基于规则的可逆Toffoli电路优化算法

程学云[1] 管致锦[1] 张海豹[2] 丁卫平[1]
(南通大学计算机科学与技术学院 南通 226019)[1] (南通大学电子信息学院 南通 226019)[2]

摘 要 可逆电路的优化是可逆逻辑综合的关键问题之一。为了解决可逆Toffoli电路优化问题中算法复杂度高和电路规模可扩充性差的问题,分析归纳了相邻Toffoli门的关系,提出并证明了可逆Toffoli电路中子序列的移动和化简规则,并基于这些规则给出了可逆Toffoli电路的优化算法。根据移动规则对可逆电路进行正向和反向扫描,寻找满足化简规则的子序列进行优化,直到可逆电路不发生变化为止。该优化算法与可逆电路的输入线数无关,无需存储额外信息,适用于各种不同类型的Toffoli电路合成方法,算法复杂度为$O(s^3)$,优于通常使用的模板优化的复杂度$O(n!t^2s^3)$。在具体实例和国际认可的所有3变量可逆函数上的验证结果表明,该优化算法能有效地减少可逆电路的门数和控制位数,降低可逆电路的代价。

关键词 可逆逻辑综合,可逆函数,Toffoli门,可逆电路优化
中图法分类号 TP302 **文献标识码** A

Rule-based Optimization of Reversible Toffoli Circuits

CHENG Xue-yun[1] GUAN Zhi-jin[1] ZHANG Hai-bao[2] DING Wei-pin[1]
(School of Computer Science and Technology, Nantong University, Nantong 226019, China)[1]
(College of Electronics and Information, Nantong University, Nantong 226019, China)[2]

Abstract Optimization of reversible circuits is one of key problems of reversible logic synthesis. To solve the problem of high algorithm complexity and poor scalability of reversible Toffoli circuits, the paper analyzed and summarized relationship between adjacent Toffoli gates, proposed and proven the moving and simplification rules of sub-sequence of reversible circuit cascaded by Toffoli gates, and gave the optimization algorithm based on these rules. The algorithm examines the circuit bidirectionally according to the moving rules, searches the sub-sequence satisfying simplification rules, performs corresponding optimization, and the process is repeated until the circuit does't change. The algorithm is irrelevant to the number of input lines, does't need to store extra information, is suitable to different Toffoli circuit synthesis methods, and its algorithm complexity is $O(s^3)$, which is superior to $O(n!\ t^2s^3)$ of generally used template optimization technique. Results of examples and experiments on all 3-bit reversible functions show that the number of gates and the control bits can be reduced effectively and the cost of reversible circuit is decreased.

Keywords Reversible logic synthesis, Reversible function, Toffoli gate, Optimization of reversible circuit

1 引言

可逆逻辑综合是可逆计算的重要内容,在量子计算[1]、低能耗设计[2]、纳米技术[3]等领域有着重要应用。可逆逻辑综合主要研究在给定的可逆门和约束条件下,利用可逆逻辑门构造可逆逻辑电路,并使得电路代价尽可能小。同类型门级联的可逆电路中,门数和控制位数越少,可逆电路的代价越小。可逆逻辑综合包括可逆电路的合成和优化两方面。可逆电路的合成是指给定一个可逆逻辑函数的输入、输出值,计算机通过相关算法得到实现该函数功能的可逆逻辑电路。常见的合成方法包括精确的方法[4]和启发式方法[5-8]。启发式方法一般具有较低的时间和空间复杂度,然而得到的可逆电路往往不是最优电路。为了得到最优电路,需要在不改变可逆电路功能的条件下,对电路进行重组、替换和逻辑门约简等,以降低可逆电路的代价。现有的优化方法包括基于简单规则的方法[9]和基于模板匹配的方法[6,10-12]等。文献[9]给出了一组正反控制(PNC)门的优化规则,用于移除可逆电路中的NOT门以及对具有相同目标位的门序列的化简。文献[10]提出了可逆电路模板优化的思想,即运用模板技术的等价性替换电路中某一部分逻辑门,从而达到减少逻辑门数量的目的。文献[11]扩展了文献[10]中模板的规模,即模板中Toffoli门的个数,目前找到的最大模板的规模为9。模板优化技

到稿日期:2012-10-26 返修日期:2013-03-22 本文受国家自然科学基金(60873069),江苏省高校自然科学基金(12KJB520013),南通市应用研究计划(BK2013043)资助。

程学云(1978—),女,硕士,讲师,CCF会员,主要研究方向为可逆计算和可逆电路优化,E-mail:chen.xy@ntu.edu.cn;管致锦(1962—),男,博士,教授,主要研究方向为可逆逻辑综合和信息安全,E-mai:guan.zj@ntu.edu.cn(通信作者);张海豹(1987—),男,硕士生,主要研究方向为可逆逻辑综合;丁卫平(1979—),男,博士,主要研究方向为模式识别。

术虽能减少可逆电路门数，但需要存储大量的模板，匹配算法复杂度高，不利于可逆电路规模的扩展。

本文分析归纳了相邻 Toffoli 门的关系，给出并证明了 Toffoli 门序列新的移动和化简规则，这些规则与输入线数无关，具有通用性，使得基于这些规则的优化算法具有很强的可扩展性。该优化算法无需线关联，无需存储模板等额外信息，降低了算法的时空复杂度。

2 基本概念

可逆门是指输入与输出之间存在一一对应关系的逻辑门。常见的有 Toffoli 门、Fredkin 门、PNC 门和 Peres 门等。

定义 1 对于变量域集合$\{x_1,x_2,\cdots,x_n\}$，广义 Toffoli 门形如 $TOF(C;T)$，其中控制线集 $C=\{x_{i_1},x_{i_2},\cdots,x_{i_k}\}$，目标位 $T=\{x_j\}$，且 $C\cap T=\Phi$。Toffoli 门将$\{x_1^0,x_2^0,\cdots,x_n^0\}$映射到$\{x_1^0,\cdots,x_{j-1}^0,x_j^0\oplus x_{i_1}^0,\cdots,x_{i_k}^0,x_{j+1}^0,\cdots,x_n^0\}$。

常用的 Toffoli 门有 NOT 门即 $TOF(\Phi;x_1)$，没有控制位；CNOT 门即 $TOF(x_1;x_2)$，带有一个控制位；带有两个控制位的 Toffoli 门 $TOF(x_1,x_2;x_3)$。3 种门的表示见图 1。

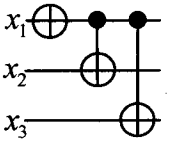

图 1 常见的 Toffoli 门

文献[13]提出了 PNC 门，它是在 Toffoli 的基础上加入反控制。

定义 2 基于 PNC 门可逆电路的基本元素由下面 5 种线型构成[18]，如图 2 所示。

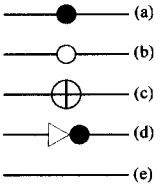

图 2 正反控制模型的 5 种线型

其中，(a)为肯定控制线，(b)为否定控制线，(c)为目标线，(d)为否定线，(e)为无关线。给定输入变量$\{x_1,x_2,\cdots,x_n\}$，控制位集控制位 $C=\{x_{i_1},x_{i_2},\cdots,x_{i_k}\}$，目标位 $T=\{x_j\}$，PNC 门记为 $PNC(C;T)$，其中控制位可以为负控制。

可逆函数是输入和输出之间存在一一映射关系的逻辑函数，满足反函数存在的条件。

定义 3 设 n 位可逆函数 $F(X)=Y$，其中输入变量集 $X=\{x_1,x_2,\cdots,x_n\}$，缺省时为$\{0,1,\cdots,2^n-1\}$，输出 $Y=\{y_1,y_2,\cdots,y_n\}$，其反函数 G 满足 $G(Y)=X$，即 $G(F(X))=X$。

例如，可逆函数 $F=[0,3,4,2,1,6,5,7]$，其反函数为 $G=[0,4,3,1,2,6,5,7]$。

3 优化规则

为进一步降低合成后可逆电路的代价，可通过重组、替换的方法对可逆电路进行优化。一个模板只能解决一个具体门序列的化简，而一条化简规则可解决一类门序列的约简，且不受输入线数的限制。通过移动规则，将可化简的门序列移动在一起，再利用化简规则对子序列进行约简。为了推导 Toffoli 门序列的优化规则，本文首先给出了 PNC 门的相关规则。

3.1 PNC 门移动规则

定理 1 设可逆电路中相邻 PNC 门分别为 A 门和 B 门，A 门为 $PNC(x_{i_1},x_{i_2},\cdots,x_{i_{m-1}};x_{i_m})$，$B$ 门为 $PNC(x_{j_1},x_{j_2},\cdots,x_{j_{n-1}};x_{j_n})$。两 PNC 门有一相同的控制位，$A$ 门为 x_{i_p}($p\in[1,m-1]$)，B 门为 x_{j_q}($q\in[1,n-1]$)，且取值相反，即 $x_{i_p}=\overline{x_{j_q}}$，则 A 门和 B 门的位置可以交换。

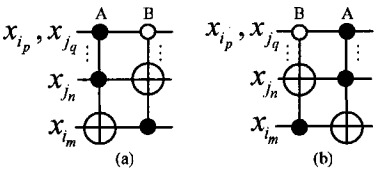

图 3 PNC 门移动规则 1

证明：设 A 门除 x_{i_p}、x_{j_n} 外其余控制位乘积为 C_1，B 门上除 x_{j_q}、x_{i_m} 外其余控制位乘积为 C_2，输入信息经过如图 3(a)所示的 A、B 门后，得到：

$$x_{i_m}'=x_{i_m}\oplus C_1x_{j_n}x_{i_p} \tag{1}$$

$$\begin{aligned}x_{j_n}'&=x_{j_n}\oplus C_2x_{j_q}(x_{i_m}\oplus C_1x_{i_p}x_{j_n})\\&=x_{j_n}\oplus C_2x_{j_q}(x_{i_m}\oplus C_1\overline{x_{j_q}}x_{j_n})\\&=x_{j_n}\oplus C_2x_{j_q}x_{i_m}\end{aligned} \tag{2}$$

输入信息经过如图 3(b)所示的 B、A 门后，得到：

$$x_{j_n}'=x_{j_n}\oplus C_2x_{i_m}x_{j_q} \tag{3}$$

$$\begin{aligned}x_{i_m}'&=x_{i_m}\oplus C_1x_{i_p}\oplus(x_{j_n}\oplus C_2x_{i_m}x_{j_q})\\&=x_{i_m}\oplus C_1x_{i_p}\oplus(x_{j_n}\oplus C_2x_{i_m}\overline{x_{i_p}})\\&=x_{i_m}\oplus C_1x_{i_p}x_{j_n}\end{aligned} \tag{4}$$

式(1)等价于式(4)，式(2)等价于式(3)，表明输入信息经过 A、B 门后的输出与经过 B、A 门后的相等，所以 A、B 两门位置可以交换。

定理 2 设两门 $A=PNC(x_{i_1},x_{i_2},\cdots,x_{i_{m-1}};x_{i_m})$ 与 $B=PNC(x_{j_1},x_{j_2},\cdots,x_{j_{n-1}};x_{j_n})$ 相邻，如果满足：$x_{i_m}\in\{x_{j_1},x_{j_2},\cdots,x_{j_{n-1}}\}$，$A$ 门控制线集是 B 门控制线集的子集即$\{x_{i_1},x_{i_2},\cdots,x_{i_{m-1}}\}\subseteq\{x_{j_1},x_{j_2},\cdots,x_{j_{n-1}}\}$，且两门相同控制线上同为正控制或同为负控制，则 A 门和 B 门位置可以交换。

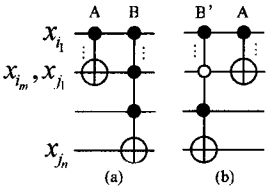

图 4 PNC 门移动规则 2

证明：设 A 门的目标位 x_{i_m} 是 B 门控制位 x_{j_1}，据 $a\oplus b=\bar{a}\oplus\bar{b}$，输入信息经过如图 4(a)所示的 A、B 门后有：

$$\begin{aligned}x_{j_n}'&=x_{j_n}\oplus x_{j_2}\cdots x_{j_{n-1}}(x_{i_m}\oplus x_{i_1}\cdots x_{i_{m-1}})\\&=x_{j_n}\oplus x_{j_2}\cdots x_{j_{n-1}}(\overline{x_{j_1}}\oplus\overline{x_{i_1}\cdots x_{i_{m-1}}})\\&=x_{j_n}\oplus x_{j_2}\cdots x_{j_{n-1}}\overline{x_{j_1}}\oplus x_{j_2}\cdots x_{j_{n-1}}\overline{x_{i_1}\cdots x_{i_{m-1}}}\end{aligned} \tag{5}$$

因为$\{x_{i_1},x_{i_2},\cdots,x_{i_{m-1}}\}\subseteq\{x_{j_1},x_{j_2},\cdots,x_{j_{n-1}}\}$且 x_{j_1} 是 A 门目标位，故$\{x_{i_1},x_{i_2},\cdots,x_{i_{m-1}}\}\subseteq\{x_{j_2},x_{j_3},\cdots,x_{j_{n-1}}\}$且相同控制位值相等，得 $x_{j_2}\cdots x_{j_{n-1}}\times\overline{x_{i_1}\cdots x_{i_{m-1}}}=0$。

$$x_{j_n}'=x_{j_n}\oplus x_{j_2}\cdots x_{j_{n-1}}\overline{x_{j_1}} \tag{6}$$

将 B 门 x_{j_1} 位取反得到 B'，B' 目标位的输出等价于式(6)，输入信息经过 B'、A 后的输出与经过 A、B 后的相等，所以 A、B 门位置可以互换，交换后 B 门被 A 门目标位影响的控制位取反。

3.2 PNC 门化简规则

同类型门级联的可逆电路，控制位数越少，电路代价越小。本文在可逆电路优化中，不仅考虑门数的约简，而且考虑了控制位数的约简。

如果相邻 PNC 门仅在一控制位上取值相反，两门可以合并为一门，新得到的门中该控制位被略去[7]，如图 5 所示。

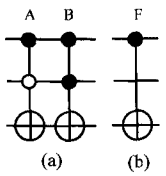

图 5 PNC 门门数约简规则 1

定义 4 图 5 中，A 门和 B 门只在一控制位上取值相反，称互为兄弟门。兄弟门合并后的 F 门定义为父门，A 门和 B 门是父门 F 的子门。

定理 3 父门和其子门合并为其另一子门。

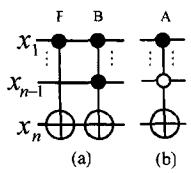

图 6 PNC 门门数约简规则 2

证明：如图 6 所示，设 F 门和 B 门分别为 $F=PNC(x_1,\cdots,x_{n-2};x_n)$，$B=PNC(x_1,\cdots,x_{n-1};x_n)$，则图 6(a)中目标位的输出为：

$$\begin{aligned}x_n'&=x_n\oplus x_1\cdots x_{n-2}\oplus x_1\cdots x_{n-2}x_{n-1}\\&=x_n\oplus x_1\cdots x_{n-2}(1\oplus x_{n-1})\\&=x_n\oplus x_1\cdots x_{n-2}\overline{x_{n-1}}\end{aligned} \tag{7}$$

式(7)等价于图 6(b)中目标位的输出，所以 F 门和 B 门可以合并为 F 的另一子门 A 门。

推论 1 父门等价于其两子门，一子门等价于其父门和其兄弟门。

定理 4 两 PNC 门具有相同的目标位和控制位，且仅在两相同的控制位上取值相反，则两 PNC 门可以各减少 1 位控制位。

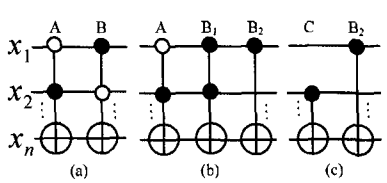

图 7 PNC 门控制位约简规则

证明：如图 7 所示，设 $A=PNC(\overline{x_1},x_2,\cdots,x_{n-1};x_n)$，$B=PNC(x_1,\overline{x_2},\cdots,x_{n-1};x_n)$。据推论 1，图 7(a)中 B 门等价于 B_1 门和 B_2 门。图 7(b)中，A 门和 B_1 合并为 C 门，所以 A 门变为 C 门略去 x_1，B 门变为 B_2 略去 x_2，控制位各减少一位。

3.3 Toffoli 门序列化简规则

相较于 PNC 门，Toffoli 门只有正控制。本文分析归纳了相邻 Toffoli 门的 5 种关系，给出了相应的化简和移动规则。

关系 1 相邻 Toffoli 门相同，即目标位相同，控制线集也相同。

定理 5 可逆电路中相邻且相同的两 Toffoli 门可删除。

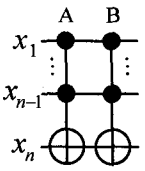

图 8 Toffoli 门删除规则

证明：如图 8 所示，设电路中相邻两门均为 $TOF(x_1,x_2,\cdots,x_{n-1};x_n)$，输入信息 x_n 经过 A、B 门后为：$x_n'=x_n\oplus x_1x_2\cdots x_{n-1}\oplus x_1x_2\cdots x_{n-1}=x_n$，目标位输出不变，故相邻且相同的两门可删除。

关系 2 相邻 Toffoli 门一个是父门，一个是子门，即满足父子关系。

定理 6 满足父子关系的相邻 Toffoli 门为 $A=TOF(x_1,\cdots,x_{n-2};x_n)$ 和 $B=TOF(x_1,\cdots,x_{n-1};x_n)$，设 B 门右侧存在 $R=TOF(x_{i_1},x_{i_2},\cdots,x_{i_p};x_{n-1})$ 且 R 门控制线集是 A 门控制线集的子集，即 $\{x_{i_1},x_{i_2},\cdots,x_{i_p}\}\subseteq\{x_1,x_2,\cdots,x_{n-1}\}$，则 A、B 和 R 3 个门可化简为 R 门和子门 B；如果在 A 门左侧存在 R 门，则 R、A 和 B 3 个门可替换为子门 B 和 R 门。

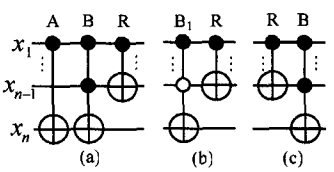

图 9 基于关系 2 的化简规则

证明：据定理 3，图 9(a)中 A 门和 B 门合并为 B_1 门，图 9(b)中 B_1 和 R 门满足定理 2，交换 B_1 和 R 的位置得到图 9(c)所示的 R 和 B 门。

当 R 门在 A 门左侧时，可同理得证。

关系 3 A 门的目标位是 B 门的控制位，且 A 门的控制线集是 B 门控制线集的子集。

定理 7 满足关系 3 的相邻 Toffoli 门为 $A=TOF(x_1,\cdots,x_{n-2};x_{n-1})$，$B=TOF(x_1,\cdots,x_{n-1};x_n)$。设在 A、B 门的右侧存在与 A 相同的门，或是在 A、B 门的左侧存在与 B 相同的门，3 个门化简后均为中间位置的门和 F 门，$F=TOF(x_1,x_2,\cdots,x_{n-2};x_n)$，即 B 门除去被 A 门目标位影响的控制位 x_{n-1} 后得到的 B 的父门。

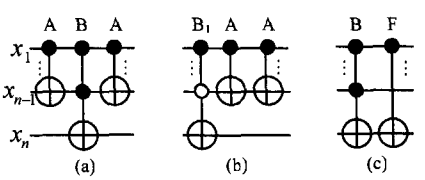

图 10 基于关系 3 的化简规则 1

证明：(1)在 B 门的右侧存在与 A 相同的门，如图 10(a)所示。

图 10(a)中，A 门和 B 门满足定理 2，交换位置后，B 门变为 B_1 门。图 10(b)中两相邻的 A 门删除，据推论 1，B_1 门等价于其兄弟门 B 和父门 F。

(2)在 A 门的左侧存在与 B 相同的门，如图 11(a)所示。

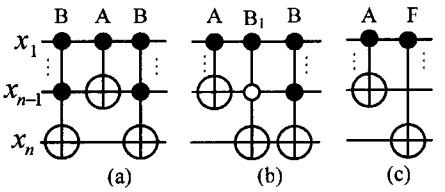

图 11　基于关系 3 的化简规则 2

图 11(a)中，B 门和 A 门满足定理 2，交换位置后，B 门变为 B_1 门。图 11(b)中 B_1 门与其右侧的 B 门合并为 B 的父门 F。

综合(1)、(2)两种情况，化简结果均为中间位置的门和 F 门。

关系 4　相邻 Toffoli 门有一相同控制位。

定理 8　设满足关系 4 的相邻 Toffoli 门为 $A=TOF(x_1,\cdots,x_{n-1};x_n)$，$B=TOF(x_1,\cdots,x_{n-2},x_n;x_{n-1})$，有一相同的控制位 x_1。如果在 B 门的右侧存在与 A 相同的门，则 B 门左右两侧 A 门中的 x_1 位可删除。

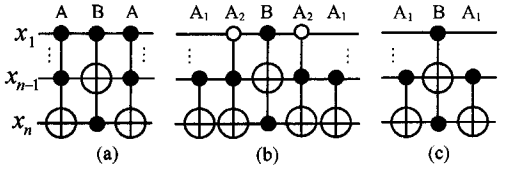

图 12　基于关系 4 的化简规则

证明：据推论 1，图 12(a)中 A 门等价于其父门 A_1 和兄弟门 A_2。图 12(b)中 A_2 和 B 据定理 1 交换后，两相邻 A_2 门删除，得到图 12(c)。可见 A 门中与 B 相同的控制位 x_1 被删除。

关系 5　设两门 $A=TOF(x_{i_1},x_{i_2},\cdots,x_{i_{m-1}};x_{i_m})$，$B=TOF(x_{j_1},x_{j_2},\cdots,x_{j_{n-1}};x_{j_n})$相邻，满足 A 门目标位是 B 门的某一控制位($x_{i_m}\in\{x_{j_1},\cdots,x_{j_{n-1}}\}$)，存在 $x_{i_p}\notin\{x_{j_1},x_{j_2},\cdots,x_{j_{n-1}}\}$($p\in[1,m-1]$)且$\{x_{i_1},x_{i_2},\cdots,x_{i_{m-1}}\}\subseteq\{x_{j_1},x_{j_2},\cdots,x_{j_{n-1}}\}\cup\{x_{i_p}\}$，如图 13(a)所示。将 B 门控制线集除去被 A 门目标位影响的 x_{i_m}，增加 A 的控制位 x_{i_p} 后得到的 Toffoli 门记为 B'门。

定理 9　对满足关系 5 的两 Toffoli 门，设在 B 门的右侧存在 A，或在 A 门的左侧存在 B，3 个门化简后的结果均为中间位置的门和 B'门；设在 A 门的左侧或 B 门的右侧存在 B'门，化简后结果均为 B 门和 A 门。

证明：(1)在 B 门右侧存在 A 门。

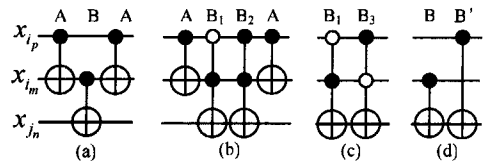

图 13　基于关系 5 的化简规则 1

图 13(a)中父门 B 等价于它的两个子门 B_1 和 B_2。图 13(b)中 A 门和 B_1 门满足定理 1，A 可以移动到 B_1 右侧，A 门和 B_2 门满足定理 2，交换位置后 B_2 门变为 B_3 门，两相邻的 A 门删除，得到图 13(c)。B_1 门和 B_3 门满足定理 4，除去各自负控制位，得到图 13(d)，其中 B'是 B 门的控制线集除去被 A 门目标位影响的控制位 x_{i_m} 加上 A 的控制位 x_{i_p} 得到的门。

(2)在 A 门的左侧存在 B。

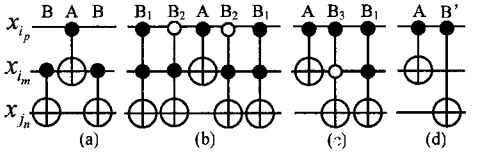

图 14　基于关系 5 的化简规则 2

图 14(a)中 B 门等价于其两子门 B_1 和 B_2。图 14(b)中 A 门与其左侧的 B_2 门满足定理 1，A 门移到 B_2 门左侧，两相邻的 B_2 门删除。A 门与其左侧的 B_1 门满足定理 2，A 与 B_1 交换位置后 B_1 门变为 B_3，得到图 14(c)。B_3 和 B_1 合并为 B'，得到图 14(d)。

综合(1)、(2)两种情况知，化简结果均为中间位置的门和 B'门。

(3)在 A、B 门的左侧或右侧存在 B'门。

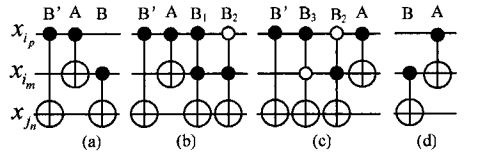

图 15　基于关系 5 的化简规则 3

设在 A、B 门的左侧存在 B'门，如图 15(a)所示，父门 B 等价于 B_1 和 B_2。图 15(b)中 A 门和 B_1 门满足定理 2，A 门可以移到 B_1 门右侧，但 B_1 门变为 B_3 门，A 门和 B_2 门满足定理 1，A 门直接移到 B_2 门右侧。图 15(c)中，B_2 门和 B_3 门满足定理 4，除去各自的负控制位，B_2 门变为 B 门，B_3 门变为 B'门，两相邻 B'门删除，得到图 15(d)。

3.4　Toffoli 门移动规则

文献[14]中给出了 Toffoli 门的一种移动规则，即对于两相邻 Toffoli 门 $TOF(C_1,t_1)$和 $TOF(C_2,t_2)$，如果 $C_1\cap t_2=\varnothing$ 且 $C_2\cap t_1=\varnothing$，即目标位互不影响对方的控制位，则两门的位置可以交换，该规则称为 Toffoli 门移动规则一。

本文根据 Toffoli 门的特点，给出了如下新的移动规则。

定理 10　A 门和 B 门为父子门，子门 B 比其父门 A 多一控制位 x_k，若存在门 R，且 x_k 为 R 门控制位，则 R 门可以与 A、B 门序列互换位置。

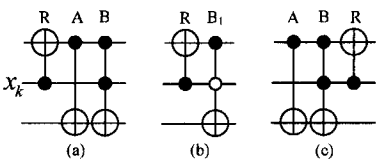

图 16　Toffoli 门移动规则 2

证明：据定理 3，图 16(a)中 A 门和 B 门合并为 B_1 门，图 16(b)中 R 和 B_1 满足定理 1，R 门和 B_1 门的位置可以互换，即 R 门可以移到 A、B 门序列之后，如图 16(c)所示。

定理 11　A 门和 B 门具有相同的目标位，除了在控制位 x_i 和 x_j 上不同外其余控制位均相同，设 A 包含控制位 x_i，B 包含控制位 x_j，如果存在 R 门，同时包含控制位 x_i 和 x_j，则

R 和 A、B 门序列的位置可以交换。

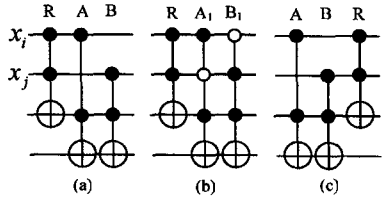

图 17　Toffoli 门移动规则 3

证明：据定理 4，图 17(a)中 A 门和 B 门等价于图 17(b)中 A_1 门和 B_1 门。图 17(b)中，R 和 A_1、R 和 B_1 均满足定理 1，所以 R 可以移动到 A_1、B_1 门右侧，等价于图 17(c)。

4　基于规则的可逆 Toffoli 电路优化算法

4.1　优化算法

根据上述一系列规则，给出了可逆 Toffoli 电路优化算法，该算法可用于任何基于 Toffoli 门合成算法得到的可逆电路。因为门的移动具有方向性，所以优化算法采用了双向扫描的方式。主要思想是：对门序列从左往右扫描，对门序列中可以移到一起的两个门，判定是否满足 5 种关系中的一种，如果满足 5 种关系之一，则继续检查是否存在可化简的子序列，如果存在就进行化简，否则根据 Toffoli 门的移动规则继续向右扫描；向右扫描结束后，再从右往左检查。依此循环，直到整个可逆电路不发生变化为止。该算法同时对可逆函数及其反函数进行综合，然后选择两者中代价较小的电路，如果反函数优化后的电路代价较小，则将其电路逆序输出作为最终结果。可逆 Toffoli 电路优化算法如下。

算法 1　可逆 Toffoli 电路优化算法

```
输入：可逆函数 F
输出：由 Toffoli 门级联的可逆电路
说明：GateList 是存储 Toffoli 门的带头结点的双向链表
S1：从左往右化简电路
p=GateList->next;
repeat
  q=p->next;
  repeat
    if(p 和 q 满足关系 1)
      {删除 q;p1=p;p=p->next;删除 p1;break;}
    if(p 和 q 满足关系 2)
      {检查电路中是否有满足定理 6 的 R 门存在，如果存在且可移
       动到 p 门左侧或 q 门右侧，则进行相应化简}
  if(p 和 q 满足关系 3)
    {检查电路中 q 门的右侧是否存在与 p 相同的门，或在 p 门的左
     侧检查是否存在与 q 相同的门，若存在且可与 p、q 门序列移动
     到一起，则据定理 7 进行化简}
  if(p 和 q 满足关系 4)
    {检查 q 门的右侧是否存在与 p 门相同的门，若存在且可移到 q
     门右侧，则据定理 8 进行化简}
  if(p 和 q 满足关系 5)
    {先检查 q 的右侧是否存在与 p 相同的门，或 p 门的左侧是否存
     在与 q 相同的门，若存在且可移动到一起，则据定理 9 化简；若
     不存在，继续检查 p 门的左侧或 q 门的右侧是否存在定理 9 中
     的 B′，若存在且可移动到一起，则进行相应化简}
  if(p 门和 q 门的目标位互不影响) q=q->next;
  else
    t2=q->next;
    if(p 和其后两门 q、t2 满足本文给出的新的移动规则) q=
      t2->next;
  else break;
 until q=NULL
 p=p->next;
until p=NULL
S2：从右往左化简电路；
S3：如果 S1 和 S2 中电路发生变化转 S1，否则算法结束。
```

4.2　性能分析

该优化算法无需存储模板，节约了存储空间。设被优化的可逆电路的输入线数为 n，门数为 s，算法的时间复杂度为 $O(s^3)$。模板优化方法中，文献[10,11]给出了 17 个具有恒等函数功能的模板。若 $G_0G_1\cdots G_{m-1}$ 是实现恒等函数的模板，则经过 k 次循环移位后 $G_kG_{(k+1) \bmod m}\cdots G_{(k-1) \bmod m}$ 也实现了恒等函数，它们均称为模板环。设电路的输入线数为 n，第 i 个模板中的门数即模板的规模为 m_i，则其中可包含 m_i 个模板环，目前找到的最大模板规模为 9。模板优化方法所需的时间复杂度为 $O(n!\cdot\sum_{i=1}^{k}m_i^2\cdot s^3)$，设 $t=\sum_{i=1}^{k}m_i$，即所有模板环的个数，复杂度可近似为 $O(n!t^2s^3)$，可见算法的运行时间不仅与输入线数相关，而且与模板环的个数相关，当输入线数和模板环数增加时，复杂度急剧增长，不利于大规模可逆电路的优化。

5　实例验证及结果分析

为验证本文提出的优化算法的正确性和有效性，首先通过具体实例分析了两个可逆函数的优化过程，然后在所有 3 变量可逆函数上进行了测试，并与已有方法的结果进行了比较。

5.1　实例

例 1　可逆函数 $F_1=[0,3,4,2,1,6,5,7]$，求实现该可逆函数的可逆电路并优化。

通过合成算法得到如图 18(a)所示的初始可逆电路。

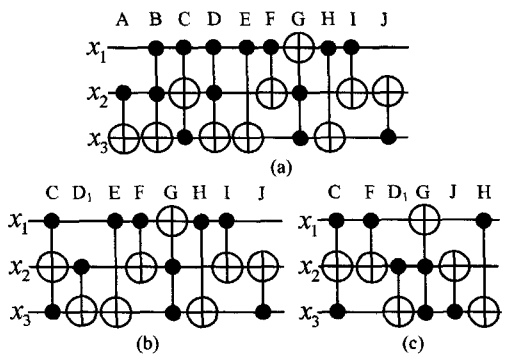

图 18　可逆函数 F_1 的优化过程

图 18(a)中，B、C 和 D 3 门满足定理 8，B 门和 D 门可以略去控制位 x_1，B 门略去 x_1 后与 A 门相同，相邻且相同的两 A 门可删除，D 门变为 D_1，得到图 18(b)。图 18(b)中，D_1、E 和 F 3 门满足定理 9，F 门的目标位是 D_1 门的控制位，化简后的结果为 F 门和 D_1 门，同时 H、I 和 J 也满足定理 9，H 门的目标位是 J 门的控制位，化简后的结果为 J 门和 H 门，得到图 18(c)。电路化简后，门数减少 4 个，控制位减少 6 位。

F_1 反函数为[0,4,3,1,2,6,5,7]，经过综合算法得到如图 19(a)所示的可逆电路。

图 19(a)中，B、C 和 D 3 门满足定理 8，B 门和 D 门可以略去 x_1，得到 B_1 和 D_1。图 19(b)中，D_1、E 和 F 3 门满足定理 9，F 门的目标位是 D_1 门的控制位，化简后得 F 门和 D_1 门，同时 H、I 和 J 也满足定理 9，化简后得到 J 和 I 门，如图 19(c)所示。图 19(c)中，D_1、G 和 J 3 门满足定理 8，控制位 x_2 可略去，化简后的 3 门满足定理 5，得到 G 和 J_1，如图 19(d)所示。优化后门数减少 3，控制位数减少 5。

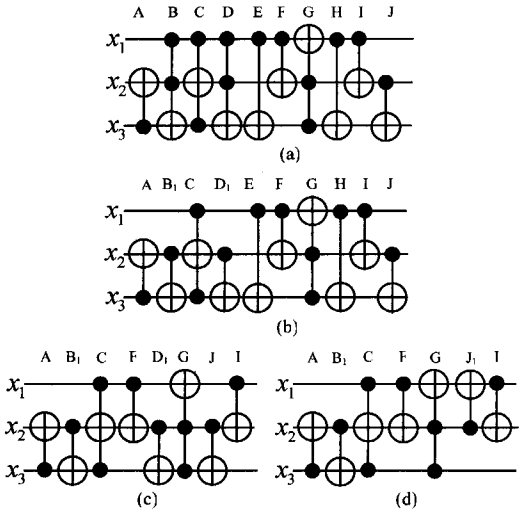

图 19　F_1 反函数的优化过程

比较可逆函数 F_1 及其反函数优化后的可逆电路，前者少一门，所以可逆函数 F_1 的最终结果如图 18(c)所示。

例 2　以 Benchmark 例题[1)] 中的 rd32 为例，函数 F_2 = [0,7,6,9,4,11,10,13,8,15,14,1,12,3,2,5]，求实现该可逆函数的可逆电路并优化。

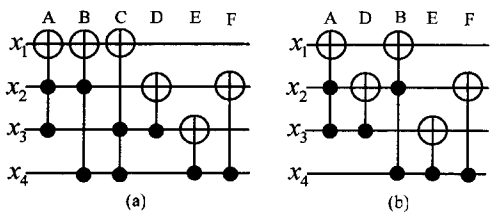

图 20　可逆函数 F_2 的优化过程

经过合成算法后，得到如图 20(a)所示的初始可逆电路，其中 B、C 和 D 3 门满足定理 9，D 门的目标位是 B 门的控制位，化简后得 D 和 B，如图 20(b)所示。

反函数[0,11,14,13,4,15,2,1,8,3,6,5,12,7,10,9]综合后得到如图 21(a)所示的可逆电路。

图 21(a)中，C、D 和 E 3 门满足定理 6，E 门和 C 门为父子门，化简后结果为 D 门和 C 门，如图 21(b)所示。

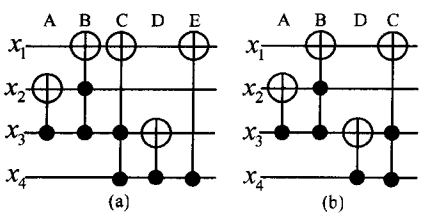

图 21　F_2 反函数的优化过程

比较 F_2 及其反函数优化后的可逆电路，后者使用的门数少一个，所以对可逆函数 F_2 综合的结果为图 21(b)的逆序输出。

5.2　实验结果及分析

为了验证所提出的优化算法的有效性，使用 C++语言实现了本文所描述的算法，在所有 3 变量可逆函数上进行了测试，对本文算法和已有算法的结果进行了比较，结果如表 1 所列。前 3 种方法均采用了文献[10]中给出的合成算法，其中(a)是未化简时的结果，(b)是文献[10]中给出的模板匹配算法的结果，(c)是利用本文给出的优化算法对(a)优化后的结果，(d)是文献[5]基于穷举的方法给出的最优结果。所有方法均基于 Toffoli 门进行合成和优化。

表 1　在所有 3 位可逆函数上的比较结果

门数	(a)	(b)	(c)	(d)
15	2	0	0	0
14	22	0	0	0
13	112	6	0	0
12	432	62	14	0
11	1191	391	130	0
10	2575	1444	607	0
9	5116	3837	1987	0
8	7842	7274	6304	577
7	8989	9965	11590	10253
6	7478	9086	10856	17049
5	4314	5448	5995	8921
4	1682	2125	2163	2780
3	463	567	559	625
2	89	102	102	102
1	12	12	12	12
0	1	1	1	1
平均	7.25	6.80	6.52	5.87

如表 1 所列，在所有 3 变量可逆函数(40320 个)上未化简时的平均门数为 7.25，所需最大门数为 15。文献[10]给出的基于模板匹配的结果为 6.80，所需的最多门数为 13。本文在所有 3 位可逆函数上的平均门数仅为 6.52，所需的最多门数仅为 12。可见经过本文算法优化后，所需的平均门数明显下降，且当门数越多时电路优化效果越显著。

文献[5]给出的最优结果为 5.87。该算法采用深度优先反复加深搜索方法构造最优门数的电路，虽然可以找到每一个可逆函数的最佳实现电路，但其扩展性较差，在综合 4 变量函数时，如果所得的最佳可逆逻辑电路的门数大于 8，则平均需要 1.5 小时[5]。文献[5]最优算法的空间复杂度为 $O(2^n!)$，而本文基于转换的合成方法空间复杂度仅为 $O(n2^n)$，远小于最优算法。

此外在所有 3 位可逆函数上，直接由合成方法生成的可逆电路的平均控制位数为 8.74，经过本文给出的算法优化后，平均控制位数下降为 7.49。

结果表明，本文给出的优化方法不仅具有较低的时空复杂度，也有效减少了可逆电路的门数和控制位数，降低了构建可逆电路的代价。

结束语　本文归纳了相邻 Toffoli 门的 5 种关系，给出并证明了 Toffoli 门序列的移动和化简规则，基于这些规则，给出了有效的可逆 Toffoli 电路优化算法。该优化算法无需存储模板等额外信息，具有较低的时间复杂度，与输入线数无关，具有很强的可扩展性。所有 3 输入可逆函数上的结果表

1) Maslov D. Reversible logic synthesis benchmarks page. http://www.cs.uvic.ca/~dmaslov/, 2012.

明，该优化算法能有效地减少可逆电路的门数和控制位数，取得了较理想的综合结果。今后将尝试将其用于输入线数更多的可逆电路优化，同时也将考虑加入 Fredkin 等新的门来进一步降低可逆电路的代价。

参 考 文 献

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

[2] De Vos A, Desoete B, Janiak F, et al. Control Gates as Building Blocks for Reversible Computers[A]// Proceedings of 11th International Workshop on Power and Timing Modeling, Optimization and Simulation[C]. Yverdon, Switzerland, Sep. 2001: 9201- 9210

[3] Merkle R C. Two types of mechanical reversible logoc[J]. Nanotechnology, 1993(4): 114-131

[4] Wille R, Grobe D. Fast exact Toffoli network synthesis of reversible logic[A]// Proceedings of International Conference on Computer-Aided Design[C]. San Jose, USA, Nov. 2007: 60-64

[5] 倪丽慧，管致锦，聂志浪. 基于可逆函数复杂性的正反控制门可逆网络综合[J]. 计算机科学，2010，37(11)：117-121

[6] Miller D M, Maslov D, Dueck G W. A transformation based algorithm for reversible logic synthesis[A]// Proceedings of DAC [C]. Anahem, California, USA, 2003: 318-323

[7] Wan Si-shuang, Chen Han-wu, Cao Ru-jin. A Novel Transformation-Based Algorithm for Reversible Logic Synthesis[A]// Proceedings of the 4th International Symposium on Intelligence Computation and Applications (ISICA)[C]. Wuhan, PRC, Oct. 2009: 70-81

[8] Zheng Y, Huang C. A novel Toffoli network synthesis algorithm for reversible logic[A]// Proceedings of the 2009 Asia and South Pacific Design Automation Conference[C]. Los Alamitos: IEEE Computer Society Press, 2009: 739-744

[9] Arabzadeh M, Saeedi M, Zamani M S. Rule-based Optimization of Reversible Circuits[A]// Proceedings of ASP-DAC' 2010 [C]. Taipei, Taiwan, Jan. 2010: 849-854

[10] Maslov D, Dueck G W, Miller D M. Toffoli network synthesis with templates [J]. Computer Aided Design of Integrated Circuits and Systems, 2005, 24(6): 807-817

[11] Maslov D, Dueck G, Miller D. Techniques for the synthesis of reversible Toffoli networks[J]. ACM Transactions on Design Automation of Electronic Systems, 2007, 12(4): 42

[12] 陈汉武，李志强，李文蓉. 量子可逆逻辑综合的关键技术及其算法的研究[J]. 软件学报，2009，12：570-583

[13] 管致锦，秦小麟，施佺，等. 基于正反控制模型的可逆逻辑综合[J]. 计算机学报，2008，31(5)：835-844

[14] Maslov D, Dueck G W, Miller D M. Simplification of Toffoli networks via templates[A]// Proceedings of Integrated Circuits and Systems Design[C]. San Paulo: IEEE Computer Society, 2003: 53-58

(上接第 23 页)

从图 3 可以看出，随着网格密度指数的增加，3 种解法产生的误差都近似指数增长。基于 DST 的泊松方程串行直接解法误差要比基于 Cholesky 方法的串行解法大一个量级左右，这主要是由于 DST 方法中两次 FFT 引入的累积误差所致。而对于 DST 解法，在网格密度较大时，基于 CUDA 的并行版本误差明显大于串行版本，这主要是由于在并行版本中引入了一些累加运算，因此在维数较大的情况下，截断误差导致的影响会更突出。

但是，在大多数应用中，这些误差均处于可以接受的水平，例如，在网格密度为(513×513)的情况下，整个线性系统的方程个数已经达到了 261121 个，而此时基于 CUDA 的并行算法产生的相对误差也小于 10^{-9}，在绝大多数的应用场景下，这一误差是完全可以忽略的。

结束语 泊松方程差分离散后产生的特殊格式的块三对角方程组利用本文描述的基于 DST 的直接求解算法求解与利用针对一般实对称稀疏矩阵的求解算法求解相比具有明显优势，在利用 GPU 加速后，即使在 512×512 的高精度网格划分下，也可以在 1ms 左右得到基本精确的结果，比传统的使用 Cholesky 分解的求解速度快了 1000 倍以上，这使得基于泊松方程求解的实时应用成为可能，同时，这一快速算法也可以大大加速基于泊松方程的科学计算应用。而且，该算法并不局限于泊松方程的求解，很多形式类似于式(1)的偏微分方程均可以离散成为类似于式(2)的形式，此时，只要其对角线矩阵与 A 矩阵具有相同的特征向量，便可以采用本文所描述的算法进行求解，因此，该算法具有十分广泛的应用范围。

参 考 文 献

[1] Kincaid D, Cheney W. 数值分析(第三版) [M]. 王国荣，等译. 北京：机械工业出版社，2005

[2] 罗正平. 托卡马克中等离子体平衡计算 [D]. 合肥：合肥工业大学，2007

[3] Ferron J R, Walker M L, Lag L L, et al. Real time equilibrium reconstruction for tokamak discharge control [J]. Nucl Fusion, 1998, 38(7): 1055-1066

[4] 廖臣，祝大军，刘盛纲. 五点差分格式求解泊松方程并行算法的研究 [J]. 电子科技大学学报，2008，37(01)：81

[5] 许秋燕. 二维泊松方程和扩散方程的一类显式并行算法 [D]. 济南：山东大学，2010

[6] 苑野，杨东华. 基于 MPI 的二维泊松方程差分并行实现与测试 [J]. 哈尔滨商业大学学报：自然科学版，2011(06)：854

[7] Ryoo S, Rodrigues C I, Baghsorkhi S S, et al. Optimization Principles and Application Performance Evaluation of a Multithreaded GPU Using CUDA [C]// Ppopp' 08: Proceedings of the 2008 Acm Sigplan Symposium on Principles and Practice of Parallel Programming. 2008: 73-82

[8] Hockney R W. A Fast Direct Solution of Poissons Equation Using Fourier Analysis [J]. J Acm, 1965, 12(1): 95

[9] Buzbee B L, Golub G H, Nielson C W. Direct Methods for Solving Poissons Equations [J]. Siam J Numer Anal, 1970, 7(4): 627

[10] Hillis W D, Steele G L. Data Parallel Algorithms [J]. Commun Acm, 1986, 29(12): 1170-1183

[11] Chen Y Q, Davis T A, Hager W W, et al. Algorithm 887: CHOLMOD, Supernodal Sparse Cholesky Factorization and Update/Downdate [J]. Acm T Math Software, 2008, 35(3)