

混合多值可逆逻辑中广义 Toffoli 门仅用 CNOT 门的实现

樊富有^{1,2} 杨国武¹ 李晓瑜¹ 罗庆斌¹

(电子科技大学计算机科学与工程学院 成都 611731)¹ (宜宾学院计算机与信息工程学院 宜宾 644007)²

摘要 混合多值量子可逆逻辑电路综合问题中, Toffoli 门的合成是整个合成过程中最为关键的一步。针对混合多值 5-qubits 量子可逆逻辑电路综合问题, 构造了 PMX 量子门, 验证了 CNOT 门的合成能力, 实现了对 Toffoli 门的合成, 并设计了双向的 BDS 搜索算法, 高效实现了量子电路的最优或者较优综合。

关键词 量子电路综合, 混合多值可逆逻辑, Toffoli 门, CNOT 门, 量子计算

中图分类号 TP302.2 文献标识码 A DOI 10.11896/j.issn.1002-137X.2014.08.025

Realization of Toffoli Gate Only Using CNOT Gate in Hybrid Multi-value Reversible Logic

FAN Fu-you^{1,2} YANG Guo-wu¹ LI Xiao-yu¹ LUO Qing-bin¹

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)¹

(School of Computer and Information Engineering, Yibin University, Yibin 644007, China)²

Abstract Synthesis of Toffoli gate is the key step in the process of synthesizing hybrid multi-valued quantum reversible logic circuit. In order to resolve the problem of hybrid multi-valued 5-qubits quantum reversible logic circuit synthesis, we constructed a special quantum gate PMX and verified the synthesis ability of CNOT gate, then achieved the synthesis of Toffoli gate, and according to the algorithm of bi-direction search, accomplished the optimum of synthesis of quantum circuits.

Keywords Synthesis of quantum circuit, Hybrid multi-valued reversible logic, Toffoli gate, CNOT gate, Quantum computation

1 引言

量子计算成为了计算机科学与物理学的连接纽带, 可逆逻辑电路综合技术在量子计算中起着至关重要的作用^[1]。量子可逆逻辑电路综合^[2]是量子计算与量子算法的线路模型表述理论, 它将可逆计算、量子搜索算法等众多技术融为一体, 为物理学、计算机科学以及量子计算与量子信息带来了更多的启发和推动。可逆逻辑电路具有诸多优点, 如: 无需擦除信息, 即保证了信息的不丢失; 可逆计算可以有效进行, 且不产生其值依赖输入的垃圾比特; 根据 Landauer 原理^[3], 可逆逻辑可降低能耗, 因此在计算机科学、信号处理与通信系统等领域具有广泛应用的潜力。因此, 近年来可逆逻辑电路综合技术及其相应算法得到了蓬勃发展。

如果一个逻辑门组成的集合可以用来计算任意的经典函数, 那么称这样的一个逻辑门集合对经典计算是通用的。对应到量子计算的通用性上, 如果一组逻辑门称为是对量子计算通用的, 那么用这组逻辑门的量子线路可以以任意精度近似任意的酉运算。通过近些年的研究, 理论上已经证明两级西门是通用的^[4], 因为 d 维 Hilbert 空间上的任意酉矩阵可以写成两级酉矩阵的乘积形式。同时, DiVincenzo 证明单量

子比特门和受控非门也是通用的^[5], Deutsch 等^[6]从理论上证明了几乎所有的二比特量子逻辑门都是通用的, 等等。随着研究的不断深入和发展, 不少研究者相继提出了不同的通用量子逻辑门库, 以及相应的可逆逻辑电路综合算法。Yang 等在 2005 年提出针对三值逻辑的量子通用逻辑门库: 三值 Swap 门、三值 NOT 门和三值 Toffoli 门^[7], 2006 年又提出三值量子逻辑门库: Swap、NOT 和 1-CNOT 门^[8]。对于量子电路逻辑综合的研究进展同样引人关注, 例如, Iwama 等于 2002 年针对特定的 CNOT 门库, 给出了逻辑电路的综合规则^[9]; Shende 等^[10]首先将可逆逻辑电路综合问题简化为置换问题, 并提出了相应的递归算法, 证明其性能的优越性; 文献^[11]主要应用谱函数实现近似最优可逆逻辑电路的简化工作; Song 等^[12]研究了量子计算中可逆逻辑门的代数特征, 提出用群论方法对量子可逆逻辑电路进行综合; 模板技术的使用主要由 Maslov 等^[13]提出, 它将真值表构造法和模板技术优化电路相结合; Yang 等^[14]提出了以 3-循环置换作为电路基元, 使之在仅使用 NOT 量子门库的情况下, 实现可逆逻辑电路的自动构造; 文献^[15]给出一般量子稳定子码的简单构造方法; 文献^[16, 17]深入研究了基于正反控制模型的可逆逻辑综合和可逆逻辑门网络的表示与级联。上述这些针对量子

到稿日期: 2013-06-01 返修日期: 2013-07-15 本文受国家自然科学基金项目(60973016, 61272175), 四川省科技厅项目(2012JY009), 四川省教育厅重点项目(2011ZA173)资助。

樊富有(1974—), 男, 博士生, 副教授, 主要研究方向为量子计算和量子可逆逻辑电路综合, E-mail: fanfuyou@163.com; 杨国武(1966—), 男, 博士, 教授, 博士生导师, 主要研究方向为量子计算、逻辑综合、形式化验证、算法优化; 李晓瑜(1984—), 女, 博士生, 主要研究方向为量子计算; 罗庆斌(1987—), 男, 博士生, 主要研究方向为可逆逻辑综合。

逻辑电路综合的算法,针对特定情况各有优劣。另外,针对二值、三值或多值/混合值的量子可逆逻辑电路的综合的研究也在不断推进中。但是,到目前为止,尚未研究出任何一个通用的量子可逆逻辑电路综合算法,由此可见,这方面的工作有待进一步研究和开展。

本文主要针对混合多值 5-qubits 量子可逆逻辑电路综合问题进行分析。基于量子逻辑电路综合中量子门库的研究,Toffoli 门的合成是整个合成过程中最为关键的一步。因为仅使用 CNOT 门合成量子电路时,需要首先合成 Toffoli 门,再利用 Toffoli 快速合成量子电路,最后对电路进行优化,实现量子电路的最优或者较优合成。在这个过程中,本文提出了 PMX 量子门的构造过程。当然在合成 Toffoli 门时需要验证 CNOT 门的合成能力,明确 Toffoli 门是否可通过 CNOT 门合成,然后实现对 Toffoli 门的合成。

2 量子多值可逆逻辑电路基本概念

根据文献[2],量子计算机是由连线和基本量子门排列起来的量子信息处理线路。同时,量子计算机可以等效为量子图灵机,即等价为一个由量子逻辑门级联构成的量子逻辑电路。最常用的量子逻辑门主要包括 NOT 门、CNOT 门、Toffoli 门、Fredkin 门、Swap 门、Hadamard 门等。这些逻辑门按其输入比特的数量又可以分为单比特量子逻辑门和多比特量子逻辑门,按其数值逻辑又可以分为二值逻辑量子门、三值逻辑和混合/多值逻辑量子门等。本节将会给出关于量子多值可逆逻辑电路的相关基本概念。

定义 1(量子比特) 一个量子比特(qubit)是一个用归一化的相互正交的量子态 $\{|0\rangle, |1\rangle\}$ 描述布尔值 0 和 1 的量子系统。这两个态形成计算基矢,量子比特的状态可以用叠加态 $\alpha|0\rangle + \beta|1\rangle$ 表示,其中 α 和 β 满足 $|\alpha|^2 + |\beta|^2 = 1$ 。一个量子比特是一个典型的微观系统,比如一个原子、一个核自旋,或者一个偏振的光子。量子比特的制备和操作必须通过酉变换实现。

定义 2(量子逻辑门) 量子逻辑门是在固定的时间周期内对选定的量子比特进行固定的酉变换操作的逻辑器件,它是处理量子信息的基本单元。量子逻辑门的级联构成量子电路,量子电路必须是可逆的,即量子信息的动态过程在复向量空间上必须保持正交变换。在量子计算中,一个量子逻辑门对应一个么正变换。

定义 3(量子可逆逻辑门库) 量子可逆逻辑门库 L_n 表示 $n \times n$ 量子可逆逻辑门的集合,它用于综合 $n \times n$ 的量子可逆逻辑电路,简称为 L_n 。用 $T(L)$ 表示库 L 能综合的所有 $n \times n$ 量子可逆逻辑电路的集合^[18]。

定义 4(受控非门 CNOT 门) 受控非门有两个输入量子比特,分别为控制量子比特和目标量子比特,线路如图 1 所示,上面的线表示控制量子比特,下面的线表示目标量子比特。该门的矩阵表示方法亦如图 1 中 U_{CN} 矩阵所示。

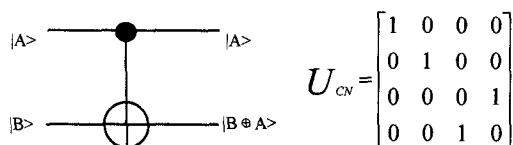


图 1 受控非门(CNOT)的线路表示和矩阵表示

CNOT 门的作用为,若控制量子比特为 0,则目标量子比

特将保持不变;若控制量子比特为 1,则目标量子比特将翻转。其方程形式表示为:

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle$$

多量子比特逻辑门的原型是 CNOT 门,它可以被视为一类推广的异或门,而且理论已经证明:任意的多量子比特门都可由受控非门和单量子比特门复合而成。

定义 5(量子 Toffoli 门) 量子 Toffoli 门有 3 个输入量子比特和 3 个输出量子比特,如图 2(a)所示,两个控制比特不受 Toffoli 门作用的影响,第 3 个比特是目标比特,在控制比特同时置为 1 时翻转,否则不变。

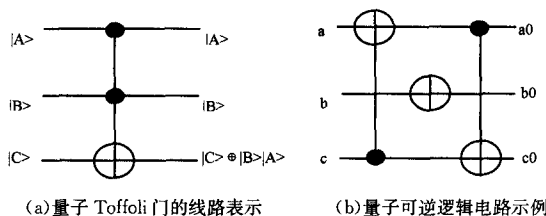


图 2

定义 6(可逆函数与可逆逻辑) 对于有 n 个输入和 n 个输出变量的布尔函数 $f(x_1, x_2, \dots, x_k) = (y_1, y_2, \dots, y_k)$ 是可逆函数,当且仅当它是双射函数,即输入与输出间是一一对应的关系。任意一个输入都对应着唯一的输出。

定义 7(可逆逻辑电路) 能用可逆逻辑函数描述的电路称为可逆逻辑电路。如图 2(b)所示,可逆逻辑电路的特点是:(1)输入线数与输出线数相等;(2)没有扇出与扇入;(3)没有反馈;(4)电路分层级联,有时为保证电路可逆,需添加一些辅助位,即垃圾位。 $n \times n$ 规模的量子电路即为 n 位输入和 n 位输出的量子逻辑电路。

定义 8(多值逻辑) 一个命题不但可以是二值的,也可以是三值的,甚至是四值、五值。因此,对每一自然数 n ,有 n 值,以至于无穷多值。研究这类命题之间逻辑关系的理论,即为多值逻辑。以 $0, 1, \dots, n-1$ 表示命题的 n 个值,而把 0 解释为真; $n-1$ 解释为假; $i(0 < i < n-1)$ 解释为不同程度的概率 $1-i/(n-1)$ 。

多值逻辑建立于 20 世纪 20 年代初,由卢卡西维茨和美国逻辑学家 E. L. 波斯特创建。卢卡西维茨在其 1920 年发表的《论三值逻辑》一文中,建立了一个三值逻辑系统。波斯特在其 1921 年发表的《初等命题的一般理论》一文中,建立了任意有穷多个值的逻辑系统。该系统对于任意的自然数 $n > 2$,序列 $t_1, t_2, \dots, t_n$ 的每一项都可以取作命题的值,其中 t_1 为真值, t_n 为假值。

3 PMX 量子门的构造

本文主要研究混合多值 5-qubits 量子可逆逻辑电路综合问题,通过构造 PMX 量子门来验证 CNOT 门合成 Toffoli 门的能力。图 3 所示为本文主要研究对象的电路模型:混合多值 5-qubits 的量子逻辑电路。其中,量子线 q_1, q_2, q_3, q_4, q_5 分别取 3, 2, 2, 2, 2 值。该量子逻辑电路直接合成 Toffoli 门还很不现实,即使使用双向搜索以及剪枝技术也同样如此。

一般的搜索算法出现空间不足非常常见,目前使用双向搜索最多前进 7~8 步,即合成的量子电路长度最多达到 16。从本课题所做的相关实验来看 Toffoli 门的最优合成的电路长度不小于 16,故而使用一般的搜索算法还不足以解决 Toffoli 门的合成。从另一个角度来考虑,根据欲合成的量子逻辑电路本身的特征,可以采取预先构造一些量子门,再用这些

量子门来合成其它更复杂的量子门的方法和思路。依据这种想法,本课题构造了一个特殊的量子门,这里称之为 PMX 门,接下来将主要介绍 PMX 门的构造过程。

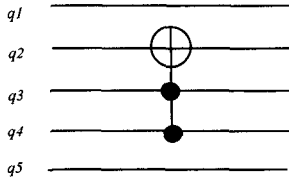


图3 多值 5-qubits 量子逻辑电路

同二值可逆逻辑不同,在多值可逆逻辑中仅使用 CNOT 门来合成 Toffoli 门是可行的,这也是同二值逻辑差别最大的地方。利用多值可逆逻辑来合成 Toffoli 门的特殊的量子门 PMX 是其最为关键的地方。故而在构造 PMX 可逆逻辑门时,需要预先构造控制量子线通过多值量子线来改变目标量子线的量子电路,以及其它可改变目标量子线的量子电路。

在合成特殊的量子门 PMX 门时,需保证除了具有多值的量子线路和目标量子线发生改变外,其它量子线在经过 PMX 门后不发生改变。为保证某条量子线路不发生改变,应使该量子线路的相同操作的重复次数与其线路的值相同。为此我们构造了一个控制量子线通过多值量子线来改变目标量子线的量子可逆逻辑电路,如图 4 所示。

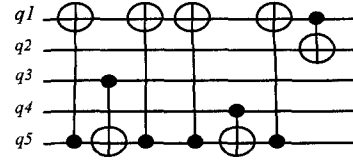


图4 多值控制量子线电路

把图 4 所示的量子电路重复级联 3 次,同时在量子电路之前加入量子线路 q1 对目标量子线 q2 的控制,可得到如图 5 所示的量子电路。

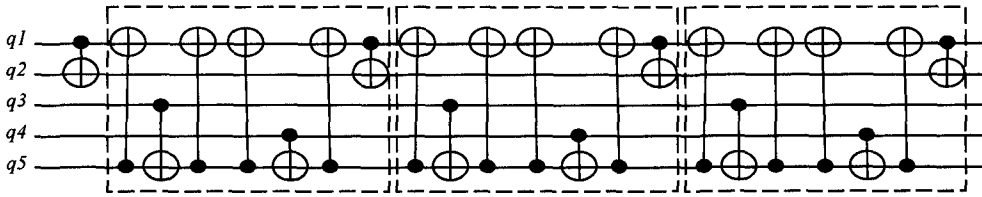


图5 增加 q1 对目标量子线 q2 的控制后电路

图 5 所示的量子电路中还没能确保量子线路 q5 不发生改变,增加量子门恢复量子线路 q5 原有值,并进一步改变目标量子线路 q2 的值。增加的量子电路如图 6 所示。

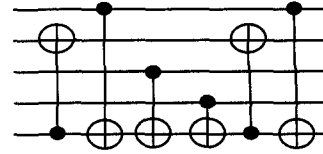


图6 恢复量子线路 q5 原有值的量子门

将图 6 所示的增加的量子电路同图 5 所示的电路连接,即可得到所想要构造的 PMX 电路,如图 7 所示。

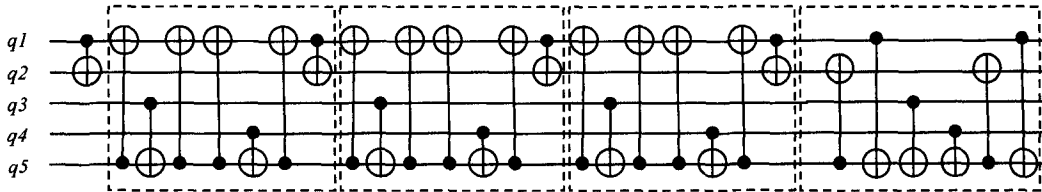


图7 PMX 门逻辑电路

4 混合多值 5-qubits 可逆逻辑电路的综合与验证

量子可逆逻辑电路综合就是根据电路功能,使用规定的量子门自动生成量子代价较小的量子可逆逻辑电路。通常认为量子综合代价是指使用量子门的数量,最优的量子电路是指使用量子门的数量最少。本节主要验证 PMX 量子逻辑门构造完成之后,使用双向搜索算法来验证 PMX 门和 CNOT 门合成 Toffoli 门的能力。

4.1 双向搜索算法

本文使用的双向搜索算法,主要是在作者前期工作^[16]的基础上实现的,算法描述如下。BDS 与一般的单边搜索算法相比在内存需求上大了一倍,效率提高了一倍。大量的实验数据与分析,亦可参考文献^[16]。

算法 双向搜索算法(Bi-direction Search, BDS)

输入:库 L,可逆函数 g

输出: leng, h₁, h₂, ..., h_{leng}

- (1) Af(0)={()}; Ab(0)={g}; Flag=0; i=1;
- (2) While Flag=0 do
- (3) Af(i)=Af(i-1)L; Ab(i)=L-1Ab(i-1);
- (4) If Af(i) ∩ Ab(i-1) ≠ ∅ then
- (5) Flag=1; leng=2i-1;
- (6) Select a in Af(i) ∩ Ab(i-1), find h₁, h₂, ..., h_i, h_{i+1}, ..., h_{2i-1} in L such that a=h₁h₂...h_i=g(h_{2i-1})-1...-(h_{i+1})-1;
- (7) Elseif Af(i) ∩ Ab(i) ≠ ∅ then
- (8) Flag=1; leng=2i;
- (9) Select a in Af(i) ∩ Ab(i), find h₁, h₂, ..., h_i, h_{i+1}, ..., h_{2i} in L such that a=h₁h₂...h_i=g(h_{2i})-1...-(h_{i+1})-1;
- (10) Else i=i+1;
- (11) End while.

4.2 基于 CNOT 门库的多值可逆逻辑综合

在第 3 节中完成 PMX 构造后,将其作为一个已有的量

(下转第 134 页)

成还需要部分人为的参与,如果 Web 服务领域本体较大,会给数据关联表的维护带来较大的困难,如何实现数据关联表的自动生成需要进一步的研究;(2)基于 Web 服务组合的 Petri 网,研究 Web 服务组合的相关结构性及服务规划等。

参考文献

- [1] Fan J, Kambhampati S. A snapshot of public Web services[J]. SIGMOD Record, 2005, 34(1): 24-32
- [2] Benatallah B, Dumas M, Fauvet M, et al. Towards Patterns of Web Services Composition [M] // Patterns and Skeletons for Parallel and Distributed Computing. Springer Verlag, UK, 2003: 265-296
- [3] Rao J H, Su X M. A Survey of Automated Web Service Composition Methods [A] // Proceedings of the First International Workshop on Semantic Web Services and Web Process Composition (SWSWPC 2004). San Diego, USA, July 2004: 43-54
- [4] Srivastava B, Koehler J. Web Service Composition-Current Solutions and Open Problems [C] // ICAPS 2003 Workshop on Planning for Web Services. Trento, Italy, June 2003: 51-59
- [5] Milano Vic N, Malek M. Current Solutions for Web Service

- Composition [J]. IEEE Internet Computing, 2004, 8(6): 51-59
- [6] 汤宪飞, 蒋昌俊, 丁志军, 等. 基于 Petri 网的语义 Web 服务自动组合方法[J]. 软件学报, 2007, 8(12): 2991-3000
- [7] 郭玉彬, 杜玉越, 奚建清. Web 服务组合的有色网模型及运算性质[J]. 计算机学报, 2006, 29(7): 1067-1075
- [8] 马炳先, 徐颖蕾. 动态描述逻辑动作间关系的 Petri 网分析方法研究[J]. 自动化学报, 2007, 33(11): 1144-1149
- [9] 范贵生, 虞慧群, 陈丽琼, 等. 基于 Petri 网的服务组合故障诊断与处理[J]. 软件学报, 2010, 21(2): 231-247
- [10] 张正明, 马炳先, 相东明. 基于 Petri 网的 Web 服务的创建与描述[J]. 系统仿真学报, 2011, 23(s1): 19-25
- [11] 马炳先, 相东明, 张正明. Web 服务组合的 Petri 网自动生成方法[J]. Journal of Chinese Computer System, 2013, 34(2)
- [12] Billington J, Christensen S, van Hee K, et al. The Petri Net Markup Language: Concepts, technology, and tools [C] // van der Aalst W, Best E, eds. 24th International Conference Application and Theory of Petri Nets 2003, LNCS 2679. Berlin: Springer, 2003, 6: 483-505
- [13] 张正明, 马炳先, 相东明. 基于 Petri 网的 Web 服务注册方法的研究与实现[J]. 电信科学, 2012, 11(28): 86-91

(上接第 117 页)

子门使用,再利用一般的量子合成算法进行合成。这里我们使用了双向搜索算法,这一点在前面已经进行了介绍。最后得到 Toffoli 门的 CNOT 合成电路,如图 8 所示,其中 PMX 指在前面构造的 PMX 量子逻辑门电路。

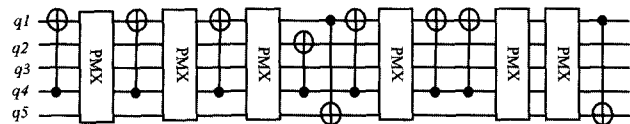


图 8 基于 CNOT 门和 PMX 门的 Toffoli 门的合成

结束语 本文研究了混合多值 5-qubits 量子可逆逻辑电路综合问题,主要针对仅使用 CNOT 门合成 Toffoli 门的可行性进行了分析。为了验证 CNOT 门合成 Toffoli 门的能力,提出了一个自行构造的特殊量子门 PMX。PMX 量子逻辑门构造完成之后,将其作为门库的一个单元,然后使用双向搜索算法来验证 PMX 门和 CNOT 门合成 Toffoli 门的能力。混合多值 5-qubits 可逆逻辑电路的综合与验证结果显示,本文构造的 PMX 量子门能有效地验证 CNOT 门对于广义 Toffoli 门的合成能力,而且双向搜索算法显示与一般的单边搜索算法相比,在效率上至少提高了一倍。

参考文献

- [1] Fredkin E, Toffoli T. Conservative logic [J]. International Journal of Theoretical Physics, 1982, 21: 219-253
- [2] Nielsen M A, Chuang I L. Quantum computation and quantum information [M]. Cambridge, UK: Cambridge University Press, 2000
- [3] Landauer R. Irreversibility and heat generation of the computing process[J]. IBM Journal of Research and Development, 1961, 5(3): 183-191
- [4] Reck M, Zeilinger A, Bernstein H J, et al. Experimental realization of any discrete unitary operator [J]. Phys. Rev. Lett., 1994, 73(1): 58431
- [5] DiVincenzo D P. Two-bit gates are universal for quantum com-

- putation [J]. Phys. Rev. A, 1995, 51(2): 1015-1022
- [6] Deutsch D, Barenco A, Ekert A. Universality in quantum computation [J]. Mathematical and Physical Sciences, 1995, 449(1937): 669-677
- [7] Yang Guo-wu, Song Xiao-yu, Perkowski M, et al. Realization ternary quantum switching networks without ancilla bits[J]. Journal of Physics A: Mathematical and General, 2005, 38(44): 9689-9698
- [8] Yang Guo-wu, Xie Fei, Song Xiao-yu, et al. Universality of 2-Qudit Ternary Reversible Gates[J]. Journal of Physics A: Mathematical and General, 2006, 39(24): 7763-7773
- [9] Iwama K, Kambayashi Y, Yamashita S. Transformation rules for designing CNOT-based quantum circuits [J]. Proceedings of Design Automation Conference. New Orleans, LA, USA, 2002, 28(4): 419-425
- [10] Shende V V, Prasad A K, Markov I L, et al. Synthesis of reversible logic circuits [J]. IEEE Trans on Circuits and Systems-I, 2003, 22(6): 723-729
- [11] Miller D M, Maslov D, Gueck G W. Spectral and two-place decomposition techniques in reversible logic [C] // Proceedings of the 45th IEEE International Midwest Symposium on Circuits and Systems. Tulsa, AR, USA, 2002: 493-496
- [12] Song X Y, Yang G W, Perkowski M, et al. Algebraic characteristics of reversible gates [J]. Theory of Computing Systems, 2004, 37(2): 311-319
- [13] Maslov D, Dueck G W, Miller D M. Toffoli network synthesis with templates [J]. IEEE Trans on Circuits and Systems-I, 2005, 24(6): 807-817
- [14] Yang Guo-wu, Song Xiao-yu, William N, et al. Group theory based synthesis of binary reversible circuits [J]. Lecture Notes in Computer Science, 2006, 3959: 365-374
- [15] 李志强, 陈汉武, 徐宝文. 基于 Hash 表的量子可逆逻辑电路综合的快速算法[J]. 计算机研究与发展, 2008, 45(12): 2162-2171
- [16] Yang Guo-wu, Song Xiao-yu, Hung W N N, et al. Bi-directional Synthesis of 4-bit reversible Circuits [J]. The Computer Journal, 2008, 51(2): 207-215