

一种 MCT 门量子可逆线路分解与优化方法



张苏嘉¹, 管致锦^{1,2*}, 杨雪婷¹

(1. 仰恩大学 工程技术学院, 泉州 362014; 2. 南通大学 信息科学技术学院, 南通 226019)

摘要 为提高可逆线路中 MCT 门的分解和优化效率, 提出了一种 MCT 门的优化分解方法, 根据该方法得出 MCT 分解模板并验证了正确性。基于该模板给出了相应的分解与优化算法, 算法对 MCT 门分解出的 Toffoli 线路进行分类, 使用优化分解模板将其分解为 NCV 线路。该算法的时间复杂度为 $O(m)$, 优于传统算法的复杂度 $O(m^2)$ 。通过对控制位 $m \in \{3, 10\}$ 的 MCT 门与 Benchmark 可逆线路的实验, 验证了该算法优化和分解的有效性。

关键词 电路优化; MCT 门; NCV 门; 量子电路; 可逆逻辑综合

中图分类号 TP791 文献标志码 A DOI 10.12178/1001-0548.2022233

A Method for Decomposing and Optimizing MCT Gate Quantum Reversible Circuits

ZHANG Sujia¹, GUAN Zhijin^{1,2*}, and YANG Xueting¹

(1. School of Engineering and Technology, Yang-En University, Quanzhou 362014, China;

2. School of Information Science and Technology, Nantong University, Nantong 226019, China)

Abstract One of the key problems in reversible logic synthesis is optimizing the reversible circuits, and the focus of research is on how to decompose advanced reversible gates into basic reversible gates more efficiently. To improve the decomposition and optimization efficiency of Multiple Control Target (MCT) gates, an optimal decomposition method of MCT gates is proposed in the paper, along with an MCT decomposition template which correctness is verified. Based on this template, the corresponding decomposition and optimization algorithm is given. Using the optimal decomposition template, the algorithm classifies the Toffoli circuits decomposed by MCT gates and decomposes them into NCV circuits. The time complexity of the algorithm is $O(m)$, which is better than $O(m^2)$ for the conventional algorithm. Experiments on MCT gates with benchmark reversible circuits for control bits $m \in \{3, 10\}$ show the effectiveness of the algorithm's optimization and decomposition.

Key words circuit optimization; MCT gate; NCV gate; quantum circuit; reversible logic synthesis

可逆逻辑综合^[1-2]是可逆计算研究的关键问题之一, 也是量子计算和量子信息技术的重要组成部分。最初可逆计算的提出是为了解决计算机中的能量消耗问题, 文献 [3] 指出在传统计算过程中, 由于擦除信息的不可逆造成了能耗的产生。文献 [4] 证明了对所有不可逆图灵机都有一个可逆图灵机, 即计算机中的每步操作均可变为可逆操作, 且可逆逻辑计算可避免传统计算过程中的能量消耗。

所有的量子计算都是可逆计算, 量子计算的算法可以通过量子可逆线路表示。可逆逻辑线路分解与优化是量子线路设计过程中至关重要的步骤, 选

取合适的分解与优化方法能够有利于将高级量子线路分解为低级量子线路, 以进一步转换为已有不同量子计算机可执行量子线路。因此, 可逆逻辑线路的分解与优化研究是量子计算技术的重要内容。

现有的可逆电路化简方法有基于规则的方法^[5-7]与基于模板^[8-9]的方法。文献 [6] 提出 Toffoli 电路的约简规则, 根据移动规则对可逆电路进行扫描, 寻找满足约简规则的进行优化, 直到电路不发生变化为止。文献 [9] 提出了可逆电路优化模板, 通过模板等价替换某部分逻辑门, 达到减少逻辑门的目的。但现有研究多针对量子线路进行设计优化^[1, 2, 8-15],

收稿日期: 2022-07-12; 修回日期: 2022-12-07

基金项目: 国家自然科学基金 (62072259); 福建省科技厅引导性项目 (2021H0029)

作者简介: 张苏嘉, 主要从事量子可逆逻辑综合方面的研究。

*通信作者 E-mail: Guan.zj@ntu.edu.cn

没有把高级量子可逆线路转换为接近物理量子计算机执行的低级量子线路，且时间代价较高，如何把高级量子线路如 MCT 门 (Multiple Control Target) 更高效地分解并优化为低级量子线路如 NCV 门的研究较少。

本文提出了一种 MCT 门分解为 NCV 门的模板，与现有分解方法相比，能降低量子代价和分解时间，提高分解效率。

1 基本概念

1.1 MCT 门库

MCT 门是指多控制单目标的量子门，可逆电路由可逆逻辑门级联组成，MCT 门是最常见的可逆逻辑门，属于高级量子线路。常用的 MCT 门包括 NOT 门、CNOT 门、Toffoli 门等。一个 MCT 门可表示为 $MCT(\{x_i, \dots, x_j\}, x_k)$ ，其中 $i, j, k = \{1, 2, \dots, n\}$ ， $k \neq i, j$ 。

为了表述方便，本文 Toffoli 门特指控制位为 2 的 MCT 门，MCT 门特指控制位大于等于 3 的 MCT 门，图 1 中 \bullet 代表控制位， \oplus 代表目标位。

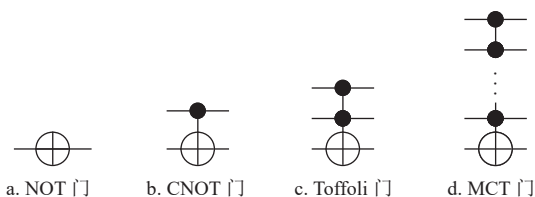


图 1 常见 MCT 门

能够被量子计算机执行的是基础量子门。常见的基础量子门有 NCV 门，其图形符号如图 2 所示。

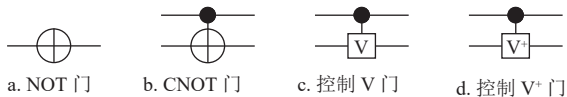


图 2 NCV 门库

1.2 量子逻辑线路

在量子线路中，一根量子线代表一个量子位，几根量子线之间的量子门代表这几个量子位之间的量子运算。如图 3a 所示线路表示当 L1、L2 线都为 1 时，L3 线取反，相当于电子线路中一个与非门。

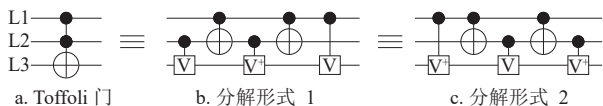


图 3 Toffoli 门的两种分解形式

量子算法可以通过量子线路来表示，所有可逆量子门都可以通过量子门串并联得到。因此可将可逆线路中每一个可逆电路分解为等价的由基础量子门组成的量子门电路^[6]。常见的分解办法是先将 MCT 门分解为 Toffoli 线路，再将 Toffoli 线路分解为 NCV 线路。

Toffoli 门可等价分解为 NCV 门组成的线路^[16]，如图 3b 所示。由文献 [17] 可知，可逆线路中，V 门和 V⁺ 门可以相互交换位置且不影响线路功能，因此 Toffoli 门还可分解为另一种形式，如图 3c 所示。

1.3 量子代价

一般常用量子代价对可逆电路的复杂度进行度量。量子代价指构建可逆量子电路所需的基础量子门的数量。由于 NCV 门是基础量子门，所以 NCV 电路中 NCV 门的数量即为其量子代价。所有可逆门均可通过基础可逆门构造^[8]。如图 3 所示，Toffoli 门可由 5 个 NCV 门组成，其量子代价为 5。

量子代价是可逆电路优化程度的重要指标，本文用量子代价来评价 MCT 门分解为 NCV 门的效果。

1.4 化简规则

交换规则：对于变量域集合 $\{x_1, x_2, \dots, x_n\}$ ，广义 MCT 门可表示为 $MCT(C, T)$ ，其中控制线集 $C = \{x_{i1}, x_{i2}, \dots, x_{im}\}$ ，目标位 $T = \{x_k\}$ 。对于两个相邻的门 $G_1 = MCT(C_1, T_1)$ 和 $G_2 = MCT(C_2, T_2)$ ，若存在 $C_1 \cap T_2 = \emptyset$ 且 $C_2 \cap T_1 = \emptyset$ ，即两个门的控制位不会影响到对方的目标位，则交换这两个门的位置不会影响原线路的逻辑功能^[8]。

图 4 中 G_1 的控制位与 G_2 的目标位在同一量子位线上，因此不可交换； G_5 和 G_6 的控制位都不影响到对方的目标位，可以进行交换。同理， G_5 也可与 $G_7 \sim G_{10}$ 进行交换。

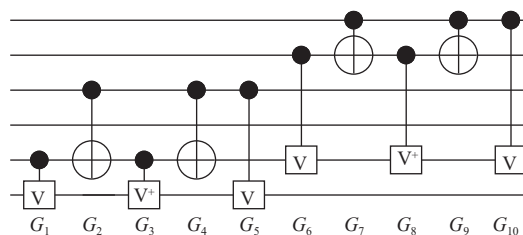


图 4 交换规则

删除规则：线路中相邻的（或移动后相邻的）具有相同控制位和目标位的两个门，能够形成单位

映射, 如图 5 所示。如两个相邻的 CNOT 门, 由于其控制位和目标位一致, 当控制位为 1 时, 目标位经两次取反后结果与原值相同, 因此可以删除该门对而不影响原线路功能^[6], 称为门删除规则。

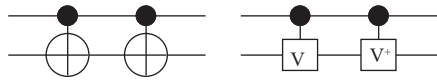


图 5 删除规则

2 MCT 门优化分解模板设计

MCT 线路是高级量子线路, 需分解为基础量子线路如 NCV 才能在量子计算机中实现对应功能。目前许多研究工作围绕着分解后的 NCV 线路进行优化, 若能将分解与优化同时进行, 可减少后续线路优化的工作量, 大幅提高量子电路的优化效果。本文提出了针对特定的 MCT 门分解为 NCV 门的分解模板, 对 MCT 分解后产生的 Toffoli 门同时进行优化和分解, 得到量子代价低的 NCV 线路, 同时也能有效降低时间复杂度。

2.1 问题分析

以下表述中, n 表示线路数, m 表示一个 MCT 门的控制位数, $n \in \{4, 5, \dots, n\}$, $m \in \{3, 4, \dots, m\}$ 。

为了实现 MCT 线路中逻辑门的分解^[18], 若 $m=n-1$, 则需在原线路上的控制位和目标位间添加一条辅助线(空线), 如图 6 所示。

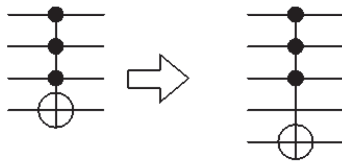


图 6 添加辅助线

由文献 [16] 可知, 若量子可逆线路数 $n \geq 5$, $m \in \{3, 4, \dots, n/2\}$, 则含有 m 个控制位的 MCT 门可分解为如下形式的含有 $4(m-2)$ 个 Toffoli 门的线路。如 $m=4$, $n=7$, $n/2$ 取 4, 则 $m \in \{3, 4\}$, 该

MCT 门可以分解为 8 个 Toffoli 门, 分解结果如图 7 所示。

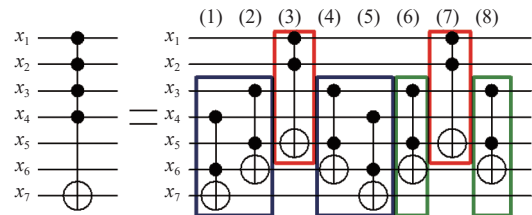


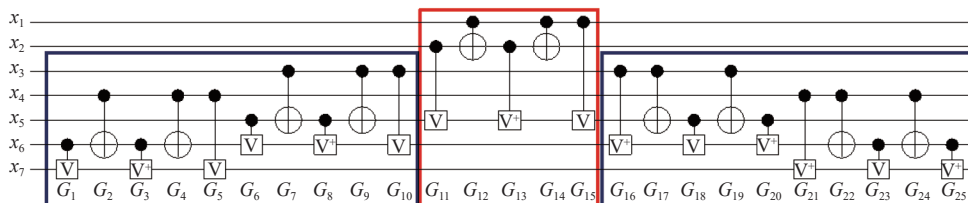
图 7 MCT 门分解为 Toffoli 线路

图 7 所示的 MCT 门中, $m=4$, $n=7$, 将 $G_{MCT} = MCT(\{x_1, x_2, x_3, x_4, x_7\})$ 分解为 Toffoli 门的组合, $G_1 = MCT(\{x_4, x_6, x_7\})$, $G_2 = MCT(\{x_3, x_5, x_6\})$, $G_3 = MCT(\{x_1, x_2, x_5\})$, $G_4 = MCT(\{x_3, x_5, x_6\})$, $G_5 = MCT(\{x_4, x_6, x_7\})$, $G_6 = MCT(\{x_3, x_5, x_6\})$, $G_7 = MCT(\{x_1, x_2, x_5\})$, $G_8 = MCT(\{x_3, x_5, x_6\})$ 。

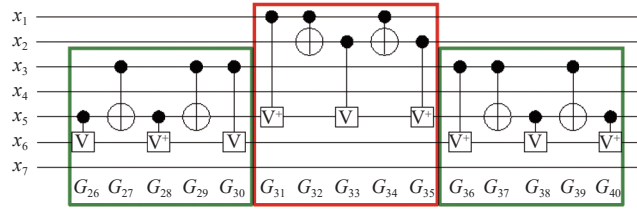
观察分解出的 Toffoli 线路, 发现其存在一定的规律和对称性。将电路分成 3 组, 每组有左右对称的 Toffoli 电路, 如 G_1 、 G_2 和 G_4 、 G_5 以 G_3 对称; 之后把 G_1 、 G_2 用图 3b, G_4 、 G_5 用图 3c 的分解方法, 分解为两种不同 NCV 电路。结果如图 8 所示。

图 8 中由于 G_1 和 G_2 的控制位与目标位不相同, 因此分解出的 NCV 所在的控制位与目标位也不相同。根据 1.4 节化简规则, G_{10} 和 G_{11} 的控制位和目标位无交集, 即 $C_{10} \cap T_{11} = \emptyset$ 且 $C_{11} \cap T_{10} = \emptyset$, 可以将两门位置互换。同理, G_{10} 与 $G_{12} \sim G_{15}$ 逐个交换后, 与 G_{16} 相邻并形成映射门对, 可同时删除 G_{10} 与 G_{16} 。遍历该电路后, 删除所有可以形成(或移动后可形成)单位映射的门对, 最终线路如图 9 所示。

对比图 8 和图 9 可发现, 使用 MCT 分解规则后, 分解出的 Toffoli 存在对称性, 用化简规则处理后, 可得到 Toffoli 分解模板。其他符合 MCT 分解规则的 MCT 门亦可分解为有规则的 Toffoli 线路, 因此均可按上述方法进行 Toffoli 线路分解为优化的 NCV 线路。



a. 图 7 中 $G_1 \sim G_5$ 的分解结果



b. 图 7 中 $G_6 \sim G_8$ 的分解结果

图 8 一般方法的分解结果

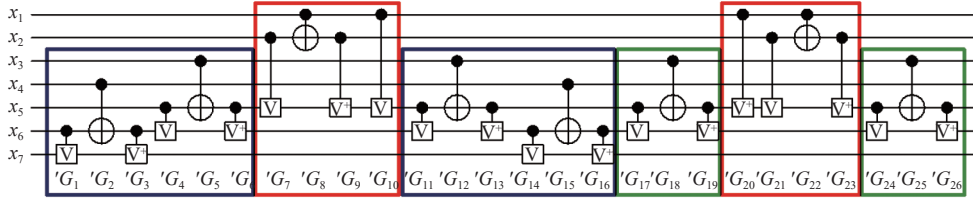


图 9 优化后的结果

2.2 分解模板

基于上述 2.1 节的分析，本文提出一种 MCT 分解模板，对分解出的 Toffoli 线路套用模板后可同时完成分解和优化工作。

分解模板 1：使用 MCT 分解规则后，若分解出的 Toffoli 门是第 $m-1$ 个或第 $3m-5$ 个 Toffoli 门时，称其为特殊 Toffoli 门。此种情况下，可将 Toffoli 门使用模板替换为量子代价为 4 的 NCV 线路。如图 10 所示。

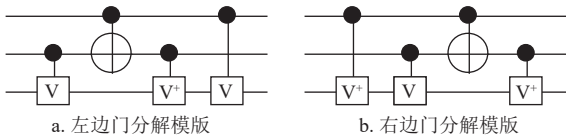


图 10 特殊 Toffoli 门优化分解模板

分解模板 2：当分解出的 Toffoli 门不是特殊门时，称为一般的 Toffoli 门。此时的 Toffoli 门可使用模板直接替换为图 11 所示的 3 量子代价的 NCV 线路。

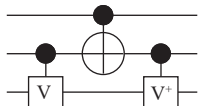


图 11 普通 Toffoli 门优化分解模板

3 MCT 门分解优化算法

根据提出的 MCT 分解为 NCV 的优化模板，给出了 MCT 分解优化算法：先对 MCT 门进行判断，若符合 MCT 分解规则，则应用 Toffoli 分解模板 1、2 进行处理。设欲优化的 MCT 门输入线数

为 n ，控制位数为 m 。MCT 门优化分解算法如下。

Input: MCT 线路 G ，线数 n ，控制位数 m

Output: NCV 线路 G'

begin

if ($m \in \{3, 4, \dots, n/2\}$)

 分解成 $4(m-2)$ 个 Toffoli 门

 for ($i=0$ to $i < 4(m-2)$) do

 if 是特殊门 应用分解模板 1

 else 应用分解模板 2

$i++$

end

本算法的时间复杂度为 $O(m)$ 。在传统的方法中，文献 [18] 先将 MCT 门分解为 NCV 线路，遍历所有分解后的 NCV 门，逐个查找后面是否有可以删除的可逆门对，直到线路无变化为止，所需时间复杂度为 $O(m^2)$ 。

4 实验结果与分析

为了验证所提优化模板的有效性，使用 C++ 语言实现了本文描述的算法，实验环境为 Intel(R) Core(TM) i5-7200U CPU@2.5 GHz、8 GB 内存及 Windows10 操作系统。分别用本文算法和已有算法对 $m \in \{3, 10\}$ 的 MCT 门进行测试，结果如表 1 所示。

为测试在实际应用中的效果，分别用本文算法和已有算法对 Benchmark 部分例题进行实验，结果如表 2 所示。可以看出，本算法的量子代价与文献 [18] 方法优化后的量子代价基本一致，但运行时间有较大改善。结果表明，本算法对于控制位越

多的 MCT 门, 分解时量子代价、执行时间的优化效果越好, 整体优化效果越明显。

表 1 MCT 门分解效果

Benchmark	量子代价			执行时间/s		
	分解后未化简	先分解, 再优化 ^[18]	本文算法	分解后未化简	先分解, 再优化 ^[18]	本文算法
3_17_13	14	14	14	-	0.002	0.002
4gt10-va_81	48	36	36	-	0.012	0.005
4gt11_84	7	7	7	-	0.003	0.001
4gt4-v0_80	58	44	44	-	0.025	0.006
4gt5_75	28	22	22	-	0.008	0.003
ham15_108	642	458	458	-	1.76	0.079
Ham7_104	111	87	87	-	0.061	0.010
Hwb4_52	23	23	23	-	0.007	0.002
Hwb6_58	170	144	146	-	0.142	0.021
ModSadder_128	111	87	87	-	0.105	0.012

表 2 Benchmark 分解效果

MCT门	量子代价			执行时间/s		
	分解后未化简	先分解, 再优化 ^[18]	本文算法	分解后未化简	先分解, 再优化 ^[18]	本文算法
$n=6, m=3$	20	14	14	0.003	0.004	0.003
$n=8, m=4$	40	26	26	0.008	0.011	0.005
$n=10, m=5$	60	38	38	0.008	0.018	0.008
$n=12, m=6$	80	50	50	0.011	0.033	0.009
$n=14, m=7$	100	62	62	0.013	0.040	0.010
$n=16, m=8$	120	74	74	0.020	0.057	0.012
$n=18, m=9$	140	86	86	0.021	0.086	0.018
$n=20, m=10$	160	98	98	0.028	0.093	0.020

5 结束语

本文提出了一种 MCT 门分解模板, 套用该模板可快速完成 MCT 转 NCV 的分解与优化。与文献 [12] 中先得到传统方法分解出的 NCV 线路, 再对 NCV 线路进行优化的方法相比, 时间复杂度由 $O(m^2)$ 降为 $O(m)$ 。通过对控制位 $m \in \{3, 10\}$ 的 MCT 门与部分 Benchmark 例题进行测试, 验证了该算法的有效性。今后将尝试其进一步分解, 同时也考虑加入 Peres 或 Fredkin 等新门, 进一步降低量子代价。

参考文献

- [1] 陈汉武, 李文骞, 阮越, 等. 基于汉明距离递减变换的可逆逻辑综合算法[J]. 计算机学报, 2014, 37(8): 1840-1845.
CHEN H W, LI W Q, RUAN Y, et al. A synthesis algorithm of reversible logic circuit based on the decreasing transform of Hamming distance[J]. Chinese Journal of Computers, 2014, 37(8): 1840-1845.
- [2] GAO FENG L, SHE XIANG J, LIANG Z. Quantum image filtering and its reversible logic circuit design[J]. International Journal of Embedded Systems, 2021, 14(3): 248-258.
- [3] LANDAUER R. Irreversibility and heat generation in the computing process (reprinted from IBM research and development, vol 5, 1961)[J]. IBM Journal of Research and Development, 2000, 44(1/2): 261-269.
- [4] BENNET M A, SELVI T M, PRIYA S M, et al. Efficient approaches for designing the logical reversibility of computation[J]. International Journal on Smart Sensing and Intelligent Systems, 2017, 10(4): 46-61.
- [5] ARABZADEH M, SAEEDI M, ZAMANI M S. Rule-Based optimization of reversible circuits[C]//2010 15th Asia and South Pacific Design Automation Conference (ASP-DAC 2010). New York: IEEE, 2010: 853-858.
- [6] 程学云, 谈莹莹, 管致锦, 等. 优化的可逆 MCT 电路化简算法[J]. 量子电子学报, 2017, 34(6): 713-720.
CHENG X Y, TAN Y Y, GUAN Z J, et al. An optimized simplification algorithm for reversible MCT circuits[J]. Chinese Journal of Quantum Electronics, 2017, 34(6): 713-720.
- [7] 王艺臻, 管致锦, 管海宇. 基于预评价的量子电路线性最近邻综合算法[J]. 量子电子学报, 2021, 38(1): 75-85.

- WANG Y Z, GUAN Z J, GUAN H Y. Linear nearest neighbor synthesis algorithm of quantum circuits based on pre-evaluation[J]. Chinese Journal of Quantum Electronics, 2021, 38(1): 75-85.
- [8] GOLUBITSKY O, MASLOV D. A study of optimal 4-bit reversible Toffoli circuits and their synthesis[J]. IEEE Transactions on Computers, 2012, 61(9): 1341-1353.
- [9] MASLOV D, DUECK G W, MILLER D M. Techniques for the synthesis of reversible Toffoli networks[J]. ACM Transactions on Design Automation of Electronic Systems (TODAES), 2007, 12(4): 42-62.
- [10] PHILIPP N, de ALEXANDRE A A A, GERHARD D, et al. Template-Based mapping of reversible circuits to IBM quantum computers[J]. Microprocessors and Microsystems, 2022, 90: 104487.
- [11] ESLAMY M, HOUSHMAND M, SEDIGHI M, et al. Optimization of one-way quantum computation measurement patterns[J]. International Journal of Theoretical Physics, 2018, 57(11): 3296-3317.
- [12] SLIMANI A, BENSLAMA A, MISRA N K. Optimal designs of reversible/quantum decoder circuit using new quantum gates[J]. International Journal of Theoretical Physics, 2022, 61: 72-91.
- [13] ADISA I A, WONG T G. Implementing quantum gates using length-3 dynamic quantum walks[J]. Physical Review Research, 2021, 104(4): 042604.
- [14] EZAWA M. Universal quantum gates, artificial neurons, and pattern recognition simulated by LC resonators[J]. Physical Review Research, 2021, 3(2): 023051.
- [15] ALI M B, RAHMAN M M, RAHMAN H A. Design and optimization of nanometric reversible 4 bit numerical comparator[C]//2012 International Conference on Informatics, Electronics & Vision (ICIEV). New York: IEEE, 2012: 577-581.
- [16] BARENCO A, BENNETT CH, CLEVE R, et al. Elementary gates for quantum computation[J]. Physical Review A, 1995, 52(5): 3457-3467.
- [17] MILLER D M, WILLE R, SASANIAN Z. Elementary quantum gate realizations for multiple-control Toffoli gates[C]//2011 41st IEEE International Symposium on Multiple-Valued Logic (ISMVL). Los Alamitos: IEEE, 2011: 288-293.
- [18] TAN Y Y, CHENG X Y, GUAN Z J, et al. Multi-Strategy based quantum cost reduction of linear nearest-neighbor quantum circuit[J]. Quantum Information Processing, 2018, 17(3): 61-73.

编辑 税 红