

“十二五”国家重点图书出版规划项目
杰出青年学者研究文丛

量子有限自动机：等价性和最小化

Quantum Finite Automata: Equivalence and Minimization

◎ 李绿周 邱道文 著

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

量子有限自动机：等价性和最小化

Quantum Finite Automata:
Equivalence and Minimization

ISBN 978-7-308-15199-3
9 787308 151993 >
定价：56.00元



“十二五”国家重点图书出版规划项目
杰出青年学者研究文丛

量子有限自动机：等价性和最小化

Quantum Finite Automata: Equivalence and Minimization

◎ 李绿周 邱道文 著

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

图书在版编目(CIP)数据

量子有限自动机：等价性和最小化 / 李绿周，邱道文著. —杭州：浙江大学出版社，2019.6
（杰出青年学者研究文丛）
ISBN 978-7-308-15199-3

Ⅰ.①量… Ⅱ.①李… ②邱… Ⅲ.①量子－计算－应用－自动机理论 Ⅳ.①TP301.1

中国版本图书馆 CIP 数据核字(2015)第 235656 号

量子有限自动机:等价性和最小化
李绿周　邱道文　著

责任编辑　张凌静　金　蕾
责任校对　候鉴峰
封面设计　刘依群
出版发行　浙江大学出版社
（杭州市天目山路 148 号　邮政编码 310007）
（网址:http://www.zjupress.com）
排　　版　杭州星云光电图文制作有限公司
印　　刷　杭州钱江彩色印务有限公司
开　　本　710mm×1000mm　1/16
印　　张　8.75
字　　数　153 千
版 印 次　2019 年 6 月第 1 版　2019 年 6 月第 1 次印刷
书　　号　ISBN 978-7-308-15199-3
定　　价　56.00 元

版权所有 翻印必究　印装差错 负责调换
浙江大学出版社市场运营中心联系方式:(0571)88925591;http://zjdxcbs.tmall.com

前　言

量子计算是计算机科学与量子力学交叉产生的新兴学科，经过30多年的发展，在理论和实验方面都已经取得了长足的进展。目前，发展量子计算已成为世界大国占领科技制高点的一个重要举措。量子计算的研究得到了政府部门、学术界以及企业界的高度重视与支持。最近，美国陆军发布的将在未来30年改变世界的20项重大科技趋势就包含了量子计算。我们国家从2006年的《国家中长期科学和技术发展规划纲要(2006—2020年)》到“十三五规划”，都把量子计算纳为重要研究内容。《国家自然科学基金“十三五”发展规划》把量子计算列为“十三五”期间拟重点布局的优先领域或研究方向。谷歌、微软、IBM等国际巨头公司都成立了量子计算方面的研究团队，致力于把量子计算推向实际应用领域。

本书从计算机科学领域自动机理论的角度来考察量子计算，力图通过有限自动机这个简单而重要的模型来探索量子计算与经典计算的一些本质差异，认识量子计算的计算能力和局限性。全书共分为6章。第1章是绪论，主要介绍量子计算和量子自动机相关的背景知识及本书要讨论的问题。第2章介绍本文要用到的一些基本概念和符号，主要包括线性空间、量子力学，以及经典自动机理论中的一些基本概念和符号。第3章介绍量子有限自动机模型及量子时序机，也是本书要讨论的对象之一。第4章集中讨论几类主要量子自动机的等价性问题，主要包括量子时序机(QSM)、测量一次的单向量子有限自动机(MO-1QFA)、测量多次的单向量子有限自

动机(MM-1QFA)、带控制语言的单向量子有限自动机(CL-1QFA)、多字符量子有限自动机的等价性问题。分别给出各类模型中两个机器等价的充分必要条件,详细地给出多项式时间的等价性判定算法。第5章讨论一般单向量子有限自动机,包括其语言识别能力和等价性问题。第6章讨论量子有限自动机的最小化问题,证明几类主要的量子有限自动机的最小化问题是可解的。

本书得以顺利完成,得了学术界众多前辈、同行的帮助和支持,也得到了作者所在工作单位中山大学数据科学与计算机学院许多领导与同事的关心和支持,在此不一一列举,诚挚地道一声谢谢!同时,特别感谢浙江大学出版社张凌静编辑在本书出版过程中给予的支持!最后,本书得以顺利完成离不开家人在背后默默的支持,感谢他们!

由于量子计算近几年发展迅速,加上作者学识浅陋,必有许多不足之处,希望大家提出意见并指正。

作　者

2019年3月

目　录

1　绪　论　(1)

1.1　量子计算　(1)

1.1.1　量子计算的影子——可逆计算　(2)

1.1.2　量子图灵机与量子线路　(2)

1.1.3　量子算法　(3)

1.2　量子自动机　(4)

1.2.1　概况　(4)

1.2.2　量子有限自动机(QFA)　(4)

1.2.3　QFA 的主要研究工作　(6)

1.2.4　QFA 和其他研究分支的联系　(8)

1.3　等价性和最小化问题　(10)

1.3.1　经典自动机情形　(10)

1.3.2　量子自动机情形　(11)

2　预备知识　(13)

2.1　线性代数的相关概念与符号　(13)

2.1.1　线性空间　(13)

2.1.2　狄拉克符号　(14)

2.1.3　矩阵的基本操作　(14)

2.1.4　特殊矩阵　(15)

2.1.5　矩阵的分解与范数　(16)

2.2　量子力学基础　(17)

2.2.1 量子比特 (17)
2.2.2 量子力学基本假设 (18)
2.2.3 密度算子 (20)
2.2.4 量子运算的算子和表示 (21)
2.3 经典自动机理论的相关概念与符号 (22)
3 量子自动机模型 (26)
3.1 测量一次的单向量子有限自动机 (27)
3.2 测量多次的单向量子有限自动机 (31)
3.3 带控制语言的单向量子有限自动机 (35)
3.4 带经典态的单向量子有限自动机 (37)
3.5 双向量子有限自动机 (40)
3.6 带量子和经典态的双向有限自动机 (41)
3.7 多字符量子有限自动机 (43)
3.8 其他量子有限自动机 (44)
3.9 量子时序机 (45)
3.10 本章小结 (47)
4 量子自动机的等价性判定 (48)
4.1 准备知识 (48)
4.1.1 双线性机及其等价性 (48)
4.1.2 量子自动机的等价性定义 (52)
4.2 量子时序机的等价性 (53)
4.2.1 方法一 (53)
4.2.2 多项式时间的等价性判定算法 (56)
4.2.3 方法二 (60)
4.3 测量一次的单向量子有限自动机的等价性 (61)
4.4 带控制语言的单向量子有限自动机的等价性 (62)
4.5 测量多次的单向量子有限自动机的等价性 (65)
4.5.1 方法一 (66)
4.5.2 方法二 (68)
4.6 多字符量子有限自动机的等价性 (72)

4.6.1　输入字母表只含一个字符　(73)
4.6.2　输入字母表为一般情况　(76)
4.7　本章小结　(79)
5　一般单向量子有限自动机　(81)
5.1　测量一次的一般单向量子有限自动机　(81)
5.1.1　闭包属性　(82)
5.1.2　语言识别能力　(84)
5.1.3　等价性问题　(88)
5.2　测量多次的一般单向量子有限自动机　(90)
5.2.1　预处理　(91)
5.2.2　语言识别能力　(97)
5.2.3　等价性问题　(100)
5.3　本章小结　(101)
6　量子自动机的最小化　(102)
6.1　最小化的主要思想　(102)
6.2　概率有限自动机的最小化　(105)
6.3　测量一次的单向量子有限自动机的最小化　(107)
6.4　测量多次的单向量子有限自动机的最小化　(110)
6.5　一般单向量子有限自动机的最小化　(112)
6.5.1　预备知识　(113)
6.5.2　最小化问题　(114)
6.6　本章小结　(119)
参考文献　(121)
索　引　(133)

1 绪 论

本章主要简要介绍本书的背景、所研究的问题，以及主要贡献。

1.1 量子计算

自20世纪中期以来，经典计算理论取得了巨大的成功。如摩尔定律所预测，集成电路芯片上所集成的电路的数目，每隔18个月就翻一番，微处理器的性能每隔18个月也提高一倍。然而，摩尔定律是存在极限的，芯片的集成度不可能无限制地增长下去。那么该如何继续保持计算性能的增长呢？为此，一些新的计算方式被提出来，并得到研究，如量子计算、DNA计算、光子计算等，其中量子计算以其内在的并行性和潜在的物理可实现性尤为引人注目。

量子计算作为20世纪两大重要科学技术（量子力学和计算机科学）相互结合产生的交叉学科，具有广阔的发展前景。近年来，世界上许多著名高校和科研机构都积极投入到这方面的研究中来，各国政府也加大了对其相关研究计划的支持。我们国家也十分重视量子计算方面的研究。为此，《国家中长期科学和技术发展规划纲要（2006—2020年）》中明确规定把“量子调控”列入基础研究中的重大科学研究计划中，量子计算就是其研究内容之一。

下面简要回顾一下量子计算的发展背景。

1.1.1 量子计算的影子——可逆计算

量子计算的历史最早可以追溯到可逆计算。我们知道,经典计算机中的信息处理过程是通过逻辑门来实现的,这些逻辑门可能是不可逆的。比如,逻辑"与"门就是不可逆的,因为它把两位输入比特变为一位输出比特,从而无法从输出结果确定输入是什么;另一方面,逻辑"非"门是可逆的,因为可以通过它的输出结果来确定输入是什么。也可以从信息擦除的角度来理解不可逆性。如果一个逻辑门是不可逆的,则在执行它时会擦除信息,比如逻辑"与"门把两位输入变成一位输出,擦除了一位信息。相反地,如果一个逻辑门是可逆的,则在执行它时不会擦除信息,比如逻辑"非"门。之所以讨论计算的可逆性问题,是因为它与计算的能耗问题紧密相关。1961 年,IBM 的科学家 Landauer 在这方面得到了较为明确的结论,他给出了所谓的 Landauer 原理[2]:假设计算机擦除一比特的信息,则散发到环境中的能量至少是 $k_B T\ln 2$,其中 k_B 是 Boltzmann 常数,T 是环境温度。Landauer 原理表明不可逆计算会引起能耗,并给出了能耗下限。Landauer 的工作激发了人们研究可逆计算的热情。1973 年,IBM 的 Bennett[3] 在这方面取得了重要进展,他证明任意一个经典图灵机都可以用一个可逆图灵机进行有效的模拟。换句话说,经典计算过程是可以以可逆方式进行的,且不影响计算能力。值得指出的是,可逆计算又有了新的发展,在这个过程中人们关注的是可逆计算与其他科学问题而非能耗问题的关系,这方面的最新研究进展可参考综述文献[4]。

尽管研究可逆计算的初衷是讨论计算的能耗问题,但是在无意识中它却与量子计算达成了共识,因为量子计算是可逆的。当然,量子计算还具有更多的特性。事实上,可逆计算的一些研究成果在进行量子计算研究时是能用到的。

1.1.2 量子图灵机与量子线路

虽然我们把量子计算的历史追溯到可逆计算,但是人们真正开始思考量子计算方面的问题则可以从 Benioff 的工作谈起。1980 年,Benioff[5] 考虑

了基于量子力学的计算设备，表明基于量子力学的计算设备可以模拟经典计算机。一年之后，Feynman[6]勾勒出以量子现象实现计算的愿景，他指出经典计算机不能有效地模拟量子力学系统，而基于量子力学规律的计算机才可能实现上述模拟①。以上工作促使 Deutsch[7]在 1985 年重新考察了丘奇-图灵论题，然后提出了以下命题：任何有限的可实现的物理系统必能被一个包含有限操作的通用计算模型精确地模拟。Deutsch 所指的包含有限操作的计算模型不可能是经典图灵机，因为经典图灵机是离散的，而现实物理中的状态空间是连续的。因此，Deutsch 定义了量子图灵机。换句话说，任何有限的可实现的物理系统必能被一个通用量子图灵机精确模拟。至此，量子计算开始具备了基本的数学模型。

量子图灵机只是一个抽象的理论模型，那么如何将它具体化呢？我们知道经典计算机是利用逻辑门构成的线路来模拟经典图灵机的，因此构造量子计算机的任务也自然归结到建立一个由量子逻辑门组成的量子线路。关于量子图灵机与量子线路关系的一个重要结论是由 Yao[8]在 1993 年给出的，他证明量子线路模型和量子图灵机是等价的，即任意在量子图灵机上可以多项式时间计算的函数，都有一个多项式规模的量子线路；反之亦然。

1.1.3 量子算法

虽然前面提到的工作为量子计算理论的发展奠定了基础，但是真正把量子计算引入大众视野、掀起研究热潮的是 Shor 算法的提出。1994 年，Shor[9]提出了著名的大数因子分解量子算法，该算法可在多项式时间内解决经典计算中的 NP 问题，是对经典算法的指数级加速。Shor 算法的提出使得经典密码系统受到了巨大的威胁，激起了人们对量子计算的极大兴趣。1996 年，Grover[10]又进一步提出了在无序数据库中寻找特定目标的量子搜索算法，该算法可比经典算法平方根加速。粗略看来，Grover 算法似乎不比经典算法优越多少，但是由于 Grover 算法所针对的问题在现实生活中具有广泛的应用背景，从而使得 Grover 算法具有很强的应用价值。因此，Grover 算法在量子计算的发展史中也占有十分重要的地位。

① Feynman 在 1981 年的一次演讲中就讲过这些内容，而将其最终发表在学术期刊上则是在 1982 年。

自从 Shor 算法开启了量子计算的新阶段后,国际上越来越多的学者加入到了量子计算的研究中来。经过二十多年的发展,量子计算已成为一门充满魅力与挑战的新兴交叉学科,相关技术的研究已成为世界各国战略竞争的焦点之一。

1.2 量子自动机

经典自动机在计算理论中扮演着十分重要的角色[11],对它们的研究有助于认识各种计算方式的能力与局限性,同时也是计算复杂性理论的基础。随着量子计算的兴起,研究量子自动机也必将对量子计算理论的发展起着重要的作用。对量子自动机的探索有助于认识量子计算的能力和局限性,同时也有助于理解量子计算与经典计算的本质差异。

1.2.1 概况

量子自动机的转移函数必须服从量子力学规律,因而具有酉性(可初略理解为可逆性),同时计算结果要通过测量以一定的概率得到。大体上可以这样来理解量子自动机:当把概率自动机中的概率换成概率振幅时,它就成了量子自动机。概率振幅是个复数,它的模的平方表示概率。正是这些特点,使得量子自动机表现出一些与经典自动机完全不同的特性。

如同经典自动机一般,量子自动机也涉及多种不同类型,包括量子有限自动机[12-15]、量子时序机[16-18]、量子下推机[12,16,19-22]、量子图灵机[7,23-28]、量子计数自动机[29-32]、量子元胞自动机[33-37],以及基于量子逻辑的自动机理论[38-47],等等。值得指出的是,量子元胞自动机作为一种重要的量子计算模型吸引了物理界和计算机界众多学者的关注,其研究成果之多需要专门的著作才可能梳理清楚。本书主要讨论量子有限自动机,其他一些计算模型虽被提及,但不做详细讨论。量子有限自动机方面的综述性文献也可参考文献[48-49]。

1.2.2 量子有限自动机(QFA)

有限自动机,作为经典计算理论中一种基本而重要的计算模型,得到了

深入系统的研究(详细信息可参考 Hopcroft 和 Ullman 的专著[11]),这自然引发人们思考它的量子情形——量子有限自动机(quantum finite automata, QFA)。另外,目前来看,量子内存是很昂贵的,因此考察利用有限的小规模量子资源能完成什么任务显得很有意义,这也为研究 QFA 提供了合适的理由。因此,作为具有有限内存的量子计算机的理论模型,QFA 被提出来并得到广泛研究。QFA 首先由 Moore 和 Crutchfield[12] 以及 Kondacs 和 Watrous[13] 分别以不同形式提出。到目前为止,已有多种不同类型的 QFA 模型得到研究,它们的差别主要表现在以下三方面:①带头的移动方向;②状态转移函数所满足的要求;③测量的次数。

第一个影响 QFA 定义的因素是自动机带头的移动方向。QFA 可以分为单向量子有限自动机(1QFA)[12-13] 和双向量子有限自动机(2QFA)[13]。1QFA 每读入一个输入字符,带头必须往右移动一格;而 2QFA 每读入一个输入字符,带头可以左移一格、右移一格,或者不动。另外,Amano 和 Iwama[50] 讨论了一种称为1.5向量子有限自动机(1.5QFA)的模型,其中带头只能右移或者不动。特别地,Amano 和 Iwama[50] 证明了空问题对 1.5QFA 是不可判的。所谓空问题,即判断一个自动机接受的语言是否为空,它是自动机理论中的基本问题之一。

第二个影响 QFA 定义的因素是状态转移函数所满足的要求。早期,通常假设 QFA 的状态转移函数满足酉性,即 QFA 每读入一个字符,都执行一个酉操作。这是为了与量子力学假设(封闭量子力学系统的状态演化由酉算子所刻画)相一致。后来,研究者发现 QFA 不一定是个封闭系统,它可以和外界环境交互,从而是一个开放系统。因此,QFA 的状态转移函数可以更具一般性。例如,文献[51]定义的 GQFA 和文献[52]定义的 LQFA,状态转移可以由投影测量与酉算子组成的有限序列来描述。事实上,在最一般的情况下,QFA 的状态转移可由保迹量子运算来描述[53-56],我们称这样的模型为 gQFA[57]。另外,由于基于测量的量子计算近年在学术界引起了强烈反响[58-60],所以也有学者开始考虑基于测量的 QFA[61-62],即每读入一个字符,QFA 只能执行测量操作。

最后一个影响 QFA 定义的因素是测量的次数。QFA 在读入输入字符的过程中,要通过测量操作来判断机器是否进入接受状态。因此,我们有两种测量方式:①测量一次的(measured-once),即在所有输入字符读完之后才做一次测量,以决定机器是接受还是拒绝;②测量多次的(measured-many),即每读入

一个输入字符都做一次测量,以决定机器是停止(接受或拒绝)还是继续读入下一字符。据此,Moore 和 Crutchfield[12] 定义的模型称为测量一次的 1QFA,简记为 MO-1QFA;而 Kondacs 和 Watrous[13] 给出的 1QFA 模型称为测量多次的 1QFA,简记为 MM-1QFA。目前已有大量文献讨论这两个模型的相关问题。

需要指出的是,在文献[63]中,有一类称为混合 QFA 的模型值得关注。这样的模型由两部分组成:一个量子部件和一个经典部件,两者之间可以相互通信。属于这类模型的有带控制语言的单向量子有限自动机(CL-1QFA)[64]、带量子和经典态的双向有限自动机(2QCFA)[65]及其单向变种 1QCFA[142],还有带经典态的单向量子有限自动机(1QFAC)[66]。这类模型的有趣之处至少可以反映在以下两个方面:

一方面,混合模型比纯量子模型更具可实现性。就目前的技术来说,制造大规模的量子处理器仍然是一个长期目标,而建立一个由经典系统加上少量的量子比特组成的混合系统则相对容易得多。另外,在混合模型中,自动机的带头可由经典部分来控制,这也使得它更容易实现。例如,考虑到 2QFA[13] 的带头是量子的,不易实现,文献[65]提出了 2QCFA 模型。2QCFA 就是一个混合模型,它的带头是经典的,从而与 2QFA 相比更容易实现,但是计算能力似乎并没有减弱。

另一方面,由于混合模型具有经典和量子两部分资源,因此给定一个问题时,可以通过适当设计,在经典资源和量子资源之间找到一种平衡。已有一些研究成果表明,在一个经典有限自动机上辅助少量量子比特,会使得自动机的计算能力快速提升或者所用资源(比如状态数)大大降低[65-70]。

1.2.3 QFA 的主要研究工作

到目前为止,关于 QFA 的主要研究工作概括起来可以分为以下三个方面:第一是对 QFA 语言识别能力的刻画①,这方面集中了大量的研究工作,例如文献[13-15]等。总体上来说,1QFA 的语言识别能力没有超越对应的经典模型——确定有限自动机(deterministic finite automata,DFA)和概率

① 本书中,称一个 QFA 接受(或识别)语言 L,默认情况是指以有界误差方式接受,具体定义见第 2 章 2.3 节。

有限自动机(probabilistic finite-state automata,PFA),有时甚至更差;即使允许执行最一般的操作——保迹量子运算,1QFA 最多只能和 DFA 一样强[57]。相反地,2QFA 比对应的经典模型的语言识别能力显著增强。Kondacs 和 Watrous[13]证明 2QFA 不仅能在线性时间内识别所有的正则语言,还能在线性时间内识别非正则语言 $L_{eq}=\{a^nb^n \mid n\geqslant 1\}$,而 2QFA 的经典对应模型——双向概率有限自动机(2PFA)不可能达到同样的效果[71-73]。事实上,2PFA 若要识别非正则语言,必须花费指数时间[72-73]。

严格来说,2QFA 违背了"有限"的精神,因为它的带头可以同时处于多个不同的位置,是个叠加态,因此用来保存带头位置的量子比特数与输入长度有关。考虑到这点,Ambainis 和 Watrous[65]提出了前面所说的 2QCFA 模型。尽管 2QCFA 的带头是经典的,但是它的计算能力似乎并没有减弱,因为在文献[65]中证明了 2QCFA 不仅能在多项式时间内识别 L_{eq},还能识别回文语言 $L_{pal}=\{x\in\{a,b\}^* \mid x=x^R\}$(指数时间内);而 2PFA 在任意时间内都无法识别回文语言 L_{pal}[74]。至于 2QFA 和 2QCFA 的计算能力之间的关系,目前还没有明确的结论。

几种主要 QFA 模型的语言识别能力的关系如图 1.1 所示,其中个别未提及的模型在后续章节中会陆续介绍。

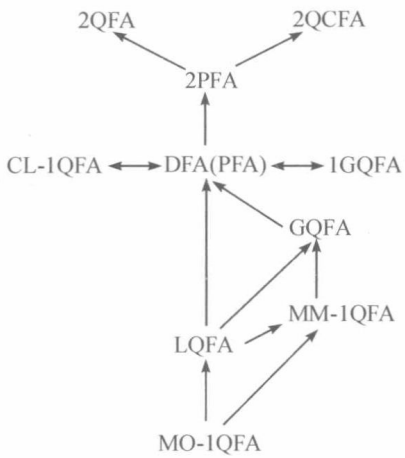


图 1.1 几类主要 QFA 模型的语言识别能力的关系

双向箭头表示相等,例如在图 1.1 中表明 CL-1QFA 和 DFA(PFA)语言识别能力相同,事实上它们都识别正则语言;单向箭头表示位于箭头尾部的模型弱于位于头部的模型,例如 2PFA 弱于 2QFA,因为如前所述,线性时间