里单电子近似不再成立。在拓扑序中每一个电子的运动状态均不同。他们之间存在着极强的长程纠缠, 这就导致了集体模式表现出了有序。要描述拓扑序, 需要描述其任意子的种类以及统计规律等性质。而物理学中的传统场论都是假设空间是无限大且没有边界的。但是在凝聚态中边界是存在的, 而且还要考虑不同场之间的关系。即边界态场与体态场的关系等。因此传统的场论与基于单电子近似的能带理论是无法有效描述拓扑序的。但张量范畴这门数学工具却能满足对于描述的需求。因此范畴论自然的引入到了物理学中。下面将介绍描述拓扑序的数学语言。

## 1.10 范畴论与拓扑序

回顾物理学史, 不难发现每一种新物理都需要引入新数学来进行描述。牛顿力学的建立将微积分引入到了物理学中, 广义相对论的建立则伴随着黎曼几何的引入, 规范理论的建立伴随着纤维丛理论的引入, 量子力学的建立伴随着线性代数的引入。而拓扑序理论<sup>[94]</sup>的建立则需要张量范畴的语言来描述。下面将介绍张量范畴是如何引入到物理学中的。

在凝聚态物理领域, 人们最关注的问题就是如何去描述一个物态的相。最开始朗道意识到可以利用对称性<sup>[95]</sup>, 以群和子群作为序参量对物态的相进行标记。直到拓扑绝缘体 (SPT) 被发现<sup>[96-99]</sup>。拓扑绝缘体是受到对称性保护的, 如果改变其对称性则 SPT 会发生相变。如果破坏其对称性那么 SPT 就退化为平庸的直积态。SPT 相的第一个例子是自旋为 1 的 Haldane 相<sup>[100-104]</sup>, 其对称性为  $SO(3)$ , 但其边界态却表现得像是费米子。这种新奇的 Haldane 相与平庸的 1 维自旋链都对应  $SO(3)$  的对称性, 因此仅用群是无法区分这两个相的。引入群的上同调群  $H^{d+1}(G, U(1))$  即可完成对 d 维 SPT 序参量的描述<sup>[105-106]</sup>。至此, 上同调的概念被引入到了物理学。

手性自旋态<sup>[107-108]</sup>以及分数量子霍尔效应<sup>[109-110]</sup>的发现导致了朗道的理论无法描述所有的序。因为分数量子霍尔效应没有任何的对称性可言，但是整体却表现出了高度有序的特性。这是一种新的序——拓扑序<sup>[94]</sup>，其低能有效理论为拓扑量子场论<sup>[111-113]</sup>。拓扑序不同于拓扑绝缘体。拓扑序拥有长程纠缠<sup>[114]</sup>，分数统计，与任意子激发。拓扑序中每个电子运动规律都不尽相同，因此无法采用基于单电子近似的能带理论来描述。表征拓扑序的理论可使用从环面上简并基态的非阿贝尔几何相位获得的，用于标记统计相互作用与准粒子自旋的模矩阵 $(\mathcal{T}, \mathcal{S})$ 以及融合规则 $\mathcal{N}_k^{ij}$ 。这种拓扑序融合和编织任意子的理论就是所谓的酉模张量范畴(UMTC)理论。至此张量范畴理论被引入到了物理学中。

这里只是简要的介绍范畴的基本定义。若想了解更多内容可参照作者在附录A整理的张量范畴基础知识简要。

**定义 1.1:** 一个范畴  $\mathcal{C}$  包含如下结构：

1. 集合  $\text{Ob}(\mathcal{C})=x, y, \dots$ , 这些集合中的元素称为范畴  $\mathcal{C}$  的对象；
2. 对于任意两个对象  $x, y$  存在集合  $\text{Hom}_{\mathcal{C}}(x, y)$ , 其中的元素称作对象  $x$  到对象  $y$  的态射；
3. 一个映射  $\circ : \text{Hom}_{\mathcal{C}}(y, z) \times \text{Hom}_{\mathcal{C}}(x, y) \rightarrow \text{Hom}_{\mathcal{C}}(x, z) : (f, g) \mapsto g \circ f$ , 这叫做态射的复合, 其中  $x, y, z \in \text{Ob}(\mathcal{C})$ ;
4. 对于任意  $x \in \text{ob}(\mathcal{C})$  存在单位态射  $\text{id}_x \in \text{Hom}_{\mathcal{C}}(x, x)$  满足如下两条：
  - 对于任意  $w, x, y, z \in \text{Ob}(\mathcal{C})$ ,  $f \in \text{Hom}_{\mathcal{C}}(x, y)$ ,  $g \in \text{Hom}_{\mathcal{C}}(y, z)$ ,  $h \in \text{Hom}_{\mathcal{C}}(z, w)$  满足结合律  $(h \circ g) \circ f = h \circ (g \circ f)$
  - 对于任意  $x, y \in \text{Ob}(\mathcal{C})$ ,  $f \in \text{Hom}_{\mathcal{C}}(x, y)$  满足酉性  $\text{id}_y \circ f = f = f \circ \text{id}_x$

比如集合范畴 **Set**, 对象为全体集合, 态射则为集合之间的映射, 态射的复合则为映射的复合。比如群范畴 **Grp**, 对象为全体群  $G, H, K$ , 态射则为群之间的同态映射, 可以证明群同态满足态射的复合和结合律。比如, 拓扑空间 **Top** 是一个范畴, 其对象为拓扑空间, 态射为连续函数。可以证明拓扑空间范畴也符合范畴的公理

函子则为范畴之间的映射, 对于函子的定义如下:

**定义 1.2:** 函子是范畴之间的映射  $F : \mathcal{C} \rightarrow \mathcal{D}$ 。该映射将

1. 范畴  $\mathcal{C}$  中的对象映射到范畴  $\mathcal{D}$ , 即  $\text{Ob}(\mathcal{C}) \rightarrow \text{Ob}(\mathcal{D})$  通过映射  $F : X \rightarrow F(X)$  来实现;
2. 范畴  $\mathcal{C}$  中的态射映射到范畴  $\mathcal{D}$ , 即  $\text{Hom}_{\mathcal{C}}(X, Y) \rightarrow \text{Hom}_{\mathcal{D}}(F(X), F(Y))$  通

- 过映射  $F : f \rightarrow F(f)$  来实现；
3. 范畴  $\mathcal{C}$  中的单位态射映射到范畴  $\mathcal{D}$ ，即  $F : \text{id}_X \rightarrow \text{id}_{F(X)}$ ；
  4. 范畴  $\mathcal{C}$  中的态射复合映射到范畴  $\mathcal{D}$ ，即  $F : gf \rightarrow F(g)F(f)$

自然变换则为函子之间的映射。对于自然变换的定义如下：

**定义 1.3：** 给定函子  $G, F : \mathcal{C} \rightarrow \mathcal{D}$ ，自然变换  $\varphi$  则是函子  $G, F$  之间的映射。给定映射的集合  $\phi_X \in \text{Hom}_{\mathcal{D}}(G(X), F(X))$ ， $F, G$  之间的自然变换则是一族映射  $\varphi = \{\varphi_X : F(X) \rightarrow G(X)\}_{X \in \text{Ob}(\mathcal{C})}$ 。对于每一个对象  $X, Y \in \text{Ob}(\mathcal{C})$ ，使得对于所有态射  $f \in \text{Hom}_{\mathcal{C}}(X, Y)$  满足： $\varphi_Y F(f) = G(f)\varphi_X$

下面将介绍如何用张量范畴来描述拓扑序。对于一个拓扑序（不包含  $E_8$  态）把其中所有可能激发出来的任意子和任意子之间演化算符的信息集中起来，则可描述这个序。这些信息构成酉模张量范畴 (Unitary modular tensor category)，这里试图构建物理情景与数学定义之间的关系。一个 UMTC 包含<sup>[115]</sup>：

- **对象** 拓扑序中的准粒子激发，任意子
- **态射** 准粒子在时间轴上演化的算符或者瞬子
- **酉性** 酉性是从希尔伯特空间内积的性质继承来的。对于态射来说这意味着算符是存在共轭转置的。举一个最简单的例子，希尔伯特空间范畴 **Hilb**，这就是在向量空间范畴 **Vec** 上增加了酉的条件。
- **融合** 就是把几个准粒子放在一起，在重整化极限下可以把他们一起看作一个准粒子。实际情况下我们需要按照一定的次序去一个一个的融合这些准粒子。这个融合过程由张量积映射来描述。定义张量积映射为  $A \otimes B$ 。则平庸的任意子（真空）就被定义为 **1**，这就是张量积的单位元，即  $\mathbf{1} \otimes A \cong A \cong A \otimes \mathbf{1}$ 。同时张量积是满足结合律的，即  $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$ 。这种结合律的映射可以用  $F$ -矩阵来表示。
- **编织** 在 2+1 维时空中，张量积的结果应该和选取的方向无关。也就是说  $A \otimes B$  自然的同构于  $B \otimes A$ 。而这个自同构的过程则是将准粒子  $A$  移动到准粒子  $B$  的另外一边。当然这个移动的路径也分为顺时针  $c_{A,B} : A \otimes B \cong B \otimes A$  和逆时针移动  $c_{A,B}^{-1} : A \otimes B \cong B \otimes A$ ，这个过程对应于  $R$ -矩阵
- **单对象** 单对象的简并度无法通过局域操作改变，单任意子一般标记为  $i, j, k$
- **直和** 一个复合任意子的激发可以退化为一系列的单任意子，这种退化是偶然的，而且是可以被局域操作干扰的。通常融合两个任意子其结果将是单任意子的直和，即  $i \otimes j \cong \bigoplus_k N_k^{ij} k$ ，其中  $N_k^{ij}$  是非负整数，描述  $k$  占  $i \otimes j$  的

组分。举一个经典的例子就是两个自旋  $1/2$  的粒子的自由度，融合起来相当于自旋为 0 和自旋为 1，即  $1/2 \otimes 1/2 = 0 \oplus 1$

- **对偶对象** 任意子  $X$  的反粒子  $X^*$ 。 $X \otimes X^*$  只含有一个真空态的自由度，即：  

$$X \otimes X^* \cong \mathbf{1} \oplus \dots$$
- **量子迹** 对于一个作用在  $X$  上的算符  $f$ ，它的量子迹  $\text{Tr } f$  是以下过程的期望值：先产生一对任意子  $X, X^*$ ，将  $f$  作用在  $X$  上，然后再湮灭这一对任意子。量子维度为  $d_i = \text{Tr id}_i$ 。系统总的维度则定义为  $D^2 = \sum_i d_i^2$ 。拓扑  $S$  与  $T$  矩阵元为  $T_{ij} = \delta_{ij} \text{Tr } c_{i,i}/d_i, S_{ij} = \text{Tr } c_{j^*,i} c_{i,j^*}/D$ 。
- **非退化**  $\left( x \otimes y \xrightarrow{c_{x,y}} y \otimes x \xrightarrow{c_{y,x}} x \otimes y \right) = \text{id}_{x \otimes y}$ ，对于  $y \in \mathcal{C}$  如果使上述关系成立则表明  $x$  是平庸的任意子即真空。非退化性表明系统中可以通过任意子编织来区分不同的任意子。

范畴论是数学的一门学科，以抽象的方式来处理数学中的结构与概念。数学中很多领域都可以形式化为范畴论（如图 1.16）。范畴论包含两种结构：对象和态射。态射就是作用在对象上的操作。事实上在物理学中可以用对象来代表物理实体，用态射代表物理测量。从哲学的角度来看范畴论就是把未知的对象当成黑盒子，只关注态射，就像对某一未知物理对象进行测量。对象  $A, B$  之间态射的集合记为  $\text{Hom}(A, B)$ 。在这里以最简单的张量范畴——向量空间范畴 **Vect** 为例<sup>[115]</sup>。其对象为所有有限维的向量空间。态射为向量空间之间的线性算子。现在假设我们对于对象即向量空间一无所知，那么我们该如何运用范畴论的观点从态射去复原这个向量空间呢？这个过程就和测量类似，因为任何向量空间  $V$  都与向量空间中从基本域到自身的线性算子相同，即  $V \cong \text{Hom}(\mathbb{C}, V)$ ，通过使用线性映射  $f(\alpha) = \alpha|x\rangle, \alpha \in \mathbb{C}$  就可识别向量  $|x\rangle$ 。因此，线性算子（态射）已经告诉了我们关于 **Vect** 的一切信息，而向量空间的内部结构则是冗余的信息。

范畴论的思想其实在物理学中是一直存在的。粒子或者物理系统作为范畴中的对象，相互作用与演化以及其他物理系统操作则为态射。事实上所有的物理系统对我们来说都是黑箱子，因为除非我们对其进行测量，否则我们对它们一无所知。我们获得的所有有关物理系统的信息都来源于我们与该系统之间的相互作用。也就是来自于态射。这就像 **Vect** 的例子<sup>[115]</sup>。我们就是基本域  $\mathbb{C}$ ，我们观察到的信息就是  $\text{Hom}(\mathbb{C}, V)$ 。在本文的第 4 章中，作者将引入张量范畴来研究量子模拟。

## 1.11 本章小结

本章首先介绍了量子比特与 Bloch 球的概念，然后给出了量子力学的基础知识和基本概念。随后阐释了量子计算的量子线路与量子门操作。并交代了运用量

子逻辑门的乘积去模拟酉演化的量子计算直乘模式与运用量子门线性组合去模拟非酉演化的量子计算对偶模式。之后介绍了更接近于实际量子计算情况的开放量子系统，引入量子噪声与退相干的概念。接下来本章介绍了抵抗量子噪声的量子纠错码理论。随后又举出了一种量子纠错码——Toric code。这种纠错码在凝聚态领域中对应  $\mathbb{Z}_2$  拓扑序的概念，接下来本章引入描述拓扑序的数学语言——张量范畴。本文的写作主要围绕带有振幅放大的对偶量子算法及其应用相关方面的成果。第 2 章将介绍量子信息处理的量子算法。第 3 章作者提出了高鲁棒量子搜索算法。这将用来实现对偶量子算法的振幅放大功能。第 4 章作者提出了范畴化量子模拟算法，这需要基于带有振幅放大的对偶量子算法来实现。第 5 章作者运用带有振幅放大的对偶量子算法构造了求解波动方程的量子算法。第 6 章则是对本文进行总结和展望。

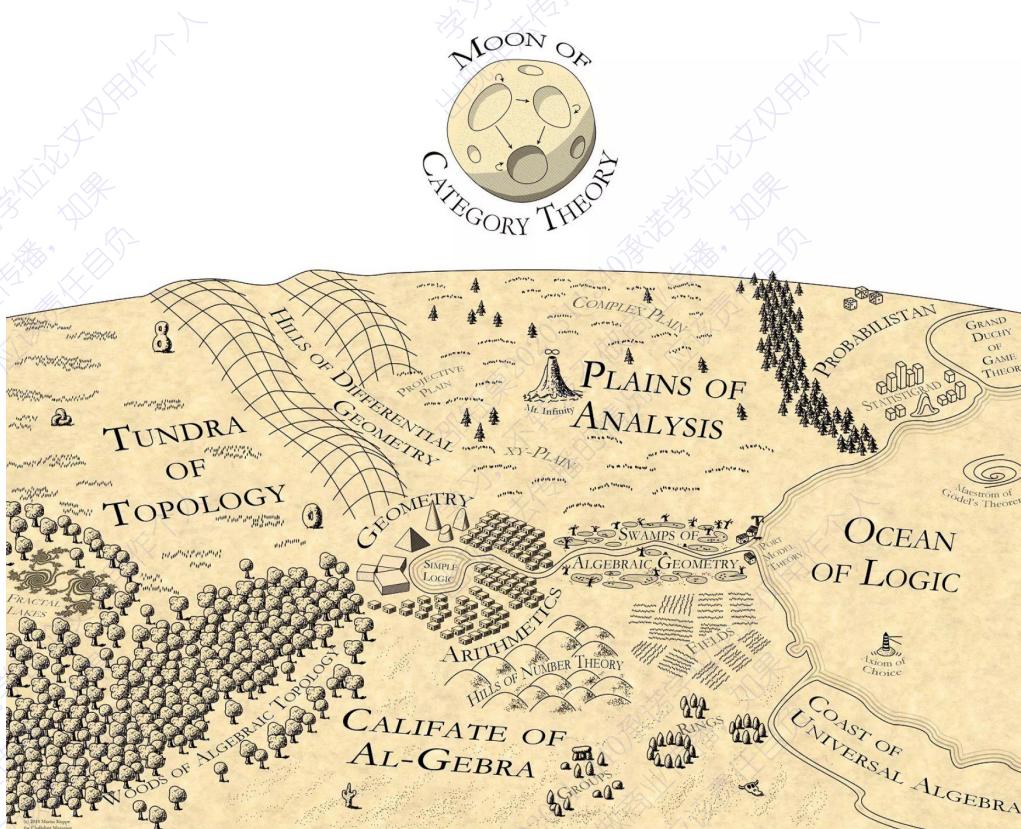


图 1.16 Martin Kuppe 的数学地图<sup>[116]</sup>

## 第2章 量子算法

### 2.1 量子傅里叶变换算法

量子傅里叶变换算法<sup>[117]</sup>是离散傅里叶变换的量子算法实现。对于长度为  $N$  的序列，运用经典快速傅里叶变换算法（FFT）计算，其计算复杂度为  $O(N \log(N))$ ，而在量子计算机上运用量子傅里叶变换，其复杂度为  $O(\log^2(N))$ 。可以看出傅里叶变换的量子版有指数加速的效果。量子傅里叶变换也是量子算法的核心之一。本章的 2.2 节将介绍的量子相位估计算法与 2.3 节介绍的 Shor 算法以及 2.4 节介绍的线性方程组求解算法都是基于量子傅里叶变换算法发展而来的。

离散傅里叶变换就是把一个长度为  $N$  的复数向量  $\{\vec{x}_n\} := (x_0, \dots, x_{N-1})$  映射到长度为  $N$  的复数向量  $\{\vec{y}_n\} := (y_0, \dots, y_{N-1})$  的过程，具体的定义如下：

$$y_k = \{\mathcal{F} \circ \{\vec{x}_n\}\}_k := \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \cdot e^{2\pi i \frac{jk}{N}} \quad (2.1)$$

其中  $y_k$  代表复数向量  $\{\vec{y}_n\}$  的第  $k$  个分量， $x_j$  代表复数向量  $\{\vec{x}_n\}$  的第  $j$  个分量，符号  $\mathcal{F}$  则代表离散傅里叶变换算符。式 (2.1) 中  $\mathcal{F} \circ \{\vec{x}_n\}$  表示对复数向量  $\{\vec{x}_n\}$  进行离散傅里叶变换。

在量子算法中要把  $\{\vec{x}_n\}$  和  $\{\vec{y}_n\}$  向量分别编码到两个不同的量子态上，即  $|X\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$  和  $|Y\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$ 。与经典算法的傅里叶变换相同，量子傅里叶变换作用在态  $|X\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$  上，并把它映射到  $|Y\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$  态上，并遵照式 (2.1)。这个过程具体在量子态上的表述为

$$|Y\rangle = U_{QFT}|X\rangle \quad (2.2)$$

$$= \sum_{j=0}^{N-1} U_{QFT} x_j |j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} x_j e^{2\pi i \frac{jk}{N}} |k\rangle \quad (2.3)$$

根据式 (2.3) 可得量子傅里叶变换算法的操作实际上是在  $N$  维希尔伯特空间中把一组正交基  $\{|j\rangle\}$  用另外一组正交基底  $\{|k\rangle\}$  来表示。具体的表述如下式：

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle \quad (2.4)$$

式 (2.3) 中的酉变换如下

$$U_{QFT} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle \langle j| \quad (2.5)$$

不难看出在式(2.4)变换后的态是各量子态的等权重叠加,仅仅是各态的相位不同。所以式(2.4)可以表示为各量子态的直积态。下面将把式(2.4)写成直积表示。

在量子信息中,通常取 $N=2^n$ ,其中 $n$ 代表量子比特的数量。即对于正交基 $\{|j\rangle\}$ 和 $\{|k\rangle\}$ 来说均包括 $N$ 个基底: $\{|0\rangle, |1\rangle, \dots, |2^n-1\rangle\}$ 。对于正交基 $\{|j\rangle\}$ 中的任何一个基底 $|j\rangle$ 可将十进制的 $j$ 写成二进制的形式,即 $j=j_1j_2\dots j_n$ ,这表示的十进制数值为 $j=j_12^{n-1}+j_22^{n-2}+\dots+j_n2^0$ 。同样二进制数 $0.j_lj_{l+1}\dots j_m$ 则代表十进制数 $j_l2^{-1}+j_{l+1}2^{-2}+\dots+j_m2^{-m-l-1}$ 。因此对于式(2.4)可以表示为:

$$|j\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle \quad (2.6)$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j \left(\sum_{l=1}^n k_l 2^{-l}\right)} |k_1 \dots k_n\rangle \quad (2.7)$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 \bigotimes_{l=1}^n e^{2\pi i j k_l 2^{-l}} |k_l\rangle \quad (2.8)$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^n \left[ \sum_{k_l=0}^1 e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \quad (2.9)$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^n \left[ |0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right] \quad (2.10)$$

$$= \frac{1}{2^{n/2}} \left( |0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle \right) \left( |0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle \right) \dots \left( |0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right) \quad (2.11)$$

其中式(2.7)是把十进制数字 $k$ 写成二进制的形式,即 $k=k_1\dots k_n, k/2^n=\sum_{l=1}^n k_l 2^{-l}$ 。式(2.8)是把 $e$ 的指数求和展开 $e$ 指数的乘积。式(2.9)则是交换乘积与求和的顺序。

这样的直积表示为下一步介绍量子傅里叶变换的量子线路有效实现打下了基础。通过对式(2.11)的分析发现,量子傅里叶变换中只包含两种基本逻辑门操作,一种是针对单量子比特的沃尔什-哈达玛门操作:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (2.12)$$

另外一种则是两量子比特受控 $U_{j,k}$ 相位门操作 $C(U_{j,k})$ ,其中 $k$ 为控制位, $j$ 为目标位,当且仅当控制位 $k$ 为 $|1\rangle$ 时,才对目标位 $j$ 施加一个 $U_{j,k}$ 相位旋转操作:

$$U_{j,k} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta_{j,k}} \end{bmatrix} \quad (2.13)$$

其中相移角为  $\theta_{j,k} = 2\pi \frac{j_k}{2^{k-j+1}}$ 。这个两量子比特受控相位门  $C(U_{j,k})$  在  $j, k$  两量子比特构成的 4 维希尔伯特空间内的计算基底下为：

$$C(U_{j,k}) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{ij_k\theta_{j,k}} \end{bmatrix} \quad (2.14)$$

可以看出当控制位  $j_k = 1$  时则对目标位施加一个  $U_{j,k}$  相移操作，当控制位  $j_k = 0$  时  $C(U_{j,k})$  则退化为单位矩阵，对量子比特不施加任何操作。

为了阐述量子傅里叶变换算法的工作原理，本文先以简单的三量子比特为例。三量子比特傅里叶变换通过量子线路图（如图 2.1）来实现。可以看到这个量子线路图对于输入态  $|j\rangle = |j_1 j_2 j_3\rangle$  执行的操作是：

$$H_3 C(U_{2,3}) H_2 C(U_{1,3}) C(U_{1,2}) H_1 \quad (2.15)$$

其中沃尔什-哈达玛门  $H$  的下标代表该门作用的量子比特编号。

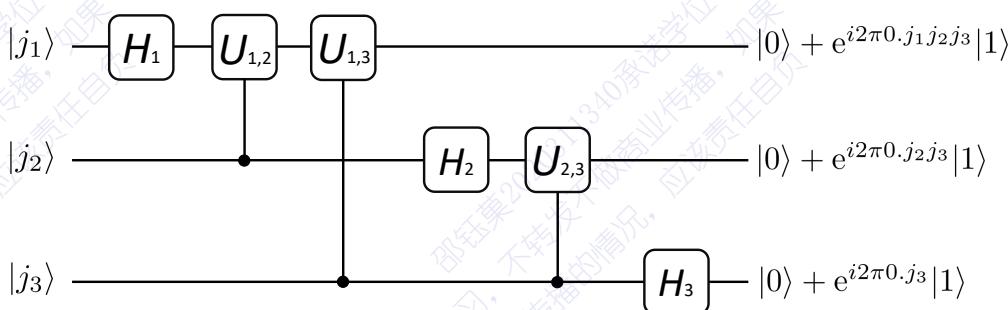


图 2.1 三比特量子傅里叶变换线路图

为了分析这个量子线路，接下来按照时序将式 (2.15) 中的算符分别作用在态  $|j_1 j_2 j_3\rangle$  上，首先看第一个量子比特

$$H_1 |j_1 j_2 j_3\rangle = (|0\rangle + e^{i2\pi 0.j_1} |1\rangle) |j_2 j_3\rangle \quad (2.16)$$

其中二进制数字  $0.j_1$  代表十进制  $j_1/2$ 。当  $j_1 = 0$  时， $e^{i2\pi 0.j_1} = 1$ 。当  $j_1 = 1$  时， $e^{i2\pi 0.j_1} = -1$ 。具体的来说式 (2.16) 可展开写成：

$$\begin{aligned} U_{QFT}|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ U_{QFT}|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \quad (2.17)$$

可以看到这正是沃尔什-哈达玛变换，同时这也是最简单的傅里叶变换。紧接着作用  $C(U_{1,2})$  操作，当  $j_2 = 0$  时不做任何操作，当  $j_2 = 1$  时则对第一量子比特  $|1\rangle$  旋转

相位  $\theta_{1,2} = 2\pi j_2/2^{2-1+1} = 2\pi 0.0 j_2$ 。紧接着再作用  $C(U_{1,3})$  操作，当  $j_3 = 0$  时不做任何操作，当  $j_3 = 1$  时则对第一量子比特  $|1\rangle$  旋转相位  $\theta_{1,3} = 2\pi j_3/2^{3-1+1} = 2\pi 0.00 j_3$ 。经过此操作第一个量子比特的输出态为：

$$\frac{1}{2^{1/2}} (|0\rangle + e^{i2\pi 0.j_1 j_2 j_3} |1\rangle) \quad (2.18)$$

下面讨论量子线路对第二个量子比特的作用。 $H_2$  作用在第二量子比特之后

$$\frac{1}{2^{1/2}} (|0\rangle + e^{i2\pi 0.j_2} |1\rangle) \quad (2.19)$$

紧接着作用  $C(U_{2,3})$  操作，当  $j_3 = 0$  时不做任何操作，当  $j_3 = 1$  时则对第二量子比特  $|1\rangle$  旋转相位  $\theta_{2,3} = 2\pi j_2/2^{3-2+1} = 2\pi 0.0 j_3$ 。这时量子态演化为：

$$\frac{1}{2^{1/2}} (|0\rangle + e^{i2\pi 0.j_2 j_3} |1\rangle) \quad (2.20)$$

最后  $H_3$  作用在第三量子比特的结果为

$$\frac{1}{2^{1/2}} (|0\rangle + e^{i2\pi 0.j_3} |1\rangle) \quad (2.21)$$

因此量子线路图 2.1 制备的量子态为

$$\frac{1}{2^{3/2}} [(|0\rangle + e^{i2\pi 0.j_1 j_2 j_3} |1\rangle) (|0\rangle + e^{i2\pi 0.j_2 j_3} |1\rangle) (|0\rangle + e^{i2\pi 0.j_3} |1\rangle)] \quad (2.22)$$

与式 (2.11) 比较可发现这正是三量子比特的傅里叶变换。这个结果可以推广到  $n$  量子比特的线路图 2.2。下面将证明图 2.2 实现的是式 (2.11) 对于  $n$  量子比特的傅里叶变换。

输入态为  $|j\rangle = |j_1 j_2, \dots, j_n\rangle$ 。 $H_1$  作用在态  $|j\rangle$  的结果为：

$$\frac{1}{2^{1/2}} (|0\rangle + e^{i2\pi 0.j_1} |1\rangle) |j_2 j_3 \dots j_n\rangle \quad (2.23)$$

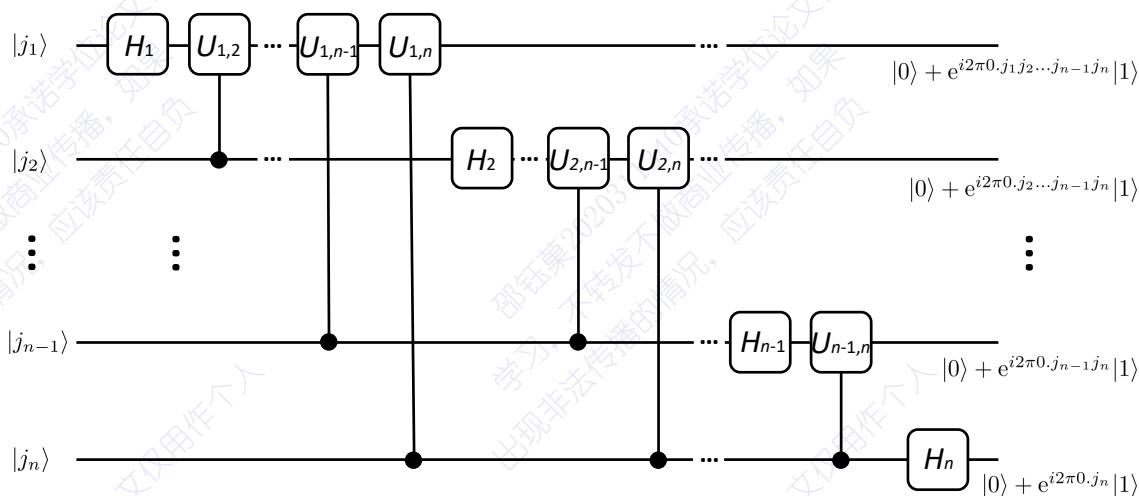


图 2.2  $n$  量子比特傅里叶变换算法线路图

紧接着作用  $C(U_{1,2})$  操作，当  $j_2 = 0$  时不做任何操作，当  $j_2 = 1$  时则对第一量子比特  $|1\rangle$  旋转相位  $\theta_{1,2} = 2\pi j_2/2^{2-1+1} = 2\pi 0.0j_2$ 。紧接着再作用  $C(U_{1,3})$  操作，当  $j_3 = 0$  时不做任何操作，当  $j_3 = 1$  时则对第一量子比特  $|1\rangle$  旋转相位  $\theta_{1,3} = 2\pi j_3/2^{3-1+1} = 2\pi 0.00j_3$ 。然后施加  $C(U_{1,3}), C(U_{1,4}), \dots$  直到  $C(U_{1,n})$ 。经过此番操作第一个量子比特的输出态为：

$$\frac{1}{2^{1/2}} (|0\rangle + e^{i2\pi 0.j_1j_2\dots j_n}|1\rangle) |j_2j_3\dots j_n\rangle \quad (2.24)$$

之后对第二个量子比特执行操作  $H_2, C(U_{2,3}), C(U_{2,4}), \dots, C(U_{2,n})$ ，可得

$$\frac{1}{2} (|0\rangle + e^{i2\pi 0.j_2j_3\dots j_n}|1\rangle) (|0\rangle + e^{i2\pi 0.j_1j_2\dots j_n}|1\rangle) |j_3j_4\dots j_n\rangle \quad (2.25)$$

按照量子线路图依次对每一位量子比特进行操作，直到第  $n$  个量子比特。最终得到的结果为

$$\frac{1}{2^{n/2}} (|0\rangle + e^{i2\pi 0.j_n}|1\rangle) (|0\rangle + e^{i2\pi 0.j_{n-1}j_n}|1\rangle) \dots (|0\rangle + e^{i2\pi 0.j_1j_2\dots j_n}|1\rangle) \quad (2.26)$$

这正是式 (2.11) 的结果。因此证明图 2.2 即为  $n$  比特量子傅里叶变换的线路图。

分析此算法可知对于  $n$  比特线路图 (图 2.2) 依次施加的逻辑门为

$$H_n C(U_{n-1,n}) H_{n-1} C(U_{n-2,n-1}) \dots H_2 C(U_{1,n}) C(U_{1,n-1}) \dots C(U_{1,2}) H_1 \quad (2.27)$$

共施加了  $n$  次  $H$  门操作， $\frac{n(n-1)}{2}$  次两比特门操作。一共进行了  $\frac{n(n+2)}{2}$  次操作，可以看出需要操作的总次数是输入位数的二次函数。因此量子傅里叶变换的复杂度为  $\Theta(n^2)$ ，而最好的经典傅里叶变换算法的复杂度则为  $\Theta(n2^n)$ 。

## 2.2 量子相位估计算法

在量子信息中，很多信息都是包含在量子态的相位当中。可以利用 2.1 节介绍的量子傅里叶变换算法来推广构建量子相位估计算法<sup>[118]</sup>。量子相位估计算法（或者称为量子本征值估计算法）可估计一个酉算符所对应某一个本征态的本征值。具体来说就是  $U$  是  $n$  量子比特希尔伯特空间中的一个酉变换。算符  $U$  对应的本征态  $|\psi\rangle$  的本征值为  $e^{2\pi i\varphi}$ ，即

$$U|\psi\rangle = e^{2\pi i\varphi}|\psi\rangle \quad (2.28)$$

其中  $0 \leq \varphi < 1$  的值是未知的。量子相位估计算法就是要通过执行受控  $U$ ，受控  $U^{2^1}$ ，受控  $U^{2^2}$  等一系列受控门来给出对于  $\varphi$  有限精确的估计值。即对于  $\varphi$  的估计值精确到  $L$  位。

对于量子相位估计算法来说量子寄存器包含两部分，第一部分寄存器由  $L$  个量子比特构成，他们的初态为  $|0\rangle$ ，这  $L$  个量子比特负责估计相位。具体  $L$  取多少

取决于想要估计相位的精度，以及希望相位估计过程的成功率。第二部分寄存器用来输入被估计相位的本征态  $|\psi\rangle$ 。第二部分寄存器的维数要等于本征态  $|\psi\rangle$  的维数。

量子相位估计算法的第一阶段量子线路图如图 2.3。

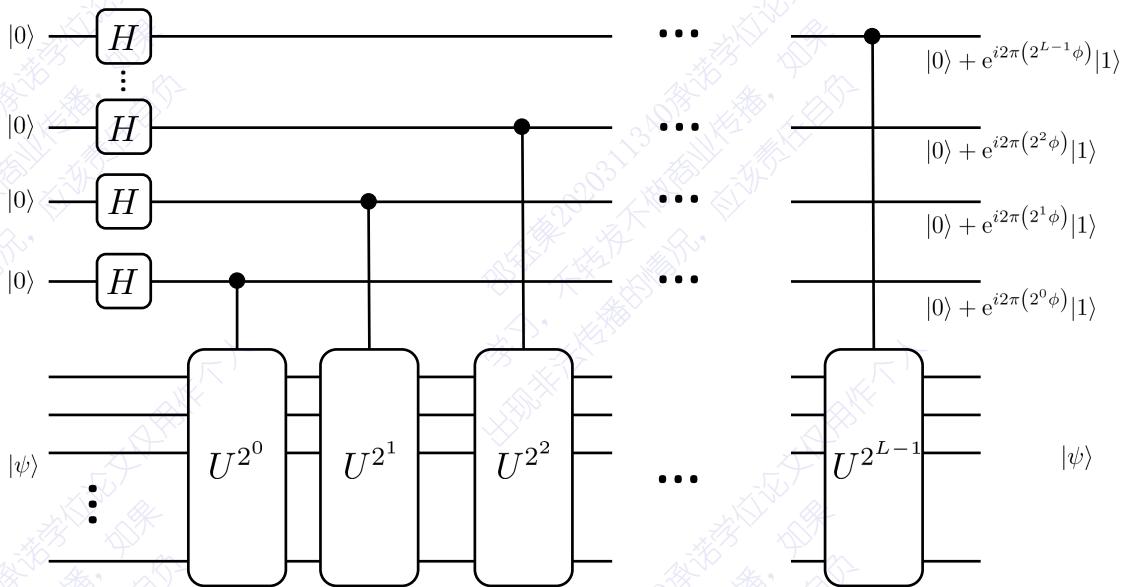


图 2.3 相位估计算法第一阶段量子线路图

首先制备初态  $|0\rangle^{\otimes L}|\psi\rangle$ 。之后对第一量子存储器  $L$  个量子比特执行  $L$  比特沃尔什-哈达玛门  $H^{\otimes L}$ :

$$\frac{1}{2^{L/2}}(|0\rangle + |1\rangle)^{\otimes L}|\psi\rangle \quad (2.29)$$

在量子线路图 2.3 中的  $U|\psi\rangle = e^{2\pi i \varphi}|\psi\rangle$ ，因此

$$U^{2^j}|\psi\rangle = U^{2^{j-1}}U|\psi\rangle = U^{2^{j-1}}e^{2\pi i \varphi}|\psi\rangle = e^{2\pi i 2^j \varphi}|\psi\rangle \quad (2.30)$$

接下来要对式 (2.30) 施加受控  $U$  操作，即第一寄存器中第  $L$  量子位为  $|1\rangle$  时对第二寄存器施加  $U^{2^0}$  操作，操作后的结果为

$$\frac{1}{2^{L/2}}\left(|0\rangle|\psi\rangle + e^{2\pi i 2^0 \varphi}|1\rangle|\psi\rangle\right) \otimes (|0\rangle + |1\rangle)^{\otimes L-1} \quad (2.31)$$

$$= \frac{1}{2^{L/2}}\left(|0\rangle + e^{2\pi i 2^0 \varphi}|1\rangle\right) \otimes (|0\rangle + |1\rangle)^{\otimes L-1}|\psi\rangle \quad (2.32)$$

之后再接着作用图 2.3 中其他  $L - 1$  个受控  $U^{2^j}$  门操作，第一量子存储器的状态变为：

$$\frac{1}{2^{L/2}}\left(|0\rangle + e^{2\pi i 2^{L-1} \varphi}|1\rangle\right) \otimes \dots \otimes \left(|0\rangle + e^{2\pi i 2^1 \varphi}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i 2^0 \varphi}|1\rangle\right) \quad (2.33)$$

$$= \frac{1}{2^{L/2}} \sum_{k=0}^{2^n-1} e^{2\pi i \varphi k} |k\rangle \quad (2.34)$$

这里将相位角  $\varphi$  用二进制表示为  $\varphi = 0.\varphi_1\varphi_2 \dots \varphi_L$  则式 (2.33) 可重写为

$$\frac{1}{2^{L/2}} (|0\rangle + e^{2\pi i 0.\varphi_L} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i 0.\varphi_{L-1}\varphi_L} |1\rangle) \otimes (|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2 \dots \varphi_L} |1\rangle) \quad (2.35)$$

比较此式与式 (2.11) 可以看出，此式正是相位态  $|\varphi_1\varphi_2 \dots \varphi_L\rangle$  的傅里叶变换。第二阶段如图 2.4 将对此态进行傅里叶逆变换。即紧接着在计算基底上对第一量子寄存器进行测量就可以精确地得到相位角  $\varphi$  的值。

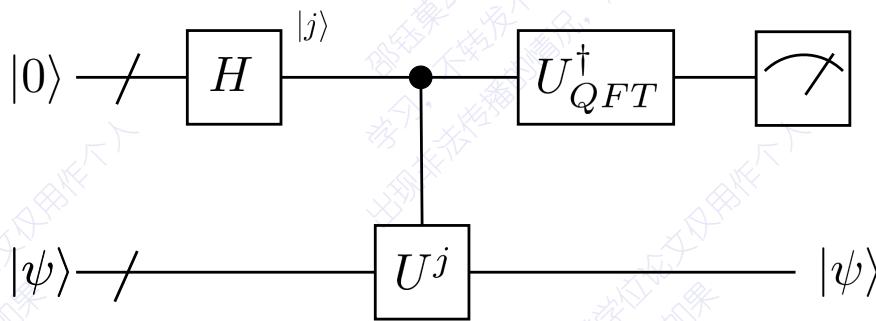


图 2.4 相位估计算法量子线路图

下面将讨论如果相位角  $\varphi \in [0, 1]$  无法严格地用  $L$  位二进制数表示的情况下，该算法的成功率。这时  $2^L \varphi$  可以被近似地表示为与其最近邻的整数  $a$ 。即表示为  $2^L \varphi = a + 2^L \delta$ ，其中  $2^L \delta$  表示与整数  $a$  的偏差，满足  $0 \leq |2^L \delta| \leq \frac{1}{2}$ 。这时对式 (2.34) 傅里叶逆变换的结果为

$$\frac{1}{2^L} \sum_{x=0}^{2^L-1} \sum_{k=0}^{2^L-1} e^{-\frac{2\pi i k}{2^L}(x-a)} e^{2\pi i \delta k} |x\rangle \quad (2.36)$$

对第一量子寄存器在计算基底上进行测量得到最准确的近似值  $|a\rangle$  的概率为

$$\begin{aligned} \Pr(a) &= \left| \langle a | \frac{1}{2^L} \sum_{x=0}^{2^L-1} \sum_{k=0}^{2^L-1} e^{-\frac{2\pi i k}{2^L}(x-a)} e^{2\pi i \delta k} |x\rangle \right|^2 = \frac{1}{2^{2L}} \left| \sum_{k=0}^{2^L-1} e^{2\pi i \delta k} \right|^2 \\ &= \begin{cases} 1 & \delta = 0 \\ \frac{1}{2^{2L}} \left| \frac{1-e^{2\pi i 2^L \delta}}{1-e^{2\pi i \delta}} \right|^2 & \delta \neq 0 \end{cases} \end{aligned} \quad (2.37)$$

当  $\delta = 0$  时，估计值是准确的（即  $a = 2^L \varphi$ ）情况下， $\Pr(a)=1$  也就是每次都能得到准确的相位估计值。

当  $\delta \neq 0$  时, 由式 (2.37) 可以得到成功率的下界

$$\Pr(a) = \frac{1}{2^{2L}} \left| \frac{1 - e^{2\pi i 2^L \delta}}{1 - e^{2\pi i \delta}} \right|^2 \geq \frac{4}{\pi^2} \approx 0.405 \quad (2.38)$$

如果希望将  $\varphi$  的估计值以成功率  $1 - \epsilon$  精确到  $1/2^{L+1}$  可以增加第一量子存储器的量子比特数到  $L' = L + \lceil \log_2 \left( \frac{1}{2\epsilon} + 2 \right) \rceil$ <sup>[119]</sup>。

## 2.3 Shor 算法

目前应用最多的加密算法则是基于大数质因子分解的 RSA 加密算法<sup>[6]</sup>。使用目前最快的经典算法——普通数域筛选法<sup>[120-121]</sup>对于一个大数  $N$  进行分解其时间复杂度为  $O(e^{1.9(\log N)^{1/3}(\log \log N)^{2/3}})$ 。在 1994 年 Peter Shor 提出了著名的 Shor 算法<sup>[7,16]</sup>, 其时间复杂度为  $O((\log N)^3)$ 。这表明大数分解问题使用量子计算机可在多项式时间内求解。因此未来一旦通用量子计算机量产, RSA 算法的安全性将受到挑战。Shor 算法包含两个部分, 首先是应用经典计算机运行的简化算法, 将大数分解简化成搜索求阶的问题。第二步则是应用量子计算机求解求阶问题。量子求阶问题则是 2.2 节介绍的量子相位估计算法的应用。下面将介绍 Shor 算法的具体过程。

### 2.3.1 大数分解问题转化为求阶问题

这里先给出需要用到的数学部分。

**定义 2.1:** 若存在最小的非零整数  $r$  使得

$$a^r \equiv 1 \pmod{N} \quad (2.39)$$

成立, 则称  $r$  为  $a$  的阶。

其中式 (2.39) 则表示  $a^r$  除以  $N$  的余数为 1。对于任意合数  $N$  有以下定理:

**定理 2.1:** 对于任意合数  $N$ , 随机选择数字  $a < N$  使得  $a$  满足如下 3 点: (1) 与  $N$  互质, (2)  $a$  的阶  $r$  为偶数, (3)  $a^{r/2} \not\equiv -1 \pmod{N}$ , 则  $\gcd(a^{r/2} + 1, N)$  与  $\gcd(a^{r/2} - 1, N)$  必是  $N$  的因子。

其中  $\gcd(a^{r/2} + 1, N)$  则代表  $a^{r/2} + 1$  与  $N$  的最大公约数。

对定理 2.1 的证明过程如下:

**证明:** 对于满足三点条件的  $a$ , 根据阶的定义 2.1:  $a^r \equiv 1 \pmod{N}$  有  $a^r - 1 \equiv 0 \pmod{N}$ , 即  $(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) \equiv 0 \pmod{N}$  这表明  $(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1)$  是  $N$

的整数倍，因此  $a^{r/2} \pm 1$  与  $N$  的最大公约数  $\gcd(a^{r/2} \pm 1, N)$  必然是  $N$  的因子。 ■

为了清楚的展示定理 2.1，这里举一个最简单的例子，考虑  $N = 15$ ，取  $a = 7$ ，可以得到

表 2.1 以 15 为例展示定理 2.1 的质因数分解

$x$	0	1	2	3	4	5	6	...
$7^x$	1	7	49	343	2401	16807	117649	...
$f_{7,15}(x)$	1	7	4	13	1	7	4	...

可以明显看出  $r = 4, a^{r/2} = 49$ ，通过计算可得  $\gcd(49+1, 15) = 5, \gcd(49-1, 15) = 3$ 。这样就得到 15 的两个质因子 3 和 5。定理 2.1 成功的把分解大数质因子问题转化为了求阶的问题。求阶问题又该如何高效的解决呢？事实上求阶问题又可以转化为求函数周期的问题。首先构造函数

$$f_{a,N}(x) = a^x \pmod{N} \quad (2.40)$$

容易证明此函数为一周期函数。在表格 2.2 可以直观地看出函数  $f_{a,N}(x)$  周期等于  $a$  的阶。

表 2.2 函数  $f_{a,N}(x)$  的周期与  $a$  的阶

$x$	0	1	2	...	$r-1$	$r$	$r+1$	...
$a^x$	1	$a$	$a^2$	...	$a^{r-1}$	$a^r$	$a^{r+1}$	...
$f_{a,N}(x)$	1	$a$	$a^2$	...	$a^{r-1}$	1	$a$	...

而函数的周期可以通过量子相位估计算法来求得。这又把分解大数的问题转换为了量子相位估计问题。具体的 Shor 算法流程图下：

- 判断  $N$  是否为偶数，若是则终止程序并且输出 2，若否则执行下一步操作
- 选择任意小于  $N$  的数  $a$
- 运用经典计算机算  $N$  与  $a$  的最大公约数  $\gcd(a, N)$ 。若  $\gcd(a, N) \neq 1$  则终止程序并且输出  $a$ ；若  $\gcd(a, N) = 1$  则执行下一步操作
- 定义函数  $f_{a,N}(x) = a^x \pmod{N}$ ，在量子计算机上寻找函数  $f_{a,N}(x)$  的周期（即  $a$  的阶  $r$ ）
- 判断  $r$  是否满足既是偶数且  $a^{r/2} \neq -1 \pmod{N}$ ，如果满足则执行下一步操作，如果不满足则返回步骤 2，选择另一个  $a$  重新计算
- 运用经典计算机算输出  $\gcd(a^{r/2} + 1, N)$  与  $\gcd(a^{r/2} - 1, N)$  并终止程序。

关于在量子计算机上寻找函数  $f_{a,N}(x)$  周期的问题将在 2.3.2 小节交代。

### 2.3.2 求阶问题的量子算法

求阶问题的量子算法是量子相位估计算法的一个应用。求解函数  $f_{a,N}(x)$  周期的量子算法实际上是针对算符  $U$  的量子相位估计算法，其中

$$U|y\rangle \equiv |ay \bmod N\rangle \quad (2.41)$$

定义量子态  $|u_s\rangle$ :

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i sk}{r}} |a^k \bmod N\rangle \quad (2.42)$$

可以证明  $|u_s\rangle$  是算符  $U$  的本征态:

$$\begin{aligned} U|u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i sk}{r}} |a^{k+1} \bmod N\rangle \\ &= e^{\frac{2\pi i s}{r}} |u_s\rangle \end{aligned} \quad (2.43)$$

这正符合量子相位估计算法的先决条件式 (2.28)，看起来把量子相位估计算法的第二量子寄存器制备到态  $|u_s\rangle$  上即可完成相位估计输出  $s/r$ 。但事实上这是一个悖论，因为制备  $|u_s\rangle$  需要知道  $s/r$  的具体值。不过幸运的是这个问题可以完美地解决。因为如果把所有满足  $0 \leq s \leq r$  的量子态  $|u_s\rangle$  线性叠加起来，除了  $|1\rangle$  态会被保留，其他的基底相位会相互抵消。即

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \quad (2.44)$$

由于进行相位估计第二量子寄存器的输入态为  $|1\rangle$  即  $|u_s\rangle$  的线性叠加态，因而相位估计的结果则是  $s/r$  的线性叠加态  $\frac{1}{\sqrt{r}} \left( |2^n \cdot \frac{1}{r}\rangle + |2^n \cdot \frac{2}{r}\rangle + \dots + |2^n \cdot \frac{r-1}{r}\rangle \right)$ ，求阶问题的量子线路图 (图 2.5) 如下

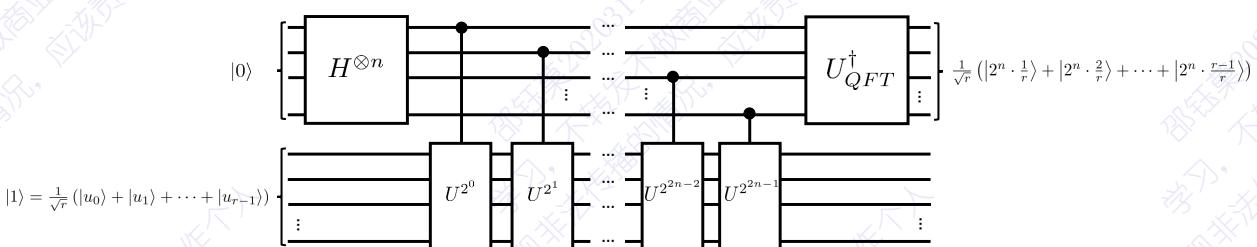


图 2.5 求阶问题的量子线路图

对于测量结果  $s/r$  可在经典计算机上使用连续分式分解算法得到  $r$ 。

## 2.4 线性方程组求解的量子算法

线性方程组求解问题在自然生活中的应用是非常广泛的，比如求解偏微分方程问题，流体力学问题，数值模拟问题。线性方程组问题就是给一个矩阵  $A \in \mathbb{C}^{N \times N}$  和一个列向量  $\vec{b} \in \mathbb{C}^N$ ，求解向量  $\vec{x} \in \mathbb{C}^N$  满足  $A\vec{x} = \vec{b}$ 。线性方程组求解的量子算法复杂度为  $O(\log(N)\kappa^2/\epsilon)$ ，其中  $N$  为变量的数目， $\kappa$  为矩阵  $A$  的最大与最小奇异值之比。 $\epsilon$  为解的误差。而求解线性方程组最好的经典算法的复杂度为  $O(N\kappa)$ 。因此可以看到量子算法相较经典算法有加速的特性。同时量子线性方程组算法也为后续量子算法的发展提供了坚实的基础。比如量子主成分分析算法<sup>[122]</sup>，量子最小二乘拟合算法<sup>[123]</sup>，量子支持向量机算法<sup>[124]</sup>等都是基于此算法发展而来的。本小节将简要介绍量子线性方程组求解算法的基本思路。

量子线性方程组求解算法<sup>[62]</sup>的第一步是将线性方程组问题编码到量子态上。通过归一化操作，将  $\vec{b}$  和  $\vec{x}$  编码到量子态  $|b\rangle$  和  $|x\rangle$  上。通常将向量  $\vec{b}$  的第  $i$  个分量编码到量子态  $|b\rangle$  的第  $i$  个概率幅上。因此在量子态上线性方程组则表示为

$$A|x\rangle = |b\rangle \quad (2.45)$$

因为  $A$  是厄米矩阵，所以可以写成谱分解的形式

$$A = \sum_{j=0}^{N-1} \lambda_j |u_j\rangle\langle u_j|, \quad \lambda_j \in \mathbb{R} \quad (2.46)$$

其中  $|u_j\rangle$  是矩阵  $A$  的第  $j$  个本征态。然后矩阵  $A$  的逆可以写为

$$A^{-1} = \sum_{j=0}^{N-1} \lambda_j^{-1} |u_j\rangle\langle u_j| \quad (2.47)$$

方程组右边可以写成  $A$  的本征态的形式

$$|b\rangle = \sum_{j=0}^{N-1} b_j |u_j\rangle, \quad b_j \in \mathbb{C} \quad (2.48)$$

最后的目标则是让量子线性方程组求解算法输出

$$|x\rangle = A^{-1}|b\rangle = \sum_{j=0}^{N-1} \lambda_j^{-1} b_j |u_j\rangle \quad (2.49)$$

具体的线性方程组求解的量子算法包含量子相位估计算法，受控  $R(\tilde{\lambda}^{-1})$  旋转部分，以及复位操作（即量子相位估计算法的逆）三部分构成（如图 2.6）。首先按照式 (2.48) 在量子寄存器 3 上制备量子态  $|b\rangle = \sum_{j=0}^{N-1} b_j |u_j\rangle$ ，则系统的总量子态

为

$$\sum_{j=0}^{N-1} b_j |u_j\rangle_3 \otimes |0\rangle_2^{\otimes n} \otimes |0\rangle_1 \quad (2.50)$$

紧接着进行相位估计算法后量子态变为

$$\sum_{j=0}^{N-1} b_j |u_j\rangle_3 \otimes |\tilde{\lambda}_j\rangle_2 \otimes |0\rangle_1 \quad (2.51)$$

其中量子态的下角标代表量子寄存器的编号,  $\tilde{\lambda}_j$  是对本征值  $\lambda_j$  有限精度的二进制表示。受控旋转则是根据  $\theta \in \mathbb{R}$  的有限比特数近似  $\tilde{\theta}$  进行受控  $R_y(\tilde{\theta})$  的旋转。具体的

$$R_y(\tilde{\theta}) = \exp(-i\tilde{\theta}\sigma_y) = \begin{bmatrix} \cos(\tilde{\theta}) & -\sin(\tilde{\theta}) \\ \sin(\tilde{\theta}) & \cos(\tilde{\theta}) \end{bmatrix}, \quad \tilde{\theta} = \arccos(C/\tilde{\lambda}) \quad (2.52)$$

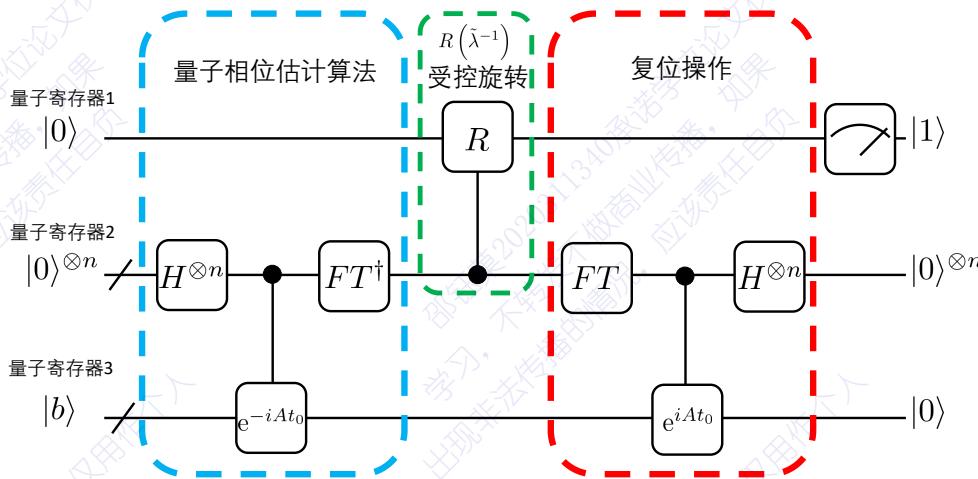


图 2.6 线性方程组求解的量子算法线路图

其中  $C$  为归一化常数。受控旋转  $R(\tilde{\lambda}^{-1})$  获取  $A^{-1}$  的本征值并根据  $\lambda_j$  进行旋转, 产生

$$\sum_{j=0}^{N-1} b_j |u_j\rangle_3 \otimes |\lambda_j\rangle_2 \otimes \left( \sqrt{1 - \frac{C^2}{\tilde{\lambda}_j^2}} |0\rangle + \frac{C}{\tilde{\lambda}_j} |1\rangle \right)_1 \quad (2.53)$$

最后进行复位操作 (即量子相位估计的逆运算) 将量子寄存器 2 复位至  $|0\rangle^{\otimes n}$ 。经过复位操作后量子态演化为

$$\sum_{j=0}^{N-1} b_j |u_j\rangle_3 \otimes |0\rangle_2^{\otimes n} \otimes \left( \sqrt{1 - \frac{C^2}{\tilde{\lambda}_j^2}} |0\rangle + \frac{C}{\tilde{\lambda}_j} |1\rangle \right)_1 \quad (2.54)$$

对量子寄存器 1 进行测量，测量结果为  $|1\rangle$  时，则该算法成功，反之重新执行此量子算法。最终得到成功时的量子寄存器 3 的输出态

$$\sum_{j=1}^N \frac{b_j}{\tilde{\lambda}_j} |u_j\rangle \quad (2.55)$$

此态即为线性方程组  $A\vec{x} = \vec{b}$  的解。

## 2.5 量子搜索算法

量子搜索算法<sup>[17,125-129]</sup>是量子算法中最重要的算法之一。如果要在容量为  $N$  的无序数据库中搜索出唯一解，经典过程需要进行  $O(N)$  次搜索。如果在量子计算机上运用量子搜索算法进行该过程只需要进行  $O(\sqrt{N})$  次搜索。因此量子搜索算法与经典的搜索算法相比具有二次加速的特点。因此，量子搜索算法可以仅用多项式时间<sup>[130-131]</sup>解决一些经典算法无法在多项式时间内解决的问题，如一些尚未解决的 NP 问题。在实际密码学应用上，量子搜索算法对于 AES 算法<sup>[132]</sup>和 Hash 加密算法<sup>[133]</sup>的破解都有着非同一般的意义。

### 2.5.1 Grover 搜索算法

Grover 提出了第一个量子搜索算法<sup>[17,61]</sup>，它仅需迭代  $O(\sqrt{\frac{N}{M}})$  次<sup>[134-135]</sup>即可从容量为  $N$  的非结构化数据库中找到  $M$  个目标态。Grover 搜索量子线路图如图 2.7，整个 Grover 搜索过程可以分解为一次次的 Grover 迭代过程（图 2.7 的虚线框代表单次 Grover 迭代）。在每次迭代中都将目标态的概率幅放大，随之而来的是非目标态的概率幅减小。在经过几次迭代后对量子态进行测量，则目标态会以较高的概率作为测量结果出现。每一次 Grover 迭代可分为四个步骤：标记过程，沃尔什-哈达玛变换，相移过程，沃尔什-哈达玛变换。首先介绍标记过程。

在一个容量为  $N$  的数据库中进行搜索，对每个态进行编码，则这些数字的范围是从 0 到  $N - 1$ 。令  $N = 2^n$  则  $n$  个量子比特可以存储这些状态。若有  $M$  个状态为目标态。其中  $1 < M < N$ 。构造函数  $f(x)$  其定义域为  $[0, N - 1]$ ，值域为  $\{0, 1\}$ 。若  $x$  所编码的状态是目标态则函数值为 1，否则为 0。

定义算符  $U_\omega$ ：

$$|x\rangle|q\rangle \xrightarrow{U_\omega} |x\rangle|q \oplus f(x)\rangle \quad (2.56)$$

其中  $|x\rangle$  为数据位， $|q\rangle$  为指示位。如果  $|x\rangle$  是目标态，则输出  $|x\rangle|q \oplus 1\rangle$ ，否则输出

$|x\rangle|q\oplus 0\rangle$ 。具体的实现可以参照 Deutsch-Jose<sup>[136]</sup> 算法。该算法完成的过程如下：

$$|x\rangle \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{U_\omega} (-1)^{f(x)} |x\rangle \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (2.57)$$

可以注意到指示位没有发生任何变化，因此为了简化书写通常略去第二位，记作：

$$|x\rangle \xrightarrow{U_\omega} (-1)^{f(x)} |x\rangle \quad (2.58)$$

这就完成了标记过程。

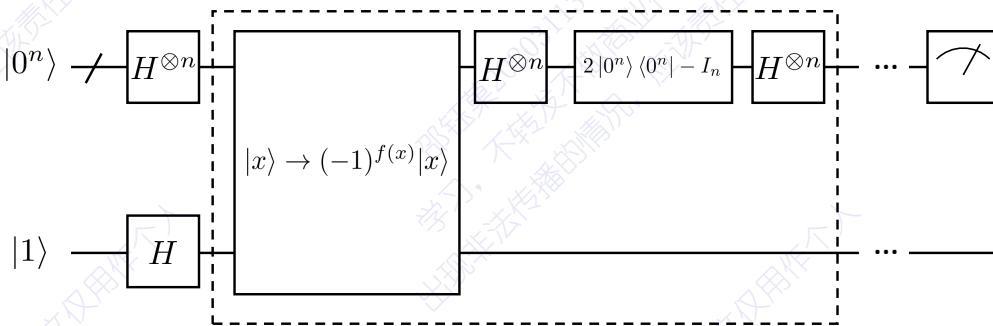


图 2.7 Grover 算法线路图

下面将介绍相移过程，相移过程的操作则是将非 0 态进行相位反转。即

$$\begin{aligned} |0\rangle &\rightarrow |0\rangle \\ |x\rangle &\rightarrow -|x\rangle \end{aligned} \quad (2.59)$$

可验证相移过程对应的算符为  $2|0^n\rangle\langle 0^n| - I_n$ 。可定义算符  $U_s$

$$U_s = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|s\rangle\langle s| - I \quad (2.60)$$

其中  $|s\rangle$  为均匀叠加态，则每次 Grover 迭代的算符为：

$$G = U_s U_\omega = (2|s\rangle\langle s| - I)U_\omega \quad (2.61)$$

迭代  $G$  算符  $O(\sqrt{N/M})$  次后对末态进行测量，则可以较高的概率得到符合目标态的目标态。

接下来将介绍 Grover 算法的几何描述，在希尔伯特空间中，算符  $G$  的作用就是通过旋转将目标态的概率幅尽可能地放大，使其从均匀叠加态通过旋转接近目标态。首先通过一个态是否是目标态定义等价关系，这可以将空间分为两大等价类。如下：

$$\begin{aligned} |s'\rangle &= \frac{1}{\sqrt{N-M}} \sum_{x \neq T} |x\rangle \\ |\omega\rangle &= \frac{1}{\sqrt{M}} \sum_{x=T} |x\rangle \end{aligned} \quad (2.62)$$

其中  $T$  代表目标态,  $|s'\rangle$  代表非目标态的叠加,  $|\omega\rangle$  代表目标态的叠加, 则初始态可写为:

$$|s\rangle = \sqrt{\frac{N-M}{N}}|s'\rangle + \sqrt{\frac{M}{N}}|\omega\rangle \quad (2.63)$$

在由  $|s'\rangle$  和  $|\omega\rangle$  这两个正交基底所张成的空间中, 则搜索过程如下图 2.8 所示

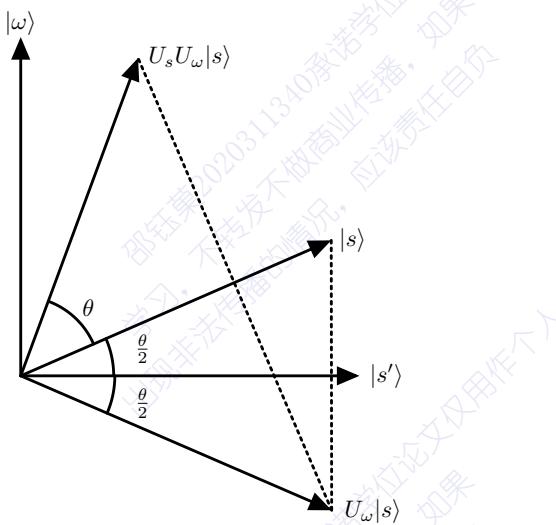


图 2.8 Grover 算法的几何描述

算符  $U_\omega$  的作用是以  $|s'\rangle$  为轴做一个镜面反演:

$$U_\omega(a|s'\rangle + b|\omega\rangle) = a|s'\rangle - b|\omega\rangle \quad (2.64)$$

然后算符  $U_s$  的作用是以初态  $|s\rangle$  为轴做一个镜面反演。对于 Grover 算符令:

$$\cos\left(\frac{\theta}{2}\right) = \sqrt{\frac{(N-M)}{N}} \quad (2.65)$$

则经过第一次搜索后的量子态为:

$$G|s\rangle = \cos\frac{3\theta}{2}|s'\rangle + \sin\frac{3\theta}{2}|\omega\rangle \quad (2.66)$$

经过  $K$  次搜索的量子态为:

$$G^k|s\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|s'\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\omega\rangle \quad (2.67)$$

Grover 算法开创了量子搜索算法的先河。但其也存在着待改进的地方, 比如 Grover 算法没有办法确定需要迭代的次数。如果迭代次数过多就会使得目标态转过极值点, 出现目标态减小的过程, 这就是搜索过度的问题<sup>[137]</sup>。其次 Grover 算法有的时候成功率很低, 甚至出现了 0 的情况, 只有少数几个特殊的状态才能达到 100%。面对这些问题, 人们提出了一些改进版的算法<sup>[125-126,138-140]</sup>。接下来将

介绍其中最有代表性的三种改进版本。

### 2.5.2 Grover-Long 算法

对于 Grover 算法的缺陷，人们提出了种种改进方案，其中最成功，最简便<sup>[129,141]</sup>的方案就是由清华大学龙桂鲁教授于 2001 年提出的 Grover-Long 算法<sup>[125-127]</sup>。Grover-Long 算法可以通过搜索  $O\left(\sqrt{\frac{N}{M}}\right)$  次。从具有  $N$  个项目的非结构化数据库中提取  $M$  个标志态。首先，从给定的比率  $\frac{M}{N}$ ，可以计算出参数  $\beta$ ，具体过程如下：

$$\beta = \arcsin \sqrt{\frac{M}{N}} \quad (2.68)$$

它进一步用于确定搜索步骤  $j_{op} = \left\lfloor \frac{\pi - 2\beta}{4\beta} \right\rfloor$  的值。这里的方括号代表取整函数。可以将迭代次数设置为

$$J \geq j_{op} \quad (2.69)$$

然后，搜索算法中的相位由下式计算

$$\phi = 2 \arcsin \left( \frac{\sin \frac{\pi}{4J+6}}{\sin \beta} \right) \quad (2.70)$$

接下来，询问算子可以表示为

$$I_\tau = I + (e^{i\phi} - 1) |\tau\rangle\langle\tau| \quad (2.71)$$

相移算子可以写作

$$I_0 = I + (e^{i\phi} - 1) |0\rangle\langle 0| \quad (2.72)$$

最后，每次迭代中的 Grover-Long 算子为

$$Q = -HI_0HI_\tau \quad (2.73)$$

其中  $H$  是沃尔什-哈达玛变换。经过  $J + 1$  步迭代，则可以以 100% 的成功率得到目标态。当  $\phi = \pi$  时，Grover-Long 算法退化为原始的 Grover 算法。Grover-Long 算法既保留了原始 Grover 算法二次加速的优点又改良了原始算法的种种缺点使得每次搜索均能达到 100% 的成功率。

### 2.5.3 定点搜索算法

面对原始 Grover 算法的不足。Grover 在 2005 年提出了定点搜索算法<sup>[128]</sup>。在该算法的搜索过程中越接近目标态旋转的越慢，永远都无法达到目标态，只是无限地趋近于目标态。这种算法是基于龙桂鲁提出的全相位量子搜索算符<sup>[126]</sup>构造。

即将原始 Grover 算法中旋转推广到更一般的复平面。具体推广后的算符如下：

$$\begin{aligned} R_s &= I - \left[ 1 - e^{i\frac{\pi}{3}} \right] |s\rangle\langle s| \\ R_t &= I - \left[ 1 - e^{i\frac{\pi}{3}} \right] |t\rangle\langle t| \end{aligned} \quad (2.74)$$

其中  $|s\rangle$  为  $|0\rangle^{\otimes n}$ ,  $|t\rangle$  为目态。其作用形式与原始 Grover 算法类似

$$UR_sU^\dagger R_tU|s\rangle \quad (2.75)$$

不同的是这里的  $U$  算符是上一次搜索算符的整体，通项公式为：

$$U_{m+1} = U_m R_s U_m^\dagger R_t U_m \quad U_0 = H \quad (2.76)$$

具体的如下：

$$\begin{aligned} U_0 &= H \\ U_1 &= U_0 R_s U_0^\dagger R_t U_0 = H R_s H^\dagger R_t H \\ U_2 &= U_1 R_s U_1^\dagger R_t U_1 = (H R_s H^\dagger R_t H) R_s (H R_s H^\dagger R_t H)^\dagger R_t (H R_s H^\dagger R_t H) \\ &= U (R_s H^\dagger R_t H) (R_s H^\dagger R_t H)^\dagger (R_s H^\dagger R_t H) (R_s H^\dagger R_t H) \end{aligned} \quad (2.77)$$

该算法虽然克服了搜索过度的问题，但却是以复杂度增加为代价的。

#### 2.5.4 Yoder-Low-Chuang 搜索算法

面对原始 Grover 算法的不足，Isaac L. Chuang 研究组提出 Yoder-Low-Chuang 搜索算法<sup>[129]</sup>，该算法通过利用切比雪夫多项式巧妙地构造了一个函数，一旦选定了误差，该函数会在一定范围内震荡。给定一个误差范围  $\delta$ ，然后成功率就在区间  $[1 - \delta^2, 1]$  之中。该算法中  $|s\rangle$  代表初始状态， $|t\rangle$  代表目态，则：

$$|s\rangle = \sqrt{1 - \lambda} |t\rangle + \sqrt{\lambda} |t\rangle \quad (2.78)$$

其中  $\lambda$  表示重叠程度

$$\langle t|s\rangle = \sqrt{\lambda} e^{i\xi} \quad (2.79)$$

$T_L$  为  $L$  阶切比雪夫多项式

$$T_L(x) = \cos [L \cos^{-1}(x)] \quad (2.80)$$

对于给定的误差范围，可由下式给出  $L$

$$L \geq \frac{\log\left(\frac{2}{\delta}\right)}{\sqrt{\lambda}} \quad (2.81)$$

其中  $L$  必须取奇数。对于选定的  $L$  可通过以下公式计算出幅角：令  $j = 1, 2, \dots, l$

$$\alpha_j = -\beta_{l-j+1} = 2 \cot^{-1} \left( \tan \left( \frac{2\pi j}{L} \right) \sqrt{1-\gamma^2} \right) \quad (2.82)$$

其中  $L = 2l + 1, \gamma^{-1} = T_{1/L} \left( \frac{1}{\delta} \right)$ , 通过以上计算确定了搜索算符：

$$\begin{aligned} S_s(\alpha) &= I - (1 - e^{-i\alpha}) |s\rangle\langle s| \\ S_t(\beta) &= I - (1 - e^{i\beta}) |t\rangle\langle t| \end{aligned} \quad (2.83)$$

其中  $\bar{\lambda} = 1 - \lambda$ 。则每一个搜索单元为

$$G(\alpha, \beta) = -S_s(\alpha)S_t(\beta)$$

搜索  $l$  次操作的算符为

$$S_L = G(\alpha_l, \beta_l) \cdots G(\alpha_1, \beta_1) = \prod_{j=1}^l G(\alpha_j, \beta_j) \quad (2.84)$$

Chuang 在文章中给出了严格的证明，按照以上方式搜索的成功率为

$$P_L = |\langle t | S_L | s \rangle|^2 = 1 - \delta^2 T_L \left( T_{1/L}(1/\delta) \sqrt{1-\lambda} \right)^2 \quad (2.85)$$

该算法克服了原始 Grover 算法的搜索过度的问题，同时保持了算法二次加速的特点。

## 2.6 全量子本征求解器

之前介绍了一系列基于量子计算直乘模式的量子算法，下面将介绍一个基于量子计算对偶模式的量子算法——全量子本征求解器<sup>[142]</sup>。这里的全量子指的是不需要在经典与量子计算机上来回交互。本算法可以完全在量子计算机上完成本征求解问题。不需要运用经典计算机来求梯度。本算法可应用于量子化学模拟。下面将介绍运用全量子本征求解器求解分子基态能级的大致过程。

对于分子系统可通过原子核与电子的哈密顿量来描述，通过 Jordan-Wigner 或 Bravyi-Kitaev 变换可将分子的哈密顿量映射到量子比特的哈密顿量上，即

$$\mathbf{H} = \sum_{i,\alpha} h_\alpha^i \sigma_\alpha^i + \sum_{i,j,\alpha,\beta} h_{\alpha\beta}^{ij} \sigma_\alpha^i \sigma_\beta^j + \dots \quad (2.86)$$

其中  $i, j$  表示作用的比特位，希腊字母则表示泡利矩阵的类型。显而易见的是式 (2.86) 的哈密顿量是酉算符的线性组合。在这里我们通过求解哈密顿量期望  $f(\mathbf{X}) = \mathbf{X}^T \mathbf{H} \mathbf{X}$  的极小值来计算分子基态的能量。在这里运用梯度下降的方法来给

出极小值。在哈密顿量最小值的问题上,  $f(\mathbf{X})$  的梯度可以表示为:

$$\nabla f(\mathbf{X}) = 2\mathbf{H}\mathbf{X} \quad (2.87)$$

运用量子算法来实现梯度下降, 被认为是量子态  $|\mathbf{X}\rangle$  在  $\mathbf{H}$  下的演化

$$|\mathbf{X}^{(t+1)}\rangle = (|\mathbf{X}^{(t)}\rangle - \gamma \mathbf{H} |\mathbf{X}^{(t)}\rangle) \quad (2.88)$$

令  $\gamma = 2\gamma_0$ , 则:

$$\mathbf{H}^g = \mathbf{I} - \gamma \mathbf{H} = \sum_{i=1}^M \beta_i \mathbf{H}_i^g \quad (2.89)$$

其中  $M$  是算符  $\mathbf{H}^g$  中泡利矩阵的个数。则梯度下降过程可写作:

$$|\mathbf{X}^{(t+1)}\rangle = \mathbf{H}^g |\mathbf{X}^{(t)}\rangle = \sum_{i=1}^M \beta_i \mathbf{H}_i^g |\mathbf{X}^{(t)}\rangle \quad (2.90)$$

在这里  $\mathbf{H}^g$  是酉算符的线性组合。因此需要使用量子计算的对偶模式<sup>[63-65]</sup>来实现, 如图 2.9。

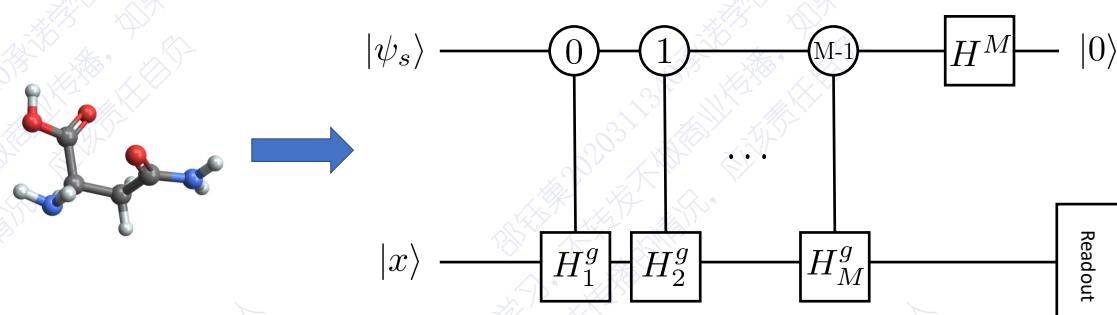


图 2.9 全量子本征求解器

首先将向量  $X = (x_1, \dots, x_N)^T$  编码到量子态  $|x^{(t)}\rangle$  上。在量子化学领域一般将 Hartree-Fock 态作为初态。将辅助比特制备为

$$|\psi_s\rangle = \frac{1}{C} \sum_{i=0}^{M-1} \beta_i |i\rangle \quad (2.91)$$

其中  $C = \sqrt{\sum_{i=0}^{M-1} \beta_i^2}$  是归一化常数。这时整个系统的状态为  $|\Psi\rangle = |\psi_s\rangle|x^{(t)}\rangle$ , 接下来作用一系列的受控泡利算符  $\sum_{i=0}^{M-1} |i\rangle\langle i| \otimes H_i^g$  后, 系统演化为

$$|\Phi\rangle \rightarrow \frac{1}{C} \left( \sum_{i=0}^{M-1} \beta_i |i\rangle H_i^g |x^{(t)}\rangle \right) \quad (2.92)$$

最后作用  $m$  个沃尔什-哈达玛门在辅助比特上, 对辅助比特进行测量并关注辅助比

特为 0 时，工作比特的状态

$$|\Phi_0\rangle = \frac{1}{C\sqrt{2^m}} \left( |0\rangle \sum_{i=0}^{M-1} \beta_i H_i^g |x^{(t)}\rangle \right) \quad (2.93)$$

此状态就是下一次量子梯度下降迭代的输入态。而每次辅助比特测量为 0 的概率为

$$P_s = \|H^g |x^{(t)}\rangle\|^2 / C^2 M \quad (2.94)$$

由于每次迭代都需要测到辅助比特为 0 才能进行下一步，因此测量次数会随着迭代的次数指数增加。但可以通过使用本文第 3 章提出的算法对每次迭代的振幅进行放大以提高算法整体的成功率。经过足够次数的迭代后， $|x\rangle$  将会收敛到基态， $\langle x|H|x\rangle$  对应的就是基态的能量。

## 2.7 本章小结

本章介绍了几个经典的量子信息处理算法。首先介绍的两类都是基于量子计算直乘模式的量子算法。第一类是以量子傅里叶变换为代表的量子相位估计算法，Shor 算法以及线性方程组求解算法，第二类则是量子搜索算法，包括原始的 Grover 搜索，Grover-Long 算法，还有两种定点搜索算法。最后介绍了基于量子计算对偶模式的全量子本征求解器。作者将在下一章提出改进版的搜索算法，该算法可用于进行对偶量子计算的振幅放大。

## 第3章 高鲁棒量子搜索算法

### 3.1 背景介绍

对于第2章2.5.1节中介绍的Grover算法，如果在最优迭代次数之后进行测量，则有 $P_{max} = \sin^2[(2j_{op} + 1)\beta]$ 的成功概率找到目标态，其中 $\beta = \arcsin \sqrt{\frac{M}{N}}$ ， $j_{op} = [\frac{\frac{\pi}{2} - \beta}{2\beta}]$ 则是最佳Grover迭代次数。可以看出只有当 $(2j_{op} + 1)\beta \approx \frac{\pi}{2}$ 时，最大成功率才接近1。这意味着只有当量子数据库的维度非常大时，Grover算法才有很高的成功率。但在某些情况下，例如结构化搜索<sup>[143]</sup>，其最终成功率是个体搜索成功率的乘积，因此每个个体搜索的高成功率都是至关重要的。另外，当维度不是那么大时，原始的Grover算法表现的也不是很好。为了解决这个问题，科学家提出了一些改进的搜索算法<sup>[125-126,138-140]</sup>。其中Grover-Long算法<sup>[125]</sup>已被证明是最简便和最优的<sup>[141,144]</sup>。该算法达到了100%的成功率，而原始的Grover算法只在4个当中找1个的情况下才能达到100%的成功率。

但在原始的Grover算法以及众多改进版算法中，都需要提前知道标记状态的确切数量。因此，如果未知确切的数量，这些算法无法确定何时停止<sup>[137]</sup>搜索。定点搜索算法是解决这一问题的方法之一。通过构造递归搜索算子，每次搜索后标记态的比例被放大，例如第2章2.5.3节介绍的Grover定点搜索算法。在该算法中，每次搜索量子态均单调地接近目标态，但该单调性以失去了原始Grover算法的二次加速为代价。

第2章2.5.4节介绍的Yoder-Low-Chuang算法保持了量子搜索的二次加速优势，同时实现了定点特性。它还解决了搜索过度的问题，但其成功率不像Grover的 $\frac{\pi}{3}$ 定点搜索算法那样单调递增，其误差 $\delta \in [0, 1]$ 可以被提前设定。但是，该算法每个搜索过程中搜索算符的相位需要通过求解超三角方程来计算。

本章提出了一种新的量子搜索算法，该算法克服了预先不知道精确的 $\frac{M}{N}$ 的问题，同时保留了原始Grover算法二次加速的优势。本算法具有搜索算子构造简单、具有一定程度的“定点”性质的优点，同时它在各种比率中都享有很高的成功率。在我们的算法中，我们不需要知道标记态的确切数目，而需要知道确切比例 $\lambda = \frac{M}{N}$ 范围内的一个近似值 $[\lambda_0, \lambda_0 + \Delta]$ 。我们算法的成功率受到参数 $\delta \in [0, 1]$ 的限制，成功率与 $\frac{\Delta}{\lambda_0}$ 有关。具体来说，我们算法中的搜索算符是由 $M/N$ 范围的下界 $\lambda_0$ 决定的。经过 $J + 1 - J_D$ 次迭代，最终搜索的成功率大于 $1 - \delta^2$ ，这里 $J_D$ 定义为 $\left\lceil \left( \frac{1}{2\sqrt{\lambda_0 + \Delta}} + \frac{4}{\pi} \right) \delta \right\rceil$ 。

本章的结构如下：首先，本章给出 Grover-Long 算法的几何描述。随后，本章研究了 Grover-Long 算法的成功率与迭代步骤的关系，并且给出迭代次数与成功率的关系式。然后，本章基于 Grover-Long 算法做出改进，提出了一个具有鲁棒性的搜索算法。并表明我们的算法对于  $\frac{M}{N}$  的误差具有鲁棒性。然后分别与 Yoder-Low-Chuang 算法、原始 Grover 算法和 Grover 定点搜索算法进行比较。最后，我们证明了对于完全未知  $\frac{M}{N}$  数值的数据库，我们的算法可以以大于 96% 的成功率找到目标态。只需要先估计  $M$ ，并且保证估计值的不确定度为  $\{M - \sqrt{M}, M + \sqrt{M}\}$ ，这可以使用量子计数算法来完成<sup>[145-146]</sup>。此外，运用对偶量子算法实现一些新奇的量子算法时需要对线路中的某一个或者多个量子位进行多次投影测量。投影测量只有在光学系统中可以完成，应用本章提出的算法可以对目标态的概率幅进行扩增，进而可等效地实现投影测量。同时，由于现实过程中会运用通用量子门集合来实现量子门操作，以及量子计算机实际操作过程中保真度不足和连续量子门之间非马尔可夫关联，导致无法给出准确的  $\frac{M}{N}$  值，需要引入不确定度。而本章提出算法的优势正是对于这种不确定度是具有鲁棒性的。本章的工作正是实现带有振幅放大的对偶量子算法的振幅放大功能。这为第 4 章与第 5 章的工作提供了铺垫。

### 3.2 Grover-Long 算法的几何描述

在这里作者将给出 Grover-Long 算法的几何描述。量子搜索算法可以使用 SO(3) 绘景<sup>[125,147]</sup> 而不是 SU(2) 来进行描述。在此绘景中，式 (2.73) 中的量子搜索算子可以映射到具有以下矩阵形式的 3 维空间旋转操作

$$R_Q = \begin{bmatrix} R_{11} & R_{12} & R_{13} \\ R_{21} & R_{22} & R_{23} \\ R_{31} & R_{32} & R_{33} \end{bmatrix} \quad (3.1)$$

其中矩阵  $R_Q$  的矩阵元<sup>[125]</sup>为

$$\begin{aligned} R_{11} &= \cos \phi (\cos^2 2\beta \cos \phi + \sin^2 2\beta) + \cos 2\beta \sin^2 \phi \\ R_{12} &= \cos \phi \sin \phi (\cos 2\beta - 1) \\ R_{13} &= -\cos \phi \sin 4\beta \sin^2 \frac{\phi}{2} + \sin 2\beta \sin^2 \phi \\ R_{21} &= -\cos 2\beta \cos \phi \sin \phi + \left(\cos^2 \frac{\phi}{2} - \cos 4\beta \sin^2 \frac{\phi}{2}\right) \sin \phi \\ R_{22} &= \cos \phi + \cos 2\beta \sin^2 \phi \end{aligned} \quad (3.2)$$

$$\begin{aligned}
 R_{23} &= -\cos \phi \sin 2\beta \sin \phi - \sin 4\beta \sin^2 \frac{\phi}{2} \sin \phi \\
 R_{31} &= -\sin 4\beta \sin^2 \frac{\theta}{2} \\
 R_{32} &= \sin 2\beta \sin \phi \\
 R_{33} &= \cos^2 2\beta + \cos \phi \sin^2 2\beta
 \end{aligned} \tag{3.3}$$

在每次搜索过程中量子态绕着  $\vec{l}$  轴旋转

$$\vec{l} = \begin{bmatrix} \cos \frac{\phi}{2} \\ \sin \frac{\phi}{2} \\ \cos \frac{\phi}{2} \tan \beta \end{bmatrix} \tag{3.4}$$

旋转的角度为

$$\alpha = 4 \arcsin \left[ \sin \left( \frac{\phi}{2} \right) \sin \beta \right] = \frac{2\pi}{2J+3} \tag{3.5}$$

在此绘景中，一个量子态  $|\psi\rangle = (a+bi)|\tau\rangle + (c+di)|\bar{\tau}\rangle$  被表示为：

$$\vec{r}_\psi = \langle \psi | \vec{\sigma} | \psi \rangle = \begin{bmatrix} 2(ac+bd) \\ 2(-bc+ad) \\ a^2+b^2-c^2-d^2 \end{bmatrix} \tag{3.6}$$

其中  $\vec{\sigma} = \sigma_x \vec{i} + \sigma_y \vec{j} + \sigma_z \vec{k}$ 。 $\vec{i}, \vec{j}, \vec{k}$  是沿着轴  $x, y, z$  的单位向量。初态为  $|\psi_i\rangle$  被表示为  $\vec{r}_i$  目标态  $|\tau\rangle$  被表示为  $\vec{r}_f$

$$\vec{r}_i = \begin{bmatrix} \sin(2\beta) \\ 0 \\ -\cos(2\beta) \end{bmatrix}, \quad \vec{r}_f = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \tag{3.7}$$

每个搜索步骤都是将  $\vec{r}_\psi$  向  $\vec{r}_f$  旋转。对于 Grover-Long 算法在 SO(3) 绘景下的描述如图 3.1。

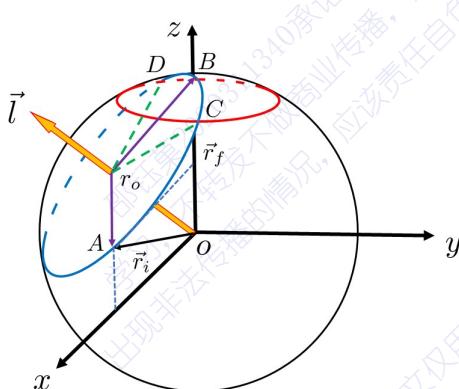


图 3.1 Grover-Long 搜索算法的几何描述。

在图 3.1 中, 每次迭代期间, 向量  $\overline{OA}$  围绕  $\vec{l}$  旋转一个角度  $\alpha$ 。经过  $J + 1$  次迭代,  $\overline{OA}$  与目标态  $|\tau\rangle$ (即  $\overline{OB}$ ) 重叠。在图 3.1 中, 若对  $\overline{OA}$  进行测量, 则找到标记态的概率是  $\frac{z_A+1}{2}$ <sup>[125]</sup>, 其中  $z_A$  是点 A 的 z 分量。

### 3.3 Grover-Long 算法的成功率与搜索迭代次数的关系

为了提出对于占比不确定度具有鲁棒性的改进版算法, 作者将先在  $SO(3)$  绘景下寻找 Grover-Long 算法成功率与迭代次数的关系。整个 Grover-Long 算法的搜索过程(如图 3.1), 就是 A 点沿着圆  $\odot r_o$  转向 B 点。在图 3.1 中, 每一瞬间测量该算法成功获得标记态的概率是  $\frac{z_A+1}{2}$ <sup>[125]</sup>, 其中  $z_A$  是点 A 的 z 分量。因此, 如果想要以大于  $1 - \delta^2$  的成功率获得目标态, 线段  $\overline{r_oA}$  上的 A 点必须要旋转到圆弧  $\widehat{CD}$  上, 其中 C 点和 D 点是圆  $\odot r_o$  与红色误差圆:  $x^2 + y^2 + (1 - 2\delta^2)^2 = 1$  的交点。只要我们可以计算出  $\widehat{CD}$  的弧长, 就可以得到满足要求的迭代次数。

上述原理, 如图 3.2 所示, 它是由单位球体和红色的误差圆圈组成。图 3.2 中的  $\overline{BC}$  是红色误差圆上的点  $B(0, 0, 1)$  到 C 点的线段。在图 3.2 中,  $\overline{OD} = 1 - 2\delta^2$ ,  $\overline{OC} = 1$ ,  $\overline{BD} = 2\delta^2$ 。

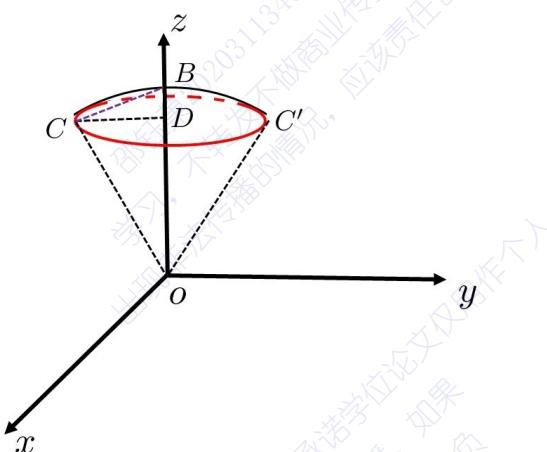


图 3.2 圆锥中的误差圆。

由几何关系可知

$$\begin{aligned}\overline{CD} &= \sqrt{\overline{OC}^2 - \overline{OD}^2} \\ &= \sqrt{1 - (1 - 2\delta^2)^2} = \sqrt{4\delta^2 - 4\delta^4} \\ \overline{BC} &= \sqrt{\overline{CD}^2 + \overline{BD}^2} \\ &= \sqrt{4\delta^2 - 4\delta^4 + 4\delta^4} = 2\delta\end{aligned}\tag{3.8}$$

$\widehat{CD}$  弧长的一半近似为  $\overline{BC} = 2\delta$ 。接下来，我们将求解蓝色圆圈  $\odot r_o$  的半径。如图 3.3 所示， $E$  点位于线段  $\overline{AB}$  的中点。

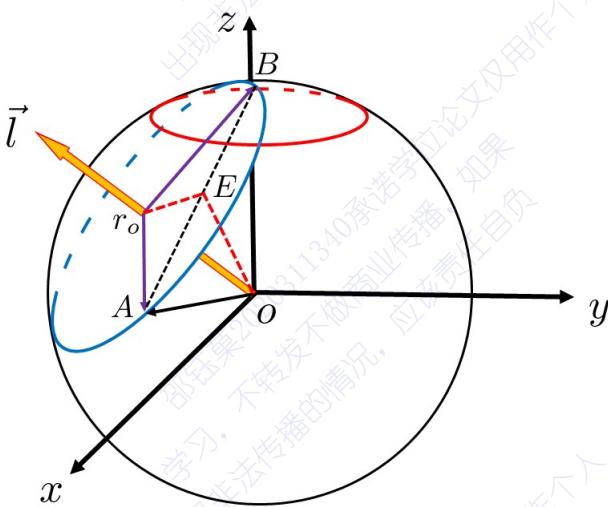


图 3.3 量子搜索算法的几何描述，根据图 3.1，将点  $A$  和  $B$  连接起来，然后取  $\overline{AB}$  的中点  $E$ ，连接点  $r_o$ 、 $E$  和  $E$ 、 $O$ 。

在图 3.3 中，由几何关系可知  $\angle AOB = \pi - 2\beta$ ,  $\overline{OA} = 1$ ,  $\angle Ar_oE = \frac{\angle Ar_oB}{2} = \frac{J+1}{2}\alpha = \frac{(J+1)\pi}{2J+3}$ 。在  $\triangle AOE$  和  $\triangle AEr_o$  中有以下关系：

$$\overline{AE} = \sin \frac{\angle AOB}{2} = \sin \frac{\pi - 2\beta}{2} = \cos \beta \quad (3.9)$$

$$\overline{Ar_o} = \overline{AE} \csc \angle Ar_oE = \cos \beta \csc \left( \frac{J+1}{2J+3}\pi \right) \quad (3.10)$$

由此可得，在弧长  $\widehat{BC}$  上的迭代次数为

$$J_\delta = \left\lceil \frac{\widehat{BC}}{\overline{Ar_o} \cdot \alpha} \right\rceil \approx \left\lceil \frac{\overline{BC}}{\overline{Ar_o} \cdot \alpha} \right\rceil \quad (3.11)$$

$$= \left\lceil \frac{(2J+3)\delta}{\pi} \sec \beta \sin \left( \frac{J+1}{2J+3}\pi \right) \right\rceil \\ \approx \left\lceil \left( \frac{\csc \beta}{2} + \frac{4}{\pi} \right) \delta \right\rceil \quad (3.12)$$

其中  $\lceil \cdot \rceil$  表示取整函数。

因此，当选择区间  $[J+1 - J_\delta, J+1 + J_\delta]$  内的数字为迭代次数时，在搜索结束后对末态进行测量，获得目标态的成功率必定将落在区间  $[1 - \delta^2, 1]$  内。图 3.4 中给出了  $\frac{1}{\lambda}$  与在给定成功率  $1 - \delta^2$  下的最小查询次数之间的关系，其中  $|\tau\rangle$  为目标态， $|s\rangle$  为初始态。进行不同成功率  $1 - \delta^2$  下的 Grover-Long 算法对比可以看出，

如果要求的成功率不高，则查询次数相应减少。

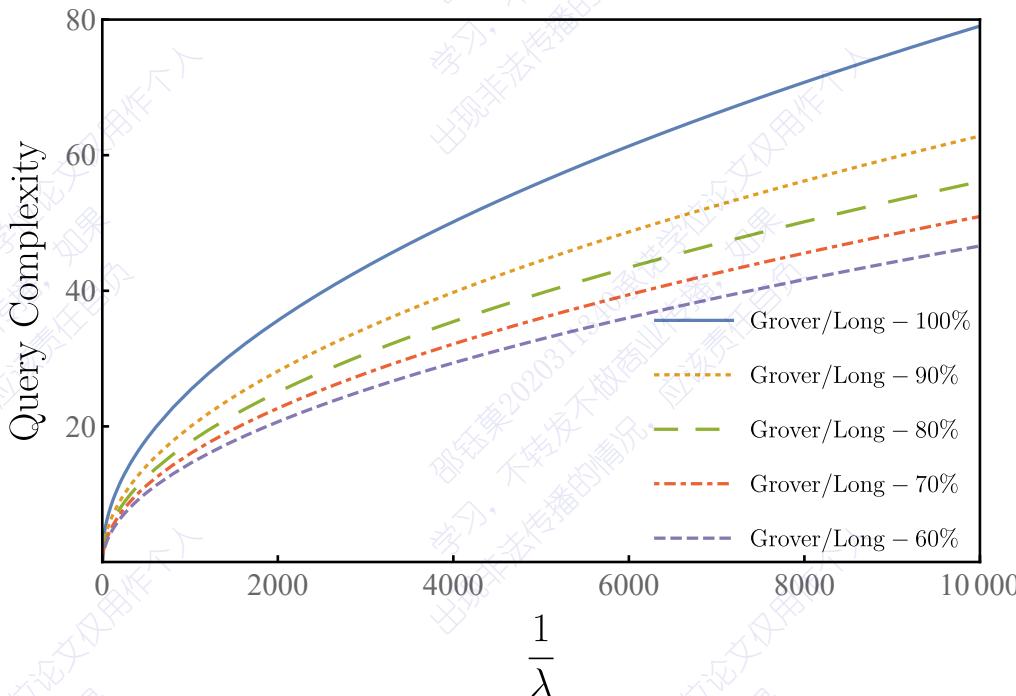


图 3.4 不同成功率  $1 - \delta^2$  下的 Grover-Long 算法对比。本图为搜索次数与初始态中目标态占比  $\lambda = |\langle \tau | s \rangle|^2$  的关系图，其中  $|\tau\rangle$  为目态， $|s\rangle$  为初始态。Grover-Long-100%（蓝色）表示 100% 成功率，Grover-Long-90%（橙色）对应  $\delta^2 = 0.1$ 。Grover-Long-80%（绿色）对应  $\delta^2 = 0.2$ ，Grover-Long-70%（红色）对应  $\delta^2 = 0.3$ ，Grover-Long-60%（紫色）对应  $\delta^2 = 0.4$ 。

### 3.4 对目标数量高鲁棒的量子搜索算法

现在，考虑占比  $\frac{M}{N}$  未知的情况。我们的目的是要以较高的成功率找到目态。在这里，我们提出了 Grover-Long 算法的改进版。在我们的算法中，误差受  $\Delta/\lambda_0$  参数  $\delta$  的限制。事实上，如果  $\Delta = 0$ ，我们的算法退化为原始的 Grover-Long 算法。我们的算法流程如下：首先，将初始状态制备为均匀叠加态  $|s\rangle$ 。然后，我们会以高于  $1 - \delta^2$  的成功率，找到目态  $|T\rangle$ ，其中重叠度  $\langle s | T \rangle = \sqrt{\lambda} e^{i\xi}$  非零且  $\delta \in [0, 1]$ 。本算法运用和 Grover-Long 算法相同的询问算符  $I_\tau$ ，如果某个分量与目态匹配，则翻转辅助量子位，即  $I_\tau |T\rangle |a\rangle = |T\rangle |a \oplus 1\rangle$ ，表示  $a = \tau$ ； $I_\tau |\bar{T}\rangle |a\rangle = |\bar{T}\rangle |a\rangle$ ，则表示  $a \neq \tau$ 。下文中我们将证明迭代  $J + 1 - J_D$  次，即可获得高于  $1 - \delta^2$  的成功率完成对  $|\bar{T}\rangle$  的搜索。

假设有一个数据库没有精确的  $\lambda$ ，但是知道其上下界  $\lambda_0 \leq \lambda \leq \lambda_0 + \Delta$ 。如果我们将下界  $\lambda_0$  作为“重叠”代入 Grover-Long 算法，我们将得到

$$\beta_0 = \arcsin \left[ \sqrt{\lambda_0} \right] \leq \arcsin \left[ \sqrt{\lambda} \right] = \beta \quad (3.13)$$

进而得到

$$J = j_{op_0} = \left\lceil \frac{\pi - 2\beta_0}{4\beta_0} \right\rceil \geq \left\lceil \frac{\pi - 2\beta}{4\beta} \right\rceil = j_{op} \quad (3.14)$$

式 (3.14) 遵守方程 (2.69)  $J \geq j_{op}$ 。因此, 可以选择  $J + 1$  作为 Grover-Long 算法的迭代次数。由于将  $J$  和  $\beta_0$  代入方程 (2.70) 时, 我们无法获得正确的匹配相位。因此, 对于沿式 (3.6) 所示的轴  $\vec{l}$  的每次迭代时, 我们不会以式 (3.5) 所示的正确旋转角度  $\alpha$  旋转。事实上, 我们得到的是:

$$\begin{aligned} \alpha_0 &= 4 \arcsin \left[ \sin \left( \frac{\phi_0}{2} \right) \sin \beta \right] \\ &= 4 \arcsin \left[ \sin \left( \frac{\pi}{4J+6} \right) \sqrt{\frac{\lambda}{\lambda_0}} \right] \\ &\leq \frac{\pi}{2J+3} + \tan \left( \frac{\pi}{4J+6} \right) \frac{\Delta}{2\lambda_0} \end{aligned} \quad (3.15)$$

$\alpha_0$  和  $\alpha$  之间的角度差  $d\alpha$  是

$$d\alpha = \alpha_0 - \alpha \leq \tan \left( \frac{\pi}{4J+6} \right) \frac{\Delta}{2\lambda_0}. \quad (3.16)$$

总旋转角度差为

$$D\alpha = (J + 1)d\alpha \quad (3.17)$$

$$\leq (J + 1) \tan \left( \frac{\pi}{4J+6} \right) \frac{\Delta}{2\lambda_0} \quad (3.18)$$

角度差  $D\alpha$  是过度旋转的角对应图 3.2 中的  $\angle CoB$  或圆弧  $\widehat{CB}$ 。我们将此过度旋转的角定义为  $2\delta$ :

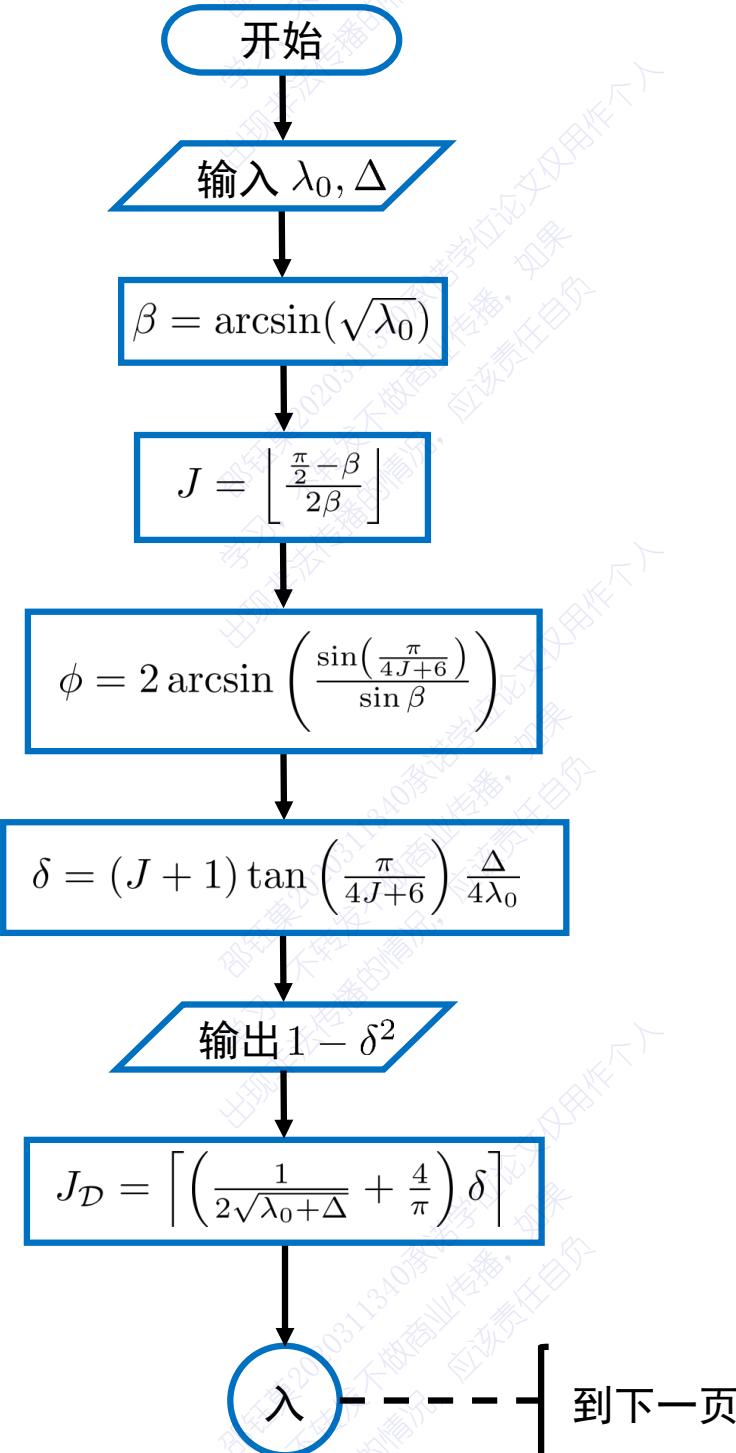
$$0 \leq D\alpha \leq (J + 1) \tan \left( \frac{\pi}{4J+6} \right) \frac{\Delta}{2\lambda_0} = 2\delta \quad (3.19)$$

我们选择减少迭代次数以提高成功率。迭代次数和误差之间的关系由方程 (3.12) 给出。所以, 减少的迭代次数是

$$\begin{aligned} J_\delta &= \left\lceil \left( \frac{\csc \beta}{2} + \frac{4}{\pi} \right) \delta \right\rceil \\ &\geq \left\lceil \left( \frac{\csc (\arcsin \sqrt{\lambda_0 + \Delta})}{2} + \frac{4}{\pi} \right) \delta \right\rceil \\ &= \left\lceil \left( \frac{1}{2\sqrt{\lambda_0 + \Delta}} + \frac{4}{\pi} \right) \delta \right\rceil = J_D \end{aligned} \quad (3.20)$$

它将使得末态旋转到弧  $\widehat{C'B}$  而不是弧  $\widehat{CB}$  上, 所以最终搜索的成功率大于  $1 - \delta^2$ 。

我们的算法流程图如图 3.5 所示



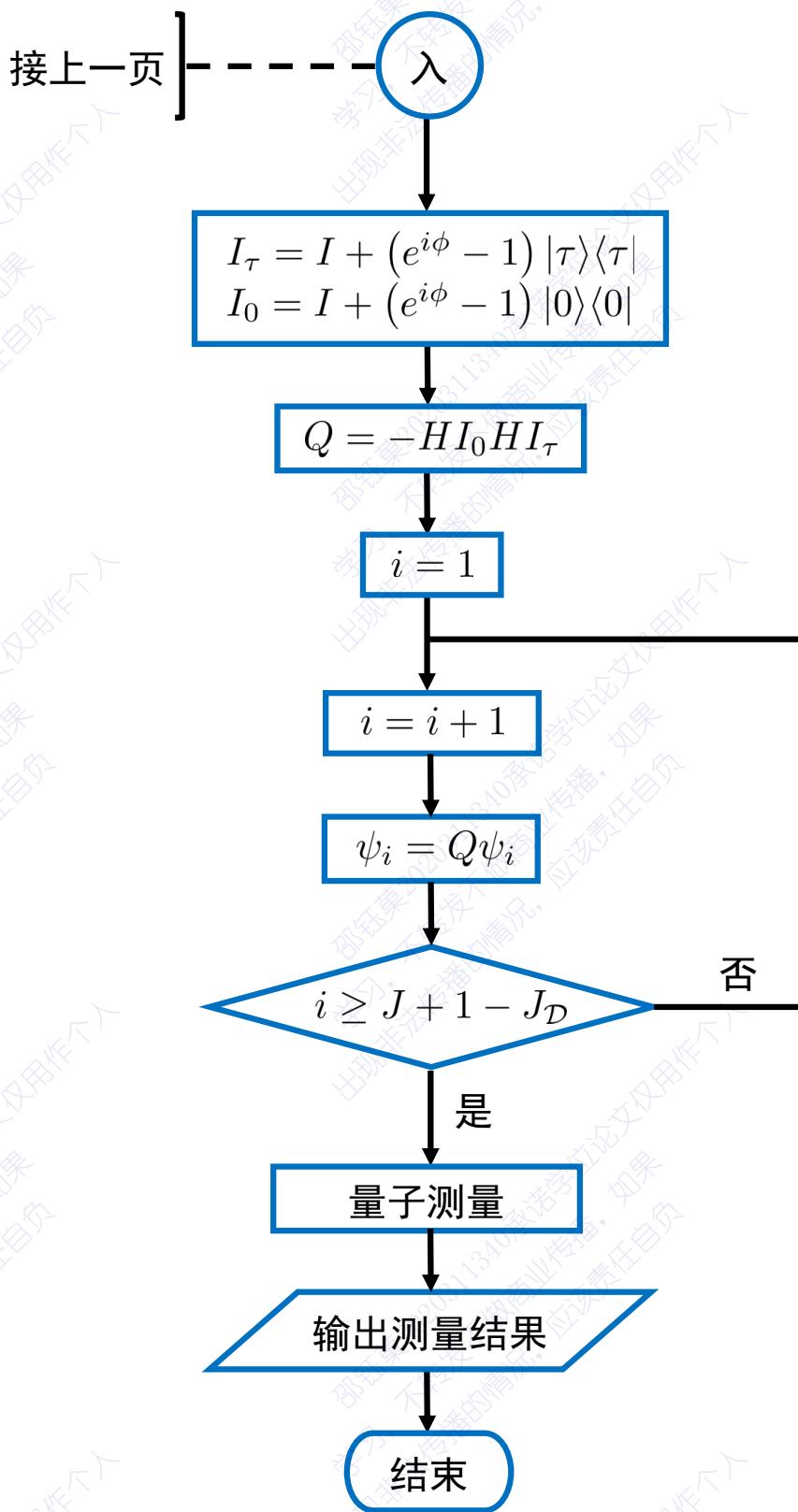


图 3.5 算法流程图

### 3.5 讨论

与其他算法相比，我们的算法保持了二次加速的特性。如图 3.6 所示，我们的算法和 Yoder-Low-Chuang 算法以及原始的 Grover 算法都具有  $O\left(\sqrt{\frac{1}{\lambda}}\right)$  的计算复杂度。在输出成功率大于  $1 - \delta^2 = 0.96$  的情况下，当  $\frac{1}{\lambda_0} = 100$  时，我们的算法进行了 8 次搜索，而 Yoder-Low-Chuang 算法进行了 10 次搜索， $\frac{\pi}{3}$ -算法进行了 160 次搜索。对于  $\frac{1}{\lambda_0} = 4000$ ，我们的算法进行了 46 次搜索，而 Yoder-Low-Chuang 算法进行了 64 次搜索， $\frac{\pi}{3}$ -算法进行了 6437 次搜索。对于  $\frac{1}{\lambda_0} = 10000$ ，我们的算法进行了 72 次搜索，而 Yoder-Low-Chuang 算法进行了 100 次搜索， $\frac{\pi}{3}$ -算法进行了 16094 次搜索。我们的算法和 Yoder-Low-Chuang 算法都具有与原始 Grover 算法相同的计算复杂度  $O\left(\sqrt{\frac{1}{\lambda_0}}\right)$ ，而  $\frac{\pi}{3}$ -算法的计算复杂度则为  $\frac{1}{\lambda}$ 。

在我们的算法中，成功率的下界由方程 (3.19) 描述。成功率的下界与  $\Delta/\lambda_0$  有关。在图 3.7 中，我们展示了在不同不确定度  $\Delta$  下，成功率下界和占比  $\lambda$  之间的关系。当不确定度为零时，每次都会达到 100% 的成功率，我们的算法退化为原始的 Grover-Long 算法。曲线随着  $\lambda$  的增加而急剧增加，当不确定性与  $\lambda$  处于同一量级时，算法的成功率在 95% 以上。当不确定性为  $\lambda$  的 2 倍时，仍可以获得高达 80% 的成功率。

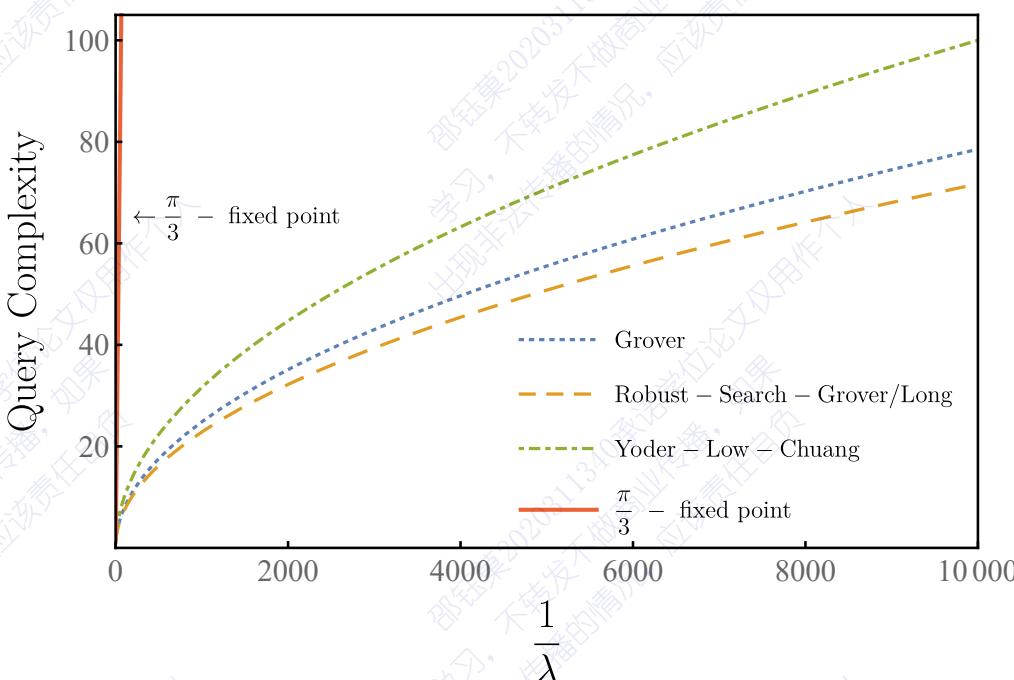


图 3.6 计算复杂度对比图，我们的算法（橙色）、Yoder-Low-Chuang 算法（绿色）、 $\pi/3$ -定点搜索算法（红色）和原始 Grover 算法（蓝色）。

因此，我们的算法对占比  $\lambda = \frac{M}{N}$  的不确定度具有很高的鲁棒性。为了看到我们算法的鲁棒性的表现，图 3.8 可体现出算法的鲁棒性。

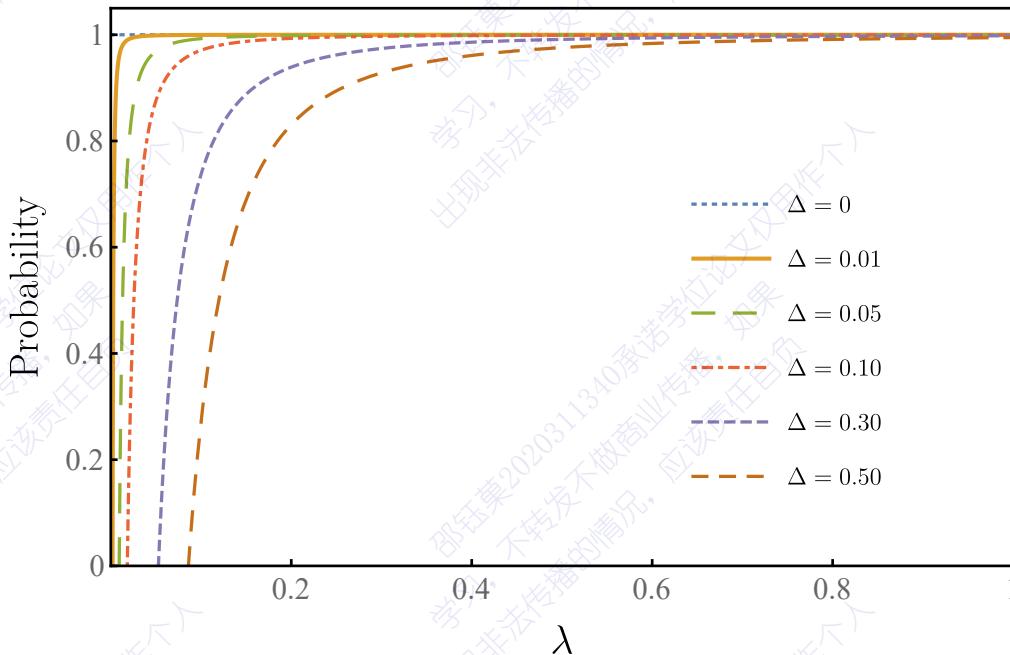


图 3.7 图的横坐标为占比  $\lambda$ , 纵坐标为成功概率的下界。图中, 我们用不同的颜色标出不同的不确定度  $\Delta$ 。可以看到, 当不确定度为零时, 每次的成功率为 100%, 这对应原始的 Grover-Long 算法。对于相同的占比  $\lambda$ , 不确定度越小则成功率越高。

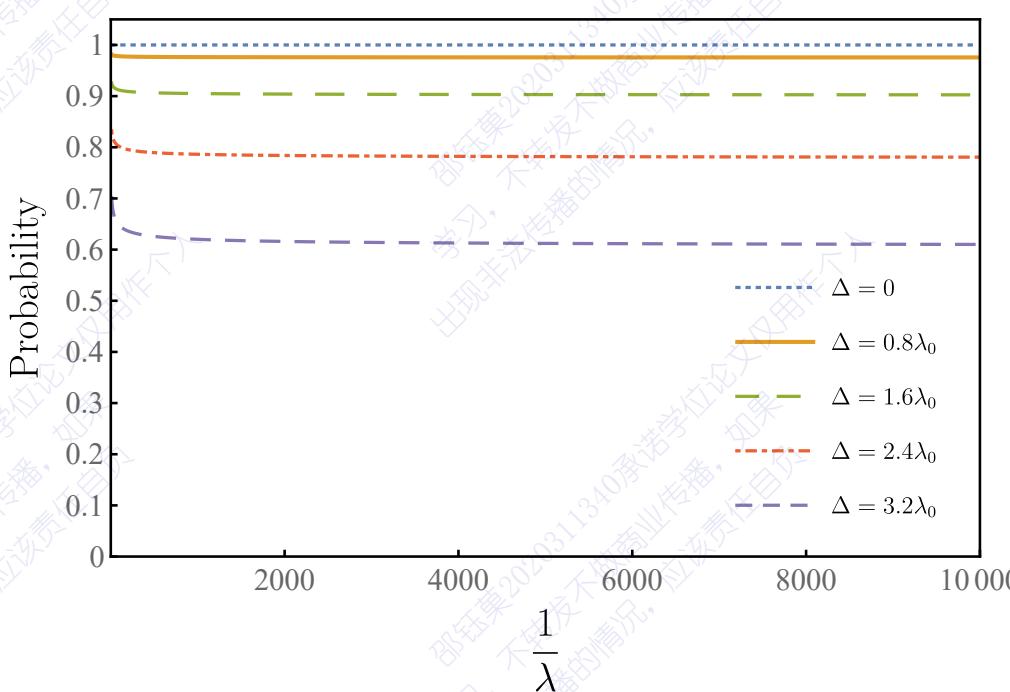


图 3.8 该图通过占比的误差与最优成功率下界之间的关系表明我们的算法对  $\lambda$  的不确定具有鲁棒性, 其中横轴为  $1/\lambda$ , 纵轴为成功率, 不同颜色代表不同偏差的曲线。

通过将  $\frac{1}{\lambda_0}$  取极限到无穷大, 可以看到: 当  $\Delta$  等于 0 时, 我们的算法退化为原始 Grover-Long 算法。当  $\Delta$  等于  $0.8\lambda_0$ , 我们算法的成功率超过 97%, 当  $\Delta$  等于  $1.6\lambda_0$

时，我们的算法成功率超过 90%。即使  $\Delta$  等于  $3.2\lambda_0$ ，我们的算法仍然有超过 60% 的成功率。

在最坏的情况下，即对  $\frac{M}{N}$  的比率一无所知，此时必须运行量子计数算法来估计  $M$  的值，同时量子计数将引入不确定度  $\sqrt{M}$ 。即便如此，我们的算法依旧运行良好，且成功率高于 96%，并保持总复杂度为  $O(\sqrt{N})$  这与原始的 Grover 算法复杂度一样。运行量子计数算法后会得到具有不确定度的占比，即  $\frac{M \pm \sqrt{M}}{N}$ 。此时， $\Delta = \frac{\lambda_0}{\sqrt{M}} \leq \lambda_0$ 。将此值代入式 (3.19)，结果表明最终算法的成功率高于 96%。

对于连续使用对偶量子算法来模拟一系列非酉量子门的操作，其成功率会随着模拟非酉量子门的个数而指数下降。因此需要在每个对偶量子算法的末尾使用量子搜索算法，对目标态的概率幅进行扩增可以等效地实现投影测量操作以提高算法整体的成功率。由于在实际的量子计算过程中，系统不存在完美的控制脉冲，因为其相位，功率，时长等都存在着一定的误差范围。而且两个相邻脉冲之间也会存在着非马尔可夫关联，这都将引入误差。另外，对于通用量子计算，很多情况会使用通用量子逻辑门集合来实现。在第 1 章第 1.5 小节介绍了运用量子逻辑门集合会引入误差。上述这些误差都将传递到待扩增的概率幅占比上，使其不再是一个确定值。经过之前的分析，我们本章提出的算法对目标太数量的不确定度是具有极强鲁棒性的。因此，实际若连续应用对偶量子算法必须在每次对偶量子算法的结尾使用本章提出的算法进行振幅放大。

此外，我们的算法可以和概率幅放大<sup>[138]</sup>以及原始 Grover 搜索算法一样作为子算法应用在相同的情景。<sup>[148-151]</sup>我们的算法在未来的量子计算中提供了许多潜在的应用<sup>[152-156]</sup>。

### 3.6 本章小结

本章提出了一种对目标态占比不确定性具有鲁棒性的量子搜索算法。不同于原始 Grover 算法与 Grover-Long 算法，本章提出的算法不需要知道确切的目标态占比，只需要知道其误差范围即可展开搜索。并且，本章的算法对于占比完全未知的情况下，匹配量子计数算法仍可以 96% 的成功概率获得目标态。此外，本算法作为基本算法用于对偶量子计算的概率幅放大算法。因此本算法是带有振幅放大的对偶量子算法不可或缺的一部分。

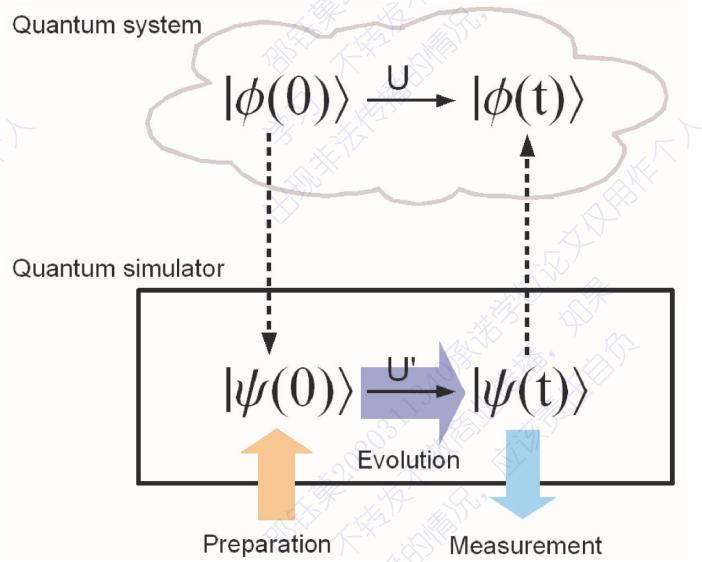
## 第4章 范畴化量子模拟的对偶量子算法

### 4.1 背景介绍

即使在今天，量子系统能否被有效模拟仍然是一个具有挑战性的问题。因为随着系统自由度或粒子数的增加，存储这些系统所需的计算机内存也要增加，而这些内存需求是随着被模拟系统的自由度增加而呈指数级增长的<sup>[157]</sup>。此外，模拟量子系统，必须要模拟其时间演化，而模拟时间演化算符所需的内存资源也是随着系统的增大而呈指数增长。这种指数增长是不可避免的，除非使用蒙特卡罗<sup>[158-160]</sup>之类的近似方法。

为解决此问题，物理学家 Richard Feynman 在 1982 年提出哈密顿量模拟<sup>[157]</sup>的概念。他意识到，如果计算机本身就是由遵守量子力学规律的量子系统构成的，那么可以用此计算机去有效地模拟量子系统。因为，量子计算机本身在演化过程中就经历了所谓的指数级爆炸。量子计算机可以处理指数级的大量物理信息，而不必使用指数级爆炸的存储资源。这使得它成为可以高效模拟量子系统的天然工具。Feynman 指出，人们可以使用受控量子系统来模拟更复杂的量子系统，该过程如图 4.1 所示。如果运用量子计算机去模拟量子系统，那么人们需要找到这两个系统的初始态、末态和哈密顿量之间的映射。具体的来说，对于一个被模拟的量子系统  $|\phi\rangle$ ，其演化过程为从初态  $|\phi(0)\rangle$  通过算符  $U = \exp\{-iH_{\text{sys}} t/\hbar\}$  作用演化到末态  $|\phi(t)\rangle$ ，其中  $H_{\text{sys}}$  是被模拟系统的哈密顿量。对于量子模拟器  $|\psi\rangle$  来说，它是一个可控的量子系统，其初始状态为  $|\psi(0)\rangle$  (要求该初态是可制备的)。它的演化算符是  $U' = \exp\{-iH_{\text{sim}} t/\hbar\}$ ，其中  $H_{\text{sim}}$  是量子模拟器的哈密顿量 (要求该哈密顿量是可以控制的)。最后的量子态是  $|\psi(t)\rangle$  (要求其末态是可测量的)。如果可以找到模拟器和系统之间的映射 ( $|\psi(0)\rangle$  和  $|\phi(0)\rangle$  之间， $|\psi(t)\rangle$  和  $|\phi(t)\rangle$ ， $H_{\text{sim}}$  与  $H_{\text{sys}}$  之间) 那么可以对此系统进行模拟<sup>[161-164,164-171]</sup>。

但仔细思考 Feynman 的量子模拟范式（哈密顿模拟），可以发现它并没有最大限度地利用量子计算资源。因为哈密顿量所能模拟的对象有一定的范围。Feynman 范式要求被模拟的系统必须是量子系统，这就大大缩小了量子计算机可以进行量子模拟的范围。事实上，许多经典的系统，如逻辑，拓扑，甚至优化问题，都需要强大的算力来解决。如果将这些问题映射到量子态或哈密顿量来描述是很难令人信服的。因此要模拟这些问题需要寻找超越 Feynman 范式的新的量子模拟范式。这是因为 Feynman 范式可以模拟的系统必须具有群的结构。具体地说，被模拟系统的演化算符形成了一个  $SU(2^n)$  群结构。而量子模拟器的演化算符也是具有  $SU(2^n)$

图 4.1 Feynman 量子模拟范式<sup>[172]</sup>

结构的。因此，只需要找到群的同态映射就可以完成量子模拟。事实上，这正是 Feynman 范式的局限性之一。因为并不是所有的系统，甚至大多数系统，都不具备群的结构。因此，要寻找超出 Feynman 量子模拟的范式，扩大量子计算机模拟的范围，需要引入新的数学理论。

此外，Feynman 量子模拟大多是先将空间离散化，使其简化为格点模型，再将每个格点上的状态编码为量子计算机的量子态。这虽然很直接，但却是对量子存储资源的浪费。事实上，在很多时候我们并不需要得到每个格点上的状态信息，所以我们不需要消耗这么大的计算资源来进行量子计算。这也是 Feynman 范式的局限性之一。实际上，当我们对被模拟系统背后的数学结构有更多的了解时，我们可以找到更简洁的编码，从而节省量子比特资源。这就好比在量子信息中，几乎从不需要直接求解薛定谔方程，而只需要知道哈密顿量  $H$  以及初始状态  $|\psi\rangle$ ，然后我们把末态写成  $e^{-iHt/\hbar}|\psi\rangle$ 。它必定是经过时间  $t$  演化后的量子态。与求解微分方程相比，这种直接的代数乘法大大减少了运算资源。为什么我们可以这么做？因为我们已经掌握了量子力学背后的代数结构。由于薛定谔方程对应的时间演化算子构成的集合有李群的结构，因此在知道初态后，人们可以直接写出演化的末态。所以，我们需要做的是为被模拟系统和量子模拟器找到新的代数结构，以便能够有效地利用量子计算资源进行编码。使得这种代数结构可以统一的描述被模拟的系统以及量子计算机本身，同时还要包含这两者之间的联系。现代数学中的范畴论无疑脱颖而出。

本章提出了一种基于范畴论这一数学工具的量子模拟新范式。该范式的实现需要借助带有振幅放大的对偶量子算法。新范式克服了 Feynman 范式的不足，极

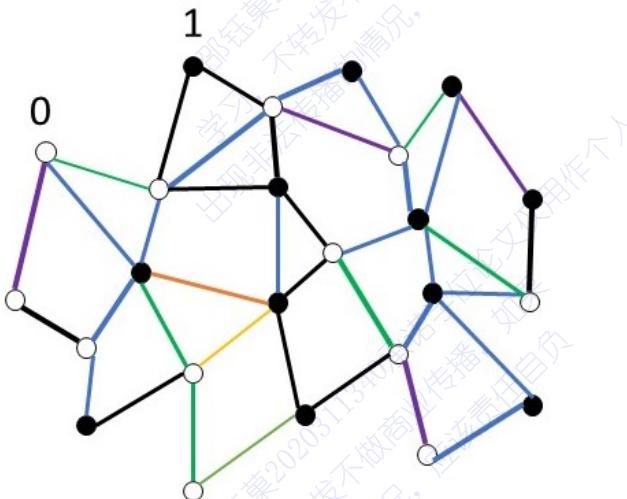


图 4.2 格点模型将连续空间离散化，传统的量子模拟是对格点模型的模拟。它将每个离散的空间点与不同点之间的关联编码到量子模拟器的量子态上。

大大扩展了量子模拟的适用范围。另外，我们的量子模拟范式引入了一种完全不同于传统的编码方式。传统量子模拟是基于几何化的格点模型来编码的。这是一种还原论的编码方式。而我们使用的是范畴论的代数学结构，它将被模拟的系统状态直接编码，这是高度抽象的，高度封装的。因此，我们的量子模拟范式是一种新的编码方式。它不是还原论的编码方式，而是一种演生论的编码方式。

## 4.2 量子线路的范畴结构

量子线路是具有范畴结构的。其构成一个  $\dagger$ -紧致范畴。一个量子线路范畴 **QC** 包括<sup>[173]</sup>：

1. 对象  $A := (\mathcal{A}, D_A)$ , 其中  $D_A = (d_{A_i})_{i=1}^{n_A}$  是一系列空间的维数,  $\mathcal{A} = \mathbb{C}_{d_1} \otimes \mathbb{C}_{d_2} \otimes \dots \otimes \mathbb{C}_{d_{n_A}}$  是有限维希尔伯特空间。 $A$  的维数是  $\dim A := \dim \mathcal{A} = \prod_{i=1}^{n_A} d_{A_i}$ 。其中  $n_A$  代表对象中子空间的维数。如果  $n_A = 1$  则称对象是单一的否则称为复合的。对于希尔伯特空间中的每一个对象  $A$  选择  $\left\{ |i_1 i_2 \dots i_{n_A}\rangle_A \right\}_{i_k=0}^{d_{A_k}-1}$  为运算基。
2. 对于任意一对对象  $A, B$ 。态射集合  $\text{Hom}_{\text{QC}}(A, B)$  包括两个希尔伯特空间  $A$  和  $B$  之间所有的有界线性映射。 $D_A$  和  $D_B$  是此有界线性映射几何的输入和输出维度。一个酉的 **QC**-态射称作量子逻辑门。
3. 复合态射。则等于线性映射的复合。
4. 张量积二元函子  $\otimes$  以及单位元  $\mathbf{1} := (\mathbb{C}, (1))$  的定义如下：

对象的张量积为:  $A \otimes B := (A \otimes B, D_A \star D_B)$ , 其中  $\star$  表示复合空间的维度。态射的张量积为  $f \otimes g$ , 其中  $f : A \rightarrow A'$ ,  $g : B \rightarrow B'$ , 由在运算基下对应

矩阵的 Kronecker 积给出：

$$\langle ij|_{A' \otimes B'} (f \otimes g) | pq \rangle_{A \otimes B} := \langle i|_{A'} f | p \rangle_A \langle j|_{B'} g | q \rangle_B \quad (4.1)$$

5.  $\dagger$  函子对于对象的作用是恒等式，对于态射则将其映射为原态射的厄米伴随。

6. 对于每个对象  $A$  的单位态射和余单位态射，可根据运算基定义为：

$$\eta_A := \sum_k |kk\rangle_{A \otimes A}, \quad \epsilon_A := \sum_k \langle kk|_{A \otimes A} = \eta_A^\dagger \quad (4.2)$$

其中每一个对象与其对偶对象相等： $A^* = A$ 。

### 4.3 不同学科的范畴论表述

在物理学中 Feynman 图<sup>[174]</sup>被用来描述量子场论的传播子。事实上对于 Feynman 图来说可以随意地扭曲其几何形状，而不改变其实际意义，因为这些传播子是拓扑的而不是几何的。20 世纪 70 年代，Penrose 意识到扩展 Feynman 图可能导致人们对时空理解的修正<sup>[175]</sup>。在 20 世纪 80 年代，这些量子物理学中的 Feynman 图和拓扑学之间建立起了清晰的类比。线性算子的行为非常像拓扑学中的配边。后来弦理论也利用了这一类比，将普通量子场论的 Feynman 图用二维配边代替，它代表了随着时间的推移弦所绘制的世界线。与此同时，逻辑学家们开始分别使用对象代表命题，用态射代表证明。意思是证明是从一个命题开始的，其过程为从一个假设到一个结论。后来，计算机科学家开始使用对象表示数据类型，运用态射表示程序。他们还开始使用流程图来描述程序。概括地说，这些和 Feynman 图非常类似。后来人们认识到，借助于范畴论，流程图和 Feynman 图可以被精准的描述<sup>[176]</sup>。具体各学科的张量范畴描述整理在下图 4.3 中<sup>[177]</sup>。图 4.3 就好比是一本多国语言对照词典，只要清楚地了解一门学科即可通过词典将未知的领域直接翻译为熟悉的学科。同时这些学科都可以被翻译为量子线路。这为量子模拟提供了坚实的基础。

### 4.4 范畴化量子模拟的定义

在这里我们提出范畴化量子模拟的定义：就是一个函子  $F$  将被模拟系统的范畴  $\mathcal{C}$  映射到量子线路范畴  $\mathbf{QC}$

$$F : \mathcal{C} \rightarrow \mathbf{QC} \quad (4.3)$$

同时存在函子的逆  $F^{-1}$  将量子线路范畴  $\mathbf{QC}$  映射回被模拟系统的范畴  $\mathcal{C}$

$$F^{-1} : \mathbf{QC} \rightarrow \mathcal{C} \quad (4.4)$$

具体的交换图见图 4.4。在范畴化量子模拟中，不再要求被模拟的系统必须具有群的代数结构，只要是拥有对象和态射即可，因此几乎所有的系统都可以满足此条件，在量子计算的角度来看即范畴化量子模拟需要打破量子态酉演化的限制，因此需要引入量子计算的对偶模式来实现量子态的非酉演化。其次，基于张量范畴强大的封装能力，并不需要基于格点模型来进行编码。只需要对对象直接进行编码即可，这无疑节省了量子比特资源。这就是演生论的编码方式。

范畴论	物理学	拓扑学	逻辑学	计算机科学	量子线路
对象 $X$	希尔伯特空间 $X$	流形 $X$	命题 $X$	数据类型 $X$	量子比特 $X$
态射 $f : X \rightarrow Y$	算符 $f : X \rightarrow Y$	配边 $f : X \rightarrow Y$	证明 $f : X \rightarrow Y$	程序 $f : X \rightarrow Y$	量子门 $f : X \rightarrow Y$
对象的张量积: $X \otimes Y$	希尔伯特空间的并: $X \otimes Y$	不相交流形的并集: $X \otimes Y$	命题的合取: $X \otimes Y$	数据类型的并: $X \otimes Y$	量子比特的张量积: $X \otimes Y$
态射的张量积: $f \otimes g$	并行过程: $f \otimes g$	不相交配边的并集: $f \otimes g$	并行进程证明: $f \otimes g$	并行执行程序: $f \otimes g$	量子门的张量积: $f \otimes g$
internal hom: $X \multimap Y$	反- $X$ 和 $Y$ 构成的希尔伯特空间: $X^* \otimes Y$	不相交且保留流形方向 $X$ 与 $Y$ 的并集: $X^* \otimes Y$	条件命题: $X \multimap Y$	程序类型: $X \multimap Y$	最大纠缠态: $X^* \otimes Y$

图 4.3 物理学, 拓扑学, 逻辑学, 计算机科学, 量子线路的范畴论描述

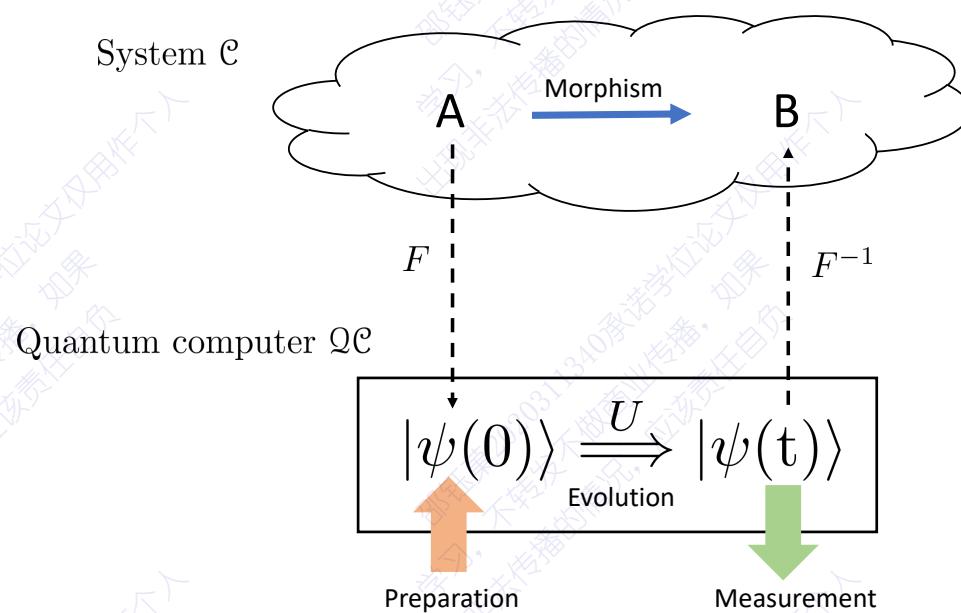


图 4.4 范畴化量子模拟

本章将以  $SU(3)$  杨-米尔斯理论为例，对其进行范畴化量子模拟。众所周知，

杨-米尔斯理论是拓扑量子场论。接下来将介绍拓扑量子场论的内容，为下一步  $SU(3)$  杨-米尔斯理论的范畴化量子模拟做铺垫。

## 4.5 拓扑量子场论

拓扑量子场论的定义是由 Atiyah 和 Segal 给出<sup>[178-179]</sup>，即是两个特殊范畴之间的函子。其中一个是几何范畴，另外一个是代数范畴。几何范畴则是配边 (Bordisms) 的范畴。对于每一个非负整数  $d$  都存在一个范畴对应的  $d$  维拓扑量子场论。这个  $d$  维配边范畴的对象是  $d - 1$  维的流形，态射则是流形之间的  $d$  维配边。对于特定的边界可以在微分同胚的意义下选取相应的配边。同时配边的复合则可以通过配边的组合来实现。对于 2 维配边范畴  $\mathbf{Bord}_2$  的定义如下：

1. 对象为圆或者不相交圆的并，即  $S^1, S^1 \sqcup S^1 \sqcup \dots$
2. 态射则为  $f : X \rightarrow Y$  (见图 4.5) 它是一个将有向边界  $X$  映射到  $Y$  的 2 维流形的微分同胚等价类。 $X$  为入射边界， $Y$  为出射边界。
3. 复合映射则为两个配边按照出射边界与入射边界相配对进行粘合
4. 单位态射则为圆柱或者圆柱的并。

而代数范畴则是复数域上的向量空间范畴  $\mathbf{Vect}_{\mathbb{C}}$ 。这个范畴由以下元素构成：

1. 他的对象是  $V, U, W, \dots$  这些是向量空间。
2. 态射  $\text{Hom}_{\mathbf{Vect}_{\mathbb{C}}}(V, W)$  则是所有将向量空间  $V$  映射到向量空间  $W$  的线性变换。
3. 态射的复合。为  $\forall V, U, W \in \text{Ob}(\mathbf{Vect}_{\mathbb{C}})$ ,

$$\circ : \text{Hom}_{\mathbf{Vect}_{\mathbb{C}}}(U, W) \times \text{Hom}_{\mathbf{Vect}_{\mathbb{C}}}(V, U) \rightarrow \text{Hom}_{\mathbf{Vect}_{\mathbb{C}}}(V, W) \quad (4.5)$$

即普通的线性变换的复合  $(g, f) \mapsto g \circ f$ 。在这种定义下可以验证满足结合律

$$(h \circ g) \circ f = h \circ (g \circ f) \quad (4.6)$$

4. 单位态射为， $\forall V \in \text{Ob}(\mathbf{Vect}_{\mathbb{C}})$ ， $\text{id}_V \in \text{Hom}_{\mathbf{Vect}_{\mathbb{C}}}(V, V)$ 。

拓扑场论的定义则为将几何范畴  $\mathbf{Bord}_d$  映射到代数范畴  $\mathbf{Vect}_{\mathbb{C}}$  的函子  $Z$ ，即

$$Z : \mathbf{Bord}_d \rightarrow \mathbf{Vect}_{\mathbb{C}} \quad (4.7)$$

这两个范畴都带有额外的结构，使得这两个范畴都是对称幺半范畴 (symmetric monoidal categories)。因此拓扑量子场论对应的函子是对称幺半函子  $Z$ 。配边范畴的对称幺半结构则是通过流形的并给出。代数范畴的对称幺半结构则是通过向量空间的直积给出。因此拓扑量子场论通过函子结合了几何与代数<sup>[180-182]</sup>，但是更让人惊讶的是拓扑量子场论阐释了一种新的代数结构<sup>[183-186]</sup>。最著名的例子则是

Folklore 给出的如下定义

**定义 4.1:** 一个 2 维有向的配边范畴是一个自由对称幺半范畴，并且其对象带有交换 Frobenius 代数的结构。特别的是，这个 2 维有向的配边范畴等价于交换 Frobenius  $k$ -代数范畴。

此定理通过生成元与关系指明了配边范畴。特别的是，2 维配边范畴等价于对称幺半范畴，其由一个单对象  $S^1$  与如图 4.5 所示的态射生成。同时此定理还指出

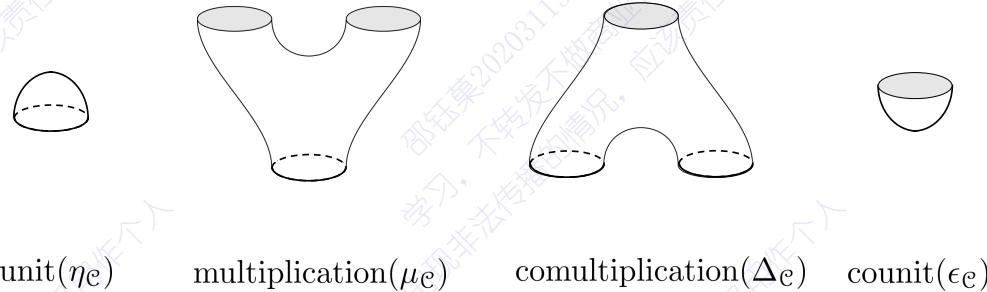
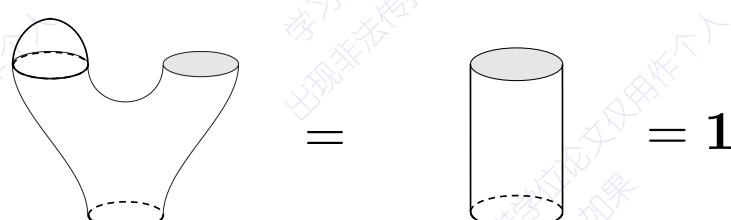


图 4.5 2 维拓扑量子场论是交换 Frobenius 代数

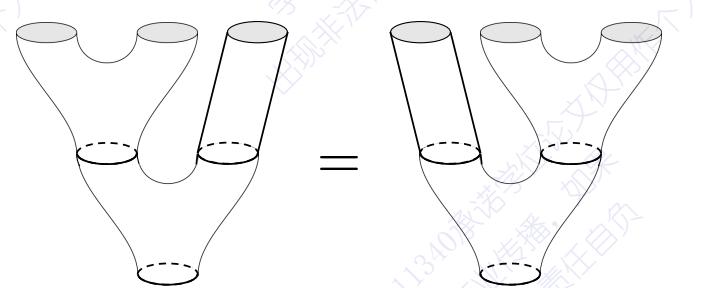
一个 2 维拓扑量子场论完全由向量空间  $Z(S^1)$  以及对于每个对象生成元通过施加拓扑量子场论操作所对应的线性映射决定。这些线性映射为：

$$\begin{aligned} \eta_c : Z(\phi) &= \mathbb{C} \rightarrow Z(S^1) \\ \mu_c : Z(S^1) \otimes Z(S^1) &\rightarrow Z(S^1) \\ \Delta_c : Z(S^1) &\rightarrow Z(S^1) \otimes Z(S^1) \\ \epsilon_c : Z(S^1) &\rightarrow Z(\phi) = \mathbb{C} \end{aligned} \tag{4.8}$$

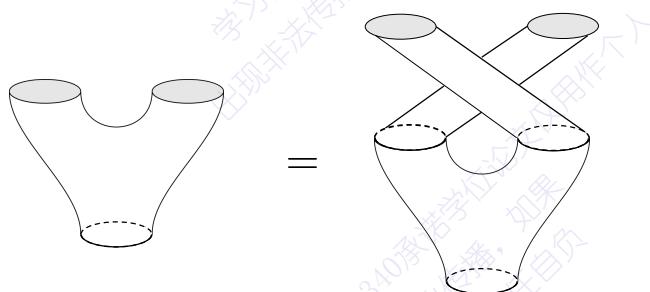
其中  $\phi$  代表空集。具体的来讲一个 2 维的闭拓扑量子场论是一个规则，它将向量空间分配给  $n$  个不相交圆的并集，并将线性映射分配到圆之间的配边。圆是有方向的，方向的变化对应于向量空间的对偶也就是狄拉克符号中的左矢与右矢。粘合配边对应于线性映射的组合。由  $\mu_c$  给出的“一条裤子”定义了配边范畴  $\mathcal{C}$  上的乘法，并且赋予其代数的结构。边界相同的配边是微分同胚的等价类。在代数学上拓扑量子场论的拓扑不变性意味 2 维封闭拓扑量子场论满足可交换 Frobenius 代数的定义。如式 (4.8)。具体表现为单位元  $\eta_c$  满足：



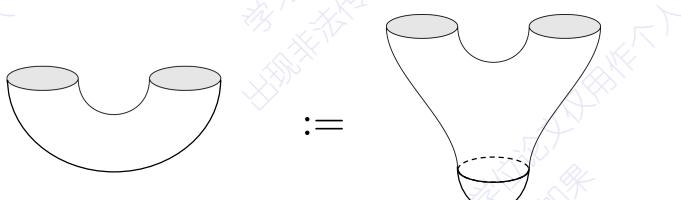
对于一个任意的紧致 2 维流形可以通过粘贴配边得到。分配律保证了不同的粘贴方式的兼容性



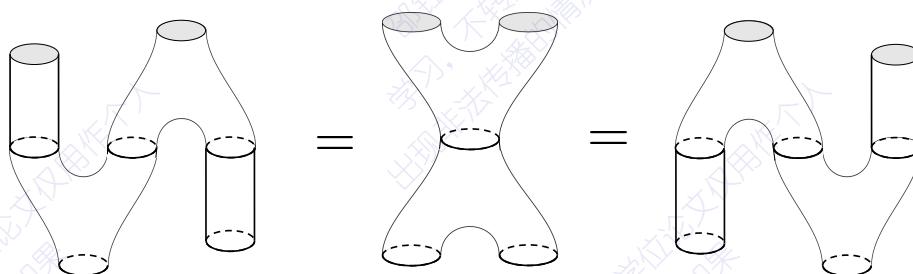
以及可交换性:  $\mu_{\mathcal{C}} = \mu_{\mathcal{C}} \circ \tau_{\mathcal{C}}$ ,



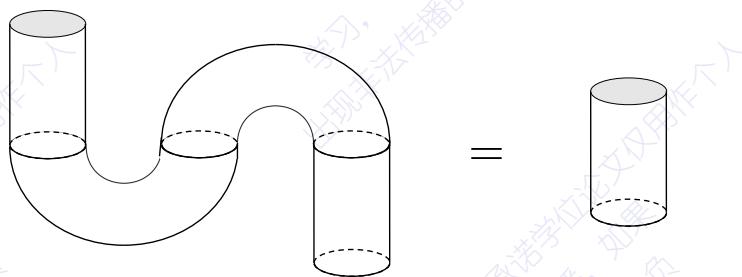
同时配边也定义了一个配对  $\pi$ , 通过组合可以自然地得到配对  $\pi = \epsilon \circ \mu : \mathcal{C} \otimes \mathcal{C} \rightarrow \mathbb{C}$



显然对于一个 Frobenius 代数  $\mathcal{C}$  满足不变条件:  $\pi(ab, c) = \pi(a, bc)$ 。以及 Frobenius 条件



同样上图也暗示了之字形等式，可以通过将单位元连接在上图来实现：



这表明配对  $\pi$  是非简并的。以上的条件就构成了对称 Frobenius 代数。2 维杨-米尔斯场则是拓扑场论的一个特例，2 维杨-米尔斯场的对应的 Frobenius 代数为<sup>[187]</sup>：

$$\begin{aligned} \mu_c &= \sum_R \frac{e^{-\beta C_2(R)}}{\dim(R)} |R\rangle\langle R| & = & \text{Diagram of a U-shaped loop with a dashed circle inside.} \\ \eta_c &= \sum_R \dim(R) e^{-\beta C_2(R)} |R\rangle & = & \text{Diagram of a small circle with a dashed line through it.} \\ \Delta_c &= \sum_R \frac{1}{\dim(R)} |R\rangle|R\rangle\langle R| & = & \text{Diagram of a cone-like shape with two legs and a dashed circle at the base.} \\ \epsilon_c &= \sum_R \dim(R) \langle R| & = & \text{Diagram of a small circle with a dashed line through it.} \end{aligned}$$

图 4.6 2 维杨-米尔斯场的 Frobenius 代数

可以看到图 4.6 将配边范畴映射到了向量空间，如果将配边范畴映射到量子线路范畴上，即可完成范畴化量子模拟。因为图 4.6 中的算符是非酉演化算子，所以要将其在量子线路中实现需要引入量子计算的对偶模式。

## 4.6 $SU(3)$ 杨-米尔斯理论的范畴化量子模拟算法

下面作者将以  $SU(3)$  杨-米尔斯规范场理论为例，来阐述范畴化量子模拟。在 2 维空间下，面积为  $A$  的任意黎曼曲面  $M$  上的杨-米尔斯规范场配分函数由下式给出：

$$\mathcal{Z} = \sum_R (\dim R)^{\chi(M)} e^{\frac{g_{YM}^2 A C_2(R)}{2}} \quad (4.9)$$

其中  $\chi(M)$  为欧拉数。 $R$  要遍历  $SU(3)$  规范群的不可约表示。为了简化模型，在这里我们做一个截断，即  $R$  只遍历  $SU(3)$  规范群表示的前几项。根据  $SU(3)$  的群表示理论可知群元  $U$  可以表示为：

$$U = e^{i \sum_k a_k \lambda_k} \quad (4.10)$$

其中  $\lambda_k$  为 8 个线性独立  $3 \times 3$  无迹厄米矩阵。这组矩阵构成李代数  $\mathfrak{su}(3)$  的基底，这组矩阵叫做 Gell-Mann 矩阵，具体的形式如下：

$$\begin{aligned} \lambda_1 &= \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} & \lambda_2 &= \begin{bmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} & \lambda_3 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \\ \lambda_4 &= \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} & \lambda_5 &= \begin{bmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{bmatrix} & & \\ \lambda_6 &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} & \lambda_7 &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{bmatrix} & \lambda_8 &= \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{bmatrix} \end{aligned} \quad (4.11)$$

可以证明，这组矩阵满足对易与反对易关系：

$$\begin{aligned} [\lambda_a, \lambda_b] &= 2i \sum_c f^{abc} \lambda_c \\ \{\lambda_a, \lambda_b\} &= \frac{4}{3} \delta_{ab} I + 2 \sum_c d^{abc} \lambda_c \end{aligned} \quad (4.12)$$

其中结构系数满足  $f^{abc} = -\frac{1}{4}i \text{tr}(\lambda_a [\lambda_b, \lambda_c])$ ,  $d^{abc} = \frac{1}{4} \text{tr}(\lambda_a \{\lambda_b, \lambda_c\})$ 。可以使用另一组归一化的基底  $F$ -自旋算子  $\hat{F}_i = \frac{1}{2} \lambda_i$  来表示李代数  $\mathfrak{su}(3)$ ，类比于李代数  $\mathfrak{su}(2)$  中的  $J^2$ ，它与所有生成元对易，这样的算子称为 Casimir 算子。可构建李代数  $\mathfrak{su}(3)$  中的两个相互独立的 Casimir 算子为：

$$\begin{aligned} \hat{C}_1 &= \sum_k \hat{F}_k \hat{F}_k \\ \hat{C}_2 &= \sum_{jkl} d_{jkl} \hat{F}_j \hat{F}_k \hat{F}_l \end{aligned} \quad (4.13)$$

其中的  $\hat{C}_2$  即为式 (4.9) 中的  $C_2$ 。利用这些 Casimir 算子可以标记李代数  $\mathfrak{su}(3)$  的不可约表示。这是因为所有生成元都与 Casimir 算子对易。因此 Casimir 算子是恒等元  $I$  的倍数。由舒尔引理可知在任何既约表示中，Casimir 算子必为恒等元的倍数。该比例常数适用于李代数表示的分类（也就是适用于李群表示的分类）。例如在量子力学中，常数  $\ell$  称为总角动量量子数。可以用其来标号不同的表示。因此  $SU(3)$  群的表示可以由这两组 Casimir 算子给出。根据 Freudenthal 公式选择两个

非负整数  $p, q$  组成数组  $D(p, q)$  来标记  $SU(3)$  群的表示，其中 Casimir 算子  $\hat{C}_1$  的本征值为：

$$\frac{p^2 + q^2 + 3p + 3q + pq}{3} \quad (4.14)$$

Casimir 算子  $\hat{C}_2$  的本征值为：

$$\frac{4}{3}(p^2 + q^2 + pq + 3p + 3q) \quad (4.15)$$

对应表示空间的维度为：

$$\dim D(p, q) = \frac{1}{2}(p+1)(q+1)(p+q+2) \quad (4.16)$$

对于  $D(0, 0)$  表示

$$C_2(D(0, 0)) = \frac{4}{3}(0^2 + 0^2 + 0 + 3 \times 0 + 3 \times 0) = 0 \quad (4.17)$$

$$\dim(D(0, 0)) = \frac{1}{2}(0+1)(0+1)(0+0+2) = 1 \quad (4.18)$$

对于  $D(1, 0)$  表示

$$C_2(D(1, 0)) = \frac{4}{3}(1^2 + 0^2 + 1 \times 0 + 3 \times 1 + 3 \times 0) = \frac{16}{3} \quad (4.19)$$

$$\dim(D(1, 0)) = \frac{1}{2}(1+1)(0+1)(1+0+2) = 3 \quad (4.20)$$

对于  $D(0, 1)$  表示

$$C_2(D(0, 1)) = \frac{4}{3}(0^2 + 1^2 + 0 \times 1 + 3 \times 0 + 3 \times 1) = \frac{16}{3} \quad (4.21)$$

$$\dim(D(0, 1)) = \frac{1}{2}(0+1)(1+1)(0+1+2) = 3 \quad (4.22)$$

对于  $D(2, 0)$  表示

$$C_2(D(2, 0)) = \frac{4}{3}(2^2 + 0^2 + 2 \times 0 + 3 \times 2 + 3 \times 0) = \frac{40}{3} \quad (4.23)$$

$$\dim(D(2, 0)) = \frac{1}{2}(2+1)(0+1)(2+0+2) = 6 \quad (4.24)$$

对于  $D(0, 2)$  表示

$$C_2(D(0, 2)) = \frac{4}{3}(0^2 + 2^2 + 0 \times 2 + 3 \times 0 + 3 \times 2) = \frac{40}{3} \quad (4.25)$$

$$\dim(D(0, 2)) = \frac{1}{2}(0+1)(2+1)(0+2+2) = 6 \quad (4.26)$$

对于  $D(1, 1)$  表示

$$C_2(D(1, 1)) = \frac{4}{3}(1^2 + 1^2 + 1 \times 1 + 1 \times 1 + 1 \times 2) = 12 \quad (4.27)$$

$$\dim(D(1,1)) = \frac{1}{2}(1+1)(1+1)(1+1+2) = 8 \quad (4.28)$$

对于  $SU(3)$  群的表示  $D(p,q)$  可直接对应到夸克模型上，其中  $p$  是夸克的数量， $q$  是反夸克的数量。 $SU(3)$  群前 6 种表示其对应的夸克模型如下：

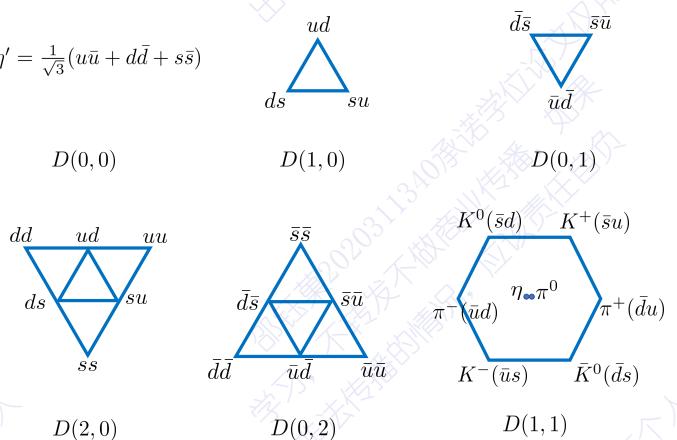


图 4.7  $SU(3)$  夸克模型。其中  $\eta = \frac{u\bar{u} + d\bar{d} - 2s\bar{s}}{\sqrt{6}}$ ,  $\pi^0 = \frac{u\bar{u} - d\bar{d}}{\sqrt{2}}$

事实上，在范畴论中并不需要知道如图 4.7 的信息，只需要把每一种群的表示进行封装，并不需要知道其内部的具体结构。因为范畴论不同于集合论。集合论的重点是元素，这包括在集合论基础上建立的群论，模论，向量空间等。基于集合论的数学结构都是还原论的思想。而范畴论关注的是对象与对象之间，范畴与范畴之间，自然变换与自然变换之间的映射关系。利用映射关系的结构去认知其结构。比如群范畴，其对象是所有的群，态射则是群与群之间的同态映射关系。在范畴论的观点中并不关注每个群具体的结构，例如群中包含哪些群元。而是通过关注群与群之间态射的代数结构，即群同态的代数结构来认知群，以后只要遇到对象之间的态射是群同态映射这种代数结构，那这些对象都是群，这是演生论的思想。对于夸克模型在这里我们只选取前 3 个表示，即  $D(0,0)$ ,  $D(1,0)$ ,  $D(0,1)$ 。基于范畴论的思想可对其进行如下编码：

真空 $ 00\rangle$  $D(1,0)$	$ 01\rangle$  $D(0,1)$
 $D(0,0)$ $ 10\rangle$	$\eta' = \frac{1}{\sqrt{3}}(u\bar{u} + d\bar{d} + s\bar{s})$ $D(0,0)$ $ 11\rangle$

图 4.8 范畴化量子模拟  $SU(3)$  杨-米尔斯理论的编码

定义4.1表明图4.6的Frobenius代数就是2维杨-米尔斯场理论。将Frobenius代数映射到量子线路上就实现了对于 $SU(3)$ 杨-米尔斯理论的范畴化量子模拟。这个过程即一个函子

$$F : \mathbf{Bord}_2 \rightarrow \mathbf{QC} \quad (4.29)$$

将配边范畴  $\mathbf{Bord}_2$  映射到量子线路范畴  $\mathbf{QC}$ 。本章接下来将完成这部分的工作。

对于Frobenius代数的第一个算符

$$\mu_c = \sum_R \frac{e^{-\beta C_2(R)}}{\dim(R)} |R\rangle\langle R| \quad (4.30)$$

为了保证量子线路是可逆运算，将式(4.30)入射态中的真空态写出。

$$\mu_c = \sum_R \frac{e^{-\beta C_2(R)}}{\dim(R)} |R\rangle|0\rangle\langle R|\langle R| \quad (4.31)$$

编码之后，取自然单位制，即 $\beta = 1$ ，则式(4.31)可以写作

$$\mu_c = |1100\rangle\langle 1111| + \frac{1}{3}e^{-\frac{16}{3}i}|1000\rangle\langle 1010| + \frac{1}{3}e^{-\frac{16}{3}i}|0100\rangle\langle 0101| \quad (4.32)$$

可以看到，式(4.32)并不是酉的，而是非酉的。因此如果要用量子线路来实现必须要运用本章1.6节所介绍的量子计算的对偶模式来实现。

首先将式(4.32)量子态拆解成直积的形式

$$\begin{aligned} &|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes |0\rangle\langle 1| \otimes |0\rangle\langle 1| + \frac{1}{3}e^{-\frac{16}{3}i}(|1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 1| \otimes |0\rangle\langle 0| \\ &\quad + |0\rangle\langle 0| \otimes |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 1|) \end{aligned} \quad (4.33)$$

将上式运用泡利算子基即式(1.31)展开

$$\begin{aligned} &(0.5\sigma_0 - 0.5\sigma_z) \otimes (0.5\sigma_0 - 0.5\sigma_z) \otimes (0.5\sigma_x + 0.5i\sigma_y) \otimes (0.5\sigma_x + 0.5i\sigma_y) \\ &+ \frac{1}{3}e^{-\frac{16}{3}i} [(0.5\sigma_0 - 0.5\sigma_z) \otimes (0.5\sigma_0 + 0.5\sigma_z) \otimes (0.5\sigma_x + 0.5i\sigma_y) \otimes (0.5\sigma_0 + 0.5\sigma_z)] \\ &+ \frac{1}{3}e^{-\frac{16}{3}i} [(0.5\sigma_0 + 0.5\sigma_z) \otimes (0.5\sigma_0 - 0.5\sigma_z) \otimes (0.5\sigma_0 + 0.5\sigma_z) \otimes (0.5\sigma_x + 0.5i\sigma_y)] \end{aligned} \quad (4.34)$$

将上式按照泡利矩阵系数的形式整理

$$\begin{aligned} &\left[ \left( 0.5 + \frac{1}{3}e^{-\frac{16}{3}i} \right) \sigma_0 - 0.5\sigma_z \right] \otimes [1.5\sigma_0 - 0.5\sigma_z] \\ &\quad \otimes [0.5\sigma_0 + \sigma_x + i\sigma_y + 0.5\sigma_z]^{\otimes 2} \end{aligned} \quad (4.35)$$

重新归一化得

$$\begin{aligned} &[0.598e^{-0.372i}\sigma_0 - 0.402\sigma_z] \otimes [0.75\sigma_0 - 0.25\sigma_z] \\ &\quad \otimes \left[ \frac{1}{\sqrt{10}}\sigma_0 + \frac{2}{\sqrt{10}}\sigma_x + \frac{2}{\sqrt{10}}i\sigma_y + \frac{1}{\sqrt{10}}\sigma_z \right]^{\otimes 2} \end{aligned} \quad (4.36)$$

为了应用量子计算的对偶模式来实现式(4.36)。我们接下来要确定  $W$  与  $V$  算符。在这里我们先来计算一个辅助比特与一个工作比特的对偶量子计算的一般形式(如图4.9)。取  $V = R_y(\theta)$ ,  $W = R_y^\dagger(\theta)$ , 其中

$$R_y(\theta) = e^{-\frac{i\sigma_y\theta}{2}} = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix} \quad (4.37)$$

初始态经过  $R_y(\theta)$  与两个受控操作  $U_0$  与  $U_1$  后演化为

$$\cos\left(\frac{\theta}{2}\right)|0\rangle U_0|\psi\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle U_1|\psi\rangle \quad (4.38)$$

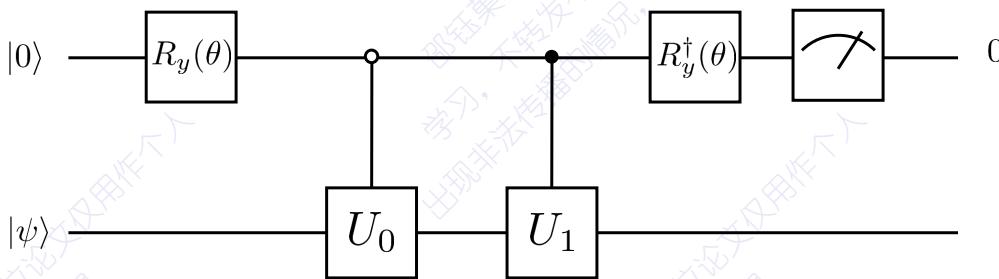


图4.9 1位辅助比特与1位工作比特的对偶量子计算线路图

经过  $R_y^\dagger(\theta)$  后演化为

$$\begin{aligned} &\cos^2\left(\frac{\theta}{2}\right)|0\rangle U_0|\psi\rangle - \cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)|1\rangle U_0|\psi\rangle \\ &+ \sin^2\left(\frac{\theta}{2}\right)|0\rangle U_1|\psi\rangle + \cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)|1\rangle U_1|\psi\rangle \end{aligned} \quad (4.39)$$

对辅助比特进行测量选择0态，则工作比特的末态为

$$\left[\cos^2\left(\frac{\theta}{2}\right)U_0 + \sin^2\left(\frac{\theta}{2}\right)U_1\right]|\psi\rangle \quad (4.40)$$

接下来计算两个辅助比特与一个工作比特的对偶量子计算的一般形式(如图4.10)。

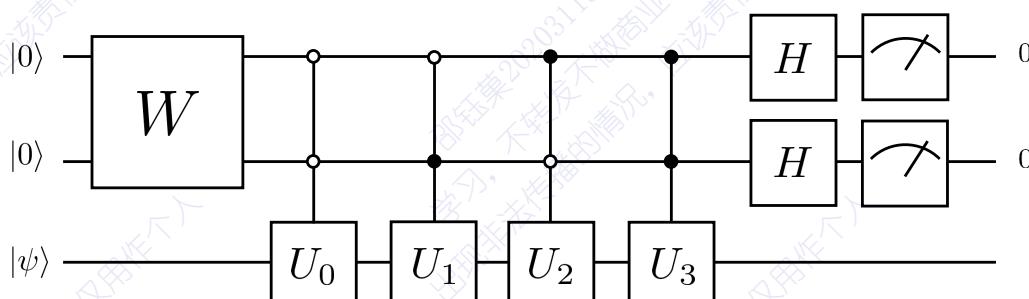


图4.10 两个辅助比特与一个工作比特的对偶量子计算的一般形式

初始态经过构造好的算符  $W$  的作用演化为

$$\{c_0|00\rangle + c_1|01\rangle + c_2|02\rangle + c_3|03\rangle\}|\psi\rangle \quad (4.41)$$

经过受控量子门  $U_0$ ,  $U_1$ ,  $U_2$ ,  $U_3$  的作用可得

$$c_0|00\rangle U_0|\psi\rangle + c_1|01\rangle U_1|\psi\rangle + c_2|10\rangle U_2|\psi\rangle + c_3|11\rangle U_3|\psi\rangle \quad (4.42)$$

再经过  $H$  变换, 则末态演化为

$$\begin{aligned} &0.25(|00\rangle + |01\rangle + |10\rangle + |11\rangle)c_0U_0|\psi\rangle + 0.25(|00\rangle - |01\rangle + |10\rangle - |11\rangle)c_1U_1|\psi\rangle \\ &+ 0.25(|00\rangle + |01\rangle - |10\rangle - |11\rangle)c_2U_2|\psi\rangle + 0.25(|00\rangle - |01\rangle - |10\rangle + |11\rangle)c_3U_3|\psi\rangle \end{aligned} \quad (4.43)$$

对辅助比特进行测量选择 0 态, 则工作比特的末态为

$$[c_0U_0 + c_1U_1 + c_2U_2 + c_3U_3]|\psi\rangle \quad (4.44)$$

下面将讨论关于式 (4.41) 中算符  $W$  的构造。算符  $W$  的实现如图 4.11 所示。

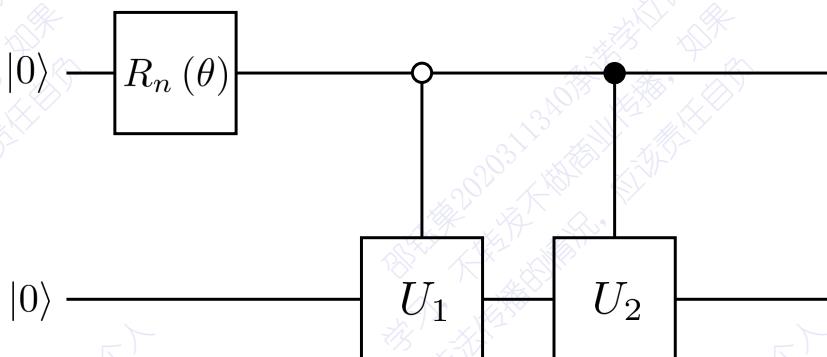


图 4.11 两比特任意量子态的制备

首先可构造旋转门  $R_n(\theta)$ , 使得

$$|00\rangle \rightarrow \left( \sqrt{c_0^2 + c_1^2}|0\rangle + \sqrt{c_2^2 + c_3^2}|1\rangle \right) |0\rangle \quad (4.45)$$

第二步, 构造受控量子门  $U_1$ ,  $U_2$ , 使得上式演化为

$$\begin{aligned} &\sqrt{c_0^2 + c_1^2}|0\rangle \left( \frac{c_0}{\sqrt{c_0^2 + c_1^2}}|0\rangle + \frac{c_1}{\sqrt{c_0^2 + c_1^2}}|1\rangle \right) \\ &+ \sqrt{c_2^2 + c_3^2}|1\rangle \left( \frac{c_2}{\sqrt{c_2^2 + c_3^2}}|0\rangle + \frac{c_3}{\sqrt{c_2^2 + c_3^2}}|1\rangle \right) \end{aligned} \quad (4.46)$$

其中

$$\begin{aligned} U_1|0\rangle &\rightarrow \frac{c_0}{\sqrt{c_0^2 + c_1^2}}|0\rangle + \frac{c_1}{\sqrt{c_0^2 + c_1^2}}|1\rangle \\ U_2|0\rangle &\rightarrow \frac{c_2}{\sqrt{c_2^2 + c_3^2}}|0\rangle + \frac{c_3}{\sqrt{c_2^2 + c_3^2}}|1\rangle \end{aligned} \quad (4.47)$$

下面对式(4.36)进行量子线路的实现,首先,第一量子位有两个操作因此需要引入一个辅助比特。对照式(4.40)。令相位门 $e^{-0.372i}\sigma_0$ 为 $U_0$ , $-\sigma_z$ 为 $U_1$ ,则对于算符 $R_y(\theta_1)$ 可由式(4.40)确定其转角 $\theta_1$ ,

$$\cos^2\left(\frac{\theta_1}{2}\right) = 0.598 \quad (4.48)$$

可得 $\theta_1=1.37$ 。

第二量子位有两个操作因此需要引入一个辅助比特。对照式(4.40)。令相位门 $\sigma_0$ 为 $U_0$ , $-\sigma_z$ 为 $U_1$ ,则对于算符 $R_y(\theta_2)$ 可由式(4.40)确定其转角 $\theta_2$ ,

$$\cos^2\left(\frac{\theta_2}{2}\right) = 0.75 \quad (4.49)$$

可得 $\theta_2=\frac{\pi}{3}$ 。

第三量子位有三个操作因此需要引入两个辅助比特来实现量子门 $c_0U_0+c_1U_1+c_2U_2+c_3U_3$ 。令相位门 $\sigma_0$ 为 $U_0$ , $\sigma_x$ 为 $U_1$ , $i\sigma_y$ 为 $U_2$ , $\sigma_z$ 为 $U_3$ 根据式(4.45)构造旋转门 $R_n(\theta)$ :

$$R_n(\theta)|00\rangle \rightarrow \left(\frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle\right)|0\rangle \quad (4.50)$$

可得 $R_n(\theta)$ 为 $R_y(\frac{\pi}{2})$ 。

根据式(4.47)可得两个受控算符 $U_1$ 与 $U_2$ 要实现以下的作用:

$$\begin{aligned} U_1|0\rangle &\rightarrow \frac{\sqrt{5}}{5}|0\rangle + \frac{2\sqrt{5}}{5}|1\rangle \\ U_2|0\rangle &\rightarrow \frac{2\sqrt{5}}{5}|0\rangle + \frac{\sqrt{5}}{5}|1\rangle \end{aligned} \quad (4.51)$$

可得 $U_1=R_y(\theta_3)$ , $U_2=R_y(\theta_4)$ ,其中 $\theta_3=2.21$ , $\theta_4=0.93$ 。对于第四工作比特和第三工作比特相同。

最后给出算符 $\mu_c$ 的量子线路表示如图4.12。其中 $|0\rangle\langle 0|$ 表示对于0态的投影测量。可以通过第3章改进的搜索算法来实现。

下面进行杨-米尔斯场的第二部分的拆解。

$$\Delta_c = \sum_R \frac{1}{\dim(R)} |R\rangle |R\rangle \langle R| \quad (4.52)$$

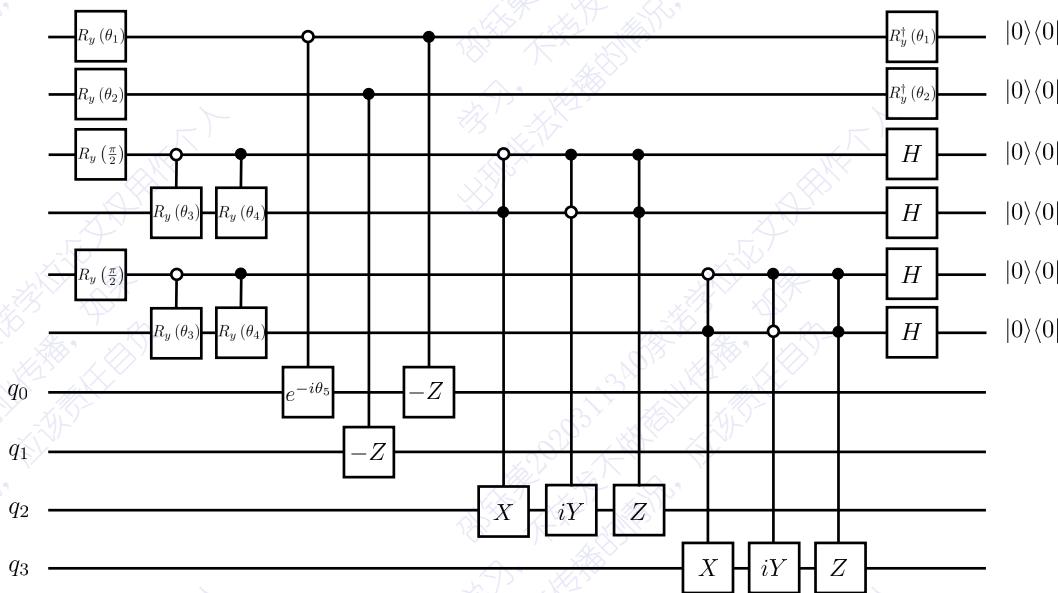


图 4.12  $\mu_c$  的量子线路表示, 其中  $q_0, q_1, q_2, q_3$  为四个工作比特,  $\theta_1 = 1.37, \theta_2 = \frac{\pi}{3}, \theta_3 = 2.21, \theta_4 = 0.93, \theta_5 = 0.372$

为了保证量子线路是可逆运算, 因此在上式的出射态增加真空态。

$$\Delta_c = \sum_R \frac{1}{\dim(R)} |R\rangle |R\rangle \langle R| \langle 0| \quad (4.53)$$

编码之后, 取自然单位制, 即  $\beta = 1$ , 则上式可以写作

$$\Delta_c = |1111\rangle \langle 1100| + \frac{1}{3} |1010\rangle \langle 1000| + \frac{1}{3} |0101\rangle \langle 0100| \quad (4.54)$$

首先将上式的量子态拆解成直积的形式

$$\begin{aligned} & |1\rangle \langle 1| \otimes |1\rangle \langle 1| \otimes |1\rangle \langle 0| \otimes |1\rangle \langle 0| + \frac{1}{3} (|1\rangle \langle 1| \otimes |0\rangle \langle 0| \otimes |1\rangle \langle 0| \otimes |0\rangle \langle 0| \\ & + |0\rangle \langle 0| \otimes |1\rangle \langle 1| \otimes |0\rangle \langle 0| \otimes |1\rangle \langle 0|) \end{aligned} \quad (4.55)$$

将上式用泡利基底展开可得

$$\begin{aligned} & (\sigma_0 - \sigma_z) \otimes (\sigma_0 - \sigma_z) \otimes (\sigma_x - i\sigma_y) \otimes (\sigma_x - i\sigma_y) \\ & + \left( \frac{1}{3}\sigma_0 - \frac{1}{3}\sigma_z \right) \otimes (\sigma_0 + \sigma_z) \otimes (\sigma_x - i\sigma_y) \otimes (\sigma_0 + \sigma_z) \\ & + \left( \frac{1}{3}\sigma_0 + \frac{1}{3}\sigma_z \right) \otimes (\sigma_0 - \sigma_z) \otimes (\sigma_0 + \sigma_z) \otimes (\sigma_x - i\sigma_y) \end{aligned} \quad (4.56)$$

将上式按照泡利矩阵系数的形式整理

$$\begin{aligned} & \left( \frac{5}{3}\sigma_0 - \sigma_z \right) \otimes (3\sigma_0 - \sigma_z) \\ & \otimes (\sigma_0 + 2\sigma_x - 2i\sigma_y + \sigma_z)^{\otimes 2} \end{aligned} \quad (4.57)$$

重新归一化

邵钰霖2020311340承诺学位论文仅用作个人学习, 不转发不公开传播, 如果出现非法传播的情况, 应该责任自负

可得

$$\left(\frac{5}{8}\sigma_0 - \frac{3}{8}\sigma_z\right) \otimes \left(\frac{3}{4}\sigma_0 - \frac{1}{4}\sigma_z\right) \otimes \left(\frac{1}{\sqrt{10}}\sigma_0 + \frac{2}{\sqrt{10}}\sigma_x - \frac{2}{\sqrt{10}}i\sigma_y + \frac{1}{\sqrt{10}}\sigma_z\right)^{\otimes 2} \quad (4.58)$$

下面对式(4.58)进行量子线路的实现, 首先, 第一量子位有两个操作因此需要引入一个辅助比特。对照式(4.40)。令相位门 $\sigma_0$ 为 $U_0$ ,  $-\sigma_z$ 为 $U_1$ , 则对于算符 $R_y(\theta_1)$ 可由式(4.40)确定其转角 $\theta_1$ ,

$$\cos^2\left(\frac{\theta_1}{2}\right) = \frac{5}{8} \quad (4.59)$$

可得 $\theta_1 = 1.32$ 。

第二量子位有两个操作, 因此需要引入一个辅助比特。对照式(4.40)。令相位门 $\sigma_0$ 为 $U_0$ ,  $-\sigma_z$ 为 $U_1$ , 则对于算符 $R_y(\theta_2)$ 可由式(4.40)确定其转角 $\theta_2$ ,

$$\cos^2\left(\frac{\theta_2}{2}\right) = \frac{3}{4} \quad (4.60)$$

可得 $\theta_2 = \frac{\pi}{3}$ 。

第三量子位有三个操作, 因此需要引入两个辅助比特来实现量子门 $c_0U_0 + c_1U_1 + c_2U_2 + c_3U_3$ 。令相位门 $\sigma_0$ 为 $U_0$ ,  $\sigma_x$ 为 $U_1$ ,  $-i\sigma_y$ 为 $U_2$ ,  $\sigma_z$ 为 $U_3$ 根据式(4.45)构造旋转门 $R_n(\theta)$ :

$$R_n(\theta)|00\rangle \rightarrow \left(\frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle\right)|0\rangle \quad (4.61)$$

可得 $R_n(\theta)$ 为 $R_y(\frac{\pi}{2})$ 。

根据式(4.47)可得两个受控算符 $U_1$ 与 $U_2$ 要实现以下的作用:

$$\begin{aligned} U_1|0\rangle &\rightarrow \frac{\sqrt{5}}{5}|0\rangle + \frac{2\sqrt{5}}{5}|1\rangle \\ U_2|0\rangle &\rightarrow \frac{2\sqrt{5}}{5}|0\rangle + \frac{\sqrt{5}}{5}|1\rangle \end{aligned} \quad (4.62)$$

可得 $U_1 = R_y(\theta_3)$ ,  $U_2 = R_y(\theta_4)$ , 其中 $\theta_3 = 2.21$ ,  $\theta_4 = 0.93$ 。对于第四工作比特和第三工作比特相同。

最后给出算符 $A_c$ 的量子线路表示如图4.13。其中 $|0\rangle\langle 0|$ 表示对于0态的投影测量。可以通过第3章改进的搜索算法来实现。

下面进行杨-米尔斯场代数结构第三部分的拆解。

$$\eta_c = \sum_R \dim(R)e^{-\beta C_2(R)}|R\rangle \quad (4.63)$$

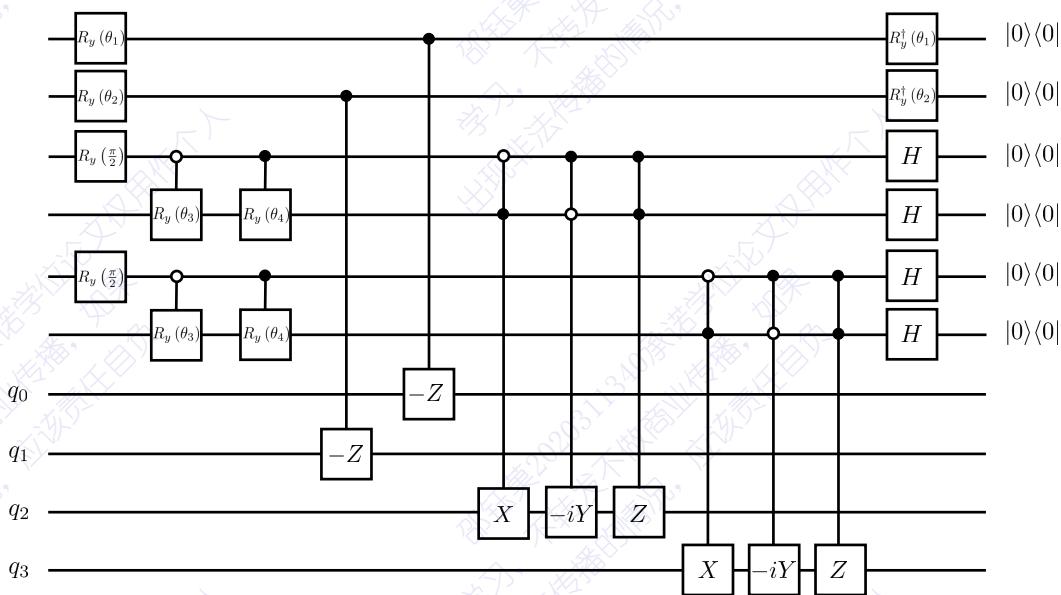


图 4.13  $\Delta_c$  的量子线路表示, 其中  $q_0, q_1, q_2, q_3$  为四个工作比特,  $\theta_1 = 1.32, \theta_2 = \frac{\pi}{3}, \theta_3 = 2.21, \theta_4 = 0.93$

将出射态的真空态写出, 可得

$$\eta_c = |11\rangle\langle 00| + 3e^{-\frac{16}{3}i}|10\rangle\langle 00| + 3e^{-\frac{16}{3}i}|01\rangle\langle 00| \quad (4.64)$$

首先将上式的量子态拆解成直积的形式

$$|1\rangle\langle 0| \otimes |1\rangle\langle 0| + 3e^{-\frac{16}{3}i}[|1\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 0| \otimes |1\rangle\langle 0|] \quad (4.65)$$

将上式利用泡利算子基展开

$$\begin{aligned} & (\sigma_x - i\sigma_y) \otimes (\sigma_x - i\sigma_y) + 3e^{-\frac{16}{3}i} (\sigma_x - i\sigma_y) \otimes (\sigma_0 + \sigma_z) \\ & + 3e^{-\frac{16}{3}i} (\sigma_0 + \sigma_z) \otimes (\sigma_x - i\sigma_y) \end{aligned} \quad (4.66)$$

将上式按照泡利矩阵系数的形式进行整理

$$\begin{aligned} & [3e^{-\frac{16}{3}i}\sigma_0 + (1 + 3e^{-\frac{16}{3}i})\sigma_x - (1 + 3e^{-\frac{16}{3}i})i\sigma_y + 3e^{-\frac{16}{3}i}\sigma_z] \\ & \otimes (\sigma_0 + 2\sigma_x - 2i\sigma_y + \sigma_z) \end{aligned} \quad (4.67)$$

重新归一化得

$$\begin{aligned} & [0.447e^{-\frac{16}{3}i}\sigma_0 + 0.548e^{-0.73i}\sigma_x + 0.548e^{-0.84i}\sigma_y + 0.447e^{-\frac{16}{3}i}\sigma_z] \\ & \otimes \left( \frac{1}{\sqrt{10}}\sigma_0 + \frac{2}{\sqrt{10}}\sigma_x - \frac{2}{\sqrt{10}}i\sigma_y + \frac{1}{\sqrt{10}}\sigma_z \right) \end{aligned} \quad (4.68)$$

下面将对式 (4.68) 进行量子线路实现。第一量子位有三个操作因此需要引入两个辅助比特。来实现量子门  $c_0U_0 + c_1U_1 + c_2U_2 + c_3U_3$ , 其中  $e^{-\frac{16}{3}i}\sigma_0$  为  $U_0$ ,  $e^{-0.73i}\sigma_x$

为  $U_1$ ,  $e^{-0.84i}\sigma_y$  为  $U_2$ ,  $e^{-\frac{16}{3}i}\sigma_z$  为  $U_3$ 。

根据式 (4.45) 构造旋转门  $R_n(\theta)$ :

$$R_n(\theta)|00\rangle \rightarrow \left( \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle \right)|0\rangle \quad (4.69)$$

可得  $R_n(\theta)$  为  $R_y(\frac{\pi}{2})$ 。

根据式 (4.47) 可得两个受控算符  $U_1$  与  $U_2$  要实现以下的作用:

$$\begin{aligned} U_1|0\rangle &\rightarrow 0.632|0\rangle + 0.775|1\rangle \\ U_2|0\rangle &\rightarrow 0.775|0\rangle + 0.642|1\rangle \end{aligned} \quad (4.70)$$

可得  $U_1 = R_y(\theta_1)$ ,  $U_2 = R_y(\theta_2)$ , 其中  $\theta_1 = 1.77$ ,  $\theta_2 = 1.37$ 。

第二量子位有三个操作, 因此需要引入两个辅助比特来实现量子门  $c_0U_0 + c_1U_1 + c_2U_2 + c_3U_3$ 。其中  $\sigma_0$  为  $U_0$ ,  $\sigma_x$  为  $U_1$ ,  $-i\sigma_y$  为  $U_2$ ,  $\sigma_z$  为  $U_3$ 。

根据式 (4.45) 构造旋转门  $R_n(\theta)$ :

$$R_n(\theta)|00\rangle \rightarrow \left( \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle \right)|0\rangle \quad (4.71)$$

可得  $R_n(\theta)$  为  $R_y(\frac{\pi}{2})$ 。

根据式 (4.47) 可得两个受控算符  $U_1$  与  $U_2$  要实现以下的作用:

$$\begin{aligned} U_1|0\rangle &\rightarrow \frac{\sqrt{5}}{5}|0\rangle + \frac{2\sqrt{5}}{5}|1\rangle \\ U_2|0\rangle &\rightarrow \frac{2\sqrt{5}}{5}|0\rangle + \frac{\sqrt{5}}{5}|1\rangle \end{aligned} \quad (4.72)$$

可得  $U_1 = R_y(\theta_3)$ ,  $U_2 = R_y(\theta_4)$ , 其中  $\theta_3 = 2.21$ ,  $\theta_4 = 0.93$ 。

最后给出算符  $\eta_c$  的量子线路表示如下:

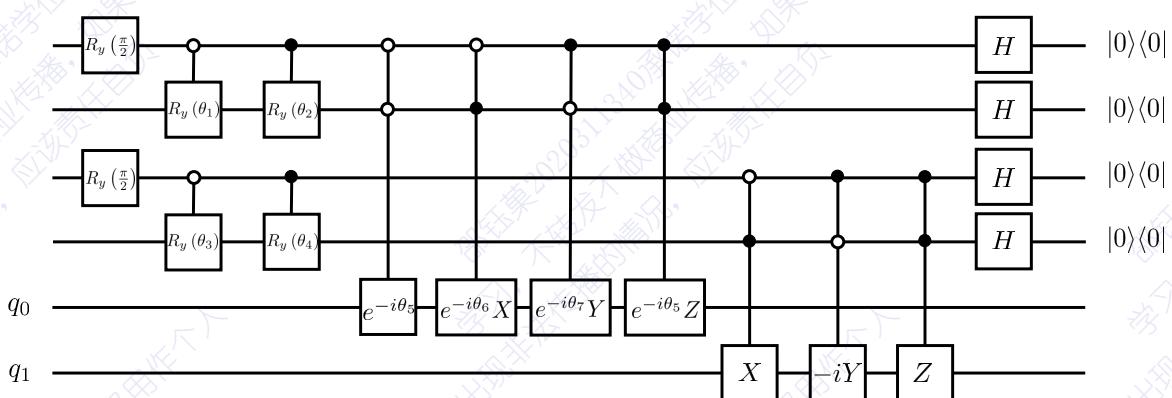


图 4.14  $\eta_c$  的量子线路表示, 其中  $q_0, q_1$  为两个工作比特,  $\theta_1 = 1.77$ ,  $\theta_2 = 1.37$ ,  $\theta_3 = 2.21$ ,  $\theta_4 = 0.93$ ,  $\theta_5 = \frac{16}{3}$ ,  $\theta_6 = 0.73$ ,  $\theta_7 = 0.84$

其中  $|0\rangle\langle 0|$  表示对于 0 态的投影测量。可以通过第 3 章改进的搜索算法来实现。

下面进行杨-米尔斯场的第四部分的拆解。

$$\epsilon_c = \sum_R \dim(R) \langle R | \quad (4.73)$$

将入射态的真空态写出：

$$\epsilon_c = |00\rangle\langle 11| + 3|00\rangle\langle 10| + 3|00\rangle\langle 01| \quad (4.74)$$

首先将上式的量子态拆解成直积的形式

$$|0\rangle\langle 1| \otimes |0\rangle\langle 1| + 3[|0\rangle\langle 1| \otimes |0\rangle\langle 0| + |0\rangle\langle 0| \otimes |0\rangle\langle 1|] \quad (4.75)$$

将上式利用泡利算子基展开

$$\begin{aligned} & (\sigma_x + i\sigma_y) \otimes (\sigma_x + i\sigma_y) + 3(\sigma_x + i\sigma_y) \otimes (\sigma_0 + \sigma_z) \\ & + 3(\sigma_0 + \sigma_z) \otimes (\sigma_x + i\sigma_y) \end{aligned} \quad (4.76)$$

将上式按照泡利矩阵系数的形式进行整理

$$[3\sigma_0 + 4\sigma_x + 4i\sigma_y + 3\sigma_z] \otimes (\sigma_0 + 2\sigma_x + 2i\sigma_y + \sigma_z) \quad (4.77)$$

重新归一化得

$$\begin{aligned} & \left( \frac{3\sqrt{2}}{10}\sigma_0 + \frac{2\sqrt{2}}{5}\sigma_x + \frac{2\sqrt{2}}{5}\sigma_y + \frac{3\sqrt{2}}{10}\sigma_z \right) \\ & \otimes \left( \frac{1}{\sqrt{10}}\sigma_0 + \frac{2}{\sqrt{10}}\sigma_x + \frac{2}{\sqrt{10}}i\sigma_y + \frac{1}{\sqrt{10}}\sigma_z \right) \end{aligned} \quad (4.78)$$

首先，看第一量子位有三个操作，因此需要引入两个辅助比特来实现量子门  $c_0U_0 + c_1U_1 + c_2U_2 + c_3U_3$ 。其中  $\sigma_0$  为  $U_0$ ,  $\sigma_x$  为  $U_1$ ,  $\sigma_y$  为  $U_2$ ,  $\sigma_z$  为  $U_3$ ，根据式 (4.45) 构造旋转门  $R_n(\theta)$ :

$$R_n(\theta)|00\rangle \rightarrow \left( \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle \right)|0\rangle \quad (4.79)$$

可得  $R_n(\theta)$  为  $R_y(\frac{\pi}{2})$ 。

根据式 (4.47) 可得两个受控算符  $U_1$  与  $U_2$  要实现以下的作用：

$$\begin{aligned} U_1|0\rangle & \rightarrow \frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle \\ U_2|0\rangle & \rightarrow \frac{4}{5}|0\rangle + \frac{3}{5}|1\rangle \end{aligned} \quad (4.80)$$

可得  $U_1 = R_y(\theta_1)$ ,  $U_2 = R_y(\theta_2)$ , 其中  $\theta_1 = 1.85$ ,  $\theta_2 = 1.29$ 。再看第二量子位有三个操作，因此需要引入两个辅助比特来实现量子门  $c_0U_0 + c_1U_1 + c_2U_2 + c_3U_3$ 。其

中  $\sigma_0$  为  $U_0$ ,  $\sigma_x$  为  $U_1$ ,  $i\sigma_y$  为  $U_2$ ,  $\sigma_z$  为  $U_3$  根据式 (4.45) 构造旋转门  $R_n(\theta)$ :

$$R_n(\theta)|00\rangle \rightarrow \left( \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle \right)|0\rangle \quad (4.81)$$

可得  $R_n(\theta)$  为  $R_y(\frac{\pi}{2})$ 。

根据式 (4.47) 可得两个受控算符  $U_1$  与  $U_2$  要实现以下的作用:

$$\begin{aligned} U_1|0\rangle &\rightarrow \frac{\sqrt{5}}{5}|0\rangle + \frac{2\sqrt{5}}{5}|1\rangle \\ U_2|0\rangle &\rightarrow \frac{2\sqrt{5}}{5}|0\rangle + \frac{\sqrt{5}}{5}|1\rangle \end{aligned} \quad (4.82)$$

可得  $U_1 = R_y(\theta_3)$ ,  $U_2 = R_y(\theta_4)$ , 其中  $\theta_3 = 2.21$ ,  $\theta_4 = 0.93$ 。

最后给出算符  $\eta_c$  的量子线路表示如下:

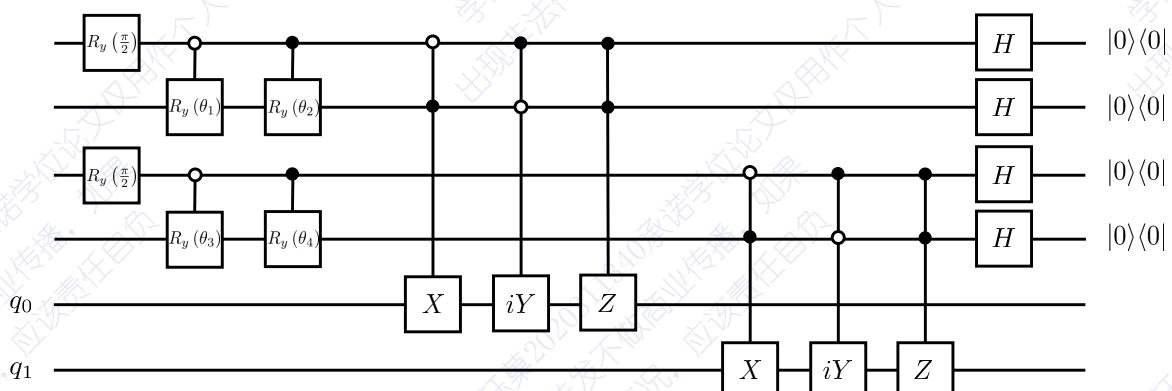


图 4.15  $\epsilon_c$  的量子线路表示, 其中  $q_0, q_1$  为两个工作比特,  $\theta_1 = 1.85$ ,  $\theta_2 = 1.29$ ,  $\theta_3 = 2.21$ ,  $\theta_4 = 0.93$

其中  $|0\rangle\langle 0|$  表示对于 0 态的投影测量。可以通过第 3 章改进的搜索算法来实现。

## 4.7 讨论

在本章作者完成对了  $SU(3)$  杨-米尔斯理论的范畴化量子模拟。作者将最终的结果整理为图 4.16。图左边则为配边范畴  $\mathbf{Bord}_2$  的态射, 右边为量子线路范畴  $\mathbf{QC}$  的态射。蓝色的箭头表示函子  $F$ 。图 4.16 正是式 (4.29) 所叙述的过程。从数学的意义上来说, 范畴化量子模拟是一个二进制的量子场论。因为该过程是将几何范畴映射到量子线路范畴的函子。结合本章 4.5 部分的介绍可知, 图 4.16  $SU(3)$  杨-米尔斯理论完全由配边范畴 (等价于交换 Frobenius 代数范畴) 所决定。而图 4.16 将配边范畴通过函子  $F$  完全的映射到了量子线路中, 将配边范畴中的对象 (不相交圆的

并) 通过图 4.8 的编码方式映射到了量子线路范畴的对象 (量子比特  $q_0, q_1, q_2, q_3$ ) 上, 将配边范畴的态射映射到了量子线路范畴的态射上 (即图 4.16 展示的内容)。

在拓扑量子场论中, 所有的传播子都可以被拆解为配边范畴中态射的复合, 即

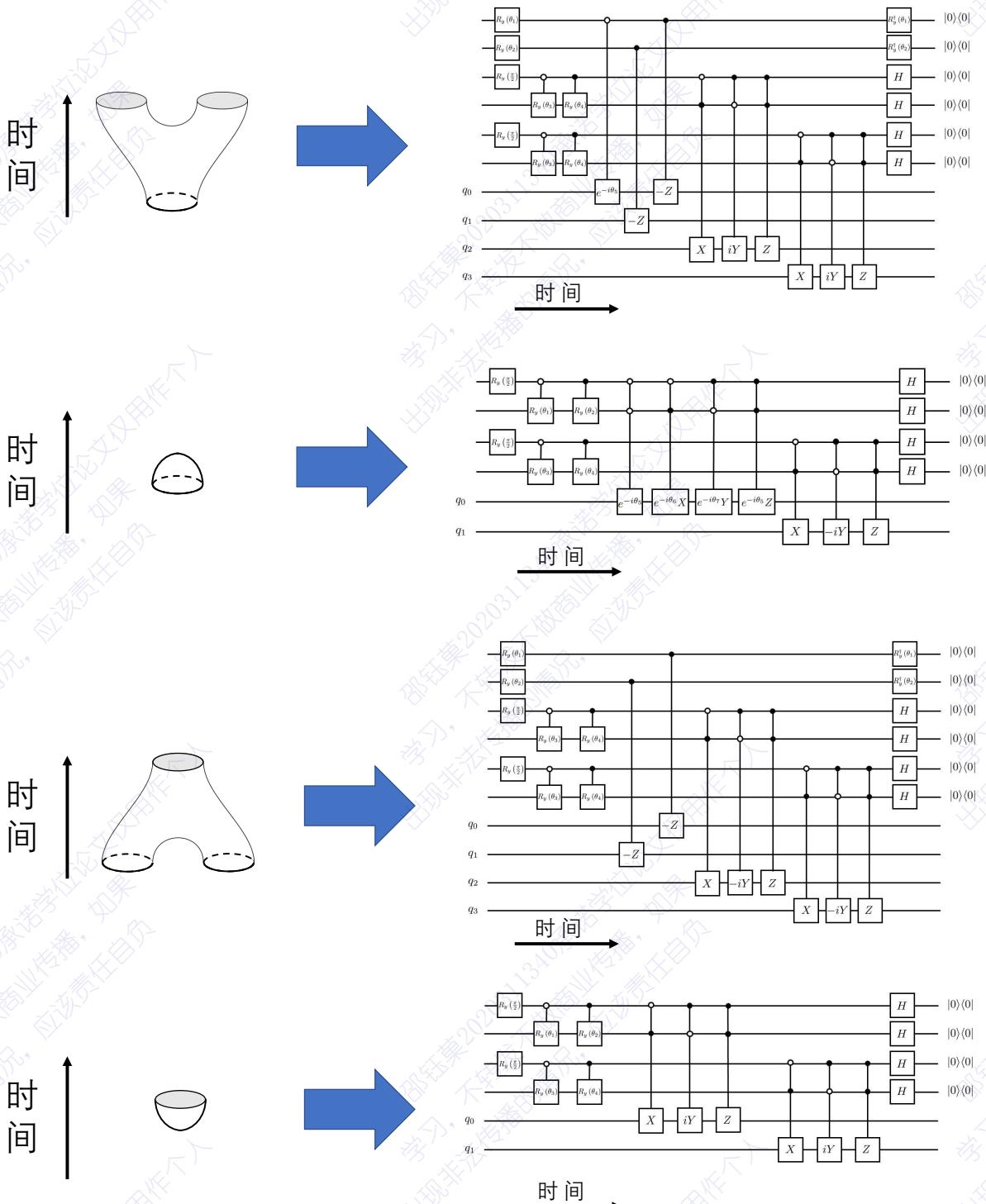


图 4.16  $SU(3)$  杨-米尔斯理论的范畴化量子模拟

把图 4.16 左边的几何图形按照出射态与入射态的时序依次进行粘合。因此若

要进行拓扑量子场论中一切行为的模拟只需要将图 4.16 右边的 4 幅量子线路图进行组合。可以看出组合后的量子线路图中存在着投影测量。考虑到实际量子计算机运算过程中误差的积累，以及运用通用量子门集合造成的误差。这要求通过概率幅放大来等效实现投影测量必须将占比的不确定度考虑进去。这使得普通的量子搜索算法无法完成这个任务。需要使用本文第 3 章高鲁棒量子搜索算法来实现。因此可以说范畴化量子模拟算法是一个带有振幅放大的对偶量子算法。

如果使用 Feynman 范式的量子模拟来完成同样的任务，需要消耗很多不必要的比特资源。因为传统的量子模拟需要将空间离散化，将空间中每一个点的状态编码到量子计算机的量子态上。而范畴化量子模拟则直接对希尔伯特空间进行编码，直接考虑其代数结构空间，而不是几何空间。因此范畴化量子模拟节省了比特资源。

图 4.16 也揭示了  $SU(3)$  杨-米尔斯理论背后深刻的物理含义。可以看出图 4.16 中的量子线路运用的是量子计算的对偶模式。即通过引入了辅助比特。这揭示了  $SU(3)$  杨-米尔斯理论中的场是存在引力规范反常的（反常指的是对于一个  $n$  维量子场无法在  $n$  维格点模型上实现）。这说明  $SU(3)$  杨-米尔斯理论存在着极强的长程纠缠现象。即低维空间的纠缠需要借助高维空间来实现。

## 4.8 本章小结

面对 Feynman 量子模拟的局限性，作者通过应用非酉演化与带有振幅放大的量子计算的对偶模式提出了应用性更广的范畴化量子模拟。该模拟算法并不需要要求被模拟的系统具备群的结构，因此这扩展了量子计算机的适用范围。其次，范畴化量子模拟并不需要先将空间离散再进行编码，而是直接对代数状态进行编码，而非离散化的格点状态，因此这节省了量子存储资源。作者最后以  $SU(3)$  杨-米尔斯规范场为例，阐述了范畴化量子模拟。

## 第 5 章 波动方程行波解的对偶量子求解算法

### 5.1 背景介绍

大多数科学问题可以通过研究物理量随时空演化的规律来解决。因此偏微分方程无疑在自然科学领域扮演着极其重要的角色。然而偏微分方程的求解问题困难度极大。但随着量子计算理论的发展，运用量子算法来求解偏微分方程相比于经典算法可实现加速的特性。

通常求解偏微分方程的量子算法流程如图 5.1。首先将空间离散，使得函数  $f(x, t)$  变为向量  $\mathbf{f}(t)$ ，将其归一化的分量映射到量子态分量上，即  $|\mathbf{x}(t)\rangle = \sum_i f'_i(t) |x_i\rangle$ ，其中  $f'_i(t)$  为向量  $\mathbf{f}(t)$  归一化后的第  $i$  分量。接下来将编码到量子态上的向量映射到固定的模型上。大多数偏微分方程求解的量子算法依赖于哈密顿量模拟<sup>[163,188-190]</sup>或线性方程组求解的量子算法（HHL 算法）<sup>[62]</sup>。

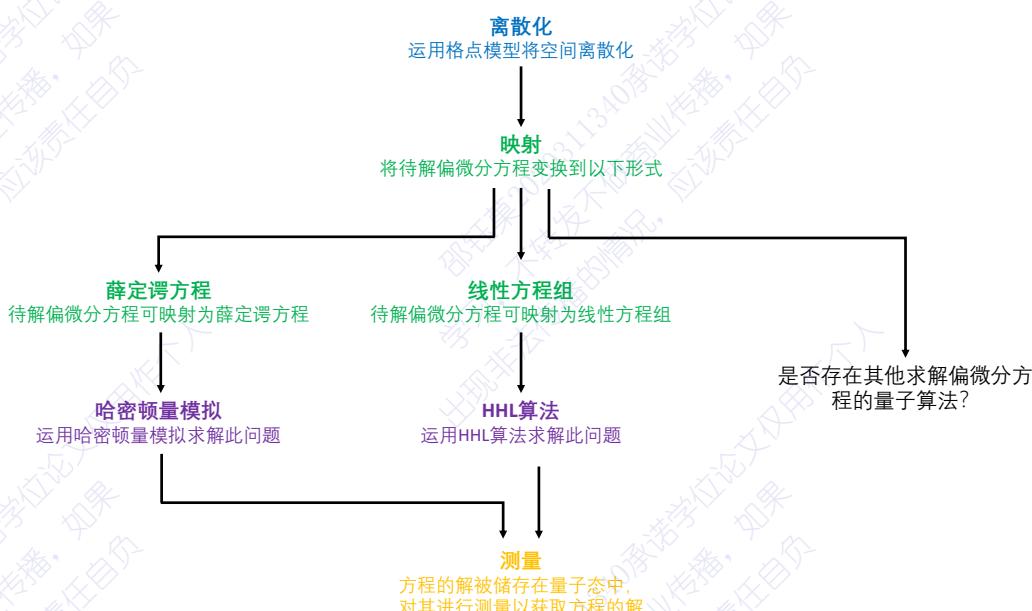


图 5.1 求解偏微分方程的量子算法<sup>[191]</sup>

下面将结合例子简要回顾以上两种求解方法的主要思想。首先将介绍将偏微分方程映射到薛定谔方程的求解方法<sup>[192-194]</sup>。该方法将方程结构与薛定谔方程相近或者类似的方程映射到薛定谔方程上，将方程求解问题转化为哈密顿量模拟问题。例如求解 Black-Scholes 方程<sup>[195]</sup>

$$\frac{\partial f}{\partial t} = af + b\frac{\partial f}{\partial x} - c\frac{\partial^2 f}{\partial x^2} \quad (5.1)$$

该方程可以写成如下的形式：

$$\frac{\partial f}{\partial t} = Af \quad (5.2)$$

可以明显地看出该方程在形式上与薛定谔方程类似。因此可以通过如下的方法将  $A$  算符映射到薛定谔方程中的哈密顿量上，令  $A = ib\hat{p} + (aI + c\hat{p}^2)$ ,  $\hat{p} = -i\partial_x$ 。可以将  $A$  拆解为厄米和反厄米部分，即  $A = A_H + A_{aH}$ :

$$A_{aH} = ib\hat{p}, \quad A_H = aI + c\hat{p}^2 \quad (5.3)$$

将函数离散化后得到的向量  $\mathbf{f}(t)$ ，编码到态向量  $|\mathbf{x}(\epsilon)\rangle$  上，使用 Trotter 乘法近似公式

$$|\mathbf{x}(\epsilon)\rangle = e^{A\epsilon} |\mathbf{x}_0\rangle \approx e^{A_H\epsilon} e^{A_{aH}\epsilon} |\mathbf{x}_0\rangle \quad (5.4)$$

将偏微分方程求解问题转化为哈密顿量模拟问题。模拟上式哈密顿量作用的过程，即量子态  $|\mathbf{x}_0\rangle$  在设计好的哈密顿量下进行演化即可得到末态。通过对迭代不同次数的末态进行测量即可得到原方程对应不同时刻的解。

事实上运用哈密顿量模拟的方法来构建求解偏微分方程的量子算法是高效的，它可以求解一阶偏微分方程（要求矩阵  $A$  拆解的厄米部分与反厄米部分是对易的）以及形如波动方程的二阶偏微分方程等。但事实上并不是所有的偏微分方程都具备薛定谔方程的代数结构。下面来介绍运用 HHL 算法来构建求解偏微分方程的量子算法<sup>[193,196-198]</sup>。对于空间离散化后有如下结构的偏微分方程

$$\dot{\mathbf{x}} = A\mathbf{x} + \mathbf{b} \quad (5.5)$$

运用欧拉方法将时间离散化可得：

$$\frac{\mathbf{x}(t_{j+1}) - \mathbf{x}(t_j)}{h} \approx A\mathbf{x}(t_j) + \mathbf{b} \quad (5.6)$$

令  $\mathbf{x}_j = \mathbf{x}(t_j)$ ，即可将偏微分方程转化为如下的线性方程组，作为举例这里只给出  $j \leq 2$  的结果：

$$\begin{bmatrix} I & 0 & 0 \\ -(I + Ah) & I & 0 \\ 0 & -(I + Ah) & I \end{bmatrix} \begin{bmatrix} \mathbf{x}_0 \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{x}_{in} \\ \mathbf{b}h \\ \mathbf{b}h \end{bmatrix} \quad (5.7)$$

之后运用 HHL 算法求解此方程组，即可得到如下的量子态：

$$|\mathbf{x}\rangle = \sum_{j=0}^{N_t} |t_j\rangle |\mathbf{x}_j\rangle \quad (5.8)$$

该量子态包含偏微分方程  $t_0$  至  $t_j$  时刻的解。那么除了以上两种方法是否存在其他高效的偏微分方程求解算法？本章将运用不同于以上两种的第三种方法——带有

振幅放大的对偶量子算法来构建求解偏微分方程的量子算法，然后运用其来求解一阶波动方程，并研究行波耗散与色散的问题。

## 5.2 一阶波动方程求解的对偶量子算法

说到波动方程人们一定第一时间想到二阶线性双曲型方程

$$\frac{\partial^2 u}{\partial t^2} + k^2 \frac{\partial^2 u}{\partial x^2} = 0 \quad (5.9)$$

其通解可以写成  $u(x, t) = f(x - kt) + g(x + kt)$ ，其中  $f, g$  是两个任意的函数。 $f(x - kt)$  与  $g(x + kt)$  代表沿  $x$  轴以恒定速度向右和向左传递的波。由于方程 (5.9) 是线性齐次方程，因此其解具有叠加性。所以  $f, g$  是两个独立传播互不干扰的行波。若只研究两列波其一的规律，则方程 (5.9) 退化为一阶线性双曲型方程：

$$\frac{\partial u}{\partial t} + k \frac{\partial u}{\partial x} = 0 \quad (5.10)$$

在本章作者将连续的自变量  $x$  离散化为  $N$  个点，即  $\mathbf{x} = (x_0, x_1, \dots, x_{N-1})$ 。则函数  $u(x, t_j)$  在  $t_j$  时刻的空间部分被离散为向量

$$\mathbf{u}(\mathbf{x}, t_j) = (u(x_0, t_j), u(x_1, t_j), \dots, u(x_{N-1}, t_j)), \quad (5.11)$$

将其编码到计算基上并定义量子态  $|\psi\rangle_j$  为

$$|\psi\rangle_j = \frac{\sum_{i=0}^{N-1} u(x_i, t_j) |i\rangle}{\sqrt{\sum_{i=0}^{N-1} u^2(x_i, t_j)}} \quad (5.12)$$

下面作者将基于量子系统的非酉演化给出求解方程 (5.10) 的量子算法，首先对式 (5.10) 各阶偏微分项作泰勒展开：

$$\begin{aligned} \frac{\partial u}{\partial t} &= \frac{u(x, t + \tau) - u(x, t)}{\tau} + o(\tau), \\ \frac{\partial u}{\partial x} &= \frac{u(x + h, t) - u(x, t)}{h} + o(h). \end{aligned} \quad (5.13)$$

将式 (5.13) 带入方程 (5.10)，可得到方程 (5.10) 的差分形式：

$$\frac{u(x_i, t_{j+1}) - u(x_i, t_j)}{\tau} + k \frac{u(x_{i+1}, t_j) - u(x_i, t_j)}{h} = 0 \quad (5.14)$$

其局部截断误差为  $o(\tau + h)$ 。当  $\tau, h \rightarrow 0$  时，方程 (5.14) 逼近原方程 (5.10)。将方程 (5.14) 整理可得：

$$u(x_i, t_{j+1}) = \frac{\tau k [u(x_i, t_j) - u(x_{i+1}, t_j)]}{h} + u(x_i, t_j) \quad (5.15)$$

令  $\Delta = \frac{\tau}{h}$ ，则由式 (5.15) 可得如下迭代关系：

$$u(x_i, t_{j+1}) = (1 + \Delta k) u(x_i, t_j) - \Delta k u(x_{i+1}, t_j) \quad (5.16)$$

取周期性边界条件, 即  $u(x_N, t) = (x_0, t)$ , 则描述整个系统的方程可以写成如下的形式

$$\begin{bmatrix} u(x_0, t_{j+1}) \\ u(x_1, t_{j+1}) \\ \dots \\ u(x_{N-1}, t_{j+1}) \end{bmatrix} = A \begin{bmatrix} u(x_0, t_j) \\ u(x_1, t_j) \\ \dots \\ u(x_{N-1}, t_j) \end{bmatrix} \quad (5.17)$$

其中

$$A = \begin{bmatrix} 1 + \Delta k & -\Delta k & 0 & \dots & 0 \\ 0 & 1 + \Delta k & -\Delta k & 0 & \dots & 0 \\ \dots & & & & & \\ -\Delta k & 0 & \dots & 0 & 1 + \Delta k & \end{bmatrix} \quad (5.18)$$

则系统的下一时刻即  $t_{j+1}$  时刻的状态  $|\psi\rangle_{j+1}$  可表示为  $A|\psi\rangle_j$ 。显而易见的是  $A$  矩阵并非是酉矩阵, 因此没有办法直接通过量子逻辑门的乘积来实现。而是要通过量子计算的对偶模式将  $A$  矩阵拆解成酉算符的线性组合来实现, 即  $A = (1 + \Delta k)A_0 - \Delta k A_1$ , 其中  $A_0$  是  $N$  阶单位矩阵,

$$A_1 = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & & & & \\ 0 & 0 & 0 & & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}_{N \otimes N} \quad (5.19)$$

通过引入一个辅助比特可实现酉算符线性组合的操作进而等效地实现非酉演化, 即  $A|\psi\rangle_j$ 。其量子线路图如图 5.2:

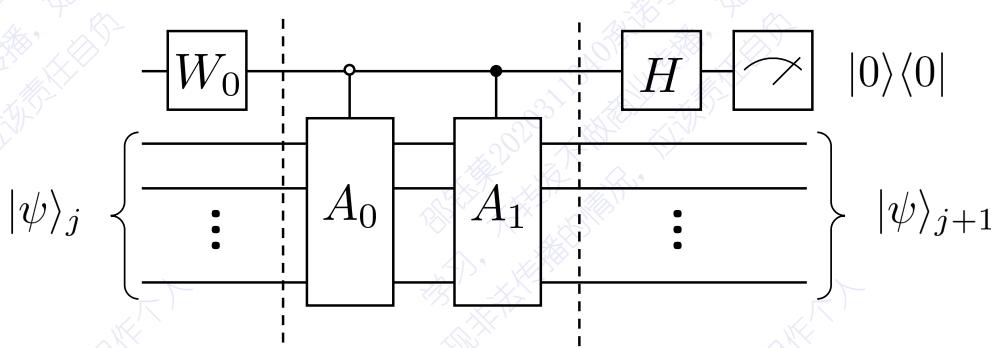


图 5.2 一阶波动方程求解的量子线路图

其中矩阵  $A_1$  可分解为  $C^n(X)$  门以及  $X$  门，其数量为  $O(\log_2 N)$ 。实现  $A_1$  操作的具体量子线路图如图 5.3：

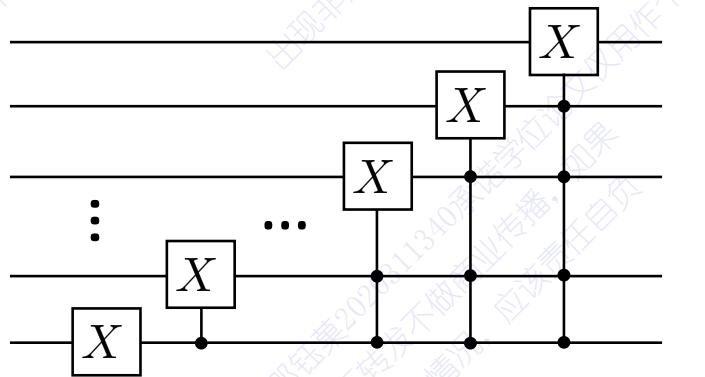


图 5.3  $A_1$  操作的量子线路图

根据文献<sup>[55]</sup>中的引理 5.5 与引理 7.1，若将  $A_1$  操作继续拆解则共需要  $4N - 5\log_2 N - 4$  个 CNOT 门和单比特旋转门。下面将根据图 5.2 来讲解一阶波动方程求解的对偶量子算法，首先辅助比特经过  $W_0$  门，其作用效果如下：

$$W_0 : |0\rangle \rightarrow \frac{(1 + \Delta k)|0\rangle - \Delta k|1\rangle}{\sqrt{(1 + \Delta k)^2 + (\Delta k)^2}} \quad (5.20)$$

接下来经过两个受控量子门  $|0\rangle\langle 0| \otimes A_0$ ,  $|1\rangle\langle 1| \otimes A_1$  则量子态演化为

$$\frac{(1 + \Delta k)|0\rangle A_0|\psi\rangle_j - \Delta k|1\rangle A_1|\psi\rangle_j}{\sqrt{(1 + \Delta k)^2 + (\Delta k)^2}} \quad (5.21)$$

然后经过  $H$  变换后的量子态为

$$\frac{1}{\sqrt{2}}|0\rangle \left[ \frac{(1 + \Delta k)A_0|\psi\rangle_j - \Delta k A_1|\psi\rangle_j}{\sqrt{(1 + \Delta k)^2 + (\Delta k)^2}} \right] + \frac{1}{\sqrt{2}}|1\rangle \left[ \frac{(1 + \Delta k)A_0|\psi\rangle_j + \Delta k A_1|\psi\rangle_j}{\sqrt{(1 + \Delta k)^2 + (\Delta k)^2}} \right] \quad (5.22)$$

最后经过测量选择辅助比特为 0 的状态，则此时工作比特的状态为  $|\psi\rangle_{j+1}$ ，即

$$\frac{(1 + \Delta k)A_0|\psi\rangle_j - \Delta k A_1|\psi\rangle_j}{\sqrt{(1 + \Delta k)^2 + (\Delta k)^2}} \quad (5.23)$$

定义系数  $C_j$  为

$$\sqrt{\sum_{i=0}^{N-1} u^2(x_i, t_j) [(1 + \Delta k)^2 + (\Delta k)^2]} \quad (5.24)$$

将量子态  $|\psi\rangle_{j+1}$  计算基下的概率幅放大  $C_j$  倍，即可得到列向量  $\mathbf{u}(x_i, t_{j+1})$ ，即  $t_{j+1}$  时刻系统的状态。分析可得本算法每次迭代的计算复杂度为  $O(N)$ ，而经典算法的

复杂度则为  $O(N^2)$ 。关于复杂度的具体计算呈现在本章的结尾。

下面将以如下方程为例

$$\begin{cases} \frac{\partial u}{\partial t} + 2 \frac{\partial u}{\partial x} = 0 \\ u(x, 0) = -\sin 2\pi x + \frac{\sin 4\pi x}{2} - \frac{\sin 6\pi x}{3} \end{cases} \quad (5.25)$$

来展示一阶波动方程求解的对偶量子算法。首先选取函数的一个周期即  $[0, 1]$ ，将此区间离散化为 32 个点，即式 (5.15) 中  $h = 0.03125$ 。因此使用 5 个量子比特即可编码 32 个离散点的函数值。选择式 (5.16) 中的  $\Delta = 0.1$ 。则  $\tau = 0.003125$ ，代表每次迭代系统演化的时间间隔。根据式 (5.20) 可确定  $W_0$  的作用效果为：

$$W_0 : |0\rangle \rightarrow \frac{6\sqrt{37}}{37}|0\rangle - \frac{\sqrt{37}}{37}|1\rangle \quad (5.26)$$

由此可得  $W_0$  为  $R_y(-0.33)$ 。至此可以给出求解方程 (5.25) 每次迭代的量子线路如图 5.4

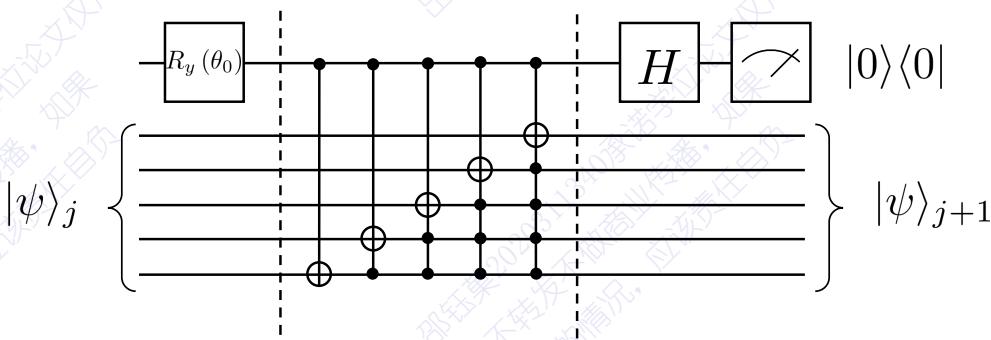


图 5.4 一阶波动方程求解的量子线路图举例，其中  $\theta_0 = -0.33$

数值模拟此量子线路的前 10 次迭代其结果如图 5.5。其中橙色曲线代表解析理论值。蓝色的点代表数值模拟量子求解算法给出的结果。

### 5.3 行波耗散问题求解的对偶量子算法

将方程 (5.10) 加入耗散项，则可得到带有耗散的行波波动方程：

$$\frac{\partial u}{\partial t} + k \frac{\partial u}{\partial x} - \alpha \frac{\partial^2 u}{\partial x^2} = 0 \quad (5.27)$$

对式 (5.27) 各项进行泰勒展开：

$$\begin{aligned} \frac{\partial u}{\partial t} &= \frac{u(x, t + \tau) - u(x, t)}{\tau} + o(\tau), \\ \frac{\partial u}{\partial x} &= \frac{u(x + h, t) - u(x, t)}{h} + o(h), \\ \frac{\partial^2 u}{\partial x^2} &= \frac{u(x - h, t) - 2u(x, t) + u(x + h, t)}{h^2} + o(h^2). \end{aligned} \quad (5.28)$$

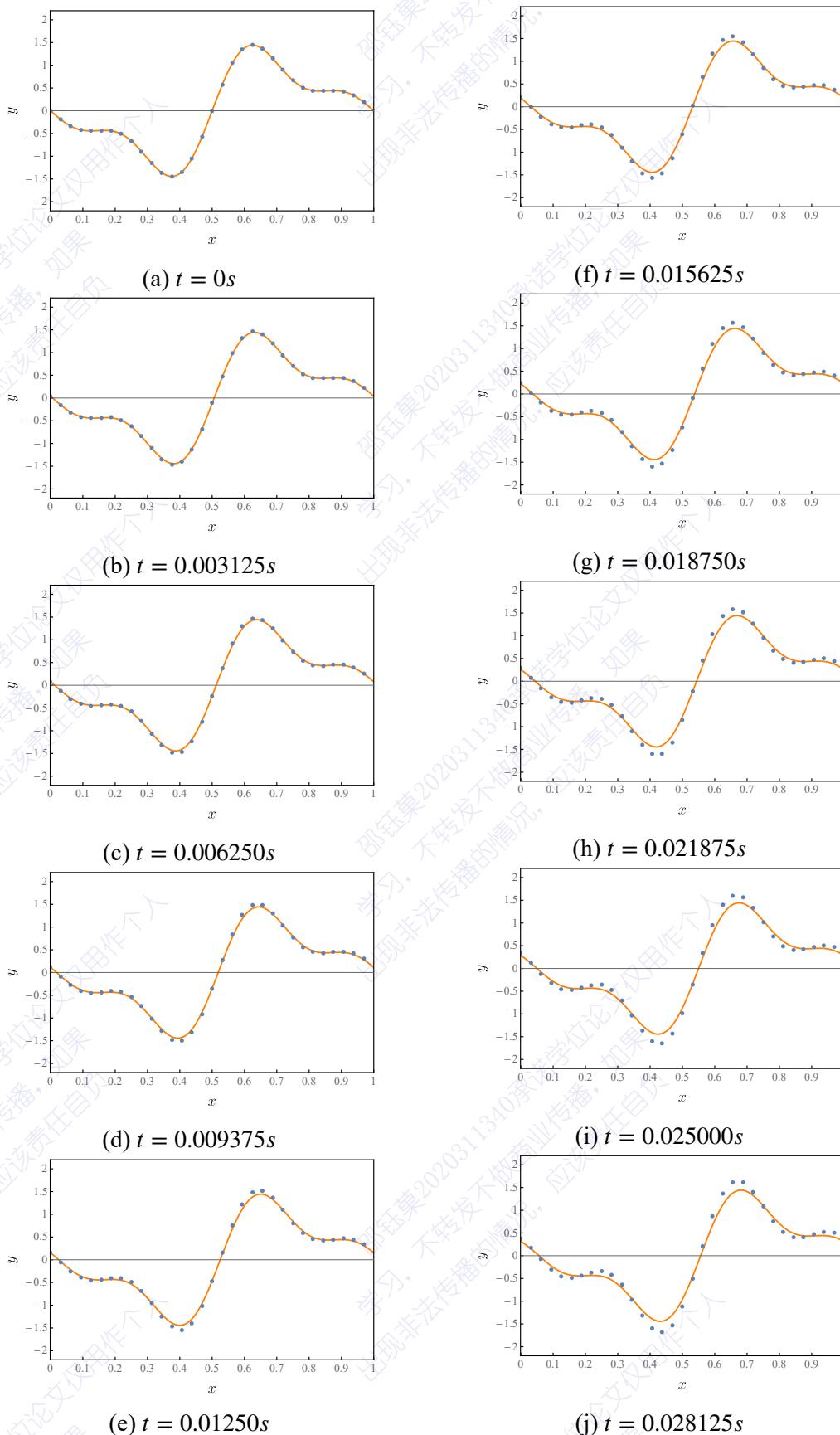


图 5.5 一阶波动方程量子求解算法的数值模拟

将方程(5.27)进行差分可得:

$$\frac{u(x_i, t_{j+1}) - u(x_i, t_j)}{\tau} + k \frac{u(x_{i+1}, t_j) - u(x_i, t_j)}{h} - \alpha \frac{u(x_{i-1}, t_j) - 2u(x_i, t_j) + u(x_{i+1}, t_j)}{h^2} = 0 \quad (5.29)$$

整理可得:

$$u(x_i, t_{j+1}) = \tau k \frac{u(x_i, t_j) - u(x_{i+1}, t_j)}{h} + \tau \alpha \frac{u(x_{i-1}, t_j) - 2u(x_i, t_j) + u(x_{i+1}, t_j)}{h^2} + u(x_i, t_j) \quad (5.30)$$

令  $\Delta = \frac{\tau}{h}$ ,  $\Delta_1 = \alpha \frac{\Delta}{h}$ , 则可得到如下迭代关系:

$$u(x_i, t_{j+1}) = \Delta_1 u(x_{i-1}, t_j) + (k\Delta - 2\Delta_1 + 1) u(x_i, t_j) + (\Delta_1 - k\Delta) u(x_{i+1}, t_j) \quad (5.31)$$

取周期性边界条件, 即  $u(x_N, t) = (x_0, t)$ 。则描述整个系统的方程可以写成如下的形式

$$\begin{bmatrix} u(x_0, t_{j+1}) \\ u(x_1, t_{j+1}) \\ \dots \\ u(x_{N-1}, t_{j+1}) \end{bmatrix} = A \begin{bmatrix} u(x_0, t_j) \\ u(x_1, t_j) \\ \dots \\ u(x_{N-1}, t_j) \end{bmatrix} \quad (5.32)$$

在式(5.32)中

$$A = \begin{bmatrix} a & b & 0 & \dots & 0 & c \\ c & a & b & 0 & \dots & 0 \\ \dots & & & & & \\ 0 & & \dots & 0 & c & a & b \\ b & 0 & \dots & 0 & c & a & \end{bmatrix} \quad (5.33)$$

其中

$$\begin{aligned} a &= k\Delta - 2\Delta_1 + 1, \\ b &= \Delta_1 - k\Delta, \\ c &= \Delta_1. \end{aligned} \quad (5.34)$$

按照式(5.12)的编码方式, 则系统在下一时刻即  $t_{j+1}$  时刻的状态  $|\psi\rangle_{j+1}$  可表示为  $A|\psi\rangle_j$ 。矩阵  $A = (k\Delta - 2\Delta_1 + 1) A_0 + (\Delta_1 - k\Delta) A_1 + \Delta_1 A_2$ , 其中  $A_2 = A_1^\dagger$ 。因此可以通过引入两个辅助比特来等效地实现酉算符线性组合的操作, 其量子线路图如图 5.6:

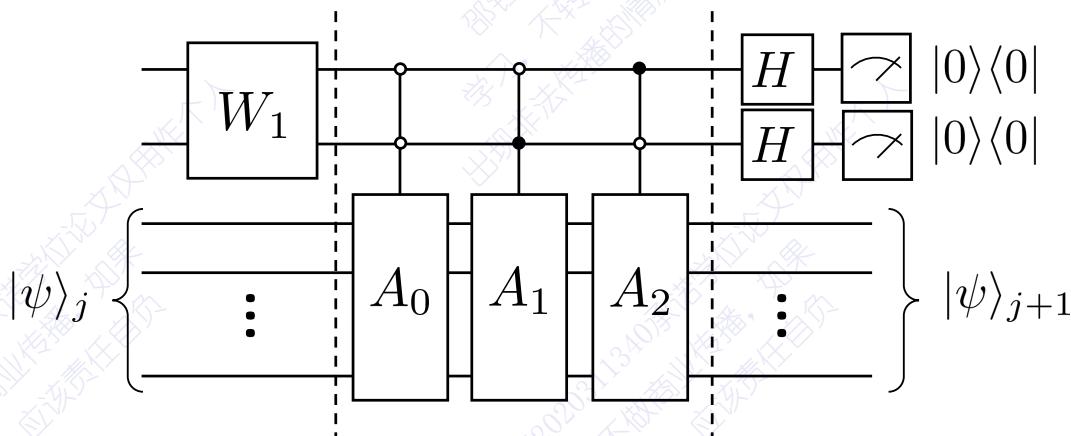


图 5.6 一阶波动方程耗散问题求解的量子线路图

下面将结合量子线路图（图 5.6）来讲解对于一阶波动方程耗散问题求解的对偶量子算法，首先辅助比特经过  $W_1$  门，其作用效果如下：

$$W_1 : |00\rangle \rightarrow \frac{(k\Delta - 2\Delta_1 + 1)|00\rangle + (\Delta_1 - k\Delta)|01\rangle + \Delta_1|10\rangle}{\sqrt{(k\Delta - 2\Delta_1 + 1)^2 + (\Delta_1 - k\Delta)^2 + \Delta_1^2}} \quad (5.35)$$

接下来经过三个受控量子门  $|00\rangle\langle 00| \otimes A_0$ ,  $|01\rangle\langle 01| \otimes A_1$ ,  $|10\rangle\langle 10| \otimes A_2$  后量子态演化为

$$\frac{(k\Delta - 2\Delta_1 + 1)|00\rangle A_0|\psi\rangle_j + (\Delta_1 - k\Delta)|01\rangle A_1|\psi\rangle_j + \Delta_1|10\rangle A_2|\psi\rangle_j}{\sqrt{(k\Delta - 2\Delta_1 + 1)^2 + (\Delta_1 - k\Delta)^2 + \Delta_1^2}} \quad (5.36)$$

然后对两个辅助比特分别做  $H$  变换后量子态演化为

$$\begin{aligned} & \frac{1}{2}|00\rangle \left[ \frac{(k\Delta - 2\Delta_1 + 1)A_0|\psi\rangle_j + (\Delta_1 - k\Delta)A_1|\psi\rangle_j + \Delta_1 A_2|\psi\rangle_j}{\sqrt{(k\Delta - 2\Delta_1 + 1)^2 + (\Delta_1 - k\Delta)^2 + \Delta_1^2}} \right] \\ & + \frac{1}{2}|01\rangle \left[ \frac{(k\Delta - 2\Delta_1 + 1)A_0|\psi\rangle_j - (\Delta_1 - k\Delta)A_1|\psi\rangle_j + \Delta_1 A_2|\psi\rangle_j}{\sqrt{(k\Delta - 2\Delta_1 + 1)^2 + (\Delta_1 - k\Delta)^2 + \Delta_1^2}} \right] \\ & + \frac{1}{2}|10\rangle \left[ \frac{(k\Delta - 2\Delta_1 + 1)A_0|\psi\rangle_j + (\Delta_1 - k\Delta)A_1|\psi\rangle_j - \Delta_1 A_2|\psi\rangle_j}{\sqrt{(k\Delta - 2\Delta_1 + 1)^2 + (\Delta_1 - k\Delta)^2 + \Delta_1^2}} \right] \\ & + \frac{1}{2}|11\rangle \left[ \frac{(k\Delta - 2\Delta_1 + 1)A_0|\psi\rangle_j - (\Delta_1 - k\Delta)A_1|\psi\rangle_j - \Delta_1 A_2|\psi\rangle_j}{\sqrt{(k\Delta - 2\Delta_1 + 1)^2 + (\Delta_1 - k\Delta)^2 + \Delta_1^2}} \right] \end{aligned} \quad (5.37)$$

最后对辅助比特进行测量选择辅助比特为 00 的状态，则此时工作比特的状态为

$|\psi\rangle_{j+1}$ , 即

$$\frac{(k\Delta - 2\Delta_1 + 1) A_0 |\psi\rangle_j + (\Delta_1 - k\Delta) A_1 |\psi\rangle_j + \Delta_1 A_2 |\psi\rangle_j}{\sqrt{(k\Delta - 2\Delta_1 + 1)^2 + (\Delta_1 - k\Delta)^2 + \Delta_1^2}} \quad (5.38)$$

定义系数  $C_j$  为

$$\sqrt{\sum_{i=0}^{N-1} u^2(x_i, t_j) \left[ (k\Delta - 2\Delta_1 + 1)^2 + (\Delta_1 - k\Delta)^2 + \Delta_1^2 \right]} \quad (5.39)$$

将量子态  $|\psi\rangle_{j+1}$  计算基下的概率幅放大  $C_j$  倍数即可得到列向量  $\mathbf{u}(x_i, t_{j+1})$ , 即  $t_{j+1}$  时刻系统状态。

根据文献<sup>[55]</sup>中的引理 5.5 与引理 7.1 并结合图 5.6, 经分析可得本算法每次迭代的计算复杂度为  $O(N)$ , 而经典算法的复杂度则为  $O(N^2)$ 。因此本算法相较于经典算法而言在每次迭代中都具有加速的特性。关于复杂度的具体计算呈现在本章的结尾。

下面将以如下方程为例

$$\begin{cases} \frac{\partial u}{\partial t} + 2\frac{\partial u}{\partial x} - 0.1\frac{\partial^2 u}{\partial x^2} = 0 \\ u(x, 0) = -\sin 2\pi x + \frac{\sin 4\pi x}{2} - \frac{\sin 6\pi x}{3} \end{cases} \quad (5.40)$$

来展示一阶波动方程耗散问题求解的对偶量子算法。首先选取函数的一个周期即  $[0, 1]$ , 将此区间离散化为 32 个点, 即式 (5.28) 中  $h = 0.03125$ 。因此使用 5 个量子比特即可编码 32 个离散点的函数值。选择式 (5.31) 中的  $\Delta = 0.2$ ,  $\Delta_1 = 1.28$ 。则  $\tau = 0.00625$ , 代表每迭代一次系统演化的时间间隔。

根据式 (5.35) 可确定  $W_1$  的作用效果为:

$$W_1 : |00\rangle \rightarrow -\frac{\sqrt{29}}{9}|00\rangle + \frac{22\sqrt{29}}{261}|01\rangle + \frac{32\sqrt{29}}{261}|10\rangle \quad (5.41)$$

其具体构造方法如图 4.11 与式 (4.45), 式 (4.46)。根据式 (4.45) 构造第一辅助比特的旋转门  $R_n(\theta)$ , 使得:

$$R_n(\theta)|00\rangle \rightarrow \left( \frac{5\sqrt{1537}}{261}|0\rangle + \frac{32\sqrt{29}}{261}|1\rangle \right)|0\rangle \quad (5.42)$$

可得  $R_n(\theta)$  为  $R_y(1.442)$ 。

根据式 (4.47) 可得受控算符  $U_1$  要实现以下作用:

$$U_1|0\rangle \rightarrow \frac{29\sqrt{53}}{265}|0\rangle + \frac{22\sqrt{53}}{265}|1\rangle \quad (5.43)$$

可得受控算符  $U_1$  为  $R_y(1.298)$ 。

至此可以给出求解方程 (5.40) 每次迭代的量子线路图如图 5.7

数值模拟此量子线路的前10次迭代过程其结果如图5.8。其中的橙色曲线代表解析的理论值。蓝色的点代表数值模拟量子算法求解出的值。

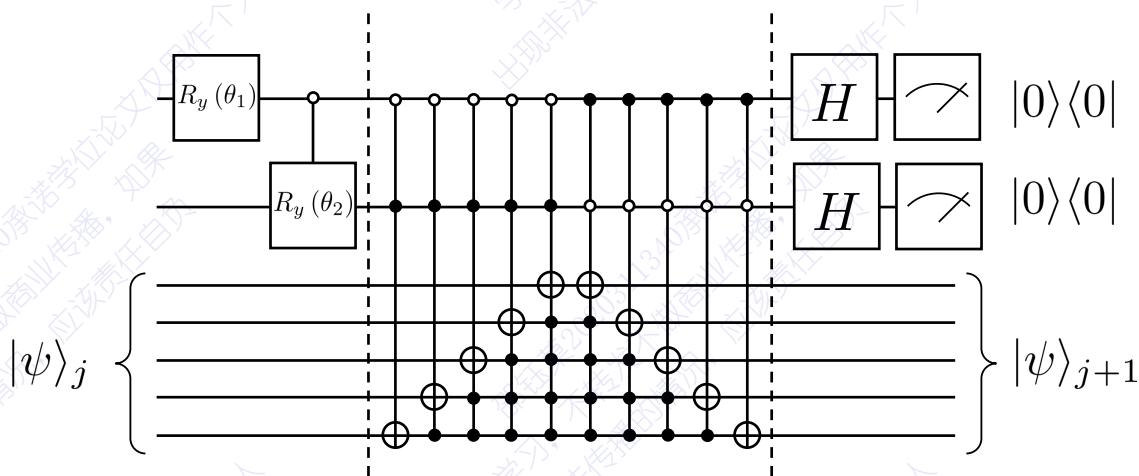


图5.7 一阶波动方程耗散问题求解的量子线路图举例，其中 $\theta_1 = 1.442, \theta_2 = 1.298$

#### 5.4 行波色散问题求解的对偶量子算法

将方程(5.10)加入色散项，则可得带有色散的行波波动方程：

$$\frac{\partial u}{\partial t} + k \frac{\partial u}{\partial x} + \beta \frac{\partial^3 u}{\partial x^3} = 0 \quad (5.44)$$

对式(5.44)各项进行泰勒展开

$$\begin{aligned} \frac{\partial u}{\partial t} &= \frac{u(x, t + \tau) - u(x, t)}{\tau} + o(\tau), \\ \frac{\partial u}{\partial x} &= \frac{u(x + h, t) - u(x, t)}{h} + o(h), \\ \frac{\partial^3 u}{\partial x^3} &= \frac{-u(x - 2h, t) + 3u(x - h, t) - 3u(x, t) + u(x + h, t)}{h^3} + o(h^3). \end{aligned} \quad (5.45)$$

将方程(5.44)进行差分可得：

$$\begin{aligned} \frac{u(x_i, t_{j+1}) - u(x_i, t_j)}{\tau} + k \frac{u(x_{i+1}, t_j) - u(x_i, t_j)}{h} \\ + \beta \frac{-u(x_{i-2}, t_j) + 3u(x_{i-1}, t_j) - 3u(x_i, t_j) + u(x_{i+1}, t_j)}{h^3} = 0 \end{aligned} \quad (5.46)$$

令 $\Delta = \frac{\tau}{h}$ ,  $\Delta_2 = \beta \frac{\Delta}{h^2}$ , 可得如下迭代关系：

$$\begin{aligned} u(x_i, t_{j+1}) &= \Delta_2 u(x_{i-2}, t_j) - 3\Delta_2 u(x_{i-1}, t_j) \\ &\quad + (k\Delta + 3\Delta_2 + 1) u(x_i, t_j) - (k\Delta + \Delta_2) u(x_{i+1}, t_j) \end{aligned} \quad (5.47)$$

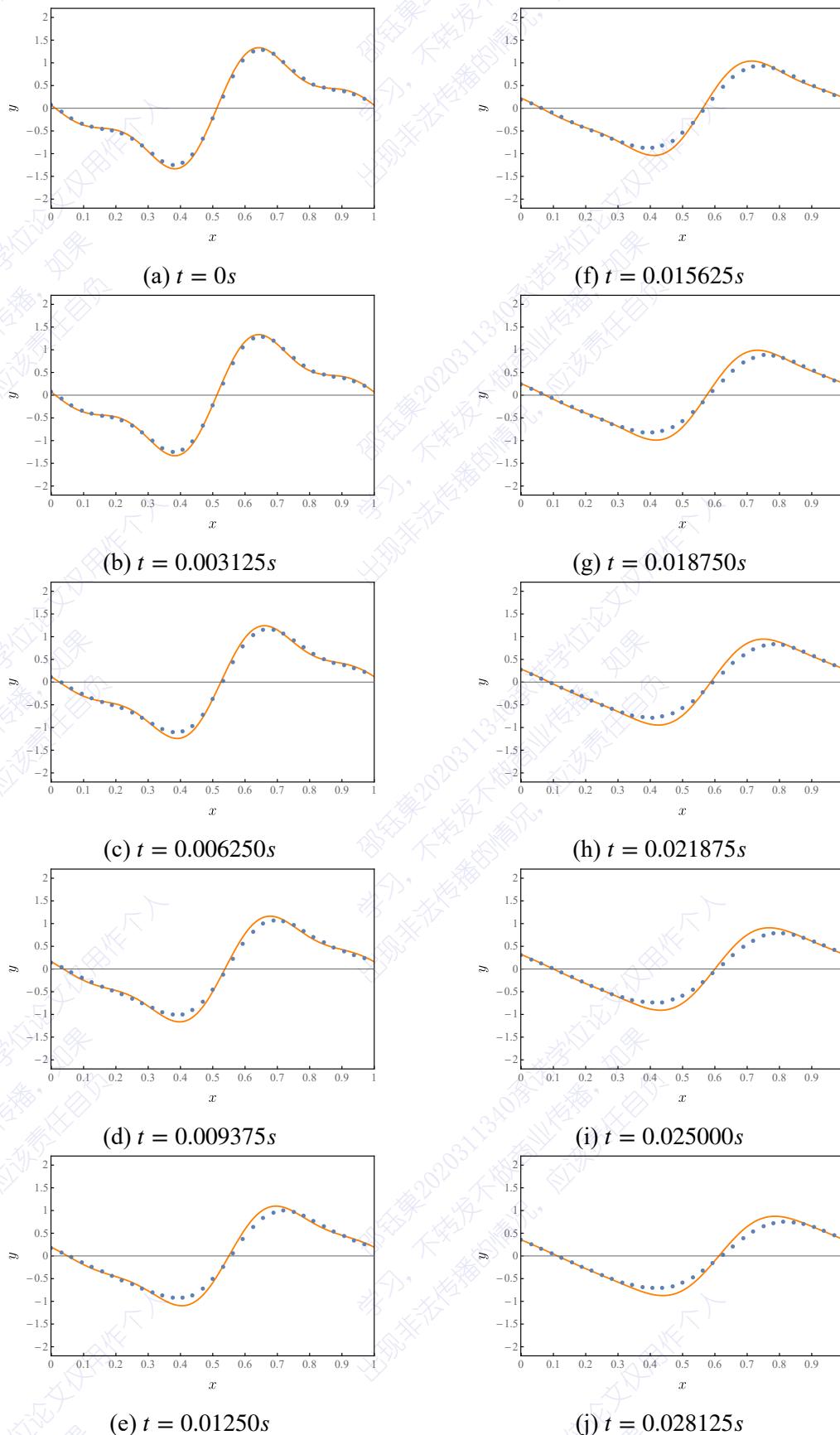


图 5.8 一阶波动方程耗散问题量子求解算法的数值模拟

取周期性边界条件，即  $u(x_N, t) = u(x_0, t)$ 。则描述整个系统的方程可以写成如下的形式

$$\begin{bmatrix} u(x_0, t_{j+1}) \\ u(x_1, t_{j+1}) \\ \dots \\ u(x_{N-1}, t_{j+1}) \end{bmatrix} = A \begin{bmatrix} u(x_0, t_j) \\ u(x_1, t_j) \\ \dots \\ u(x_{N-1}, t_j) \end{bmatrix} \quad (5.48)$$

其中

$$A = \begin{bmatrix} a & b & 0 & & \dots & \dots & 0 & d & c \\ c & a & b & 0 & & \dots & \dots & 0 & d \\ d & c & a & b & 0 & \dots & \dots & & 0 \\ 0 & d & c & a & b & 0 & \dots & & 0 \\ \dots & & \dots & & \dots & & \dots & & \\ 0 & & \dots & & \dots & 0 & d & c & a & b & 0 \\ 0 & & \dots & & \dots & 0 & d & c & a & b \\ b & 0 & & \dots & & \dots & 0 & d & c & a \end{bmatrix} \quad (5.49)$$

其中

$$\begin{aligned} a &= k\Delta + 3\Delta_2 + 1, \\ b &= -(k\Delta + \Delta_2), \\ c &= -3\Delta_2, \\ d &= \Delta_2. \end{aligned} \quad (5.50)$$

可以看出  $A = (k\Delta + 3\Delta_2 + 1) A_0 - (k\Delta + \Delta_2) A_1 - 3\Delta_2 A_2 + \Delta_2 A_3$ ，其中

$$A_3 = \begin{bmatrix} 0 & 0 & & 0 & 0 & 1 & 0 \\ 0 & 0 & & 0 & 0 & 0 & 1 \\ 1 & 0 & & \dots & 0 & 0 & 0 & 0 \\ 0 & 1 & & 0 & 0 & 0 & 0 & 0 \\ \dots & & \dots & & & & & \\ \dots & & & 1 & 0 & 0 & 0 & 0 & 0 \\ & & & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}_{N \otimes N} \quad (5.51)$$

因此可以通过引入两个辅助比特来等效地实现酉算符线性组合的操作，其量子线路图如图 5.9：

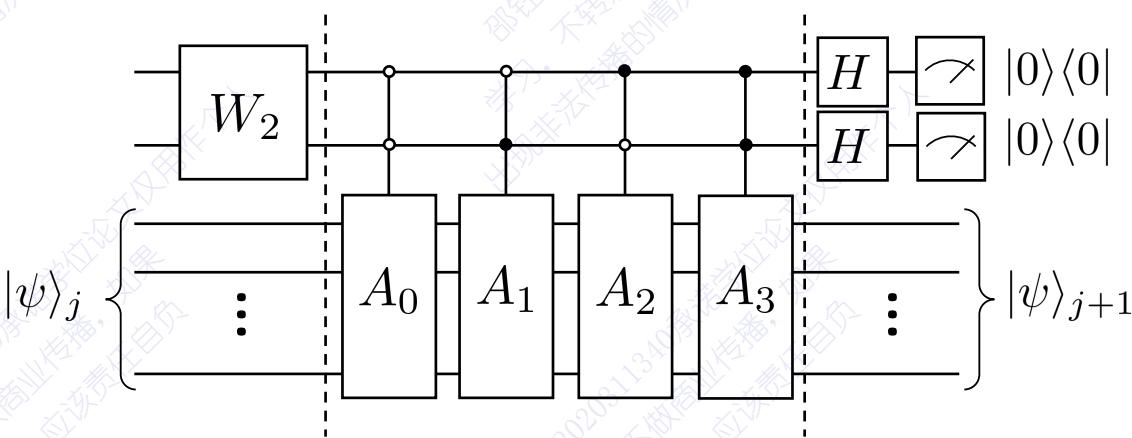


图 5.9 一阶波动方程色散问题求解的量子线路图

不难发现  $A_3 = A_2^2$ , 下面将结合量子线路图 (图 5.9) 来讲解对于一阶波动方程色散问题求解的对偶量子算法, 首先辅助比特经过  $W_2$  门, 其作用效果如下:

$$W_2 : |00\rangle \rightarrow \frac{(k\Delta + 3\Delta_2 + 1)|00\rangle + (k\Delta + \Delta_2)|01\rangle - 3\Delta_2|10\rangle + \Delta_2|11\rangle}{\sqrt{(k\Delta + 3\Delta_2 + 1)^2 + (k\Delta + \Delta_2)^2 + 10\Delta_2^2}} \quad (5.52)$$

接下来经过四个受控量子门  $|00\rangle\langle 00| \otimes A_0, |01\rangle\langle 01| \otimes A_1, |10\rangle\langle 10| \otimes A_2, |11\rangle\langle 11| \otimes A_3$  后量子态演化为

$$\frac{(k\Delta + 3\Delta_2 + 1)|00\rangle A_0|\psi\rangle_j + (k\Delta + \Delta_2)|01\rangle A_1|\psi\rangle_j - 3\Delta_2|10\rangle A_2|\psi\rangle_j + \Delta_2|11\rangle A_3|\psi\rangle_j}{\sqrt{(k\Delta + 3\Delta_2 + 1)^2 + (k\Delta + \Delta_2)^2 + 10\Delta_2^2}} \quad (5.53)$$

然后对两个辅助比特分别做  $H$  变换, 则量子态演化为

$$\begin{aligned} & \frac{1}{2}|00\rangle \left[ \frac{(k\Delta + 3\Delta_2 + 1)A_0|\psi\rangle_j + (k\Delta + \Delta_2)A_1|\psi\rangle_j - 3\Delta_2A_2|\psi\rangle_j + \Delta_2A_3|\psi\rangle_j}{\sqrt{(k\Delta + 3\Delta_2 + 1)^2 + (k\Delta + \Delta_2)^2 + 10\Delta_2^2}} \right] \\ & + \frac{1}{2}|01\rangle \left[ \frac{(k\Delta + 3\Delta_2 + 1)A_0|\psi\rangle_j - (k\Delta + \Delta_2)A_1|\psi\rangle_j - 3\Delta_2A_2|\psi\rangle_j - \Delta_2A_3|\psi\rangle_j}{\sqrt{(k\Delta + 3\Delta_2 + 1)^2 + (k\Delta + \Delta_2)^2 + 10\Delta_2^2}} \right] \\ & + \frac{1}{2}|10\rangle \left[ \frac{(k\Delta + 3\Delta_2 + 1)A_0|\psi\rangle_j + (k\Delta + \Delta_2)A_1|\psi\rangle_j + 3\Delta_2A_2|\psi\rangle_j - \Delta_2A_3|\psi\rangle_j}{\sqrt{(k\Delta + 3\Delta_2 + 1)^2 + (k\Delta + \Delta_2)^2 + 10\Delta_2^2}} \right] \\ & + \frac{1}{2}|11\rangle \left[ \frac{(k\Delta + 3\Delta_2 + 1)A_0|\psi\rangle_j - (k\Delta + \Delta_2)A_1|\psi\rangle_j + 3\Delta_2A_2|\psi\rangle_j + \Delta_2A_3|\psi\rangle_j}{\sqrt{(k\Delta + 3\Delta_2 + 1)^2 + (k\Delta + \Delta_2)^2 + 10\Delta_2^2}} \right] \end{aligned} \quad (5.54)$$

最后经过测量选择辅助比特为 00 的状态，则此时工作比特的状态为  $|\psi\rangle_{j+1}$ ，即

$$\frac{(k\Delta + 3\Delta_2 + 1)A_0|\psi\rangle_j + (k\Delta + \Delta_2)A_1|\psi\rangle_j - 3\Delta_2 A_2|\psi\rangle_j + \Delta_2 A_3|\psi\rangle_j}{\sqrt{(k\Delta + 3\Delta_2 + 1)^2 + (k\Delta + \Delta_2)^2 + 10\Delta_2^2}} \quad (5.55)$$

定义系数  $C_j$  为

$$\sqrt{\sum_{i=0}^{N-1} u^2(x_i, t_j) \left[ (k\Delta + 3\Delta_2 + 1)^2 + (k\Delta + \Delta_2)^2 + 10\Delta_2^2 \right]} \quad (5.56)$$

将量子态  $|\psi\rangle_{j+1}$  计算基下的概率幅放大  $C_j$  倍，即可得到列向量  $\mathbf{u}(x_i, t_{j+1})$ ，即  $t_{j+1}$  时刻系统的状态。根据文献[55]中的引理 5.5 与引理 7.1，并结合图 5.9 分析可得本算法每次迭代的计算复杂度为  $O(N)$ ，而经典算法的复杂度则为  $O(N^2)$ 。关于复杂度的具体计算呈现在本章的结尾。

下面将以如下方程为例

$$\begin{cases} \frac{\partial u}{\partial t} + 2\frac{\partial u}{\partial x} + 0.01\frac{\partial^3 u}{\partial x^3} = 0 \\ u(x, 0) = -\sin 2\pi x + \frac{\sin 4\pi x}{2} - \frac{\sin 6\pi x}{3} \end{cases} \quad (5.57)$$

来展示一阶波动方程色散问题求解的对偶量子算法。首先选取函数的一个周期即  $[0, 1]$ ，将此区间离散化为 32 个点，即式 (5.47) 中  $h = 0.03125$ 。因此使用 5 个量子比特即可编码 32 个离散点的函数值。选择式 (5.47) 中的  $\Delta = 0.05$ ,  $\Delta_2 = 0.512$ 。则  $\tau = 0.0015625$ ，代表每迭代一次系统演化的时间间隔。

根据式 (5.52) 可确定  $W_2$  的作用效果为：

$$W_2 : |00\rangle \rightarrow 0.8359|00\rangle + 0.1941|01\rangle - 0.4871|10\rangle + 0.1624|11\rangle \quad (5.58)$$

其具体构造方法如图 4.11 与式 (4.45), 式 (4.46)。

根据式 (4.45) 构造第一辅助比特的旋转门  $R_n(\theta)$ ，使得：

$$R_n(\theta)|00\rangle \rightarrow (0.8581|0\rangle + 0.5135|1\rangle)|0\rangle \quad (5.59)$$

可得  $R_n(\theta)$  为  $R_y(1.078)$ 。

根据式 (4.47) 可得两个受控算符  $U_1$ ,  $U_2$  要实现以下作用：

$$\begin{aligned} U_1|0\rangle &\rightarrow 0.9741|0\rangle + 0.2262|1\rangle \\ U_2|0\rangle &\rightarrow -0.9486|0\rangle + 0.3163|1\rangle \end{aligned} \quad (5.60)$$

可得受控算符  $U_1$  为  $R_y(0.4563)$ ,  $U_2$  为  $R_y(5.639)$ 。至此可以给出求解方程 (5.57) 每次迭代的量子线路图如图 5.10。

数值模拟此量子线路的前 10 次迭代过程其结果如图 5.12。其中的橙色曲线代表解析理论值。蓝色的点代表数值模拟量子算法解出的值。

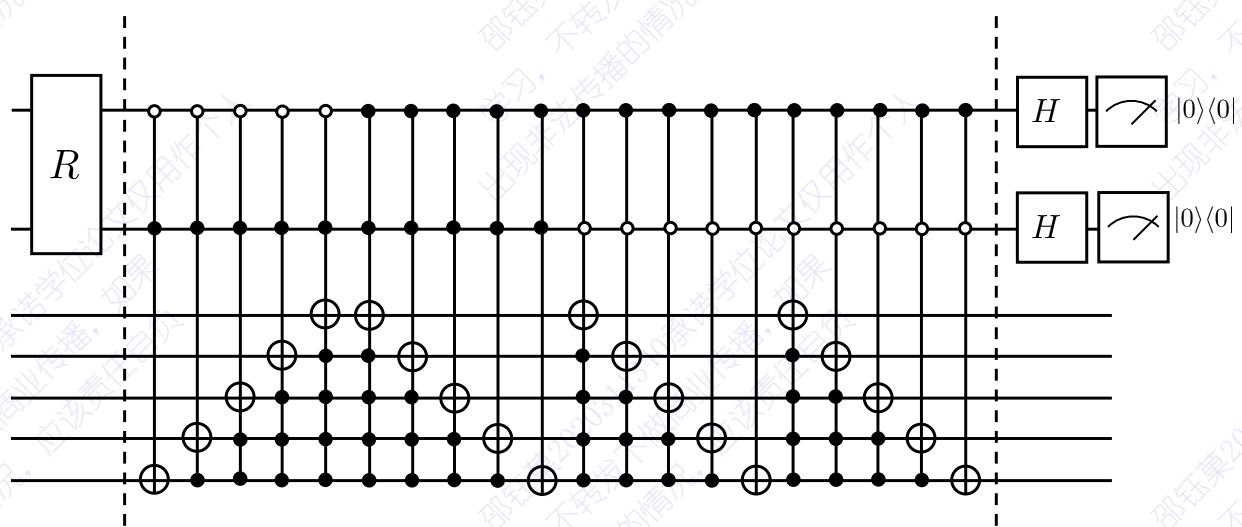
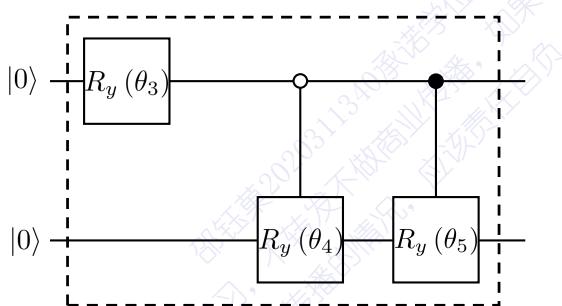


图 5.10 一阶波动方程色散问题求解的量子线路图举例

其中  $R$  操作的具体形式如图 5.11:

图 5.11  $R$  操作的具体形式, 其中  $\theta_3 = 1.078$ ,  $\theta_4 = 0.4563$ ,  $\theta_5 = 5.639$ 

## 5.5 讨论

对于一个空间离散格点数为  $N$ , 求解  $d$ -维偏微分方程 (指的是有  $d$  个空间变量) 的量子算法, 其输出为函数  $f$  的近似值  $C(f)$ , 误差为  $\epsilon$ 。事实上对于量子算法求解偏微分方程的问题, 其离散点数  $N$  与误差  $\epsilon$  是相互关联的<sup>[198-199]</sup>。其关联关系如下:

$$N = O\left(\text{poly}\left(\frac{1}{\epsilon^d}\right)\right) \quad (5.61)$$

对于初态的制备其复杂度为  $O(\text{poly log}(N))$ 。下面将给出本章算法每次迭代的复杂度。首先根据文献<sup>[55]</sup>中的引理 5.5 与引理 7.1 可得对于  $n$  比特拥有  $n - 1$  个控制位的受控门  $C^{n-1}(U)$  可拆解为 CNOT 门与单比特门共  $2^{n+1} - 5$  个, 其中  $n \geq 3$ 。对

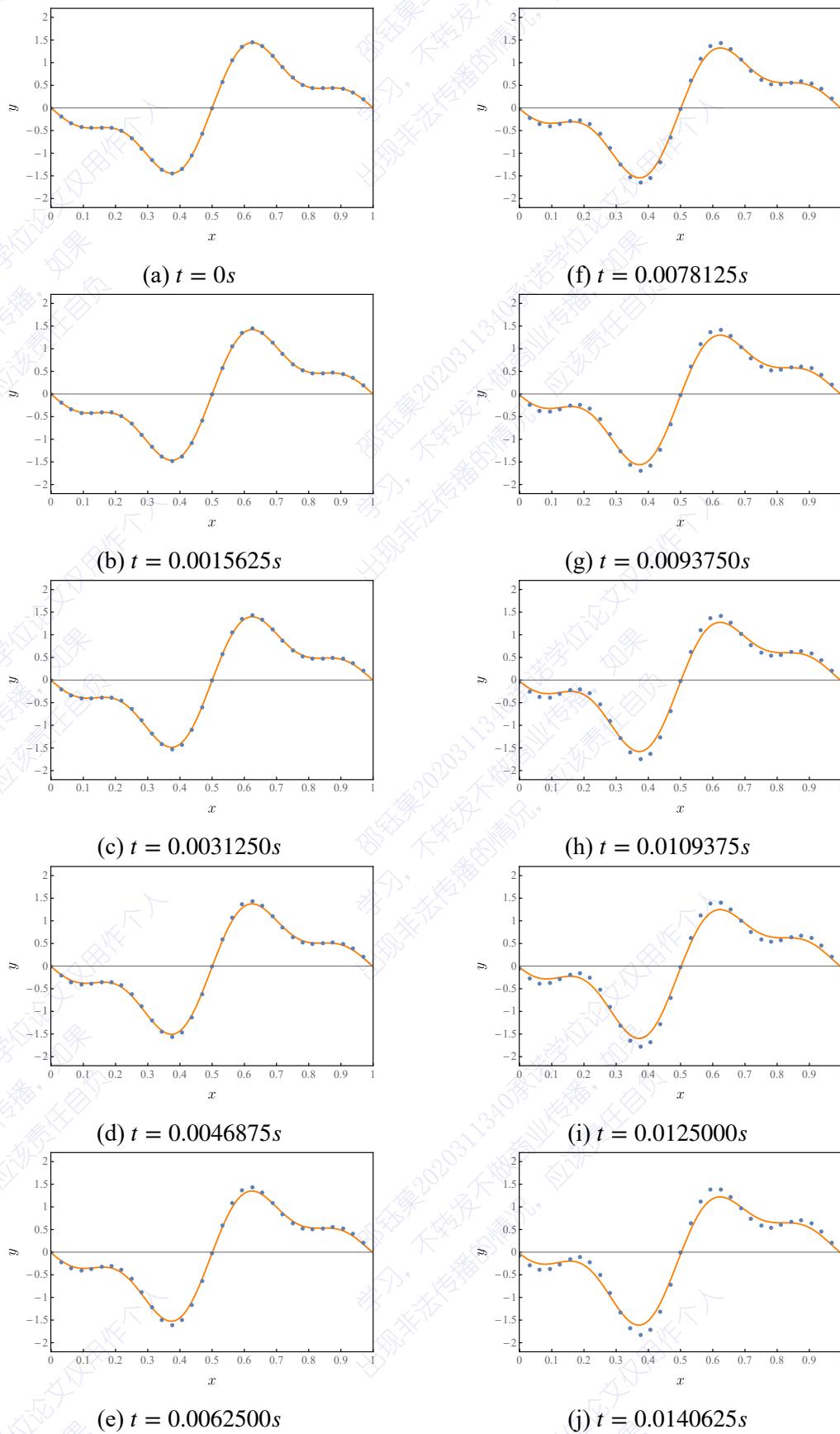


图 5.12 一阶波动方程色散问题的量子求解算法的数值模拟

于线路图 5.2, 共需要的基本量子门数量为:

$$\begin{aligned} & 3 + O(C^2(U)) + \cdots + O(C^n(U)) \\ & = 2^{n+1} - 5n - 8 = 8N - 5\log_2 N - 8 \simeq O(N) \end{aligned} \quad (5.62)$$

对于线路图 5.6, 共需要的基本量子门数量为:

$$\begin{aligned} & 8 + 2 [O(C^2(U)) + \cdots + O(C^{n+1}(U))] \\ & = 2^{n+5} - 10n - 24 = 32N - 10\log_2 N - 24 \simeq O(N) \end{aligned} \quad (5.63)$$

对于线路图 5.9, 共需要的基本量子门数量为:

$$\begin{aligned} & 8 + 4 [O(C^2(U)) + \cdots + O(C^{n+1}(U))] \\ & = 2^{n+6} - 20n - 56 = 64N - 20\log_2 N - 24 \simeq O(N) \end{aligned} \quad (5.64)$$

可以发现本章给出的对偶量子算法每次迭代与经典算法相比拥有二次加速的特性。然而每次迭代结束都需要测量后选择辅助比特的状态。而这种结果是具有概率性的, 若每次迭代都是测量后选择, 则整体算法的成功率会随着迭代次数的增加而指数下降。因此若要保证整体较高的成功率需要使用第 3 章改进的搜索算法对目标态的振幅先放大再进行测量。所以本章的算法是带有振幅放大的对偶量子算法。

## 5.6 本章小结

对于偏微分方程的求解问题, 作者在本章运用量子计算的对偶模式, 利用带有振幅放大的对偶量子算法设计了求解波动方程的量子算法。并研究了行波的传播、耗散与色散问题。本章利用数值模拟的方法模拟了这三种方程的量子求解结果。本章给出的对偶量子算法每次迭代与经典算法相比拥有二次加速的特性。

## 第6章 总结与展望

量子信息是一门交叉学科，其结合了量子力学与信息科学。从最初纸上的量子图灵机模型，到第一台量子计算机演示平台的出现，再到现在量子优越性的实现都是一个又一个里程碑式的成果。通过运用量子力学的纠缠特性科学家提出了一系列量子算法。但这些量子算法都受限于量子态的酉演化，因此其存在一定的局限性。直到量子计算的对偶模式提出，可突破对于酉演化的限制。运用此工具可实现量子态的非酉演化。这为量子算法的研究提供了新的思路。本文研究了带有振幅放大的对偶量子算法。本文首先介绍了量子计算的学科背景以及发展该学科的必要性。然后第二部分回顾了量子信息的基本知识，接下来介绍了几种常见的量子算法。最后展示了作者在博士期间的主要工作：

(1) 通过对 Grover-Long 算法的改进，提出了高鲁棒量子搜索算法，使其对于占比的不确定度具有良好的鲁棒性。在此算法中并不需要知道确切的占比，只需要知道一个误差范围，即可以较高的成功概率获得目标态。即使在对于占比完全未知的情况下，匹配量子计数算法仍然可以 96% 的成功率获得目标态。同时该算法可用于对偶量子算法的振幅放大算法。该部分成果对应于本文第 3 章内容。

(2) 将范畴论与量子模拟相结合提出了范畴化量子模拟的对偶量子算法，并且以  $SU(3)$  杨-米尔斯规范场为例展示了如何进行范畴化量子模拟。范畴化量子模拟扩大了量子计算机可使用的范围，同时不再要求被模拟的系统必须具有群的结构。使得之前部分无法被量子模拟的系统变得可能。同时采用基于代数结构的编码方式而非基于格点模型几何结构的编码方式，这节省了量子内存资源。同时该编码方式采用了演生论的思想而非还原论。该部分成果对应文章第 4 章的内容。

(3) 基于量子计算的对偶模式，以波动方程为例，给出了不同于以往的偏微分方程求解的对偶量子算法，在该算法中每次迭代相较于经典算法具有二次加速的特性。这为偏微分方程求解的量子算法提供了新的可行方案。该部分成果对应文章第 5 章的内容。

传统的量子算法运用的是量子计算的直乘模式，即运用量子逻辑门的乘积去模拟量子态的酉演化。而量子计算对偶模式的引入可模拟量子态的非酉演化。在该算法的框架下通过引入辅助比特将非酉算符拆解成酉算符的线性组合。量子计算对偶模式的引入可将超越群论的数学结构引入量子算法领域，比如本文第 4 章将张量范畴引入了量子信息领域，这使得原来无法描述的物理现象变得可能。进而为进一步利用量子效应提供了有力的理论基础。事实上，范畴论这一数学语言

建立起了量子线路与其他学科之间的联系。使得被模拟的系统可以直接翻译（或编码）到量子计算机上。这无疑打通了量子物理与其它学科的联系。在数学的观点上看，通过带有振幅放大的对偶量子算法实现的范畴化量子模拟事实上是一个二进制的量子场论。这揭示了更深层次的道理，即物理学中的万物起源于量子比特。万物都是通过量子比特演生（或编码）出来的。作者认为传统的基于格点模型几何结构的还原论编码方式与基于张量范畴代数结构的演生论编码方式之间存在着对偶关系。就好像拓扑序的全息原理一样，即  $d$  维的边界态可以完全复原出  $d+1$  维体态的信息。此外，量子计算对偶模式的引入可使得对于量子算法的设计不必拘泥于酉演化的限制。这无疑可以将经典算法的部分优秀设计思路应用于设计量子算法，比如本文第 5 章的工作。

图 6.1 描述了量子信息处理的发展，量子信息处理的发展要经过七个阶段。

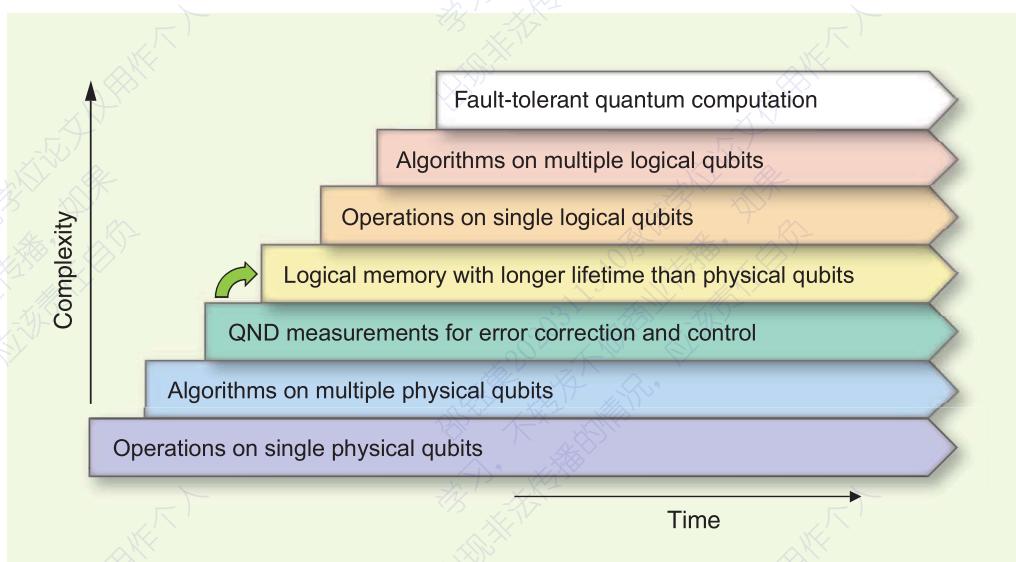


图 6.1 量子信息处理发展的 7 个阶段<sup>[200]</sup>

每一次进步都需要掌握前面的阶段。目前已实现前三个阶段：对于单个物理比特的操控，在多位物理比特上演示量子算法，对于量子纠错和量子控制的非破坏性测量。现在的目标是要达到第四阶段，即实现比物理比特更长相干时间的逻辑比特。在将来会逐步实现对于单逻辑比特操作的第五阶段，在多位逻辑比特上演示量子算法的第六阶段，以及实现容错量子计算的第七阶段，一旦达到第七阶段则标志着量子计算机研制成功，将引发新一轮的信息革命。目前在量子计算领域不断出现的里程碑式的成果一直在鼓舞着人们。量子计算正走向实用化与大规模化。虽然个人的力量很渺小，但是作者有幸能加入其中。相信在科研工作者的努力下，量子信息时代终将会到来。

## 参考文献

- [1] Moore G E. Cramming more components onto integrated circuits, reprinted from electronics, volume 38, number 8, april 19, 1965, pp.114 ff.[J]. IEEE Solid-State Circuits Society Newsletter, 2006, 11(3): 33-35.
- [2] Roser M, Ritchie H. Moore's law transistor count 1970-2020[EB/OL]. 2020[March 16, 2022]. <https://ourworldindata.org/uploads/2020/11/Transistor-Count-over-time.png>.
- [3] Landauer R. Irreversibility and heat generation in the computing process[J]. IBM Journal of Research and Development, 1961, 5(3): 183-191.
- [4] Bennett C H. Notes on landauer's principle, reversible computation, and maxwell's demon [J]. Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics, 2003, 34(3): 501-510.
- [5] Lloyd S, Garnerone S, Zanardi P. Quantum algorithms for topological and geometric analysis of data[J]. Nature Communications, 2016, 7: 10138.
- [6] Rivest R L, Shamir A, Adleman L M. A method for obtaining digital signatures and public-key cryptosystems[J]. Commun. ACM, 1983, 26: 96-99.
- [7] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]// Proceedings 35th annual symposium on foundations of computer science. IEEE, 1994: 124-134.
- [8] Aaronson S. The limits of quantum computers[J]. Scientific American, 2008, 3: 62-69.
- [9] Benioff P. Quantum mechanical hamiltonian models of turing machines[J]. Journal of Statistical Physics, 1982, 29(3): 515-546.
- [10] Deutsch D. Quantum theory, the church-turing principle and the universal quantum computer [J]. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 1985, 400(1818): 97-117.
- [11] Feynman R P. Simulating physics with computers[J]. International journal of theoretical physics, 1982, 21(6): 467-488.
- [12] Feynman R P. Quantum mechanical computers[J]. Foundations of physics, 1986, 16(6): 507-531.
- [13] Deutsch D E. Quantum computational networks[J]. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 1989, 425(1868): 73-90.
- [14] Berthiaume A, Brassard G. The quantum challenge to structural complexity theory[C]//[1992] Proceedings of the Seventh Annual Structure in Complexity Theory Conference. IEEE, 1992: 132-137.
- [15] Berthiaume A, Brassard G. Oracle quantum computing[J]. Journal of modern optics, 1994, 41 (12): 2521-2535.
- [16] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM J. Comput., 1999, 26: 1484-1509.

- [17] Grover L K. A fast quantum mechanical algorithm for database search[C]/Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. New York, NY, USA, 1996: 212–219.
- [18] Preskill J. Quantum computing and the entanglement frontier[A]. 2012.
- [19] Arute F, Arya K, Babbush R, et al. Quantum supremacy using a programmable superconducting processor[J]. Nature, 2019, 574(7779): 505-510.
- [20] Arute F, et al. Quantum supremacy using a programmable superconducting processor[J]. Nature, 2019, 574(7779): 505-510.
- [21] Shor P W. Scheme for reducing decoherence in quantum computer memory[J]. Phys. Rev. A, 1995, 52: R2493-R2496.
- [22] Steane A M. Error correcting codes in quantum theory[J]. Phys. Rev. Lett., 1996, 77: 793-797.
- [23] Kitaev A. Fault-tolerant quantum computation by anyons[J]. Annals of Physics, 2003, 303(1): 2-30.
- [24] Divincenzo D P. The Physical Implementation of Quantum Computation[J]. Fortschritte der Physik, 2000, 48(9-11): 771-783.
- [25] Castelvecchi D. Quantum computers ready to leap out of the lab in 2017[J/OL]. , 2017, 541 (7635): 9-10. DOI: 10.1038/541009a.
- [26] Ryan C A, Johnson B R, Ristè D, et al. Hardware for dynamic quantum computing[J]. Review of Scientific Instruments, 2017, 88(10): 104703.
- [27] Kelly J, Barends R, Fowler A G, et al. State preservation by repetitive error detection in a superconducting quantum circuit[J]. Nature, 2015, 519(7541): 66-69.
- [28] Friis N, Marty O, Maier C, et al. Observation of Entangled States of a Fully Controlled 20-Qubit System[J]. Physical Review X, 2018, 8(2): 021012.
- [29] Wu Y, Bao W S, Cao S, et al. Strong quantum computational advantage using a superconducting quantum processor[J]. Physical Review Letters, 2021, 127(18).
- [30] Zhu Q, Cao S, Chen F, et al. Quantum computational advantage via 60-qubit 24-cycle random circuit sampling[J]. Science Bulletin, 2022, 67(3): 240-245.
- [31] Martinis J M, Nam S, Aumentado J, et al. Rabi oscillations in a large josephson-junction qubit [J]. Phys. Rev. Lett., 2002, 89: 117901.
- [32] Devoret M H, Schoelkopf R J. Superconducting Circuits for Quantum Information: An Outlook [J]. Science, 2013, 339(6124): 1169-1174.
- [33] Gambetta J M, Chow J M, Steffen M. Building logical qubits in a superconducting quantum computing system[J]. npj Quantum Information, 2017, 3: 2.
- [34] Kielpinski D, Monroe C, Wineland D J. Architecture for a large-scale ion-trap quantum computer[J]. , 2002, 417(6890): 709-711.
- [35] Monz T, Schindler P, Barreiro J T, et al. 14-qubit entanglement: Creation and coherence[J]. Phys. Rev. Lett., 2011, 106: 130506.
- [36] Bruzewicz C D, Chiaverini J, McConnell R, et al. Trapped-ion quantum computing: Progress and challenges[J]. Applied Physics Reviews, 2019, 6(2): 021314.

## 参考文献

- [37] Loss D, DiVincenzo D P. Quantum computation with quantum dots[J]. Physical Review A, 1998, 57: 120-126.
- [38] Eriksson M A, Friesen M, Coppersmith S N, et al. Spin-based quantum dot quantum computing in silicon[J]. Quantum Information Processing, 2004, 3: 133-146.
- [39] Chuang I L, Vandersypen L M K, Zhou X, et al. Experimental realization of a quantum algorithm [J]. Nature, 1998, 393: 143-146.
- [40] Chuang I L, Gershenfeld N A, Kubinec M. Experimental implementation of fast quantum searching[J]. Physical Review Letters, 1998, 80: 3408-3411.
- [41] Vandersypen L M K, Steffen M, Breyta G, et al. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance[J]. Nature, 2001, 414: 883-887.
- [42] Bloch F. Nuclear induction[J]. Phys. Rev., 1946, 70: 460-474.
- [43] Einstein A B, Podolsky B, Rosen N. Can quantum-mechanical description of physical reality be considered complete?[J]. Physical Review, 1935, 47: 777-780.
- [44] Bohm D. Prentice-hall physics series: Quantum theory[M]. Prentice-Hall, Inc., 1951.
- [45] Bell J S. On the einstein-podolsky-rosen paradox[J]. Physics, 1964, 1: 195-200.
- [46] Bell J S. On the problem of hidden variables in quantum mechanics[J]. Reviews of Modern Physics, 1966, 38: 447-452.
- [47] Clauser J F, Horne M A, Shimony A, et al. Proposed experiment to test local hidden variable theories.[J]. Physical Review Letters, 1969, 23: 880-884.
- [48] Freedman S J, Clauser J F. Experimental test of local hidden-variable theories[J]. Physical Review Letters, 1972, 28: 938-941.
- [49] Aspect A, Grangier P, Roger G. Experimental tests of realistic local theories via bell's theorem [J]. Physical Review Letters, 1981, 47: 460-463.
- [50] Rowe M A, Kielpinski D, Meyer V, et al. Experimental violation of a bell's inequality with efficient detection[J]. Nature, 2001, 409: 791-794.
- [51] Ansmann M, Wang H, Bialczak R C, et al. Violation of bell's inequality in josephson phase qubits[J]. Nature, 2009, 461: 504-506.
- [52] Giustina M, Mech A, Ramelow S, et al. Bell violation using entangled photons without the fair-sampling assumption[J]. Nature, 2013, 497: 227-230.
- [53] Hensen B, Bernien H, Dréau A, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres[J]. Nature, 2015, 526: 682-686.
- [54] Wootters W K, Zurek W. A single quantum cannot be cloned[J]. Nature, 1982, 299: 802-803.
- [55] Barenco, Bennett, Cleve, et al. Elementary gates for quantum computation[J]. Physical review. A, Atomic, molecular, and optical physics, 1995, 52 5: 3457-3467.
- [56] Sleator, Weinfurter. Realizable universal quantum logic gates.[J]. Physical review letters, 1995, 74 20: 4087-4090.
- [57] Dawson C M, Nielsen M A. The solovay-kitaev algorithm[J]. Quantum Inf. Comput., 2006, 6: 81-95.

- [58] Kitaev A Y. Quantum computations: algorithms and error correction[J]. Russian Mathematical Surveys, 1997, 52: 1191-1249.
- [59] Gottesman D. The heisenberg representation of quantum computers[C]//1998.
- [60] Aaronson S, Gottesman D. Improved simulation of stabilizer circuits: quant-ph/0406196[A]. 2004.
- [61] Grover L K. Quantum mechanics helps in searching for a needle in a haystack[J]. Physical review letters, 1997, 79(2): 325.
- [62] Harrow A W, Hassidim A, Lloyd S. Quantum algorithm for linear systems of equations.[J]. Physical review letters, 2009, 103 15: 150502.
- [63] Gui-lu L. General quantum interference principle and duality computer[J]. Communications in Theoretical Physics, 2006, 45: 825-844.
- [64] Long G L, Liu Y. Duality quantum computing[J]. Frontiers of Computer Science in China, 2008, 2: 167-178.
- [65] Gui-lu L, Yang L, Chuan W. Allowable generalized quantum gates[J]. Communications in Theoretical Physics, 2009, 51: 65-67.
- [66] Gudder S P. Mathematical theory of duality quantum computers[J]. Quantum Information Processing, 2007, 6: 37-48.
- [67] Berry D W, Childs A M, Kothari R. Hamiltonian simulation with nearly optimal dependence on all parameters[J]. 2015 IEEE 56th Annual Symposium on Foundations of Computer Science, 2015: 792-809.
- [68] Wei S, Ruan D, Long G L. Duality quantum algorithm efficiently simulates open quantum systems[J]. Scientific Reports, 2016, 6: 30727.
- [69] Childs A M, Kothari R, Somma R D. Quantum algorithm for systems of linear equations with exponentially improved dependence on precision[J]. SIAM J. Comput., 2017, 46: 1920-1950.
- [70] Гельфанд И.М., Наймарк М. А. On the imbedding of normed rings into the ring of operators in Hilbert space[C]//1943.
- [71] Paulsen V I. Completely bounded maps and operator algebras[C]//2003.
- [72] Oszmaniec M, Guerini L, Wittek P, et al. Simulating positive-operator-valued measures with projective measurements.[J]. Physical review letters, 2017, 119 19: 190501.
- [73] Nakajima S. On quantum theory of transport phenomena steady diffusion[J]. Progress of Theoretical Physics, 1958, 20: 948-959.
- [74] Zwanzig R W. Ensemble method in the theory of irreversibility[J]. Journal of Chemical Physics, 1960, 33: 1338-1341.
- [75] Chen J. Measuring non-markovianity of noise in the central spin system[D]. University of Waterloo, 2019.
- [76] Louisell W H. Wiley series in pure and applied optics: Quantum statistical properties of radiation[M]. John Wiley Sons, 1990.
- [77] Heinz-Peter Breuer F P. The theory of open quantum systems[M]. Oxford University Press, 2002.

## 参考文献

- [78] Clerk A A, Devoret M H, Girvin S M, et al. Introduction to quantum noise, measurement, and amplification[J]. *Reviews of Modern Physics*, 2010, 82: 1155-1208.
- [79] Kraus K, Bohm A R, Dollard J D, et al. States, effects, and operations : fundamental notions of quantum theory : lectures in mathematical physics at the university of texas at austin[C]//1983.
- [80] Steane A M. Multiple-particle interference and quantum error correction[J]. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 1996, 452: 2551 - 2577.
- [81] Koppens F H L, Buizert C, Tielrooij K J, et al. Driven coherent oscillations of a single electron spin in a quantum dot[J]. *Nature*, 2006, 442: 766-771.
- [82] Lidar D A, Bacon D, Whaley K B. Concatenating decoherence-free subspaces with quantum error correcting codes[J]. *Physical Review Letters*, 1999, 82: 4556-4559.
- [83] Gottesman D. Stabilizer codes and quantum error correction[A]. 1997.
- [84] Kitaev A Y. Fault tolerant quantum computation by anyons[J]. *Annals of Physics*, 2003, 303: 2-30.
- [85] Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. [J]. *Physical review. A, Atomic, molecular, and optical physics*, 1996, 54 3: 1862-1868.
- [86] Waldherr G, Wang Y, Zaiser S, et al. Quantum error correction in a solid-state hybrid spin register[J]. *Nature*, 2014, 506: 204-207.
- [87] Laflamme, Miquel, Paz, et al. Perfect quantum error correcting code.[J]. *Physical review letters*, 1996, 77 1: 198-201.
- [88] Gottesman D. Pasting quantum codes[A]. 1996.
- [89] Calderbank A R, Rains E M, Shor P W, et al. Quantum error correction via codes over  $gf(4)$ [J]. *IEEE Trans. Inf. Theory*, 1998, 44: 1369-1387.
- [90] Cleve R, Gottesman D. Efficient computations of encodings for quantum error correction[J]. *Physical Review A*, 1997, 56: 76-82.
- [91] Kitaev A Y. Anyons in an exactly solved model and beyond[J]. *Annals of Physics*, 2006, 321: 2-111.
- [92] Ferrari F, for Advanced Stud Center F B S I S, Cnr I, et al. Spectral signatures of fractionalization in the frustrated heisenberg model on the square lattice[J]. *Physical Review B*, 2018, 98(10): 100405.1-100405.6.
- [93] Wen. Mean-field theory of spin-liquid states with finite energy gap and topological orders.[J]. *Physical review. B, Condensed matter*, 1991, 44 6: 2664-2672.
- [94] Wen X G. Topological orders in rigid states[J]. *International Journal of Modern Physics B*, 1990, 4: 239-271.
- [95] Landau L D. On the theory of phase transitions. ii.[C]//1937.
- [96] Pollmann F, Berg E, Turner A M, et al. Symmetry protection of topological phases in one-dimensional quantum spin systems[J]. *Physical Review B*, 2012, 85: 075125.
- [97] Fu L, Kane C L. Topological insulators with inversion symmetry[J]. *Physical Review B*, 2007, 76: 045302.

## 参考文献

- [98] Hsieh D, Qian D, Wray L A, et al. A topological dirac insulator in a quantum spin hall phase [J]. *Nature*, 2008, 452: 970-974.
- [99] Hasan M Z, Moore J E. Three-dimensional topological insulators[J]. *Annual Review of Condensed Matter Physics*, 2010, 2: 55-78.
- [100] Haldane F D M. Nonlinear field theory of large-spin heisenberg antiferromagnets: Semiclassically quantized solitons of the one-dimensional easy-axis néel state[J]. *Physical Review Letters*, 1983, 50: 1153-1156.
- [101] Haldane F D M. Continuum dynamics of the 1-d heisenberg antiferromagnet: Identification with the o(3) nonlinear sigma model[J]. *Physics Letters A*, 1983, 93: 464-468.
- [102] Affleck, Haldane. Critical theory of quantum spin chains.[J]. *Physical review. B, Condensed matter*, 1987, 36 10: 5291-5300.
- [103] Affleck I. Quantum spin chains and the haldane gap[J]. *Journal of Physics: Condensed Matter*, 1988, 1: 3047-3072.
- [104] Mishra S, Catarina G, Wu F, et al. Observation of fractional edge excitations in nanographene spin chains.[J]. *Nature*, 2021, 598 7880: 287-292.
- [105] Gu Z C, Wen X G. Tensor-entanglement-filtering renormalization approach and symmetry protected topological order[J]. *Physical Review B*, 2009, 80: 155131.
- [106] Chen X, Gu Z C, Liu Z, et al. Symmetry protected topological orders and the group cohomology of their symmetry group[J]. *Physical Review B*, 2013, 87: 155114.
- [107] Kalmeyer, Laughlin. Equivalence of the resonating-valence-bond and fractional quantum hall states.[J]. *Physical review letters*, 1987, 59 18: 2095-2098.
- [108] Wen, Wilczek, Zee. Chiral spin states and superconductivity.[J]. *Physical review. B, Condensed matter*, 1989, 39 16: 11413-11423.
- [109] Tsui D C, Stormer H L, Gossard A C. Two-dimensional magnetotransport in the extreme quantum limit[J]. *Physical Review Letters*, 1982, 48: 1559-1562.
- [110] Laughlin R B. Anomalous quantum hall effect: An incompressible quantum fluid with fractionally charged excitations[J]. *Physical Review Letters*, 1983, 50: 1395-1398.
- [111] Atiyah M F. Topological quantum field theory[J]. *Publications Mathématiques de l'IHÉS*, 1988, 68: 175-186.
- [112] Witten E. Topological quantum field theory[J]. *Communications in Mathematical Physics*, 1988, 117(3): 353-386.
- [113] Yetter D N. Tqft's from homotopy 2-types[J]. *Journal of Knot Theory and Its Ramifications*, 1993, 02: 113-123.
- [114] Chen X, Gu Z C, Wen X G. Local unitary transformation, long-range quantum entanglement, wave function renormalization, and topological order[J]. *Physical Review B*, 2010, 82: 155138.
- [115] Lan T. A classification of (2+1)d topological phases with symmetries[D]. University of Waterloo, 2017.
- [116] Kuppe M. Map of the mathematical landscape[EB/OL]. 2018[March 16, 2022]. <https://chalkdustmagazine.com/features/an-invitation-to-category-theory/>.

## 参考文献

- [117] Coppersmith D. An approximate fourier transform useful in quantum factoring[C]//volume 119. 2002: 331-352.
- [118] Kitaev A Y. Quantum measurements and the abelian stabilizer problem[J]. Electron. Colloquium Comput. Complex., 1996, 3.
- [119] Michael A. Nielsen I L C. Cambridge series on information and the natural sciences: Quantum computation and quantum information[M]. 1st ed. Cambridge University Press, 2004.
- [120] H. W. Lenstra Jr. (auth.) H W L J e, Arjen K. Lenstra. The development of the number field sieve[M]. Springer-Verlag Berlin Heidelberg, 1993.
- [121] Pomerance C, Erdös P. A tale of two sieves[C]//1998.
- [122] Lloyd S, Mohseni M, Rebentrost P. Quantum principal component analysis[J]. Nature Physics, 2014, 10: 631-633.
- [123] Wiebe N, Braun D, Lloyd S. Quantum algorithm for data fitting.[J]. Physical review letters, 2012, 109 5: 050505.
- [124] Rebentrost P, Mohseni M, Lloyd S. Quantum support vector machine for big feature and big data classification[J]. Physical review letters, 2014, 113 13: 130503.
- [125] Long G L. Grover algorithm with zero theoretical failure rate[J]. Physical Review A, 2001, 64 (2): 022307.
- [126] Guilu L, Weilin Z, Yansong L, et al. Arbitrary phase rotation of the marked state cannot be used for grover's quantum search algorithm[J]. Communications in Theoretical Physics, 1999, 32 (3): 335.
- [127] Long G L, Li Y S, Zhang W L, et al. Phase matching in quantum searching[J]. Physics Letters A, 1999, 262(1): 27-34.
- [128] Grover L K. Fixed-point quantum search[J]. Physical Review Letters, 2005, 95(15): 150501.
- [129] Yoder T J, Low G H, Chuang I L. Fixed-point quantum search with an optimal number of queries[J]. Physical review letters, 2014, 113(21): 210501.
- [130] Bennett C H, Bernstein E, Brassard G, et al. Strengths and weaknesses of quantum computing [J]. SIAM J. Comput., 1997, 26: 1510-1523.
- [131] Cerf N J, Grover L K, Williams C P. Nested quantum search and structured problems[J]. Phys. Rev. A, 2000, 61: 032303.
- [132] Daemen J, Rijmen V. The design of rijndael: Aes - the advanced encryption standard[C]//2002.
- [133] Halevi S, Krawczyk H. Strengthening digital signatures via randomized hashing[C]//CRYPTO. 2006.
- [134] Aharonov D. Quantum computation[C]//Annual Reviews of Computational Physics VI. World Scientific, 1998: 259-346.
- [135] Zalka C. Grover's quantum searching algorithm is optimal[J]. Phys. Rev. A, 1999, 60: 2746-2751.
- [136] Deutsch D, Jozsa R. Rapid solution of problems by quantum computation[J]. Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences, 1992, 439(1907): 553-558.

## 参考文献

- [137] Brassard G. Searching a quantum phone book[J]. *Science*, 1997, 275(5300): 627-628.
- [138] Michele M. Quantum searching, counting and amplitude amplification by eigenvector analysis[C]//Proceedings of Randomized Algorithms, Workshop of Mathematical Foundations of Computer Science. 1998: 90-100.
- [139] Brassard G, Høyer P, Michele M, et al. Quantum amplitude amplification and estimation: volume 305[M]. *Contemporary Mathematics*, 2002: 53-84.
- [140] Liu Y. An exact quantum search algorithm with arbitrary database[J]. *International Journal of Theoretical Physics*, 2014, 53: 2571-2578.
- [141] Toyama F, Van Dijk W, Nogami Y. Quantum search with certainty based on modified grover algorithms: optimum choice of parameters[J]. *Quantum information processing*, 2013, 12(5): 1897-1914.
- [142] Wei S, Li H, Long G. A full quantum eigensolver for quantum chemistry simulations[J]. *Research*, 2020, 2020: 1486935.
- [143] Hunziker M, Meyer D A. Quantum algorithms for highly structured search problems[J]. *Quantum Information Processing*, 2002, 1(3): 145-15.
- [144] Castagnoli G. Highlighting the mechanism of the quantum speedup by time-symmetric and relational quantum mechanics[J]. *Foundations of Physics*, 2016, 46(3): 360-381.
- [145] Boyer M, Brassard G, Høyer P, et al. Tight bounds on quantum searching[J]. *Fortsch. Phys.*, 1998, 46: 493-506.
- [146] Brassard G, Høyer P, Tapp A. Quantum counting[C]//International Colloquium on Automata, Languages, and Programming. Springer, 1998: 820-831.
- [147] Zhao L J, Li Y S, Hao L, et al. Geometric pictures for quantum search algorithms[J]. *Quantum Information Processing*, 2012, 11: 325-340.
- [148] Ambainis A. A new protocol and lower bounds for quantum coin flipping[J]. *Journal of Computer and System Sciences*, 2004, 68(2): 398-416.
- [149] Ozols M, Roetteler M, Roland J. Quantum rejection sampling[A]. 2011. arXiv: 1103.2774.
- [150] Zhang Y, Ni Q. Recent advances in quantum machine learning[J]. *Quantum Engineering*, 2020, 2(1): e34.
- [151] Brassard G, Høyer P, Tapp A. Quantum algorithm for the collision problem[M]. Boston, MA,USA: Springer, 2008: 682-683.
- [152] Mahmud N, El-Araby E, Caliga D. Scaling reconfigurable emulation of quantum algorithms at high precision and high throughput[J]. *Quantum Engineering*, 2019, 1(2): e19.
- [153] Wen J, Lv D, Yung M H, et al. Variational quantum packaged deflation for arbitrary excited states[J]. *Quantum Engineering*, 2021: e80.
- [154] Jin S, Wu S, Zhou G, et al. A query-based quantum eigensolver[J]. *Quantum Engineering*, 2020, 2(3): e49.
- [155] Gao H, Wang J, Han Y, et al. Enhancing crystal structure prediction by decomposition and evolution schemes based on graph theory[J]. *Fundamental Research*, 2021, 1(4): 466-471.

## 参考文献

- [156] CHANG C R, LIN Y C, CHIU K L, et al. The second quantum revolution with quantum computers[J]. AAPPS Bulletin, 2020, 30(1): 9-22.
- [157] Feynman R P. Simulating physics with computers[J]. International Journal of Theoretical Physics, 1982, 21: 467-488.
- [158] Kroese D P, Brereton T J, Taimre T, et al. Why the monte carlo method is so important today [J]. Wiley Interdisciplinary Reviews: Computational Statistics, 2014, 6: 386-392.
- [159] Metropolis N, Ulam S M. The monte carlo method.[J]. Journal of the American Statistical Association, 1949, 44: 335-341.
- [160] Rubinstein R Y. Simulation and the monte carlo method[C]//Wiley series in probability and mathematical statistics. 1981.
- [161] Abrams D S, of Physics S L D, of Technology Department of Mechanical Engineering M I, et al. Simulation of many-body fermi systems on a universal quantum computer[J]. Physical Review Letters, 1997, 79: 2586-2589.
- [162] Lidar D A, Biham O. Simulating ising spin glasses on a quantum computer[J]. Physical Review E, 1997, 56: 3661-3681.
- [163] Lloyd S. Universal quantum simulators[J]. Science, 1996, 273: 1073 - 1078.
- [164] Marzuoli A, Rasetti M. Spin network quantum simulator[J]. Physics Letters A, 2002, 306: 79-87.
- [165] Ortiz G G, Gubernatis J E, Knill E, et al. Quantum algorithms for fermionic simulations[J]. Physical Review A, 2001, 64: 022319.
- [166] Raeisi S, Wiebe N, Sanders B C. Quantum-circuit design for efficient simulations of many-body quantum dynamics[J]. New Journal of Physics, 2012, 14: 103017.
- [167] Terhal B M, DiVincenzo D P. Problem of equilibration and the computation of correlation functions on a quantum computer[J]. Physical Review A, 2000, 61: 022301.
- [168] Verstraete F, Cirac J I, Latorre J I. Quantum circuits for strongly correlated quantum systems: abs/0804.1888[A]. 2008.
- [169] Wiesner S. Simulations of many-body quantum systems by a quantum computer[A]. 1996.
- [170] Zalka C. Efficient simulation of quantum systems by quantum computers[A]. 1996.
- [171] Zalka C. Simulating quantum systems on a quantum computer[J]. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 1998, 454: 313 - 322.
- [172] Georgescu I M, Ashhab S, Nori F. Quantum simulation[J]. Rev. Mod. Phys., 2014, 86: 153-185.
- [173] Bergholm V, Biamonte J D. Categorical quantum circuits[J]. Journal of Physics A, 2011, 44: 245304.
- [174] Kaiser D. Drawing theories apart: The dispersion of feynman diagrams in postwar physics[C]// 2005.
- [175] Nicholson G E. Combinatorial mathematics and its applications year.[C]//1971.
- [176] Abramsky S, Coecke B. A categorical semantics of quantum protocols[J]. Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, 2004., 2004: 415-425.

## 参考文献

- [177] Baez J C, Stay M. Physics, topology, logic and computation: A rosetta stone[J]. Lecture Notes in Physics, 2009, 813: 95-172.
- [178] L' I.H.É.S D, Atiyah M F, Atiyah M F. Topological quantum field theory[C]/2003.
- [179] Segal G B. The definition of conformal field theory[C]/1988.
- [180] Dijkgraaf R H. A geometrical approach to two-dimensional conformal field theory[C]/1989.
- [181] Voronov A A. Topological field theories, string backgrounds and homotopy algebras[A]. 1994.
- [182] StreetBaltimore C. Two-dimensional topological quantum field theories and frobenius algebras [C]/1996.
- [183] Sawin S F. Direct sum decompositions and indecomposable tqfts[J]. Journal of Mathematical Physics, 1995, 36: 6673-6680.
- [184] Quinn F. Lectures on axiomatic topological quantum field theory[C]/1991.
- [185] Dubrovin B. Geometry of 2d topological field theories[J]. Lecture Notes in Mathematics, 1994, 1620: 120-348.
- [186] Kock J. Frobenius algebras and 2-d topological quantum field theories[C]/2004.
- [187] Donnelly W, Wong G. Entanglement branes, modular flow, and extended topological quantum field theory[J]. Journal of High Energy Physics, 2019.
- [188] Aharonov D, Ta-Shma A. Adiabatic quantum state generation and statistical zero knowledge [C]/STOC '03. 2003.
- [189] Berry D W, Childs A M, Cleve R, et al. Simulating hamiltonian dynamics with a truncated taylor series.[J]. Physical review letters, 2015, 114 9: 090502.
- [190] Low G H, Chuang I L. Hamiltonian simulation by qubitization[J]. Quantum, 2019, 3: 163.
- [191] Pesah A. Quantum algorithms for solving partial differential equations[EB/OL]. 2020[July 19, 2022]. <https://arthurpesah.me/assets/pdf/case-study-quantum-algorithms-pde.pdf>.
- [192] Leyton S K, Osborne T J. A quantum algorithm to solve nonlinear differential equations[A]. 2008.
- [193] Berry D W. High-order quantum algorithm for solving linear differential equations[J]. Journal of Physics A: Mathematical and Theoretical, 2014, 47(10): 105301.
- [194] Costa P C S, Jordan S P, Ostrander A. Quantum algorithm for simulating the wave equation[J]. Physical Review A, 2019.
- [195] Gonzalez-Conde J, Rodríguez-Rozas Á, Solano E, et al. Pricing financial derivatives with exponential quantum speedup[C]/2021.
- [196] Berry D W, Childs A M, Ostrander A, et al. Quantum algorithm for linear differential equations with exponentially improved dependence on precision[J]. Communications in Mathematical Physics, 2017, 356: 1057-1081.
- [197] Childs A M, Liu J P. Quantum spectral methods for differential equations[J]. Communications in Mathematical Physics, 2020, 375: 1427-1457.
- [198] Cao Y, Papageorgiou A, Petras I, et al. Quantum algorithm and circuit design solving the poisson equation[J]. New Journal of Physics, 2013, 15: 013021.
- [199] Montanaro A, Pallister S. Quantum algorithms and the finite element method[J]. Physical Review A, 2016, 93: 032324.
- [200] Devoret M H, Schoelkopf R J. Superconducting circuits for quantum information: An outlook [J]. Science, 2013, 339: 1169 - 1174.

## 附录 A 张量范畴基础知识简要

### A.1 兮半范畴

一个兮半范畴（或称为张量范畴） $\mathcal{C} = (\mathcal{C}, \otimes, \mathbb{1}, \alpha, l, r)$  是一个范畴带有如下的结构：

- 一个函子  $\otimes : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$
- 一个单位对象  $\mathbb{1} \in \text{Ob}(\mathcal{C})$ , 匹配两个自然变换

$$l = \{l_X : \mathbb{1} \otimes X \rightarrow X\}_{X \in \text{Ob}(\mathcal{C})} \quad (\text{A.1})$$

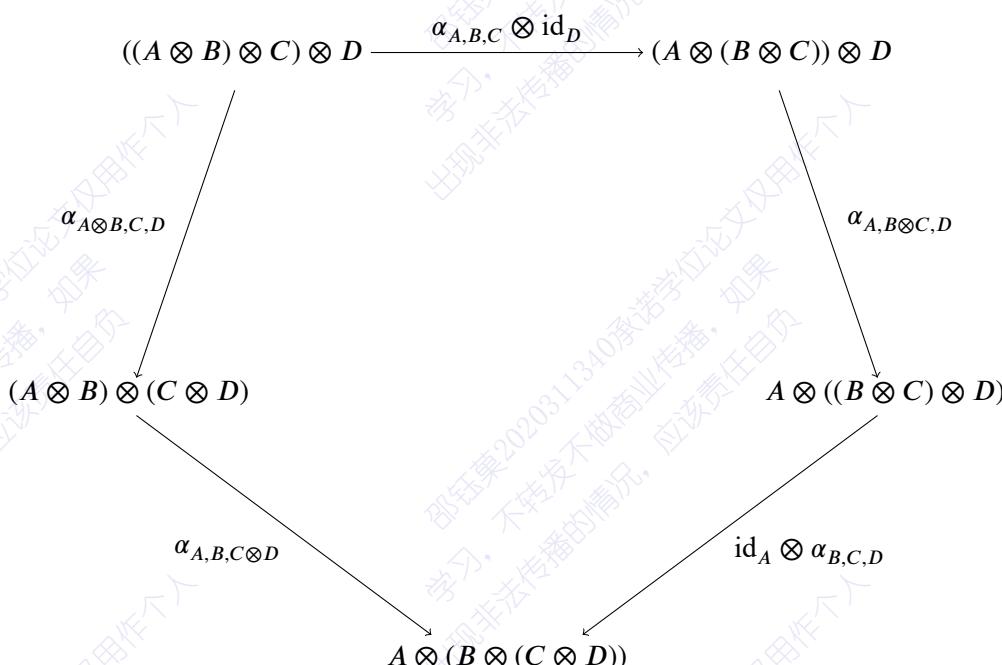
$$r = \{r_X : X \otimes \mathbb{1} \rightarrow X\}_{X \in \text{Ob}(\mathcal{C})} \quad (\text{A.2})$$

- $\otimes(\otimes \times \text{id}_{\mathcal{C}}) : \mathcal{C} \times \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$  和  $\otimes(\text{id}_{\mathcal{C}} \times \otimes) : \mathcal{C} \times \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$  两个函子之间满足结合律的自然自同构

$$\alpha : \otimes(\otimes \times \text{id}_{\mathcal{C}}) \rightarrow \otimes(\text{id}_{\mathcal{C}} \times \otimes) \quad (\text{A.3})$$

$$\alpha = \{\alpha_{X,Y,Z} : (X \otimes Y) \otimes Z \rightarrow X \otimes (Y \otimes Z)\}_{X,Y,Z \in \text{Ob}(\mathcal{C})} \quad (\text{A.4})$$

- 对所有对象  $A, B, C, D \in \text{Ob}(\mathcal{C})$  满足五边形交换图：



- 对于对象  $A, B \in \mathcal{C}$  满足三角恒等式交换图：

## 附录 A 张量范畴基础知识简要

$$\begin{array}{ccc}
 (A \otimes \mathbb{1}) \otimes B & \xrightarrow{\alpha_{A, \mathbb{1}, B}} & A \otimes (\mathbb{1} \otimes B) \\
 r_A \otimes \text{id}_B \searrow & & \swarrow \text{id}_A \otimes l_B \\
 & A \otimes B &
 \end{array}$$

- 对任意  $f \in \text{Hom}_{\mathcal{C}}(A, A')$ ,  $g \in \text{Hom}_{\mathcal{C}}(B, B')$ ,  $h \in \text{Hom}_{\mathcal{C}}(C, C')$  满足交换图:

$$\begin{array}{ccc}
 (A \otimes B) \otimes C & \xrightarrow{\alpha_{A, B, C}} & A \otimes (B \otimes C) \\
 (f \otimes g) \otimes h \downarrow & & \downarrow f \otimes (g \otimes h) \\
 (A' \otimes B') \otimes C' & \xrightarrow{\alpha_{A', B', C'}} & A' \otimes (B' \otimes C')
 \end{array}$$

- 对任意  $f \in \text{Hom}_{\mathcal{C}}(X, X')$  满足交换图:

$$\begin{array}{ccc}
 \mathbb{1} \otimes X & \xrightarrow{\text{id}_{\mathbb{1}} \otimes f} & \mathbb{1} \otimes X' \\
 l_X \downarrow & & \downarrow l_{X'} \\
 X & \xrightarrow{f} & X'
 \end{array}$$
  

$$\begin{array}{ccc}
 X \otimes \mathbb{1} & \xrightarrow{f \otimes \text{id}_{\mathbb{1}}} & X' \otimes \mathbb{1} \\
 r_X \downarrow & & \downarrow r_{X'} \\
 X & \xrightarrow{f} & X'
 \end{array}$$

## A.2 兮半函子

令  $\mathcal{C} = (\mathcal{C}, \otimes, \mathbb{1}, \alpha, l, r)$  与  $\mathcal{D} = (\mathcal{D}, \otimes', \mathbb{1}', \alpha', l', r')$  为两个兮半范畴。兮半函子  $(F, \xi, f_0)$  将一个范畴  $\mathcal{C}$  映射到范畴  $\mathcal{D}$ 。其中  $F : \mathcal{C} \rightarrow \mathcal{D}$  是一个函子。 $f_0 : \mathbb{1}' \rightarrow F(\mathbb{1})$  是正则自同态。

$$\xi = \{\xi_{X,Y} : F(X) \otimes' F(Y) \rightarrow F(X \otimes Y)\}_{X,Y \in \text{Ob}(\mathcal{C})} \quad (\text{A.5})$$

是函子  $\otimes'(F \times F) : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{D}$  与函子  $F \otimes : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{D}$  之间的自然变换, 使得对所有对象  $X, Y, Z \in \text{Ob}(\mathcal{C})$ , 以下交换图成立:

$$\begin{array}{ccc}
 (F(X) \otimes' F(Y)) \otimes' F(Z) & \xrightarrow{\alpha'_{F(X), F(Y), F(Z)}} & F(X) \otimes' (F(Y) \otimes' F(Z)) \\
 \xi_{X,Y} \otimes' \text{id}_{F(Z)} \downarrow & & \downarrow \text{id}_{F(X)} \otimes' \xi_{Y,Z} \\
 F(X \otimes Y) \otimes' F(Z) & & F(X) \otimes' F(Y \otimes Z) \\
 \xi_{X \otimes Y, Z} \downarrow & & \downarrow \xi_{X, Y \otimes Z} \\
 F((X \otimes Y) \otimes Z) & \xrightarrow{F(\alpha_{X,Y,Z})} & F(X \otimes (Y \otimes Z))
 \end{array}$$
  

$$\begin{array}{ccc}
 \mathbb{1}' \otimes' F(X) & \xrightarrow{l'_{F(X)}} & F(X) \\
 f_0 \otimes' \text{id}_{F(X)} \downarrow & & \uparrow F(l_X) \\
 F(\mathbb{1}) \otimes' F(X) & \xrightarrow{\xi_{\mathbb{1}, X}} & F(\mathbb{1} \otimes X)
 \end{array}$$
  

$$\begin{array}{ccc}
 F(X) \otimes' \mathbb{1}' & \xrightarrow{r'_{F(X)}} & F(X) \\
 \text{id}_{F(X)} \otimes' f_0 \downarrow & & \uparrow F(r_X) \\
 F(X) \otimes' F(\mathbb{1}) & \xrightarrow{\xi_{X, \mathbb{1}}} & F(X \otimes \mathbb{1})
 \end{array}$$

### A.3 幺半自然变换

一个幺半自然变换  $\varphi$  将一个幺半函子  $F : \mathcal{C} \rightarrow \mathcal{D}$  映射到另一个幺半函子  $G : \mathcal{C} \rightarrow \mathcal{D}$  满足以下交换图：

$$\begin{array}{ccc}
 F(X) \otimes F(Y) & \xrightarrow{\varphi_X \otimes \varphi_Y} & G(X) \otimes G(Y) \\
 \xi_{X,Y}^F \downarrow & & \downarrow \xi_{X,Y}^G \\
 F(X \otimes Y) & \xrightarrow{\varphi_{X \otimes Y}} & G(X \otimes Y)
 \end{array}$$

以及自然的关系：

$$\varphi_{\mathbb{1}} f_0 = g_0 \quad \varphi_{X \otimes Y} \xi_{X,Y}^F = \xi_{X,Y}^G \varphi_X \otimes \varphi_Y \quad (\text{A.6})$$

#### A.4 Rigid 范畴

对象  $X \in \text{Ob}(\mathcal{C}, \otimes, \mathbb{1}, \alpha, l, r)$  的左对偶是一个对  $({}^\vee X, \text{ev}_X)$ , 其中  ${}^\vee X$  是  $\mathcal{C}$  的对象,  $\text{ev}_X : {}^\vee X \otimes X \rightarrow \mathbb{1}$  是一个非退化的配对。左对偶  $\text{ev}_X$  的逆为  $\text{coev}_X : \mathbb{1} \rightarrow X \otimes {}^\vee X$ 。 $(\mathcal{C}, \otimes, \mathbb{1}, \alpha, l, r)$  的左对偶是  $({}^\vee X, \text{ev}_X)_{X \in \text{Ob}(\mathcal{C})}$ 。一个幺半范畴如果存在左对偶则称其为左 Rigid 范畴。

对象  $X \in \text{Ob}(\mathcal{C}, \otimes, \mathbb{1}, \alpha, l, r)$  的右对偶是一个配对  $(X^\vee, \tilde{\text{ev}}_X)$ , 其中  $X^\vee$  是  $\mathcal{C}$  的对象,  $\tilde{\text{ev}}_X : X \otimes X^\vee \rightarrow \mathbb{1}$  是一个非退化的配对。右对偶  $\tilde{\text{ev}}_X$  的逆为  $\widetilde{\text{coev}}_X : \mathbb{1} \rightarrow X^\vee \otimes X$ 。 $(\mathcal{C}, \otimes, \mathbb{1}, \alpha, l, r)$  的右对偶是  $(X^\vee, \tilde{\text{ev}}_X)_{X \in \text{Ob}(\mathcal{C})}$ 。一个幺半范畴如果存在左对偶则称其为右 Rigid 范畴。

如果一个幺半范畴同时存在左对偶与右对偶则称其为 Rigid 范畴。

#### A.5 融合范畴

一个多融合范畴是一个  $\mathbb{C}$ -线性有限半单 Rigid 张量范畴  $\mathcal{C}$  带有有限维 Hom 集合。如果  $\mathcal{C}$  中张量的单位元是单的, 则  $\mathcal{C}$  叫做融合范畴。

#### A.6 球状融合范畴

对于融合范畴  $\mathcal{C}$  中的对象  $U$ , 自然的有  $({}^\vee U)^\vee = U$ ,  ${}^\vee(U^\vee) = U$ , 如果  $a \in \text{hom}_{\mathcal{C}}(U, U^{\vee\vee})$ , 那么可以定义左迹:

$$\text{Tr}^L(a) : \mathbf{1} \xrightarrow{b_U} U \otimes U^\vee \xrightarrow{a^1} U^{\vee\vee} \otimes U^\vee \xrightarrow{d_{U^\vee}} \mathbf{1} \quad (\text{A.7})$$

如果  $a \in \text{hom}_{\mathcal{C}}(U^{\vee\vee}, U)$ , 那么可以定义右迹:

$$\text{Tr}^R(a) : \mathbf{1} \xrightarrow{b_{U^\vee}} {}^\vee U \otimes U \xrightarrow{a^1} {}^\vee U \otimes {}^{\vee\vee} U \xrightarrow{d_{{}^{\vee\vee} U}} \mathbf{1}. \quad (\text{A.8})$$

Rigid 张量范畴  $\mathcal{C}$  上的一个 pivotal 结构是一个同构  $a : \text{id}_c \rightarrow \vee\vee$ , 例如  $U$  自然的同构  $a_U : U \xrightarrow{\cong} U^{\vee\vee}$  满足  $a_{U \otimes V} = a_U \otimes a_V$ 。如果对于所有的  $U \in \mathcal{C}$ , 均满足  $\text{Tr}^L(a_U) = \text{Tr}^R(a_U)$ , 则称  $\mathcal{C}$  为球状融合范畴。

#### A.7 Ribbon 范畴

Ribbon 范畴是一个 Rigid 张量范畴  $\mathcal{C}$ , 带有映射  $\theta_U : U \rightarrow U$ , 并满足如下条件:

$$\theta_1 = \text{id}_1, \quad \theta_{U^\vee} = (\theta_U)^\vee, \quad \theta_{U \otimes V} = c_{V,U} \circ c_{U,V} \circ (\theta_U \otimes \theta_V) \quad (\text{A.9})$$

其中

$$(\theta_U)^\vee := (d_U \otimes \text{id}_{U^\vee}) \circ (\text{id}_{U^\vee} \otimes \theta_U \otimes \text{id}_{U^\vee}) \circ (\text{id}_{U^\vee} \otimes b_U) \quad (\text{A.10})$$

## A.8 酉模张量范畴

酉模张量范畴是一个  $\mathbb{C}$ -线性有限半单酉 Ribbon 范畴，使得  $S$  矩阵（其矩阵元为  $S_{ij} = \text{Tr } c_{j^*,i} c_{i,j^*} / D$ ）非退化。

## A.9 范畴中的代数

$\mathcal{C}$  为缠绕张量范畴。 $\mathcal{C}$  中的代数为  $(A, \mu, \iota)$ , 其中  $A$  是  $\mathcal{C}$  中的对象。 $\mu$  为映射： $A \otimes A \rightarrow A$ ,  $\iota$  为映射： $\mathbf{1} \rightarrow A$ , 满足如下条件：

$$\begin{aligned} \mu \circ (\mu \otimes \text{id}_A) \circ \alpha_{A,A,A} &= \mu \circ (\text{id}_A \otimes \mu) \\ \mu \circ (\iota \otimes \text{id}_A) &= \text{id}_A = \mu \circ (\text{id}_A \otimes \iota) \end{aligned} \quad (\text{A.11})$$

代数  $A$  叫做可交换代数如果满足： $\mu = \mu \circ c_{A,A}$ 。

$\mathcal{C}$  中的余代数为  $(A, \Delta, \epsilon)$ , 其中  $A$  是  $\mathcal{C}$  中的对象。 $\Delta$  为映射： $A \otimes A \rightarrow A$ ,  $\epsilon$  为映射： $A \rightarrow \mathbf{1}$ , 满足如下条件：

$$\Delta \circ (\Delta \otimes \text{id}_A) = \alpha_{A,A,A} \circ \Delta \circ (\text{id}_A \otimes \Delta) \quad (\text{A.12})$$

$$(\epsilon \otimes \text{id}_A) \circ \Delta = \text{id}_A = (\text{id}_A \otimes \epsilon) \circ \Delta \quad (\text{A.13})$$

一个 Frobenius 代数  $A = (A, \mu, \iota, \Delta, \epsilon)$  包含代数与余代数，并满足

$$(\text{id}_A \otimes \mu) \circ (\Delta \otimes \text{id}_A) = \Delta \circ \mu = (\mu \otimes \text{id}_A) \circ (\text{id}_A \otimes \Delta) \quad (\text{A.14})$$

## A.10 范畴中代数的模

一个代数  $(A, \mu, \iota)$  上的左模为  $(M, \mu_M)$ , 其中  $M$  为范畴  $\mathcal{C}$  中的对象，映射  $\mu_M : A \otimes M \rightarrow M$  使得  $\mu_M \circ (\mu \otimes \text{id}_M) \circ \alpha_{A,A,M} = \mu_M \circ (\text{id}_A \otimes \mu_M)$ ,  $\mu_M \circ (\iota_A \otimes \text{id}_M) = \text{id}_M$ ，用同样的方式也可以定义右模。

对于一个可交换代数  $A$ , 如果一个模  $(M, \mu_M)$  满足： $\mu_M = \mu_M \circ c_{M,A} \circ c_{A,M}$ 。则称之为局域的。

一个  $\mathcal{C}$  代数  $(A, \mu, \iota)$  称作可分离的，如果映射  $\mu$  为  $A$  双模的映射。一个可分离代数称之为连带如果满足  $\dim \text{Hom}_{\mathcal{C}}(\mathbf{1}, A) = 1$ 。

## 致 谢

回想起当年刚刚入学一切都还历历在目，转眼间博士期间的生活将接近尾声。在清华大学读博阶段是我重要的人生经历。在这里我收获了很多。清华大学的校训“自强不息，厚德载物”深深影响了我。衷心感谢导师龙桂鲁教授对本人的精心指导。导师言传身教将使我终生受益。导师为我指明科研方向，在面对困难时会对我鼓励，在生活中对我无微不至地关怀。

在加拿大滑铁卢大学量子计算研究中心进行十六个月的合作研究期间，承蒙 David Cory 教授热心指导与帮助，不胜感激。感谢香港中文大学兰天助理教授，南方科技大学孔良研究员，清华大学丘成桐数学中心郑浩教授，犹他大学吴咏时教授带我进入数学物理——张量范畴这一方向。感谢周增荣，魏世杰，王泽国，王碧雪，张飞昊，李可仁，孔祥宇，闫宝对我在学习和科研上的帮助。感谢樊政，王明宇，雷雨霆，吴家为，王博梽，李小刚帮我校对论文。最后，感谢父母含辛茹苦的培养和默默付出。

声 明

声 明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签 名：朱垣华 日 期：2022.09.14

## 个人简历、在学期间完成的相关学术成果

### 个人简历

1993年9月12日出生于辽宁省大连市。

2012年9月考入吉林大学物理学院物理学（国家基础学科拔尖人才培养试验计划）专业，2016年7月本科毕业并获得理学学士学位。

2016年9月免试进入清华大学物理系攻读理学博士学位至今。

### 在学期间完成的相关学术成果

#### 学术论文：

- [1] **Yuanye Zhu**, Zeguo Wang, Bao Yan and Shijie Wei. Robust Quantum Search with Uncertain Number of Target States. *Entropy*, 2021, 23(12):1649 (SCI 收录, 检索号:000738901900001)
- [2] Kong Xiangyu, **Yuanye Zhu**, Jingwei Wen, Tao Xin, Keren Li, Guilu Long. New research progress of nuclear magnetic resonance quantum information processing. *Acta Phys. Sin.*, 2018, 67(22): 220301(SCI 收录, 检索号:000455402400001.)
- [3] Keren Li, Tao Xin, **Yuanye Zhu**, Xiangyu Kong and Guilu Long, The Research Status of Nuclear Magnetic Resonance for Quantum Computing, *AAPPS Bulletin*, 2018, 28(1):p3-11 (DOI: 10.22661/AAPPSBL.2018.28.1.03)

## 指导教师学术评语

朱垣晔同学的博士论文是独立完成，论文围绕带振幅放大的对偶量子算法及其应用展开，选题在理论和应用上具有重要价值。

该论文的主要成果如下：

1. 提出了对于数据库占比不确定的高鲁棒性量子搜索算法，这个改进算法减少了 Grover-Long 算法中对于确切占比的要求，提升了算法成功率。
2. 利用带振幅放大的对偶量子算法，设计并提出了范畴化量子模拟算法，运用演生论的编码方式节约量子比特资源，并使得之前部分不能被有效量子模拟的系统变得可能。
3. 利用带振幅放大的对偶量子算法构造了求解波动方程的量子算法，演示并给出了求解线性偏微分方程的一种新量子算法。

该论文写作规范，逻辑严密，行文流畅，文献综述系统全面，创新性强，达到了博士学位水平。

## 答辩委员会决议书

本论文研究了带振幅放大的对偶量子算法及其应用，选题具有重要的科学意义和潜在的应用价值。

论文的主要创新性成果包括：

1. 提出了对于数据库占比不确定的鲁棒量子搜索算法，降低了 Grover-Long 算法中确切占比的要求，具有较高的搜索成功率；
2. 利用带振幅放大的对偶量子算法，设计了范畴化量子模拟算法，通过演生论编码，节约了量子比特资源；
3. 利用带有振幅放大的对偶量子算法，构造了求解波动方程的一种新的量子算法。

论文写作规范，逻辑严谨，计算准确，文献综述全面。论文工作表明作者具有扎实的理论基础，系统的专业知识，以及独立进行科学的研究能力。

答辩过程中表述清晰，回答问题正确。经答辩委员会无记名投票表决，一致同意通过（7票）论文答辩，并建议授予朱垣畔理学博士学位。