

Methods&Practices of
Quantum Reversible Circuit Synthesis

量子可逆电路综合的 方法与实践

陈汉武 李志强 · 著



东南大学出版社
SOUTHEAST UNIVERSITY PRESS

Methods & Practices of Quantum Reversible Circuit Synthesis

量子可逆电路综合的方法与实践

物理问题/数学建模/算法设计/程序实践

东南大学计算机科学与工程学院

量子计算与量子信息研究室

陈汉武 李志强 著



东南大学出版社
SOUTHEAST UNIVERSITY PRESS

· 南京 ·

内容简介

本书的主要思路源自作者近年来开设的关于量子计算科普性新生研讨课的教学实践,主要内容选自作者及其学生多年来在量子可逆逻辑电路综合设计理论与方法的科学研究实践中获得的部分成果。针对《量子可逆逻辑电路》计算机设计的唯一问题,借鉴成熟的、不同的数学理论,展现物理问题、数学建模、算法设计、程序实践的基于计算机的计算逻辑思维方法。全书共分六章,第一与第二章主要讲述量子可逆逻辑电路研究的意义及其在代数演算中的基本定义,第三至第五章,分别讲述了基于真值表、R-M 方法、置换群代数方法的设计方法,第六章通过实例重点讲述了 4 量子可逆逻辑电路综合程序设计的算法思想和程序实现。

本书问题唯一,方法多样,因举一反三可开阔思路,重点突出,思路新颖,因案例驱动可解说计算思维,问题明确,寥寥数字,因结果的可比性可作为程序设计大赛的竞赛命题,亦可作为量子计算兴趣者的自学用书。

图书在版编目(CIP)数据

量子可逆电路综合的方法与实践 / 陈汉武, 李志强著.

—南京: 东南大学出版社, 2017. 9

ISBN 978-7-5641-7241-1

I. ①量… II. ①陈…②李… III. ①量子电子学—研究

IV. ①TN201

中国版本图书馆 CIP 数据核字(2017)第 156539 号

量子可逆电路综合的方法与实践

出版发行 东南大学出版社

出 版 人 江建中

责任编辑 姜晓乐(joy_supe@126.com)

社 址 南京市四牌楼 2 号 邮编 210096

网 址 <http://www.seupress.com>

经 销 各地新华书店

印 刷 江苏凤凰数码印务有限公司

开 本 700 mm×1000 mm 1/16

印 张 10.5

字 数 206 千字

版 次 2017 年 9 月第 1 版

印 次 2017 年 9 月第 1 次印刷

书 号 ISBN 978-7-5641-7241-1

定 价 39.00 元

* 本社图书若有印装质量问题,请直接与营销部联系,电话:025-83791830。

写在全书之前想说的话

本书的写作纯属偶然。我从 2012 年开始面对本科生开设量子计算的新生研讨课,旨在科普量子计算与量子信息知识,传播、普及计算机科学发展新领域、新知识和新思维。课程安排了 4 个系列的科普讲座:量子计算机杂谈、量子安全通信杂谈、量子可逆逻辑电路设计杂谈、量子容错计算杂谈。除了量子计算机杂谈的内容以外,其余三个杂谈的内容都包含在我们研究室 2004 年以来主要的学习和研究内容之中。

开设这门新生研讨课的初衷,一是给新生科普计算机科学技术发展的前沿,通过介绍量子、量子比特、量子信息、量子计算、量子通信、量子计算机的入门常识,以此打开学生们关注量子科技、量子计算机发展的新视野,点燃他们对量子科技的兴趣,并使他们具备阅读量子科技相关科普文献的基本能力;二是那个年头“计算思维”的热潮似乎正裹挟着整个计算机学界,我无法脱俗,我潜意识地期待在教学过程中实践培养“计算思维”的一种教学模式。就是想把量子计算的思维、方法和相关理论的基本内容通过课程告诉学生,期待影响他们今后在软件设计或算法构建中的思维。教学实践后我亲身体会或了解到,第一个想法基本可以实现,因为从课堂的研讨和课后的作业中可以感觉到大多数选课的新生通过短短的 32 个学时的学习和讨论,对量子计算与量子信息会萌发出兴趣,至少他们在课程学习结束后会比一般的学生更加关注量子信息科技的新进展,从他们口中说出的关于某些科普新闻报道的评论更加科学或靠谱、用词也更加准确了。但第二个目标是我的心太大了,原因当然在于我。我是半路出家做了一点量子信息和量子计算相关的基础研究,实践阅历不足,没有功底和能力将量子信息与量子计算理论背后的、计算机专业需要的思维和方法很好地凝练出来,然后通过课程朴素地告诉学生。但我又想,我虽然笨拙,却已通过授课将这粒有益的种子播在了一些学生的思维里,我期待着这粒种子会在今后某一恰当的时候突然发芽、开花、结出可口的果子。

课程开设之初,因为课程内容是基于“量子”讨论信息和计算的内容,不在我们的宏观现实和宏观思维之中,现实中除去专业从事相关领域研究的人,我们从小到大几乎都未接受过相关教育,哪怕是科普教育,因此当课程挂上选课网,选课的学生因为课程名中出现“量子”会感到或陌生或畏惧而拒绝,也有少数学生会因为或陌生或好奇,想了解、想学习。其实学生们和我一样,我是半路出家,我能够理解。因此我会在每一轮、每一次的讲稿和 PPT 中更新内容,将相关的最新的国内外各种新闻媒体的文字、图片和视频报道融入到授课中去,想与时俱进地主动讲好这 4 个讲座中的每一个故事。

在量子可逆逻辑电路设计杂谈的讲座中,想通过量子可逆逻辑电路设计中一个非常简单的、但学生们却从未见过的物理问题(已知逻辑函数的值求解逻辑电路),启发学生运用一些简单数学方法解决问题,让学生亲身感受到什么是现实问题、什么是数学模型,亲身触摸到“物理模型—数学模型—解决方案”间的关系,在学生的思维里种下这粒种子,并让学生们意识到数学的普适性意义。在教学中,通过课堂互动和学生研讨的环节,我发现大多数同学可以较快地掌握一些基本概念并能够大致理解问题(已知逻辑函数的值求解逻辑电路),了解把问题的物理模型抽象成逻辑门输入/输出数值间的数字问题,通过选择恰当的数学工具(真值表、矩阵与代数演算、置换等)讲解,再把数字问题转换成数学问题,然后建立问题求解的数学模型,再基于数学工具的运算规则加工数字,最终达成问题的解决方案,最后将解决方案的文字与计算公式转换成算法。一般的学生此时能够完成问题求解的代数计算,条件好的学生能够进一步给出采用基本方法的程序设计结果。对于条件更好的学生进一步推荐“解决方案—算法设计—程序实现”的实践环节,活用数据结构与程序设计中的技巧,真正体会科学计算程序设计的乐趣。因为有这样的教学活动体会,我确实曾经想过把相关内容以数学建模为主线归纳小结成讲义。

说到本书的写作纯属偶然,其实还受到一件事的触发。某一日同学聚会,有同学问我有没有适合数学建模程序竞赛题目的建议,此时我的头脑中真的突然闪现这个想法:量子可逆逻辑电路综合可以成为一个好的命题内容,还可以作为程序设计语言课程设计的选题之一。首先命题者如若善于表达,量子可逆逻辑电路综合的问题是易于表述且目标明确的,问题本身有助于数学建模与代数优化,程序实现时能够采用多种程序设计和数据结构的技巧达到提高自动生成逻辑电路的效率。再者就是3量子可逆逻辑电路有开放的标准数据,4量子可逆逻辑电路全体的综合依然是一个技术上的开放问题,因此无论是竞赛还是课程设计的结果都可以得到公平、公正和是否创新的评判。原本想写,有一些积累,遇上这一件事触发,于是就写出了这本书。

新兴学科量子信息论与量子计算理论的基础是量子力学原理,本书的撰写过程中涉及一些量子信息和量子计算的概念及其表达方法,又因我们的教育和研究背景是计算机科学与应用,加之编写的动因突发,且希望一气呵成,时间仓促、修养不足,因此本书难免有疏漏和不当之处,敬请读者批评指正。

回头看,成就本书的编撰,要感谢我的多位博士研究生:李志强、肖芳英、李文骞、王冬,以及万四爽、安博、杨忠明等硕士,感谢他(她)们早期的多年努力的结果,特别是李志强为本书编撰提供了大量翔实材料,以及基于Hash函数的3量子全部40320个可逆逻辑电路的计算结果。同时感谢谈佳宁博士为全书提供规范的全部可逆逻辑电路图。

陈汉武

2017年3月31日

序

量子可逆逻辑的研究源于可逆计算机的研究。20 世纪中叶,人们发现集成电路芯片的能耗导致计算机系统发热,既限制了芯片集成度,又影响到计算机的运行速度。IBM 的科学家 R. Landauer 指出,集成电路芯片的能耗主要源于芯片中门电路的信号演算不可逆操作。因此,降低芯片能耗、抑制发热的关键是将不可逆操作变为可逆操作。在信息领域,众所周知:经典计算机的本质是一个通用图灵机,是不可逆的,但所有不可逆通用图灵机都对应一个可逆图灵机,且两者的计算能力和计算效率完全相同,C. Bennett 对此有严格证明。由于量子门与酉算子对应,量子逻辑门是可逆的,因此可以用可逆逻辑的设计方法综合量子逻辑电路。由于量子可逆逻辑门电路理论上不丢失信息,因此不存在热耗散,从而在理论上可以有效地解决集成芯片的能耗与发热的问题。C. Bennett 证明:只要是可逆门构造的网络,能量零损耗是可能的。量子可逆逻辑综合技术已逐步广泛地应用于量子计算、低功耗 CMOS 电路、纳米技术、光计算、加密技术等一些科技领域,随着科学技术与电子工业工艺的进步,量子可逆逻辑的研究将会逐步进入更多学科的研究领域,将会变得越来越活跃、越来越重要。

随着量子可逆逻辑研究的深入,会涉及一些量子计算和量子信息处理的新思维和新方法,也会对计算机科学技术的发展起到促进的作用。量子逻辑门的代数抽象为可逆算子,最近 30 年来,研究者们提出了多种可逆量子门,除单个量子逻辑非门外,还有若干多量子可逆门,例如控制非门、Toffoli 门、Fredkin 门以及 Peres 门等。若干量子可逆门的级联与综合可构成基本量子电路,量子电路是构建量子设备与量子计算机的基本元素,因此研制性能优良的量子逻辑门、量子可逆逻辑电路既可解决芯片能耗导致发热的问题,又可提高芯片的集成度与运行速度。量子可逆逻辑电路的设计与综合的方法与规则也是构建未来低功耗电路科技的基础。不仅如此,研究量子可逆逻辑的综合理论、量子可逆逻辑电路的自动生成技术、量子可逆逻辑电路的错误检测与定位技术,也有助于基于量子计算问题解决方案的算法的量子线路描述与算法正确性验证的研究。虽然量子可逆逻辑综合的研究工作如此有意义,但作为大学本科生或研究生的科普读物,本书只是重点讲述一些基本内容,例如,如何根据给定的量子门完成可逆逻辑函数对应的可逆逻辑电路的代数计算,进一步,如何根据要求设计问题求解的算法,完成自动生成门阵列最短、量子代价最小的量子可逆电路的程序设计。

本书共六章内容:

第一章主要介绍量子信息与量子计算的基本知识,以为什么要研究量子可逆

逻辑电路为引子,讲解量子可逆逻辑电路从设计问题的数学建模到算法设计的基本过程。

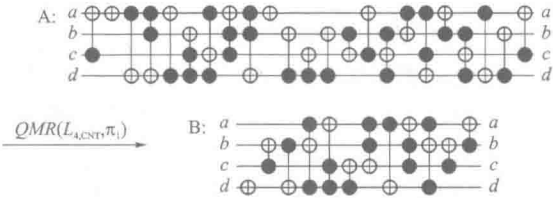
第二章介绍量子可逆逻辑电路设计中两个关键的代数定义以及可逆逻辑门的定义及其运算规则。

第三章介绍基于真值表数学建模的可逆逻辑电路综合方法,汉明距离求解方法和两个基于真值表的量子逻辑电路综合算法:二分法与图解法,以及案例的代数求解。

第四章介绍基于代数建模的可逆逻辑电路综合方法,以及一个完整可再实现的基于 R-M 代数建模的量子可逆逻辑门电路综合算法与程序实现。

第五章介绍基于置换群建模的可逆逻辑电路综合方法,基于 28 个对换元素组成的 3 量子可逆逻辑电路的快速综合方法,以及一个完整可再实现的基于 Hash 表的量子逻辑电路综合算法与程序实现,同时给出 3 量子 40320 个使用 NCT 门的全部量子可逆逻辑门电路的代数计算结果。

第六章介绍 4 量子比特可逆逻辑电路综合方法,并给出一个完整可再实现的基于 Hash 表及其多种优化元素的 4 量子逻辑电路综合的算法与程序实现。最后给出我们的算法关于 4 量子置换(15,2,3,12,5,9,1,11,0,10,14,6,4,8,7,13)的计算结果:电路 A 是 Maslov 的结果,B 是我们的计算结果,两个可逆逻辑电路完成相同的信号变换。



本书各章节的主要内容和案例均选自东南大学计算机学院量子计算与量子信息研究室研究生早期发表在《计算机学报》《软件学报》《计算机研究与发展》《电子学报》《通信学报》以及《东南大学学报》上的研究论文。特别是第四章的 4.3 节和第五章的 5.3 节,以及第六章相关部分的核心内容是取自于李志强博士的相关论文及其博士学位论文的有章节,通过围绕主线编撰后完成。全书由陈汉武执笔撰写。由于撰写本书的目的在于对学生的新科学的教育启蒙和兴趣培养,期待通过一个现实的物理问题的数学建模演绎出不同的求解方法,通过不同的解决方案让学生了解数学作为工具在问题解决过程中的作用,同时理解问题解决过程中数学建模的意义和内涵,通过举一反三培养学生的计算思维与数学建模的意识和能力。期待更多愿意动手的学生通过学习和讨论,结合程序设计与数据结构的教学,能够完成相关算法的程序实现。

陈汉武

2017 年 3 月 13 日

目 录

第一章 为什么要研究量子可逆逻辑电路?	1
1.1 集成电路产业大事记、摩尔定律与芯片集成度及其可预见的发展极限	1
1.2 不可逆逻辑门、不可逆电路与计算机硬件的能耗与降温	3
1.3 理论上量子可逆门电路可以解决以上两个瓶颈问题	4
1.4 可逆逻辑门、可逆逻辑门集合的稠密子集	5
1.5 量子比特与张量乘积	6
1.6 量子态的叠加与并行计算	11
1.7 量子态叠加与量子态纠缠物理现象的代数表达式	13
1.8 量子可逆逻辑电路的基本概念、发展简史与问题解决的基本方法	15
1.9 物理模型,数学模型,学习的任务	16
第二章 量子可逆逻辑电路代数演算中的基本定义	20
2.1 可逆函数、可逆逻辑门与可逆逻辑门电路的基本定义	20
2.2 量子逻辑门及其演算	21
第三章 真值表方法	24
3.1 逻辑函数与真值表及其运算规则	24
3.2 用真值表求解可逆逻辑门电路的汉明距离方法	28
3.3 基于真值表的二分法可逆逻辑电路综合算法	31
3.3.1 相关概念与约定	32
3.3.2 以3量子为例解说二分电路综合算法	33
3.3.3 算法分析	36
3.3.4 优化	36
3.3.5 实验计算结果	37
3.4 基于真值表的图表示法可逆逻辑电路综合算法	39
3.4.1 相关概念与约定	40
3.4.2 算法描述	43
3.4.3 优化	48
3.4.4 实验计算结果和分析	51

3.5	基于真值表的图表示法可逆逻辑电路综合算法的 4 量子可逆函数综合举例	53
第四章	代数方法	59
4.1	逻辑代数与逻辑电路	59
4.2	基于 R-M 方法求解逻辑函数的可逆逻辑电路	60
4.3	用 R-M 方法求解可逆逻辑门电路例题	63
4.4	一个基于 R-M 方法的量子可逆逻辑电路综合的算法	67
4.4.1	三个基本定义	69
4.4.2	三个优化规则	71
4.4.3	基于 R-M 的量子可逆逻辑门电路综合方法	73
4.4.4	基于 R-M 的量子可逆逻辑电路综合的快速算法	78
4.4.5	算法结果与分析	83
第五章	置换群方法	88
5.1	用置换群建模的相关基础知识	88
5.1.1	映射函数 $f(x)$ 的置换表示	88
5.1.2	置换里的映射和置换群上的乘积运算	89
5.1.3	置换中的换位运算与一个置换的换位表达	91
5.2	3 量子比特的换位元素组与量子可逆逻辑电路的综合方法	93
5.3	基于 Hash 表的量子逻辑电路综合算法	98
5.3.1	基本概念(Fredkin 门和 Peres 门的定义)	99
5.3.2	基于最小完备 Hash 函数的量子可逆逻辑电路综合算法	102
5.3.3	基于位运算的 Hash 函数量子可逆逻辑电路综合算法	112
5.3.4	实验结果与分析	119
第六章	4 量子可逆逻辑电路综合算法	122
6.1	基本概念	123
6.2	量子可逆逻辑电路综合的新算法	132
6.2.1	最小长度整体综合算法	133
6.2.2	量子电路序列生成算法	135
6.3	实验结果与分析	137
附录 A		138
附录 B	模板及其模板优化技术	147
附录 C	Hash 表的逻辑结构与物理构造	155
综合练习		156
量子可逆逻辑电路综合论文列表		159

第一章 为什么要研究量子可逆逻辑电路？

我们的研究领域还处在酝酿阶段，所幸我们不是在一个已发展了 2000 年的领域，我们尚处在非常重要的、结果不断涌现的阶段。

——Michael Rabin(迈克尔·拉宾)

自然科学中，自然已经给了我们一个世界，而我们只是去发现它的规律。在计算机上，我们可以教给计算机规律来创造一个世界。

——Alan Kay(艾伦·凯)

新兴学科量子信息论与量子计算理论的基础是量子力学原理，作为 21 世纪信息世界的新理论，势不可挡的气势已初见端倪。2016 年 8 月 16 日，世界首颗量子科学实验卫星“墨子号”在我国发射成功，标志着量子信息时代离我们的生活越来越近了。

无名氏

特别提示：以下是根据“量子可逆逻辑电路设计杂谈”讲座内容整理出的文稿。

随着科学技术的发展，21 世纪的人类与电脑已经无法切割，电子计算机和各种智能终端设备如同人类血脉的延伸、智慧的延伸、能力的延伸，已经无法切割。电脑与智能设备的进化离不开集成电路技术的发展。1965 年，Gordon Moore(戈登·摩尔)曾经预言：当价格不变时，集成电路上可容纳的晶体管数目，每年(1975 年被修正为每两年，但更流行的说法是每 18 个月)增加一倍，性能也提升一倍。这就是著名的、对半导体产业和计算机产业有着深远影响的“摩尔定律”。然而随着集成密度的不断翻倍，集成电路的快速发展将使得计算机硬件必然迎来两个无法回避的瓶颈问题：

- 1) 集成电路芯片的集成度及其可预见的发展极限。
- 2) 不可逆门电路与计算机硬件的能耗与降温。

1.1 集成电路产业大事记、摩尔定律与芯片集成度及其可预见的发展极限

简单回顾代表性集成电路产业的大事记，稍加演算即可验证摩尔定律预言：1958

年,美国仙童公司与德州仪器公司分别发明了集成电路;1971 年,Intel 研制出第一台微处理器 4004,该处理器在面积为 12 mm^2 的芯片上集成了 2 250 个晶体管,运算能力超过 ENIAC;1974 年,Intel 研制出第一只 8 位微处理器芯片 8080;1982 年,Intel 推出了 80286 芯片,该芯片含有 13.4 万个晶体管;1989 年,Intel 发布 80486 芯片集成有 120 万个晶体管;1999 年,Intel 推出 Pentium III 芯片集成 2 800 万个晶体管;2006 年,Intel 推出 Core 2 Duo 芯片集成 2.91 亿个晶体管;直到 2013 年日本京都超大规模集成电路研讨会上,Intel 发布第三代英特尔酷睿:Haswell GT3e(采用 22 nm 技术,集成几十亿个晶体管);同时在 2013 年,ARM 与台积电宣布采用新工艺实现 20 nm 技术节点的量产;2016 年 7 月,中国手机芯片厂展讯获得 Intel 代工,将采用 14 nm 工艺制作芯片;2016 年 12 月 12 日,据半导体行业观察报道:比利时微电子(IMEC)在 2016 年国际电子元件会议中首度提出由硅纳米线垂直堆叠的环绕式闸极(GAA)金属氧化物半导体场效电晶体(MOSFETs)的 CMOS 集成电路,实现 7 nm 以下技术的超大规模集成电路的开发。各种技术的发明期待延续摩尔定律,热闹非凡!

基于摩尔定律推算,2010 年芯片 Power 7 采用了 32 nm 工艺,那么到 2022 年芯片晶体管尺寸应该进一步缩小达到 4 nm,然而科普中原子的尺寸大约是 0.2 nm,显然随着半导体晶体管的尺寸接近纳米级,集成电路刻画的密集程度将逼近物理极限。物理学家指出:那时导线中移动电子产生的电磁效应将会相互干扰,集成电路中的量子效应将逐渐显现,电子的运动将不再遵守经典物理学规律,电路也将不再可靠。这就是基于摩尔定律推导出可预见的集成电路发展的极限,彼时集成电路的工程技术就需要重新认识和重新学习了。图 1.1 和图 1.2 选自于

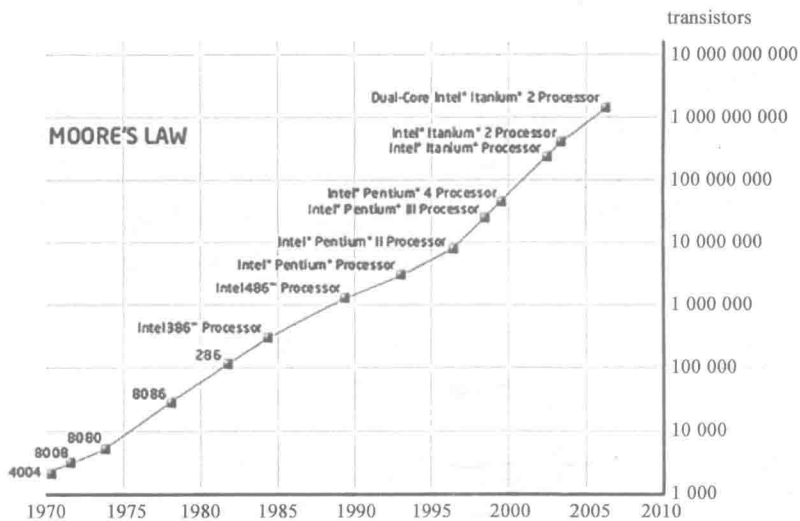


图 1.1 1971—2011 年集成电路集成度变换图(选自百度图集)

相关网站,分别表示 1971—2011 年期间集成电路的集成度统计结果的变化数据,以及随着集成度的倍增芯片的发热能耗与发热的图表。

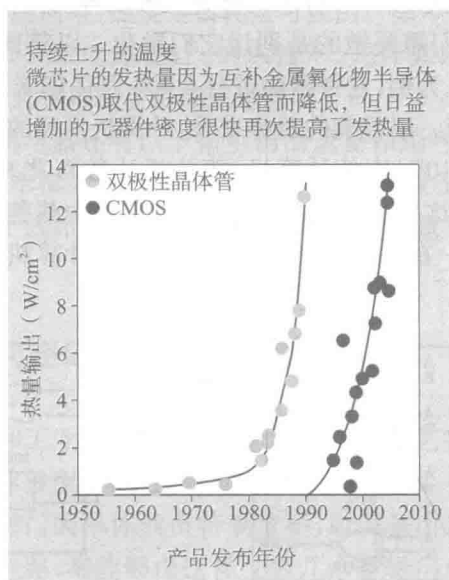


图 1.2 能耗与发热图表 (选自《环球科学》)

1.2 不可逆逻辑门、不可逆电路与计算机硬件的能耗与降温

经典集成电路采用不可逆逻辑门的级联。图 1.3 中的逻辑门都是不可逆逻辑门,它们的输入与输出比特数不相等,例如图中逻辑门的输入信息的比特位数多于输出信息的比特位数,那么输出时那些丢失的比特位信息去了哪里呢? 2011 年 5 月版《环球科学》转载了 *Scientific American* (《科学美国人》) 期刊上 Mark G. Raizen (马克·雷曾) 的撰文《熵中妖精挑战绝对零度》,文章描述了科学家如何采用 19 世纪物理学家麦克斯韦的思想实验,通过单光子将气体冷却到绝对零度的百万分之一 (10^{-6}),实验过程中的理论推导讲述 (佐证) 了“信息具有实际物理意义”的判断。那么根据能量守恒定律: 能量既不会凭空产生,也不会凭空消失,它只能从一种形式转化为其他形式,或者从一个物体转移到另一个物体,在转化或转移的过程中,能量的总量不变。因为不可逆逻辑门中的信息载体具有这样的属性,所以信息的丢失便产生了热量。大家可能都有这样的生活体验,在寒冷的办公室里笔记本电脑可以拿来温暖手或膝盖,再大一点的台式机为了散热就需要配备风扇,而对于像谷歌数据中心那样规模的计算机阵列,则需要大量的水 (或者其他方法) 来降温。研究人员指出: 作为全球最大的搜索引擎之一,Google 数据中心的能耗与

降温的问题不容小觑,对此,Google 的工程师们计划将数据中心建造在海上,利用海水来为其散热。《环球科学》曾在 2013 年 2 月号上转载 *Scientific American* 上 Philip Ball(菲利普·鲍尔)的撰文,谈到计算机的能耗与降温时有如下叙述:“至于尖端的超级计算机,我们需要做的是别让它们融化。以德国莱布尼茨超级计算中心的一台超级计算机为例,它每秒能进行 3 000 万亿(3×10^{15})次计算,产生的热量可以为几栋大楼供暖。以目前的趋势来看,计算机发展的下一个里程碑,将是出现运算速度达百亿亿(10^{18})次的计算机,其功耗达数百兆瓦(相当于一个小型核电厂的输出功率)——这些最终几乎全部都能转化为热能”。因此,不可逆逻辑电路的能耗和降温也一直备受科研人员关注,也是计算机硬件发展中不可忽视的问题。

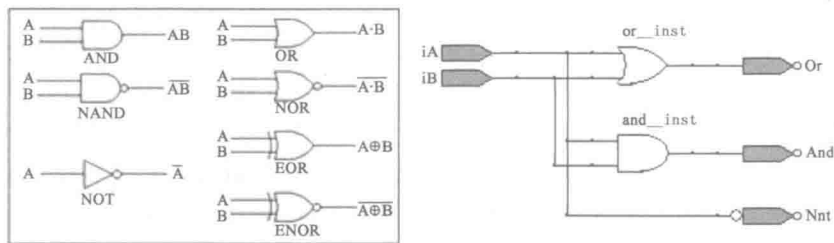


图 1.3 不可逆逻辑门与不可逆逻辑电路示意图(选自百度图集)

1.3 理论上量子可逆门电路可以解决以上两个瓶颈问题

理论上研究量子可逆门电路可以解决经典计算机硬件构造上的一些问题及上述两个瓶颈问题。其一,量子计算机将单个微观粒子作为信息载体,可以构建新体系下的信息存储和计算系统。其二,每一个量子门都对应一个酉演算,而酉量子门总是可逆的,使用量子门构成可逆逻辑电路,可逆逻辑电路的能耗在理论上几乎为零。

据文献描述,量子可逆逻辑的研究源于可逆计算机的研究。20 世纪中叶,人们发现计算机芯片的能耗导致芯片本体发热,不可逆电路与生俱来的缺陷限制了芯片的集成度,影响到经典计算机的运行速度。Landauer(兰道尔)指出:芯片能耗主要源于计算中的不可逆操作。因此降低能耗的关键是将不可逆操作变为可逆操作,“众所周知,经典计算机的本质是一个通用图灵机,是不可逆的,但所有不可逆通用图灵机,都对应一个可逆图灵机,且两者的计算能力和计算效率完全相同。”Bennett(贝内特)对以上的论述有严格证明。由于量子可逆逻辑门是可逆的,因此可以用可逆逻辑的设计方法综合量子逻辑电路(量子可逆逻辑门电路的设计是通过级联不同的可逆逻辑门完成的,因此可逆逻辑电路的设计有专用名词:综合)。

量子可逆门具有相同位数的输入/输出位,信息变换过程中不丢失输入信息,因此理论上不存在热耗散,可有效地解决芯片的热耗问题。Bennett 还证明了以下结论:只要是可逆门构造的网络,能量零损耗是可能的。如今可逆逻辑门电路已应用于量子计算、低功耗 CMOS 电路设计、纳米技术、光计算以及加密技术等若干领域,因此可逆逻辑的研究将可能变得越来越重要。

研究量子可逆逻辑电路还有以下衍生出的重要作用,如建立量子线路基本模块,构建量子计算的基本模型;构建量子线路模型,描述量子计算的通用语言(量子图灵机模型等价于量子线路的模型,单量子比特门和双量子比特门可以实现通用量子计算)。

1.4 可逆逻辑门、可逆逻辑门集合的稠密子集

随着人类的需求和工业技术的进步,现代工业与工艺技术可以设计和构造出各种各样的逻辑门单体或组合体,这些逻辑门的全体组成一个大家族,在这个大家族中总有少数几个逻辑门的单体成员特别重要,原因是由这个大家族中任何复杂的逻辑门组成的逻辑电路,都能够由这样少数几个逻辑门单体成员通过有限次级联实现。用集合论的数学语言重复上述的内容:大家族就是一个大集合,少数几个单体成员就是这个集合的一个子集,任何复杂的逻辑门电路都可通过少数单体成员的有限次组合表达(实现),(数学的语言就)说这个子集是大集合的一个稠密子集。量子可逆逻辑门含有各种相位逻辑门,更为复杂,那么量子可逆逻辑门组成的大家族(集合)是否也存在这样稠密子集呢?Deutsch(多伊奇)等人已证明:几乎所有的 2 比特量子逻辑门都是通用的,这里“通用逻辑门”的含义是指:通过这些逻辑门的级联,可以任意精度逼近任何一个量子门操作;“几乎”的含义是指,2 比特通用量子逻辑门的集合是所有 2 比特逻辑门集合的一个稠密子集;进一步,单量子比特门和受控可逆非门(双量子比特门)能够组成量子可逆逻辑门集合的一个稠密子集。

2007 年 5 月 3 日,NEC 美国公司在美国科学促进会(EurekAlert)科学新闻刊物上报道:NEC(日本电气公司),JST(日本科学技术局)和 RIKEN(物理化学研究所)一起成功地演示了世界上第一个可以控制量子比特之间的耦合强度的实验。实现量子位间的耦合强度控制的技术对于实现实用的量子计算机是至关重要的。图 1.4 是 NEC、JST 和 RIKEN 在更早之前发表的论文插图,插图中描述到,NEC 和 JST 在 1999 年研制出单量子比特的可逆逻辑门,2003 年 NEC 和 RIKEN 开发出双量子比特的可逆逻辑门,于是得出:如果在一个系统中能够实现两种量子门操作,就能够实现量子计算。图 1.5 告诉我们物理学家是如何通过用激光照射原子

来操控这种信息的(实现非门和控制非门)。当一束具有恰当频率、时间长度和振幅的激光脉冲(π 脉冲)照射原子,就能将 0 态转化为 1 态(电子的能级通过吸收或释放光子发生跃迁,电子不同的能级可以稳定地表示不同的态势),反之亦然。物理学家还能调整激光脉冲的频率,来操控两个相互作用的原子,让其中一个原子控制另一个的行为。这样,我们就拥有了 1 比特和 2 比特逻辑门的所有要素,它们是构成量子计算机的基本单位。

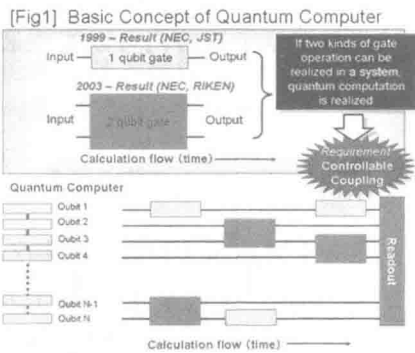


图 1.4 量子逻辑门与量子计算

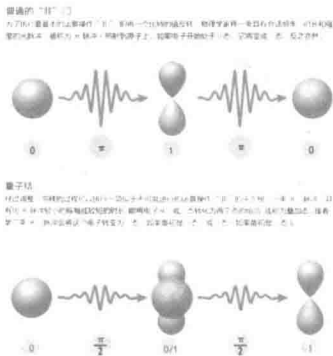


图 1.5 量子非门与控制非门的物理实现原理(选自《环球科学》)

1.5 量子比特与张量乘积

在传统观念下,信息的最基本片段是比特。在物理学家眼里,1 个比特就是 1 个能在两种不同“态”之间来回转换的物理系统,它代表两个逻辑值:是或非、假或真、0 或 1。在数字计算机里,电容器的平板带或不带电就是 1 个比特。与传统信息片段类似,量子计算所操纵的最基本单元也是比特,只不过是量子世界的比特(Quantum Bit, Qbit)。对于传统计算机来说,一个电路不是“开”就是“关”,相对应的一个传统比特不是 0 就是 1。而量子比特可以采用微观粒子的稳定状态表示,如图 1.6 所示。

图 1.7 归纳出经典比特和量子比特的信息存储载体发生的革命性变化(类型、测量、状态演化、确定的、概率的、酉性的),显然量子比特的代数刻画能力要远远超过经典比特。

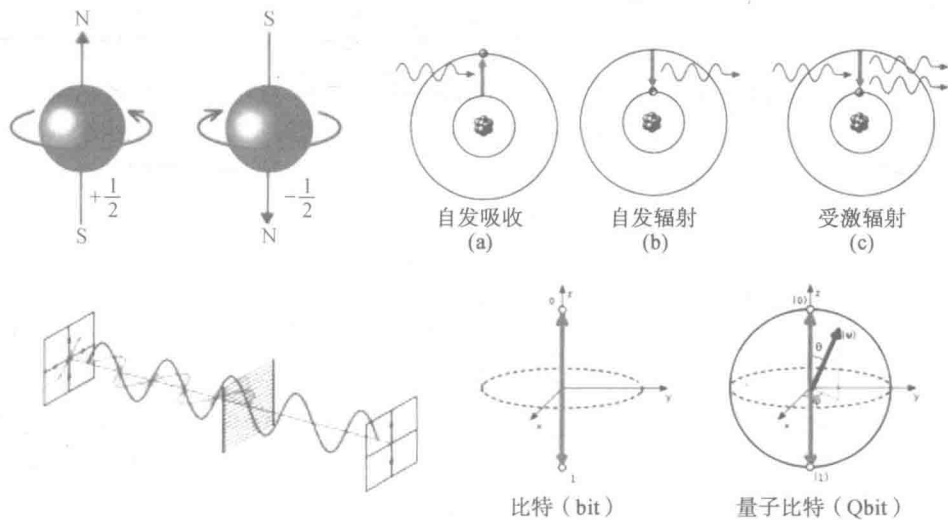


图 1.6 微观粒子中的两态系统及其经典比特、量子比特示意图

(电子的自旋态:0 表示左旋,1 表示右旋)(原子中电子态:0 表示基态,1 表示激活态)(光子的偏振态:0 表示水平,1 表示垂直)(经典比特,量子比特示意图)

Bits, Pbits, Qubits			
	bit	probabilistic bit	quantum bit
Configurations:	$\begin{bmatrix} 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \end{bmatrix}$
Description:	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} p \\ 1-p \end{bmatrix}$ $p \in \mathbb{R}$	$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ $\alpha, \beta \in \mathbb{C}$
Observation:	$\begin{bmatrix} 0 \end{bmatrix}$ certainty	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ p percent $1-p$ percent	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ $ \alpha ^2$ percent $ \beta ^2$ percent
Evolution:	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ deterministic	$\begin{bmatrix} 1-q & r \\ q & 1-r \end{bmatrix}$ stochastic	$\begin{bmatrix} u & v \\ w & x \end{bmatrix}$ unitary

图 1.7 比特、概率比特、量子比特的比较

[经典比特、概率比特、量子比特在类型、配置、描述、测量、演化上的代数描述(选自《环球科学》)]

图 1.8 将 1 个量子比特示意图标示在布洛赫球球面上,通过式(1.1)抽象出一个代数表达式,用狄拉克符号 $|\psi\rangle$ 描述,一个简单的 $|\ast\rangle$ 符号刻画一个复空间的向量,就将量子比特描述为具有特定属性的数学对象。把量子比特当作抽象对象的绝妙之处在于,它为我们建立一个不依赖特定系统的一般量子计算与量子信息理

论讨论的自由空间。既然量子比特表示为一个单位球面上的向量,那么球面上的每一个向量都可以用这个球的两个极向量(北极 $|0\rangle$ 和南极 $|1\rangle$,也称为量子比特的一组基向量)来表示[参阅 *Quantum Computation and Quantum Information* (《量子计算与量子信息》) 的 1.2 节 Quantum Bit 相关内容,或对照布洛赫球],如式 (1.1) 所示。

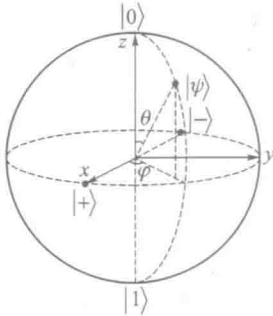


图 1.8 一个量子比特和它的表示

(1 个量子比特可以表示单位球面上的任何一点,根据量子的物理特性,具有经典比特无法比拟的表现能力。)

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \tag{1.1}$$

其中 $0 \leq \theta \leq \pi, 0 \leq \varphi \leq 2\pi$ 。显然,如果不考虑围绕中心轴 Z 旋转的话,以 Z 轴为轴心的圆上任何一点可以表示为:

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} |1\rangle = \begin{bmatrix} \cos \frac{\theta}{2} \\ \sin \frac{\theta}{2} \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \text{ 显然 } \alpha^2 + \beta^2 = 1 \tag{1.2}$$

此处 $|0\rangle$ 和 $|1\rangle$ 分别对应经典比特状态中的 0 和 1。符号 $|*\rangle$ 取自量子物理,称为 Dirac* 记号,由图 1.8 可知,符号 $|*\rangle$ 在复数空间中表示一个向量, $|0\rangle$ 和 $|1\rangle$ 分别表示向量 $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ 和 $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$,量子力学中量子态向量采用这种表示形式是为了方便量子力学量的表示和计算。显然有以下结论:两个向量的内积 $\langle 0|1\rangle = [1 \ 0] \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0$,且 $|0\rangle$ 和 $|1\rangle$ 的模都等于 1,因此 $|0\rangle$ 和 $|1\rangle$ 是一组标准正交基。而且

* 注:保罗·狄拉克,1902. 8. 8—1984. 10. 20,英国理论物理学家,量子力学的奠基者之一,1933 年,因为“发现了在原子理论里很有用的新形式”(即量子力学的基本方程——薛定谔方程和狄拉克方程),狄拉克和埃尔温·薛定谔共同获得了诺贝尔物理学奖。