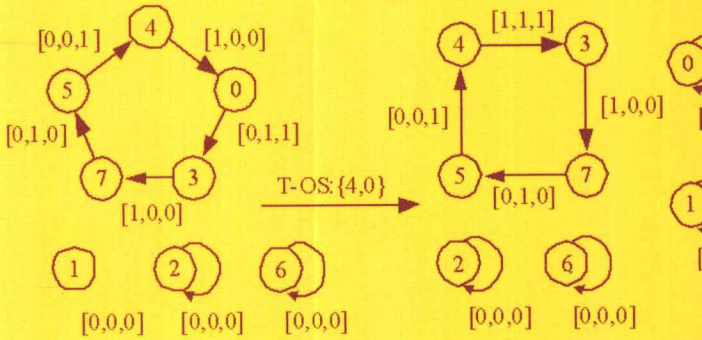
可逆逻辑综合

管致锦 著



科学出版社

可逆逻辑综合

管致锦 著

科学出版社
北京

内 容 简 介

本书以作者和课题组多年来可逆逻辑综合工作为基础，但又不囿于此。撰写中把可逆逻辑综合基础与最新研究成果相融合，以可逆逻辑门级联为主线，从简单可逆逻辑门级联出发，逐步拓展可逆门级联的种类，引入相关的可逆逻辑综合理论和方法。本书系统介绍可逆逻辑门、可逆逻辑函数与可逆逻辑门网络及其相互关系，分析可逆逻辑和可逆逻辑门的本质特征，反映可逆逻辑门网络的结构特点和内涵特性，并给出相应的表示；较为全面地给出传统可逆逻辑门到扩展可逆逻辑门可逆逻辑综合的相关理论和方法。

本书可作为高等院校计算机、电子信息、通信等专业高年级本科生和研究生课程的参考用书，同时对相关研究人员也具有指导意义和参考价值。

图书在版编目(CIP)数据

可逆逻辑综合/管致锦著. —北京：科学出版社，2011.2

ISBN 978-7-03-030049-2

Ⅰ.①可… Ⅱ.①管… Ⅲ.①电子计算机-逻辑设计 Ⅳ.①TP302.2

中国版本图书馆 CIP 数据核字（2011）第 009955 号

责任编辑：任 静 王国华 / 责任校对：邹慧卿
责任印制：赵 博 / 封面设计：耕者设计工作室

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

丽源印刷厂印刷

科学出版社发行 各地新华书店经销

*

2011 年 2 月第 一 版 开本：B5（720×1000）
2011 年 2 月第一次印刷 印张：14
印数：1—2 500 字数：263 000

定价：50.00 元

（如有印装质量问题，我社负责调换）

前　言

计算复杂性是求解一个计算问题所需要的时间和空间的度量，时间和空间量是计算的重要资源。计算过程中还有一类资源往往被人们忽略，那就是能量。可逆计算是解决计算过程中能量资源损耗的重要手段。从逻辑的观点，可以对一个基本计算步骤所消耗的能量进行计算。抛开计算机制造过程中工艺和材料的因素，计算机中能耗问题主要是逻辑上的不可逆操作产生的。自 Landauer(1961)提出计算过程中能量消耗与计算的可逆性有着必然联系的论点以来，对信息、能耗和计算之间关系的研究虽然经历了漫长的过程，但只有近十几年来随着量子计算的发展和低功耗集成电路技术的要求才被真正重视起来。

可逆逻辑综合是可逆计算研究的关键问题之一，它是量子计算和量子信息技术研究的重要组成部分，并在低功耗网络设计、信息安全、纳米技术等其他一些现代科学领域有着重要应用(Long et al., 2001; Nielsen et al., 2000; Picton, 2000; Merkle, 1993; Peres, 1985)。其潜在的巨大实际应用价值和重大的科学理论意义，正引起越来越多的关注。

可逆计算中的逻辑综合是近年来发展起来的新兴研究领域，是交叉性很强的学科，有诸多问题需要进行研究。可逆逻辑综合的关键问题是如何构造和优化可逆逻辑网络，主要表现在可逆逻辑设计算法、规模、优化及代价等。研究可逆逻辑综合的理论和方法，能够让新兴的相关技术领域通过使用可逆门网络的级联结果得以更好地发展。

由于可逆逻辑综合在可逆计算中的基础地位和在光计算、纳米技术以及信息安全方面的重要应用，近十年来研究成果不断涌现。因此，总结国际上近十年来可逆逻辑综合的研究成果，反映我国学者在该领域的贡献，引导更多的人投身该领域开展研究是十分迫切和非常必要的。本书对相关问题给出了一系列解决方案，各章的具体安排是：

第 1 章阐述了可逆逻辑综合的研究背景，介绍了可逆计算及可逆计算中逻辑综合的研究内容和研究现状，分析了可逆逻辑综合目前的研究方法和存在的问题，并概述了本书的主要研究内容。

第 2 章对可逆的物理意义和逻辑意义进行了探讨，给出了可逆逻辑的数学基础——布尔代数的相关内容，分析研究了可逆逻辑门的演化过程，给出了一般可逆逻辑门及其表示方法，研究了可逆逻辑门和一般可逆逻辑门之间的关系。

第 3 章分析了可逆逻辑网络结构和可逆网络级联的基础，提出了一种可逆网

络门的计数方法，给出了可逆网络的表示方法，提出了一种可逆逻辑门网络基本元素的产生方法和可逆逻辑门的级联方法。

第 4 章给出了一种可逆逻辑门网络的基本构造方法。

第 5 章介绍了典型的 Toffoli 门序列可逆逻辑综合，将给定的可逆函数转换为恒等函数，避免了大规模的查找，有利于扩充可逆网络的规模。

第 6 章将 Toffoli 门、SWAP 门和 Fredkin 门统一到一个可逆逻辑门库中进行讨论，并给出了一种组合级联方法，实现了不同输入下典型可逆门簇网络的级联方法。

第 7 章对传统可逆逻辑门进行了扩展，提出了一种基于正/反控制门簇的可逆网络级联算法，该算法采用逐个门添加的方法，引入了正/反控制交换门(PNCSG)的概念，验证了正/反控制门簇在可逆网络级联中的优越性。

第 8 章提出了可逆函数复杂性网络综合方法。该方法根据可逆函数的输出排列，逐次交换输出向量，在交换过程中减少函数的复杂性，完成可逆网络的构建与优化。

第 9 章给出了一种可逆函数复杂性网络综合方法，并对一些具有代表性的可逆函数进行了综合。

第 10 章给出了不可逆逻辑函数转化为可逆函数的方法，并针对扩展的可逆逻辑门(MCMT 门)给出了相应转化实例。

第 11 章给出了可逆网络的优化方法。运用模板的方式等价替换可逆网络中的某一部分可逆逻辑门，减少可逆逻辑门的数量，优化可逆网络。

第 12 章主要介绍了通过 PPRM 扩展式综合可逆网络的方法。该方法通过识别候选因子，把候选因子替换成为新的 Reed-Muller 展开式，来判断能否优化可逆网络。

作者无意在本书中简单罗列近年来可逆逻辑综合的方法，而试图以可逆门级联为主线，从基本理论出发，以简单可逆逻辑门级联为基础，逐步拓展可逆门的种类，引入相关的可逆逻辑综合方法，反映近年来国际国内可逆逻辑综合研究成果，其中以作者和课题组成员近年来所做的工作为主。

国家自然科学基金(60873069)、南通大学学术著作出版基金、南通大学信息与通信工程学科科研项目基金，江苏省高等学校优秀科技创新团队项目基金为本书的出版和相关研究工作提供了资金保证。

感谢中国科学院计算技术研究所倪光南院士、清华大学龙桂鲁教授、南京大学宋方敏教授为本书出版给予推荐；感谢南京航空航天大学秦小麟教授、南通大学包志华校长和景为平教授、南京理工大学刘凤玉教授、南京大学许满武教授一直对作者的研究工作给予支持、指导和帮助。感谢 Maslov 博士、Yang 教授、Miller 教授、陈汉武教授、李志强博士、张小颖博士等诸多本领域学者以及研究生朱文颖和倪丽

惠同学的研究成果为本书提供相关素材。感谢我的夫人张义清女士对本书作出贡献以及对我工作上持之以恒地给予理解和支持。特别感谢吕彦鸣教授等老师和朋友，感谢他们多年来给予的专业上的指导、生活上的照顾、工作上的支持和精神上的鼓励。感谢南通大学计算机科学与技术学院支持和帮助我的同仁，他们为我的研究工作创造了良好的环境，并给予充分的时间保障，让我的研究得以顺利进行。

在本书的写作过程中，研究生倪丽惠同学对本书的书稿进行了细致的校对和修正，在这里表示衷心感谢。

由于可逆逻辑综合的研究尚未成熟，加之写作时间仓促、作者水平有限、部分内容还是课题组所取得的阶段性研究成果，不妥之处在所难免，殷切期待读者给予批评指正。

管致锦

2010 年 10 月 1 日于南通

目　录

第1章 绪 论

可逆计算理论是基于保持命题规则的可逆转性。目前可逆计算在计算处理过程中还不能在功能和结构方面达到满意的效果，其主要原因是抽象计算系统的行为与物理法则之间没有得到相应的匹配。构造等价可逆网络是解决上述相关问题的关键内容之一。

1.1 引 言

计算复杂性是求解一个计算问题所需要的时间和空间量(Turing，1936；Church，1936)，时间和空间量是计算的重要资源；计算过程中还有一类资源往往会被人们忽略，那就是能量。可逆计算(von Neumann，1966；Landauer，1961；Bennett，1973，1982；Maslov et al.，2004)最初的提出就是为了解决计算机中的能量消耗问题。

对信息、能耗和计算之间关系的研究经历了很长的历史。主要的工作始于Landauer(1961)的论文《计算过程的不可逆性与热量的产生》，该文提出了著名的Landauer原理。事实上，1929年Szilard(1929)的论文和von Neumann(1949)的演讲已经提出了接近于Landaure原理的结论，但还没有找到擦除信息需要消耗能量的本质。

计算过程的能量消耗与计算的可逆性有着必然的联系(Landauer，1961)。20世纪60年代以来，计算机硬件以惊人的速度发展，1965年Moore把这种现象概括为一条规律(Wikipedia，2006)，即Moore定律。Moore定律在几十年里都近似成立。然而，大多数业内人士认为，Moore定律将在21世纪的前20年内结束(Chen，2003)。其主要原因是：一方面，电子器件越做越小，功能会受到量子效应的干扰；另一方面，单位面积中器件的数量增加，产生的热量会越来越多。这些将会使硅芯片的发展最终走到极限。

Landauer(1961)最早考虑了能耗导致计算机芯片发热的问题，他研究了能耗的来源，指出能耗产生于计算过程中的不可逆操作。例如，对两位的异或操作，因为只有一位的输出，这一过程损失了一个自由度，因此是不可逆的，按照热力学理论，必然会产生一定的热量。Keyes和Landauer(1970)证明了每一位(bit)不可逆信息的丢失会产生$kT\lg 2$焦的热量，其中k是Boltzmann常量、T是热力学温度。这种热量的消耗对于每一信息位来说看起来很小(2.9×10^{-21} J)，但不可忽略不

计。由于信息的丢失使得热量的产生呈指数增长，在未来的集成电路设计中，热量的产生是特别要考虑的。Stinson 和 Rusu(2003)给出了 Madison Itanium-2 处理器信息丢失发热的精确计算。为了避免这种逻辑上的不可逆性，Landauer 认为可以对异或门的操作进行简单改进，即保留一个无用的信息位(或称垃圾信息)，该操作就变为可逆。就是说，逻辑上消除能耗的关键是将不可逆操作改造为可逆操作。

Bennett(1973)更严格地考虑了可逆计算的问题。经典计算机实际上就是一个通用图灵机(Turing, 1936)，通用图灵机是计算机的抽象数学模型，图灵机的模型是不可逆的。Bennett(1973)证明了一个基本结论，即对所有不可逆的通用图灵机，都可以找到对应的可逆图灵机，使得两者具有完全相同的计算能力。也就是说，计算机中的每步操作都可以变为可逆操作。

早在 20 世纪 70 年代，可逆操作就与量子计算建立了紧密的联系，因为所有的量子计算必须是可逆的(David,1998)，在量子力学中，它可以用一个幺正变换来代表。Benioff(1982)最早用量子力学来描述可逆计算机。1982 年，Fredkin 和 Toffoli(1982)设计了一种没有信息量损失的方案，引入了计算的可逆网络模型。考虑到传统逻辑门(如 AND、OR 门等)通常有两个输入和一个输出，是不可逆的，Fredkin 和 Toffoli(1982)设想，如果人们作出安排，使它既能传递逻辑门的输出值，也能传递它的输入值，这样就不会有信息位丢失。按照 Bennett 的理论，使用这种逻辑门设计的计算机能计算常规计算机所能计算的任何事情。因此，Fredkin 和 Toffoli 找到了使计算可逆的方法。Feynman(1986)发明了一种序列可逆计算的全量子模型，这一工作大大推动了量子计算研究的发展。在大约同一时间，Charles 等(1985)和他在加利福尼亚州的同事描述了一种新的叫做 MOSFET 的实现可逆计算的新技术，这一技术只要求很少数量的大感应器，用来起隔断作用，使得制造和测试可逆芯片设计的实验变得容易了。然而，在可逆计算能够成为超省能源、高性能计算的一个实用依据之前，还有很多挑战性的研究工作需要去解决，这些将在 1.3 节加以介绍。

1.2 可逆计算

可逆计算是一门新兴的交叉学科，其研究角度各有不同，并产生了不同的流派。但不论从哪个角度进行研究，其基础都是可逆逻辑，基本的计算和命题规则都需要保持可逆性。

按照 Toffoli(1980)的观点，如果一个动态系统从它的状态集合任意一点能够唯一地及时按照原来的轨迹返回，就说这个动态系统是可逆的。换句话说，如果一个动态半群能够扩充成一个群，就说这个动态系统是可逆的(George, 2004)。

通常情况下，抽象计算是不可逆过程，因为它可能是多对一函数的对应关系。

因此，对于一个在物理系统中通过数字网络意义下的处理过程实现的抽象计算任务，在建模层面需要由给定计算过程的不可逆性替换物理法则的可逆性。在传统的方法中，这种转换是在低级的物理层面通过逻辑门完成的。这样的物理变换过程涉及热量转换过程的具体问题，超出了通常计算模型概念的范畴。

在任何数字计算机中，一个 0 和 1 的数组代表一个数。计算机中的每个操作对应着相应的位操作，例如，从 0 到 1 翻转为 0 或 1。本质上，计算机是由成千上万实现逻辑操作的门组成的。在大多数情况下，这些逻辑运算是所谓“不可逆”的。也就是说，每次一个逻辑操作(功能)的执行，有关的信息输入信息可能被删除。因此，我们不能从得到的输出推断出唯一的输入。

如果一个逻辑门是不可逆的，则部分输入信息在逻辑门运算的时候将不可恢复地丢失掉，或者说某些信息被擦除了。但在可逆计算中，不存在信息的擦除，因为输入信息可由输出信息推知。换句话说，计算是可逆的等价于计算过程中没有信息被擦除。所谓信息被擦除，是指由计算的输出状态无法反推回输入状态。例如，传统的“OR”门，如果输出是 0，可知两个输入都是 0；如果输出是 1，由于其三种输入状态(0，1)、(1，0)、(1，1)的输出结果都为 1，所以无法确定原始输入。如果一个逻辑门网络是可逆的，可以从输出结果推知输入结果；反之亦然。可逆布尔网络，输入和输出数目是相等的。传统的逻辑“或”门和“与”门都是不可逆的，有 3/4 输出和输入不一一对应。同样，“异或”门、“与非”门和“或非”门也是不可逆的。而“非”门是可逆逻辑门，因为给定其输出就可以确定其输入值。

Toffoli(1980)阐述了一般计算模型下的不可逆行为与机器层面上的可逆性之间的关系，解决了物理定律的可逆性与计算机运算的不可逆性如何统一的问题。通常可以用因果关系网络图的形式表示一个函数组合(Wasaki，1988；王锵和石纯一，1997)，这是一个基本的非循环有向图。这样的构造中，因果关系网是“自由环”，即它们不包含循环路径。一个组合网络是一个不包含无限路径因果关系的网络。一个有限因果关系网络等同于一个组合的网络。如果一个因果关系网络能够通过可逆组合实现，就说这个因果关系网络是可逆的。一个可逆的组合网络总可以定义为一个可逆函数。因此，在组合网络结构中，可逆性的形式与可颠倒性的形式是一致的。

可逆计算的研究告诉我们，普通的不可逆逻辑运算会引起一个基本最小单位的能量损耗(Landauer，1961)，该现象本身并不是由于热噪声引起的。这一事实将影响未来几十年内计算机性能的发展。然而，基于可逆逻辑运算的计算机可以对一部分信号能量进行重新利用，并且随着硬件质量的提升，理论上能够重新利用的信号能量可以任意地接近于 100%，这就为在一个给定功率损耗水平内任意高性能计算机的实现提供了可能。自从这种方法的理论可行性首先由 Bennett (1973)提出后，对于怎样设计和实现基于可逆逻辑实用机器的理解有了极大的提

高。但是目前有很多有意义的、具有挑战性的研究工作需要做(Frank, 2005):①快速廉价且绝热能量系数比晶体管小得多的转换装置;②高可逆性的时钟系统;③可逆逻辑设计算法、规模、优化及代价等。本书主要讨论上述第三个问题,并给出一系列解决方案。

1.3 可逆计算中的逻辑综合

1.3.1 可逆逻辑综合的概念

可逆逻辑综合是可逆计算的重要研究内容(Andrel et al., 2002; Miller et al., 2003a; 2003b; Maslov, 2003; 2003a; 2003b)。可逆逻辑综合,就是用给定的可逆逻辑门,按照可逆网络无扇出、无反馈等约束条件和限制,实现相应的可逆逻辑网络,并使得代价尽可能小。

可逆逻辑门的级联是可逆逻辑综合的关键问题之一。可逆逻辑门网络是输入数与输出数相等,并且输入向量与输出向量为一一映射的可逆逻辑门集合。因此,输入向量的状态可以唯一地被输出向量重构。通过函数的方式描述即为:如果函数的每一个输入向量唯一地映射一个输出向量,则称该函数是可逆的。一个 n 变量的可逆函数也可以定义为整数集 $\{0,1,\cdots,2^n-1\}$ 的自身映射。一个不可逆函数总可以通过变换找到它的可逆函数,即可以把不可逆网络变为可逆网络,但一般需要在输入端添加相应的常量,在输出端添加无用输出信息。在可逆逻辑综合问题的研究中,不只是为了找寻构造可逆网络的方法,而且要使得构造代价尽可能小。可逆逻辑门的数量和无用输出信息输出的数量是影响可逆门逻辑级联代价的重要因素,也是衡量可逆逻辑综合好坏的主要依据。也就是说,一个较优的可逆逻辑综合算法既要保证可逆逻辑综合过程中使用的可逆逻辑门数尽可能少,同时也要使添加的无用输出信息数尽可能少。实现可逆网络的每一种技术,都需要有一个合理的代价。

1.3.2 可逆逻辑综合的意义

可逆逻辑综合是可逆计算研究的关键问题之一,它是量子计算和量子信息技术研究的重要组成部分,并在低功耗网络设计、信息安全、纳米技术等其他一些现代科学领域有着重要应用(Nielsen et al., 2000; Picton, 2000; Merkle, 1993; Peres, 1985; Long et al., 2001)。可逆逻辑综合由于潜在的巨大实际应用价值和重大的科学理论意义,正引起越来越多的关注。

传统逻辑的不可逆性是造成集成电路发热的重要原因,也是影响集成电路发展的主要因素。为了避免这种不可逆性,可以对"异或"门的操作进行改进,即保留

(添加)一个无用位,该操作就变为可逆。为了降低能耗,可以将不可逆操作改造为可逆操作。由于可逆逻辑门都是可逆的,可以用可逆的设计方法级联可逆逻辑门网络,使得不会因信息丢失而产生热耗散,从理论上解决芯片的发热问题。因此,可逆性成为未来网络设计的基本特性之一。可逆逻辑设计是未来低功耗网络设计的基础。

量子计算可以解决多项式时间复杂性难度的问题,所有的量子计算必须是可逆的(Nielsen et al., 2000; Gershenfeld et al., 1998)。因此,基于可逆逻辑的研究,对未来量子信息技术的发展是十分有益的。可逆逻辑设计方法可以推出量子可逆网络结构的方法,以此产生更强大的计算能力。不只是量子信息技术具有可逆性(Smolin et al., 1996; Miller et al., 2003a; Kim et al., 2000; Kim, 2002; Price et al., 1999),在其他一些的现代科学技术领域,如在低功耗 CMOS 的设计技术(Feynman, 1986; Merkle, 1993; Rentergem et al., 2005)、光子技术(Picton, 2000)、热力学技术(Merkle et al., 1996)、纳米技术(Merkle, 1993)和 DNA 技术(Thapliyal et al., 2005)中,都应用了可逆实现。

如果能将集成电路变为可逆网络,则它们产生的热量会更少,消耗的能量也将变少。采用可逆计算的信息技术领域将对全社会的节能降耗产生重要的意义。

如果接受可逆计算的概念,可以开始尝试一些革命性的想法。因为热量问题要求目前的网络只能是二维的,而采用可逆逻辑设计的无热网络,使得制造大型的三维网络成为可能。理论上,没有任何尺寸上的限制,计算能力也将没有限制。

研究可逆逻辑综合的理论和方法,能够让新兴的相关技术领域通过使用可逆门网络的级联结果得以更好地发展。

因此,可逆逻辑综合规模与代价的研究具有重要的理论意义和实际的应用价值。

1.4 可逆逻辑综合中的主要问题

可逆计算中的逻辑综合是近年来发展起来的新研究领域,是交叉性很强的学科,有诸多问题需要进行研究。主要表现在可逆逻辑设计算法、规模、优化及代价等。本节将对一些关键问题进行归纳和概括。

1.4.1 可逆逻辑门的级联

传统数字电路设计中的逻辑门多数都是不可逆操作。例如,逻辑门 AND、OR、XOR 和 NOT 中,只有 NOT 门是可逆的。要设计可逆网络,需要使用可逆逻辑门集合。在最近二十多年中,已经产生了几种可逆逻辑门,如控制非门(Con-

trolled-Not，即 CNOT 门)(Feynman，1985)、Toffoli 门(Toffoli，1980)和 Fredkin 门(Fredkin et al.，1982)等。这些可逆逻辑门从各个角度已经有很多研究。关于可逆逻辑门的级联，Shende 等(2002)提出了一个 3 输入变量的综合方法。Iwama 等(2002)给出了 CNOT 网络的转换规则，这些转换可以应用到可逆逻辑的综合上。Miller(2002)应用谱技术找到了接近最优的网络。Yang 等(2005a)给出了 3 输入/输出精确的综合方法。Mishchenko 和 Perkowski(2002)提出了可逆波级联的规则结构，并且证明了与用 ESOP 积项相比，这样的结构不需要更多级联函数。已有的方法要么受到约束条件很强的限制，要么不具有完备性，要么级联的规模太小。人们一直希望找到更好的综合方法。

1.4.2 最小代价问题及其实现

在可逆逻辑综合问题的研究中，一方面要找到可逆网络的实现方法，另一方面要尽可能地减小可逆网络的实现代价。实现可逆逻辑网络的每一种技术，都需要有一个合理的代价。可逆门的数量和无用输出信息输出的数量是影响可逆逻辑综合代价的重要因素，也是衡量可逆逻辑综合过程好坏的主要依据。所以，可逆网络代价问题在可逆计算的逻辑综合研究中具有重要意义和实际应用价值。龙桂鲁等提出了初始化量子寄存器方案(Long et al.，2001)，该方案在没有引入附加量子位的情况下，只需要 $O(Nn^2)$ 标准的 1 位和 2 位可逆门就能实现。Barenco 等(1995)给出了利用简单的单比特量子门和两比特 CNOT 门构造任意量子酉变换的方法，并给出了 4 个比特以下情况的结果。龙桂鲁等发展了 Barenco 等的方法，给出了任意比特数目的量子体系的酉变换的分解的解析公式(Liu et al.，2008)。利用广义量子干涉原理，龙桂鲁提出了对偶量子计算机的概念(龙桂鲁等，2008)。对偶计算机的明显特点是允许非酉的变换，Gudder(2007)给出了对偶量子计算机的数学理论，并且证明了任意有界线性变换都可以在对偶量子计算机的广义量子门中实现。杜鸿科等给出了无穷维下广义量子门的性质(Wang et al.，2008)。邱道文等研究了对偶量子计算机的数学理论(Zou et al.，2009)，曹怀信等给出了复数广义量子门的数学性质，以及任意广义量子门的构造方法(Cao et al.，2010)。Mottonen 等(2004)提出了基于余弦-正弦矩阵分解的最小化基本门序列方法。Vartiainen(2004)通过可逆门的分解消除多可逆逻辑门中多余的控制位，得到总数较少的基本可逆门，以优化可逆门的实现。Tucci(1999)提出了化简任意幺正矩阵 U 为一个基本操作序列的算法。

实际上，网络代价的计算在不同的技术中是不一样的。目前，不同研究领域对网络代价的计算还不能做到信息共享，部分原因是研究人员根据特定的设备产生相应的网络代价计算方法。使用不同可逆逻辑门模型实现网络综合的代价也不同。常用的可逆逻辑门有 Toffoli 门、Fredkin 门和 Feynman 门等。Maslov 等