

基于正反控制模型的可逆逻辑综合

管致锦^{1),2)} 秦小麟¹⁾ 施 佺²⁾ 郑吉平³⁾

¹⁾(南京航空航天大学信息科学与技术学院 南京 210016)

²⁾(南通大学计算机科学与技术学院 江苏 南通 226019)

³⁾(清华大学计算机科学与技术系 北京 100084)

摘 要 对一般 Toffoli 门进行了衍变和推广,给出了一个正反控制可逆级联模型(PNCRC),该模型拥有五种基本线型,并能正反控制目标位的输出.基于该模型给出了相应的可逆综合算法.对输入数不大于 16 的 NCMC Benchmark 函数进行测试并与已有的可逆综合方法比较,结果表明,利用该模型进行的可逆综合,垃圾信息数和可逆门数的优化效果都具有一定程度的改善.

关键词 可逆逻辑;可逆门;垃圾信息;正反控制;可逆网络

中图法分类号 TP302

Reversible Logic Synthesis with Positive/Negative Control Model

GUAN Zhi-Jin^{1),2)} QIN Xiao-Lin¹⁾ SHI Quan²⁾ ZHENG Ji-Ping³⁾

¹⁾(College of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016)

²⁾(College of Computer Science and Technology, Nantong University, Nantong, Jiangsu 226019)

³⁾(Department of Computer Science and Technology, Tsinghua University, Beijing 100084)

Abstract Based on traditional Toffoli gate, a new reversible network cascade model PNCRC is proposed. The model consists of five line-styles, and it is able to control output of target bits with positive/negative way effectively. A reversible synthesis algorithm corresponding to the proposed model is also designed in this paper. Compared to the previously reported results, some experiments on NCMC Benchmark functions (less than or equal 16 variables) show that PNCRC decrease the number of garbage output and number of reversible gates as a whole.

Keywords reversible logic; quantum gate; garbage; positive/negative control; reversible network

1 引 言

可逆逻辑综合是一个新兴的研究领域,它是量子计算和量子信息技术研究的重要组成部分^[1],并在低功耗电路设计、信息安全、纳米技术等其它一些现代科学领域有着重要应用^[2-4].由于它潜在的巨大

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.

可逆逻辑综合,就是用给定的可逆门和可逆网络的约束条件及限制等,实现所需要的可逆逻辑网络,并使得代价尽可能小.可逆逻辑综合使用的基本可逆逻辑门与经典的非可逆逻辑综合使用的逻辑门有着根本的不同.

收稿日期:2006-08-24;最终修改稿收到日期:2007-12-11.本课题得到国家自然科学基金(60673127)、国家“八六三”高技术研究发展计划项目基金(2007AA01Z404)、江苏省高校自然科学基金(05KJB520107)资助.管致锦,男,1962年生,博士研究生,教授,主要研究领域为可逆计算、信息安全和逻辑综合. E-mail: guan_zj@nuaa.edu.cn. 秦小麟,男,1953年生,教授,博士生导师,主要研究领域为数据库技术、空间信息处理、信息安全技术. 施 佺,男,1973年生,硕士,副教授,研究方向为网络数据库、软件工程. 郑吉平,男,1979年生,博士,现在清华大学从事博士后研究工作,主要研究方向为场境感知的智能数据管理、数据库安全.

可逆逻辑网络为输入数与输出数相等并且输入向量与输出向量是一一映射的网络. 因此, 输入向量的状态可以唯一地被输出向量重构. 通过函数的方式可描述为: 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 $\{0, 1, 2, \dots, 2^n - 1\}$ 自身的映射. 一个不可逆逻辑函数总可以通过变换找到它的可逆函数, 一般地, 会因此产生相应的垃圾信息.

在可逆逻辑综合的研究中, 一方面要找到可逆网络的实现方法, 另一方面要考虑如何在实现可逆网络过程中尽可能花费较低的代价. 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. 可逆门的数量和垃圾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. 在很多技术中只要增加一个可逆门或无用输出信息位就可能给网络的实现带来昂贵的代价, 甚至不可能实现. 所以, 可逆网络代价问题在量子计算等领域的研究中具有重要意义和实际应用价值. 龙桂鲁等人提出了一个初始化量子寄存器方案, 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^[5]. Mottonen 等人提出了基于余弦-正弦矩阵分解的最小化基本门序列方法^[6]. Vartiainen 通过量子门的分解消除多量子位门中多余的控制位, 得到总数较少的基本量子门, 以优化量子门的实现^[7]. Tucci 提出了化简任意幺正矩阵 U 为一个基本操作序列的算法^[8].

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, 部分原因是网络代价的计算是针对他们特定的设备而设计的. Maslov 等人对可逆逻辑综合代价和规模进行了详细分析^[9]. Barenco 等人提出了网络代价的近似计算方法^[10].

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^[11-13].

近年来, 随着量子信息和集成电路等技术的迅速发展, 可逆逻辑综合才真正开始被重视, 尚处于很不完善的发展阶段. Khlopotine 等人运用复合与分解的方法进行了可逆逻辑综合的研究^[14]. Miller 提出了基于置换的可逆逻辑综合算法^[15]. Shende 提出了 3 输入变量的综合方法^[16]. Khan 和 Perkowski 首先把分解因式方法用到可逆逻辑设计中^[17]. Iwama 等人给出了以 CNOT 为基础的网络转换规

则^[18]. 该方法的输入部分是一个以 Toffoli 门为基本元素的可逆逻辑网络, 其输出是一个标准型的 Toffoli 门可逆逻辑网络. 这个标准型是 PPRM 的直接可逆实现, 同时也是一个 Zhegalkin 多项式. Iwama 证明了任何一个可逆网络都能通过确定的可逆操作得到一个标准型. 因此, 标准型可以转化成一个最小化网络. 遗憾的是, 他们没有给出任何通过转换化简网络的方法. Perkowski 等人提出的规则结构综合方法^[19], 其主要特点是建立常规的可逆组合逻辑设计输出目标, 然后用已知的逻辑综合技术去建立可逆的规范. 这样的方法通常会产生大量的垃圾信息. Miller 应用谱技术找到了接近最优的可逆网络^[20]. Mishchenko 和 Perkowski 提出了可逆波级联的规则结构^[21], 并且证明了实现这样的结构需要的级联函数比 ESOP 积项要少. 但这个方法只适合于小规模可逆逻辑综合, 而且不容易测量, 同时它还需要一个可逆的规范.

对于可逆逻辑综合, 目前尚缺少有效的算法. Shende 等人提出的最优穷举算法太慢^[22], Miller, Maslov^[23], Kerntopf^[24] 给出了几个启发式算法, 但这些算法没有得到很好的验证, 而且它们大多需要附加另外的模板进行处理, 其相应的代价也比较高. Perkowski 等人提出了一类规则对称结构函数^[25], 在带有相关垃圾信息的完全可逆门规则结构中实现了任意对称函数的优化. 因为可以通过重复输入变量使每一个逻辑函数对称, 该方法是用任意的多输入多输出布尔函数实现任意函数相关附加输出门的最小化, 但该方法只是在可逆门的数量较小的时候或带有任意输出的不完全特殊函数的综合方面有优势.

可逆门级联模型是可逆逻辑综合的基础. 目前, 可逆门的级联模型及其相关算法所能实现的综合存在着网络规模小、综合代价高、综合过程中时空复杂度高等一系列问题.

本文给出了一个新的可逆门级联模型——正反控制级联模型, 并给出了相应的可逆综合算法; 完成了现有可逆综合的 NCMC Benchmark 实验 (变量不大于 16). 结果表明该模型在减少垃圾数量和可逆门的数量方面是有效的.

2 基本定义

2.1 多输出函数的表示

在布尔代数中, 含有两个常数 0 和 1. n 变量的布尔函数 $f(x_1, x_2, \dots, x_n)$ 的表示方法之一是用真

值表表示,表的结构为 $n+1$ 列和 2^n 行,表的最右边一列函数值由对应的每一行的 n 列输入给定. 对于一个 n 变量的布尔函数,不同输入数是 2^n ,因此这个结构的高度是 2^n ,或者说这个表有 2^n 行. 这里所有的 2^n 个布尔模式是按字典排序的. 可以看出,真值表自始至终需要大量的存储空间. 为了简化格式,也可以使用真值向量的方法. n 变量函数的真值向量是长度为 2^n 的布尔数序列.

n 输入 k 输出的多输出函数 $(f_1(x_1, x_2, \cdots, x_n), f_2(x_1, x_2, \cdots, x_n), \cdots, f_k(x_1, x_2, \cdots, x_n))$ 是一个 $n+k$ 列的真值表,这里前 n 列为输入模式,后 k 列是输出模式. 即 n 输入 k 输出的多输出布尔函数是一个 k 布尔值的向量函数. 一个多输出函数同样可以写成一个真值向量. 该向量 2^n 个元素中的每一个元素分别是 $[0, 1, \cdots, 2^n - 1]$ 中的一个整数,它们的二进制表示是输出模式.

例 1. 表 1 给出的 3 输入 3 输出函数可以用真值向量 $[0, 1, 2, 3, 4, 5, 7, 6]$ 表示.

表 1 3 输入 3 输出函数真值表					
x_1	x_2	x_3	f_1	f_2	f_3
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

一个布尔函数同样可用“与 (&)”、“或 (or)”、“非 (¬)”和“异或 (⊕)”操作的运算符以公式的形式表示.

2.2 可逆逻辑函数

可逆逻辑理论的主要研究对象是可逆函数. 下面给出可逆函数的定义.

定义 1. n 布尔变量的多输出函数 $F(x_1, x_2, \cdots, x_n)$ 是可逆的,如果输出数等于输入数且任一输出模式存在一个唯一的原象,即可逆函数是输入向量集合的一个置换.

例 2. 公式 $(x, y) \rightarrow (\bar{x}, x \oplus y)$ 和真值向量 $[2, 3, 1, 0]$ 给出了一个 2 输入 2 输出的可逆函数. 这个例子的正确性可通过真值表(表 2)得以验证.

表 2 $(x, y) \rightarrow (\bar{x}, x \oplus y)$ 的真值表			
x	y	\bar{x}	$x \oplus y$
0	0	1	0
0	1	1	1
1	0	0	1
1	1	0	0

例 3. 2 输入 1 输出函数 $(x, y) \rightarrow x \oplus y$ 是不可逆的,因为它不是一个 n 输入 n 输出的函数. 但是,由例 2 知,可以很容易地通过添加输出 \bar{x} 使函数可逆.

例 4. 函数 $(x, y) \rightarrow xy$ 是不可逆的,通过添加一个单输出也不可能使其可逆,但可以通过添加一个输入和两个输出使函数可逆. 如表 3.

表 3 $(x, y) \rightarrow xy$ 添加输入输出后的真值表					
x	y	z	x	y	$z \oplus xy$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

前面的例子说明,要使函数可逆,添加输入/输出是必需的,因此有下面的定义.

定义 2. 添加输出数使一个 n 输入 k 输出函数 $((n, k) (k \leq n)$ 函数)可逆,这些被添加的输出信息称为垃圾信息.

用“常量输入”表示输入预先设置的值添加到一个 (n, k) 函数上使其可逆. 在例 4 中添加了一个单常量输入,也就是带有值为 0 的变量 z .

下面通过简单的公式可以看出垃圾信息输出和“常量输入”之间的关系.

输入 + 常量输入 = 输出 + 垃圾信息.

2.3 可逆网络的结构

一个可逆网络的结构是 S 个可逆逻辑门 G_1, G_2, \cdots, G_S 的组合,这里没有两个门在相同时间被激活, G_i 只有在 G_{i-1} 产生一个输出后才工作. 即一个可逆网络在可逆门感应集合上通过信号传播定义了一个总的时序. 一般地,信号在网络中从左向右传播,无扇出和无反馈是对构建可逆网络结构的一个自然约束. 可逆逻辑网络结构如图 1.

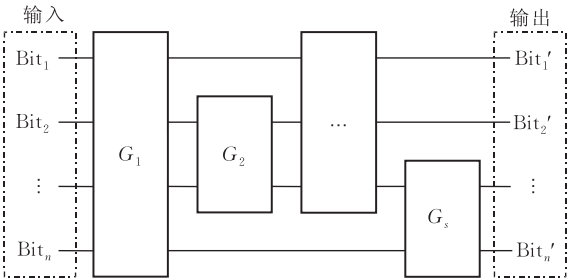


图 1 可逆逻辑网络结构图

可逆网络的结构是量子门构造的一个级联. 可

逆的限制使得级联网络结构的设计非常困难,为此,首先给出下面的引理.

引理 1. 可逆函数 f 给出的一个网络,如果信号是向后传播的,则输出函数是函数 f 的反函数 f^{-1} .

事实上,信号的向后传播和找到反函数本质上是相同的操作.

当构造一个可逆网络拓扑结构的时候,所有网络设计可能的集合都受到很强的限制.但可以变换当前的门,而变换本身对门的规模要求很高.

可逆门的规模是一个自然数,这个自然数通过函数的输入/输出数表现出来.

2.4 可逆逻辑门

按照本文的需求,只给出 Toffoli 门的定义^[26].

定义 3. 对于变量域集合 $\{x_1, x_2, \dots, x_n\}$,一般 Toffoli 门表示为 $TOF(C; T)$, 这里 $C = \{x_{i_1}^0, x_{i_2}^0, \dots, x_{i_k}^0\}$, $T = \{x_j\}$, $C \cap T = \emptyset$. Toffoli 门把布尔模式 $(x_1^0, x_2^0, \dots, x_n^0)$ 映射到 $(x_1^0, x_2^0, \dots, x_{j-1}^0, x_j^0 \oplus x_{i_1}^0 x_{i_2}^0 \dots x_{i_k}^0, x_{j+1}^0, \dots, x_n^0)$.

NOT 门 $TOF(x_j)$ 是没有控制位的 Toffoli 门; CNOT 门 $TOF(x_i; x_j)$, 也称 Feynman 门, 一般带有一个控制位; 原始的 Toffoli 门为 $TOF(x_{i_1}, x_{i_2}; x_j)$, 这样的 Toffoli 门带有两个控制位. 这三种门的表示见图 2, 带有更多控制门的描述与上面类似. 门的描述方法只是一种习惯, 与门的实现方法无关. 一般 Toffoli 门的集合被证明是完备的. 即任何可逆函数可以通过 Toffoli 门的级联实现.

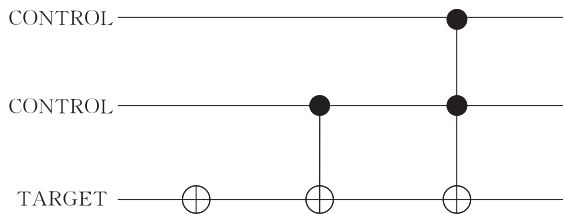


图 2 NOT 门、CNOT 门和 Toffoli 门

在可逆逻辑综合过程中, 因为 EXOR 使用的门可以描述成最简单形式, 并拥有如下操作性质:

$$a \oplus b = b \oplus a; a \oplus 0 = a; a \oplus 1 = \bar{a}; a \oplus a = 0.$$

这种方法允许启发式综合并且易于化简已经建立起来的网络.

3 正反控制的逆网络模型

要使一个多输出函数可逆, 可以有许多方法, 但每一种方法一般都需要一定数量的可逆逻辑门和不

同数量的垃圾信息位. 一般地, 使用不同网络模型建立的可逆网络, 垃圾信息位也不同.

选择可逆逻辑门的集合构造可逆网络, 就是对给定的多输出函数用设计的模型选择适当的可逆门级联可逆网络, 其过程可以通过下面的步骤实现. 首先, 通过使函数可逆找到最小的垃圾信息位(这个数目不依赖于综合模型). 然后, 通过一个总是与有效网络一起结束的过程对可逆函数进行综合. 如此可以保证垃圾信息位最小, 但产生的网络中级联的可逆门数可能会很大. 因此, 需要找到最小化垃圾信息位的可逆方法, 相应的变量数添加到 Don't cares 多输出函数中. 按照减少 Hamming 距离的思想, 通过选择可逆门, 最大限度减少距离的启发式思想对函数进行综合. 这种方法保证了垃圾信息位的最小化并能产生最优的可逆网络.

3.1 正反控制可逆级联模型(PNCRC)

本文在一般 Toffoli 门的基础上, 进行了衍变和推广, 得到一个新的可逆逻辑网络模型, 即正反控制可逆级联模型. 该模型的基本元素由两类控制线、一类目标线和一条无关线组成.

定义 4. 正反控制可逆级联模型结构的元素由下面五种线型构成(如图 3).

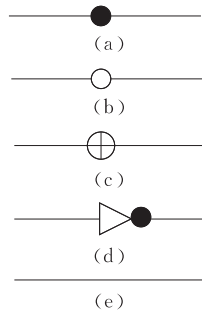


图 3 正反控制模型的 5 种基本线型

(1) 肯定控制线(图 3(a)). 如果在这条线上输入是 0, 则目标线的值将不改变. 如果输入是 1, 则其它的肯定/否定控制线确定在目标控制线上的值是否被否定. 通过肯定控制线的值不变.

(2) 否定控制线(图 3(b)). 如果在这条线上输入是 1, 则目标线的值将不改变. 如果输入是 0, 则其它的肯定/否定控制线确定在目标控制线上的值是否被否定. 通过否定控制线的值不变.

(3) 目标线(图 3(c)). 每一个门在位置 j 将只有一个目标线出现. 通过目标线的值受肯定/否定线控制.

(4) 否定线(图 3(d)). 通过否定线的值取反.

(5) 无关(Don't care)线(图 3(e)). 通过这条线

网络结构的一个块. 门 S^1 最后的 NOT 阵列称为 T . 如果 S^1 是 $\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}$ 之一, 则添加到 T 上.

3. 从网络中取下一个门 $S^2 \in S$. 如果 $S^2 \notin \{\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}\}$, 通过计算它与 S^2 的第一个 NOT 阵列做异或运算更新 T 阵列, 每条线保持 NOT 数模 2 的和. 如果 T 阵列中的 NOT 门遇到一个目标线或一个“Don’t care”线, 则可以通过这个门, 从 T 阵列删除发生的事件, 把它们添加到门的输出阵列.

4. 结合 T 阵列与 AND-EXOR 阵列建立一个新的块, 让 $S^1 \leftarrow S^2$, 执行第 2 步.

5. 如果 S^2 门是门 $\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}$ 之一, 则通过 S^2 与 T 的“异或”运算来更新 T 阵列. 让 $S^1 \leftarrow S^2$, 执行第 2 步.

6. 当 PNCRC 网络结构结束时, 把 T 阵列放到网络, 建立最后一个块.

容易看出, 描述块的网络组成等价于用门 S 构建网络. 裁剪网络块数是从初始的 S 网络门数减去从 S -网络集合 $\{\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}\}$ 加上 T 阵列的门数. 因此, NOT 门集合与结构的长度只能被减少.

NOT 门裁剪过程是一个加速处理的过程, 不影响将要完成的综合方法.

3.3 基于 PNCRC 模型的可逆综合

设 S 是所有可能的 n 输入可逆门的集合. 综合问题是用已知模型找到函数的一种实现方法, 用可逆门集合 S 的一个门序列写出该函数. 为解决这个问题, 借鉴文献[26], 通过一个递增的方法, 重复地选择可逆门, 逐步使其接近期望的函数. 为此, 需要测量两个函数接近的程度, 称其为两个函数之间的距离. 即选择可逆门使得函数到目标函数之间的距离递减, 继续这样的操作直到两函数之间的距离为零.

下面给出距离的相关定义.

定义 7. 函数 f 的局部实现是相同变量集合的任意函数 f' .

定义 8. 一个可逆函数和它的局部实现 f' 之间的距离是它们真值表的输出部分之间的 Hamming 距离.

定义 9. 函数 f 的误差是该函数到其恒等函数的距离.

例 6. 从可逆函数

$$f(x_1, x_2, x_3) = (x_1, \overline{x_1} \oplus x_2, x_3 \oplus x_1 \overline{x_2})$$

的真值表(表 4)可以看出, 一共有 6 个误差点(见下划线部分).

例 7. 前面例子中可逆函数的局部实现函数 $f'(x_1, x_2, x_3) = (x_1, x_2, x_3 \oplus x_1 \overline{x_2})$ 与函数 f 的距离是 4(见表 5).

表 5 $f'(x_1, x_2, x_3) = (x_1, x_2, x_3 \oplus x_1 \overline{x_2})$ 真值表					
x_1	x_2	x_3	f_1	f_2	f_3
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	<u>1</u>
1	0	1	1	0	<u>0</u>
1	1	0	1	1	0
1	1	1	1	1	1

前面的例子中有一个偶数数目的误差位, 并且 1-bits 误差位的数目与 0-bits 误差位的数目相等, 该结果不失一般性. Maslov 等人在文献[23]中给出了下面引理.

引理 2. 可逆函数的误差数是偶数. 在误差位中, 等于 1 的数目与等于 0 的数目相等.

证明. 给出可逆函数的真值表, 并考虑输出部分的列. 假设在这些列中出现的误差有 k 个 0 位和 s 个 1 位. 因为函数是可逆的, 真值表输出部分的每一列包含 2^{n-1} 个 0 位和 2^{n-1} 个 1 位. 因此这些列有 $(2^{n-1} - k)$ 个 0 位和 $(2^{n-1} - s)$ 个 1 位. 如果翻转函数的误差位, 它是 n 位的恒等函数(同样也是可逆的). 观察 0 和 1 的数量, 在所考虑的列中进行加 s 个 0 和 k 个 1 的操作. 修改后的真值表中, 0 和 1 的数目分别变为 $(2^{n-1} - k + s)$ 和 $(2^{n-1} - s + k)$. 因为函数是可逆的, 0 的数目与 1 的数目保持 2^{n-1} , 则有下面的方程:

$$2^{n-1} - k + s = 2^{n-1} - s + k = 2^{n-1}.$$

这个方程只有一个解 $k = s$. 因此, 该行中的误差总数是 $2k$, 是一个偶数. 对于每一个 n 输出列, 可给出同样的证明. 故, 总的误差数是一个偶数.

实际上, 上面证明给出了一个重要的事实, 即输出部分的每一列误差是一个偶数. 以此也可以得到另外一个结论, 一个可逆函数和它的局部实现之间的距离总是一个偶数. 不难看出 1 的数目与 0 的数目相同. 证毕.

因此, 对于可逆逻辑综合方法, 可以给出一个简单思想, 它将是后面启发式可逆综合的基础. 从一个恒等函数开始, 在集合 S 中找到一个门, 添加到部分实现 f' 中, 以减少与 f 的距离. 有时可能找不到能够降低与 f 距离的可逆门. 但在任何时候都可以选择至少不增加与 f 之间距离的可逆门. 见例 8.

例 8. 可逆函数和恒等函数 $(x, y) \rightarrow (\overline{y}, \overline{x})$, 具有不改善函数距离可逆门的性质.

使用步的概念对级联网络增加可逆门. 因此, 在

网络中步数就是构造门数. 如果距离增加一步称为正的, 距离减少一步则称为负的.

引理 3. 如果函数 f 与 f' 之间的距离大于 0 (局部实现函数 f' 仍然不是函数 f 本身), 在 S 中存在门 f' 到 f'' 的变换, 使得 f 与 f'' 之间的距离小于或等于 f 与 f' 之间的距离.

证明. 设带有误差位 X 局部实现的真值表输出部分 $(a_1, a_2, \dots, a_{n-1}, X)$ 是一个串 (假设在第 n 个位置没有丢失). 让其与距离 -1 串 $(a_1, a_2, \dots, a_{n-1}, a_n)$ 相互交换, 这里 $a_n = \bar{X}$. 相应地, 使用门做线型 $4-a_1, 4-a_2, \dots, 4-a_{n-1}, 1$, 这里, 布尔数 a_1, a_2, \dots, a_{n-1} 作为自然数处理. 容易看出, 误差在第一个 $(n-1)$ 位出现不同, 由表 6 可见, 对于最后一位, 所有可能的交换都会发生. 所以, 得到一个 0 步或负步.

证毕.

表 6 改变 1 位的效果

X	a_n	a_n 的正确性	误差	误差的改变	步
0	1	Y	1	1	0
1	0	Y	1	1	0
0	1	N	2	0	-2
1	0	N	2	0	-3

定理 1. 存在一个增加可逆门的综合方法, 仅当对函数距离实现非正变化, 这样的方法对任意可逆函数都收敛.

下面给出基于 PNCRC 模型的综合算法.

1. 初始化“最大移动”数.
2. 当所有 S 门中距离都大于 0 时, 则找“最大移动”步. 从剩下所有步中, 找出最大移动步, 作为步 2.
3. 在列表中有“最大移动”门对, 对 2 门序列进行搜索, 最大可能地改善存在于局部实现与可逆函数自身之间的距离. 如果这样的对是唯一的, 附加第 1 个门到级联网络, 返回到步 2.
4. 如果两个或更多的门对的距离有同样改善, 激活从每一对中找到第 3 个最好的门函数. 如果其中的一对有更好的第 3 个门 (最小的距离函数), 则选择这一对. 所选对的第 1 个门附加到级联网络, 并返回到步 2.
5. 如果第 3 个最好门函数中没能找到一个对, 而第 3 步给出了一个更好的改善结果, 则为第 1 个门取一对作为最好的结果, 返回到步 2.
6. 如果指派的门仍然没有被选择, 从步 2 产生的列表中取选择的门中第一对作为最好的结果. 返回到步 2.

因为有效的总是 0 步, 所以定理 1 中的情形距

离不会增加. 尽管这里尝试了每一个函数收敛的情况, 一般还不能保证这种方法的收敛性. 由于后面可能会给出的步数很大, 而距离只能通过最多两步减少. 所以使用这个算法, 可以保证函数收敛.

一般地, 一个 (n, n) 可逆函数 f_1, f_2, \dots, f_n 能够通过 $n!$ 中一种可能的设计实现. 假设这种情况发生, 函数输出的序列将不做任何改变. 在任意序中能够列举输出, 从而实现不同函数. 因此, 对于大变量函数的输出排列, 使用启发式对函数或它的补取输出排列给出最小误差. 如果是小变量可逆函数, 给出所有可能的排列以选择最好的结果.

例 9. 对于例 8 中可逆恒等函数 $(x, y) \rightarrow (\bar{y}, \bar{x})$, 没有输出交换, 至少要使用 3 个门为函数建立一个可逆网络: 步 1 是一个 0 步 (如前面例子中说明的那样). 因为最好每一种情况一次可预料至少一个输出位, 在两个输出位的每一个中有两个误差, 这需要至少 2 个以上的门. 所以理论上最小的是 3 门 (事实上, 这里的算法在步 3 中止). 一个带有输出排列的函数 $(x, y) \rightarrow (\bar{x}, \bar{y})$, 很容易用两步实现, 即步 1 1 负的和步 2 输入位.

4 基准测试及其结果分析

4.1 垃圾信息分析

一般地, 垃圾信息是在使函数可逆的过程处理前被引入的. 任何一种综合方法的垃圾信息输出值都可以调整, 这些调整会因为变量的不同导致变化结果复杂.

关于垃圾信息位的分析, 只集中考虑输出添加的垃圾信息. PNCRC 模型中垃圾信息的规模是 $(n+N)$, 这里 n 是多输出函数 f 的输入数, N 是函数的部分级联中顶点的级联数. 因此, 每一个顶点的级联本身没有导致新的垃圾信息位.

Khan、Perkowski 和 Mishchenk 等人提出了相似的模型结构, 其综合方法的垃圾信息结果在本质上是相同的. 这里计算了 PNCRC 模型的一些 Benchmark 函数的垃圾信息数. 表 7 概括了文献 [17, 21, 26] 提出的方法中使用 Benchmark 函数的结果, 并和 PNCRC 模型的垃圾信息做了比较.

表 7 几种方法垃圾信息数

函数名称	输入位数	输出位数	垃圾信息数及代价				Min garbage
			RWCG	RPGAG	KPG	PNCRC	
5xpl	7	10	38(7)	>28	53	31	0
9sym	9	1	60(9)	45	60	52	9
B12	15	9	43(15)	>120	120	84	13

(续 表)

函数名称	输入位数	输出位数	垃圾信息数及代价				Min garbage
			RWCG	RPGAG	KPG	PNCRC	
clip	9	5	72(9)	>45	N/A	44	6
In7	26	10	61(26)	>351	N/A	Nd	24
Rd53	5	3	19(5)	15	19	17	4
Rd73	7	3	43(7)	28	47	33	6
Rd84	8	4	66(8)	36	68	41	7
Sao2	10	4	38(10)	>55	52	35	10
T481	16	1	29(16)	>136	28	54	16
Vg2	25	8	209(25)	>325	217	Nd	24

表 7 中第 1 列为函数名,第 2 列和第 3 列分别是输入和输出位数,第 4 列是 Mishchenko 和 Perkowski 波级联方法的垃圾信息数,第 5 列是 Maslov 的 RPGAG 方法的垃圾信息数. 因为每个非对称函数可以通过添加新的输出使其对称,使函数可逆的过程可以预先用 Perkowski 提出的算法. 但一般这样的过程需要添加许多输入,导致每一个结果都需要较高的垃圾信息代价,这里用符号“>”去描述实际操作中垃圾量比较高的情况. 第 6 列是 Khan 系列门综合的垃圾信息代价. 第 7 列是 PNCRC 垃圾信息数,其中函数 In7 和 Vg2 由于其输入变量太大,这里没有进行测试(目前算法只实现不大于 16 变量的函数),所以用“Nd”标识. 第 8 列,添加最小垃圾信息数使相应的函数可逆.

最好,但 PNCRC 的方法在垃圾信息位的数量上有明显的改善. 在不同函数中 PNCRC 在门数和垃圾信息数方面不总是最优的. 但是,如果综合考虑 Benchmark 函数的门数和垃圾信息数,PNCRC 方法是有优势的.

表 8 几种方法的代价

函数名称	输入位数	输出位数	垃圾信息输出数量			代价		
			MP	RC	PN	MP	RC	PN
5xpl	7	10	38	0	12	31	43	36
9sym	9	1	56	9	24	52	60	57
Rd53	5	3	19	4	11	14	13	13
Rd73	7	3	43	6	14	36	36	38

表 8 中 MP、RC 和 PN 分别表示 Mishchenko-perkowski、RCMG 和 PNCRC 方法.

5 结 论

本文给出了正反控制可逆级联综合模型,并给出了相应的可逆综合算法. 部分 NCMC Benchmark 函数测试和结果分析表明,综合过程中标志可逆网络最小化代价的最重要因素,即可逆网络的垃圾信息和门的数量都取得了较为理想的效果. 目前 PNCRC 算法实现的规模只是在输入数不大于 16 的情况,将来的工作将在优化垃圾信息和门数的基础上提高可逆综合的规模.

参 考 文 献

[1] Nielsen M, Chuang I. Quantum Computation and Quantum Information. Cambridge, UK: Cambridge University Press, 2000

[2] Picton P. A universal architecture for multiple-valued reversible logic. Multiple-Valued Logic Journal, 2000, 153(5): 27-37

① Maslov D. Reversible logic synthesis benchmarks page. <http://www.cs.uvic.ca/~dmaslov/>, 2005

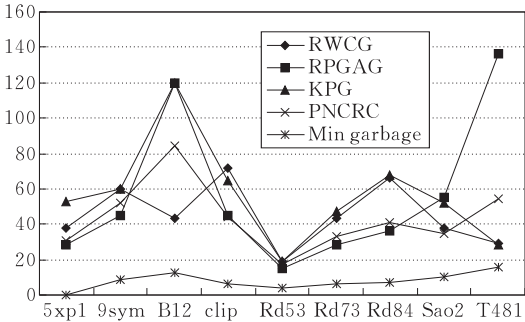


图 6 几种方法垃圾信息比较

从测试的结果分析看,PNCRC 的垃圾信息数与理论上的最小化相比还有很大差距. 但与已有的几种方法比较,PNCRC 在大部分函数上都具有优势.

4.2 基准测试

可逆逻辑综合是近几年才发展起来的研究领域,加之综合过程的复杂性,目前的 Benchmark 测试用例还不多. 本文采用的测试用例主要取自可逆逻辑综合基准页^①和文献[21,26]. 把 PNCRC 的结果与 Mishchenko-perkowski 和 RCMG 两个系统的结果进行了比较. 表 8 的比较结果表明,尽管 PNCRC 的代价与 Mishchenko 和 Perkowski 的相比不都是

- [3] Merkle R C. Two types of mechanical reversible logic. *Nano-technology*, 1993(4): 114-131
- [4] Peres A. Reversible logic and quantum computers. *Physical Review A*, 1985, 32(6): 3266-3276-10
- [5] Long G L, Sun Y. Efficient scheme for initializing a quantum register with an arbitrary superposed state. *Physical Review A*, 2001, 64(1): 014303-4
- [6] Mottonen M, Vartiainen J J, Bergholm V, Salomaa M M. Quantum circuits for general multiqubit gates. *Physical Review Letters*, 2004, 93(13): 130502-7
- [7] Vartiainen J J, Mottonen M, Salomaa M. Efficient decomposition of quantum gates. *Physical Review Letters*, 2004, 92(17): 177902-4
- [8] Tucci R R. *A Rudimentary Quantum Compiler* (2nd Ed.). Los Alamos eprint quant-ph, 1999: 9902062
- [9] Maslov D, Miller D M. Comparison of the cost metrics for reversible and quantum logic synthesis. *IET Computers & Digital Techniques*, 2007(2): 98-104
- [10] Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A, Weinfurter H. Elementary gates for quantum computation. *The American Physical Society*, 1995(52): 3457-3467
- [11] Toffoli T T. Reversible computing//*Proceedings of the 7th Colloquium on Automata, Languages and Programming*. Berlin, Germany, 1980: 632-644
- [12] Feynman R. Quantum mechanical computers. *Optic News*, 1985(11): 11-20
- [13] Fredkin E, Toffoli T. Conservative logic. *International Journal of Theoretical Physics*, 1982(21): 219-253
- [14] Khlopotine A, Perkowski M, Kerntopf P. Reversible logic synthesis by iterative compositions//*Proceedings of the International Workshop Logic and Synthesis*. New Orleans, Louisiana, USA, 2002: 261-266
- [15] Miller D M, Maslov D, Dueck G W. A transformation based algorithm for reversible logic synthesis//*Design Automation Conference*. Anaheim, California, USA, 2003: 318-323
- [16] Shende V V, Prasad A K, Markov I L, Hayes J P. Synthesis of reversible logic circuits. *IEEE Transactions on CAD*, 2003, 22(6): 723-729
- [17] Khan M H A, Perkowski M. Multi-output ESOP synthesis with cascades of new reversible gate family//*Proceedings of the International Symposium on Representations and Methodology of Future Computing Technologies*. Trier, Germany, 2003: 144-153
- [18] Iwama K, Kambayashi Y, Yamashita S. Transformation rules for designing CNOT-based quantum circuits//*Proceedings of the Design Automation Conference*. New Orleans, Louisiana, USA, 2002(149): 419-424
- [19] Perkowski M, Jozwiak L et al. A general decomposition for reversible logic//*Proceedings of the International Reed-Muller Workshop*. Starkville, Mississippi, USA, 2001: 119-138
- [20] Miller D M. Spectral and two-place decomposition techniques in reversible logic. *Lida Ray Technologies*, 2002, 45(2): 493-496
- [21] Mishchenko A, Perkowski M. Logic synthesis of reversible wave cascades//*Proceedings of International Workshop Logic and Synthesis*. New Orleans, Louisiana, USA, 2002: 197-202
- [22] Shende V V, Prasad A K et al. Reversible logic circuit synthesis//*Proceedings of the International Workshop Logic and Synthesis*. New Orleans, Louisiana, USA, 2002: 125-132
- [23] Maslov D, Dueck G W. Garbage in reversible design of multiple output functions//*Proceedings of the International Symposium on Representations and Methodology of Future Computing Technologies*. Trier, Germany, 2003: 162-170
- [24] Kerntopf P. A comparison of logical efficiency of reversible and conventional gates//*Proceedings of the International Workshop on Logic Synthesis*. Dana Point, California, USA, 2000: 261-269
- [25] Perkowski M, Kerntopf P, Buller A, Mishchenko A, Song X, Al-Rabadi A, Jozwiak L, Coppola A, Massey B. Regular realization of symmetric functions using reversible logic//*Proceedings of the Euromicro Symposium on Digital System Design*. Warsaw, Poland, 2001: 245-252
- [26] Maslov D, Dueck G W, Miller D M. Synthesis of Fridkin-Toffoli reversible networks. *IEEE Transactions on VLSI Systems*, 2005, 13(6): 765-769



GUAN Zhi-Jin, born in 1962, Ph. D. candidate, professor. His current research interests include reversible computation, information security and logic synthesis.

visor. His current research interests include database, data mining technology, information security, etc.

SHI Quan, born in 1973, M. S., associate professor. His current research interests include network database, software engineering.

ZHENG Ji-Ping, born in 1979, Ph. D., assistant researcher. His current research interests include context-aware intelligent database management and database security.

QIN Xiao-Lin, born in 1953, professor, Ph. D. super-

Background

This work is supported by the National Natural Science Foundation of China under grant No. 60673127, the National High Technology Research and Development Program (863 Program) of China under grant No. 2007AA01Z404, and Natural Science Foundation for colleges and universities of Jiangsu province of China under grant No. 05KJB520107.

Reversible logic synthesis is considered as a rapidly developing research area. Interest in reversible logic is sparked by its necessity in quantum technologies. Reversible implementations are also found in cryptography, Information security, nanotechnology, and so on.

The amount of reversible logic gate and amount of garbage are a very important criterion for a good synthesis procedure, since in most technologies the addition of only one bit

of garbage is expensive or even impossible to implement. Based on this information, a crucial way to help reversible logic to evolve and become usable is to design a synthesis method which uses the theoretically minimal number of reversible gate and number of garbage bits.

In this paper, a reversible network cascade model is provided. This model can be controlled with positive/negative, and the algorithm of reversible synthesis is proposed for the model. Using the approach, the authors create a program and run it to synthesis the NCMC Benchmark functions with less than twelve variables. The experimental results show a proper improvement for the number of garbage outputs and number of gates, and the method can minimize the number of NOTs in reversible network.