

文章编号:1005-0523(2011)06-0091-05

基于 Toffoli 门的可逆数值比较器的设计与优化

李明翠

(华东交通大学信息工程学院,江西 南昌 330013)

摘要:作为众多复杂量子电路的重要组成部分之一的可逆数值比较器还鲜有研究。首先基于 Pauli-X 门、CNOT 门和 Toffoli 门设计了 1 位可逆数值比较器和级联模块。多位数值比较器可在 1 位比较电路的基础上添加级联模块扩展得到。尔后对 4 位可逆数值比较器进行了优化设计以便作为更多位数值比较电路的基本模块。优化的电路垃圾输出减少 36%、量子门总数减少 24%,较好的提高了电路的性能。

关键词:量子;可逆;Toffoli;数值比较

中图分类号:TP387;TP302.2

文献标识码:A

实现量子计算机是量子计算科学的最重要的目标之一,如果一旦成为现实,将直接影响整个经济社会,极有可能成为新一轮产业革命的开端。量子电路的设计是实现该目标的重要一环。量子计算机的概念源于对可逆计算机的研究。随着芯片体积的缩小和集成度的提高,计算机的能耗对芯片的影响越来越大。能耗制约着集成度,也限制着计算机的运行速度。20 世纪 60 年代,IBM 公司的 Rolf Landauer^[1]考察了能耗问题后指出:能耗产生于计算过程中的不可逆操作。从物理原理上讲,无需擦除信息的可逆操作可以实现无能耗的计算^[2]。可逆电路的输入和输出存在一对一的映射关系,在操作的过程中不会丢失信息^[3],因此无需擦除信息。一个量子可逆逻辑电路是由可逆逻辑门构成的无循环网络。基本的可逆门包括:Pauli-X 门、受控非门(CNOT)、Toffoli 门等。迄今为止,已经提出了各种可逆加法器、乘法器等量子电路^[4-6],但对于数值比较器还缺乏研究。本文探索基于 Toffoli 门的可逆数值比较器的设计和优化。

1 可逆电路的设计原则

设计可逆量子电路的基本方法是:首先确定完成特定计算功能所需的量子门和量子门之间的联系;接下来进一步确定用这些量子门实现计算功能的最小量子门序列。

设计可逆电路的基本原则包括:① 最少垃圾输出原则。垃圾输出是指既不作为下一个可逆门的输入也不是当前需要的计算结果的输出。最少垃圾输出是可逆逻辑电路设计的一个最主要的挑战之一,在设计的过程中应尽可能多的使用每个量子门的输出。② 尽量少用常量输入。③ 最少可逆门原则。④ 尽量避免扇出,因为扇出需要额外的复制电路。⑤ 模块化设计原则。对小的电路进行模块化设计,这样可以很方便的用小模块组装出复杂的电路。

2 几个基本的可逆门

在一定时间间隔内实现逻辑变换的量子装置称为量子逻辑门。一个可逆门电路不仅可以由输入推断出输出,还能由输出推断出输入。传统的逻辑门如 AND 与门有两个输入 1 个输出,无法由单独的输出推断出具体的两个输入数据。为了实现可逆功能,电路中的量子门的输入和输出都是一一对应的,输入线和输出线的数目相同,即量子门的输入和输出是 1×1 、 2×2 、 3×3 等,这样才能由输出结果推断出输入数据。

收稿日期:2011-10-15

作者简介:李明翠(1980—),女,讲师,研究方向为智能信息处理。

迄今为止,共提出了4 000多个可逆门,所有的量子门都可以用酉矩阵表示。量子门按照它作用的量子位的数目可分为一位门、二位门和三位门等。在此仅介绍用来构建数值比较器的 Pauli-X 门、受控非门(CNOT)和 Toffoli 门。

2.1 Pauli-X 门

Pauli-X 门,也叫非门,是1位可逆量子门,其作用是对输入进行逻辑取反。即对经典位的0和1进行互换。当它作用于态矢 $|\varphi\rangle$ 上时,如果 $|\varphi\rangle$ 为 $|0\rangle$,输出就是 $|1\rangle$;同理,如果态矢是 $|1\rangle$,输出就是 $|0\rangle$ 。但在量子情况下存在着经典中没有的情况,就是当态矢为两个基矢 $|0\rangle$ 和 $|1\rangle$ 的线性叠加态时,量子非门的作用表现为 $X|\varphi\rangle = X(A|0\rangle + B|1\rangle) = A|1\rangle + B|0\rangle$ 。Pauli-X 门的线路符号用一个带有方框的X表示。

2.2 受控非门(CNOT)

受控非门是一个2位可逆量子门,具有两个输入和两个输出。在两个输入位中,一位是控制位,另一位是目标位,即受控位。受控非门的作用是:当控制比特是 $|1\rangle$ 时,受控比特取非;否则,受控比特不发生变化。它的另一种表达形式为: $|A, B\rangle \rightarrow |A, B \oplus A\rangle$,其中, $\oplus$ 表示模2加,因此受控非门实际上实现的是异或的功能。受控非门的线路符号如图1所示,图中的实心圆点表示控制位,另一个大圆圈符号表示目标位。

2.3 Toffoli 门

Toffoli 门是3位量子门。该门有两个控制位,一个目标位。当两个控制位都为 $|1\rangle$ 时,目标位反转。Toffoli 门的逻辑关系表示为: $|A, B, C\rangle \rightarrow |A, B, C \oplus AB\rangle$ 。Toffoli 门对于布尔逻辑来说,是一个完备的量子门。如果把 Toffoli 门的某些输入位固定,忽略某些输出位,就可以用它来构成任何逻辑函数。Toffoli 门的线路符号如图2所示。

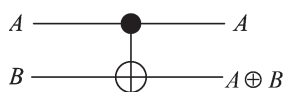


图1 受控非门的线路符号
Fig.1 Wiring symbols of CNOT gate

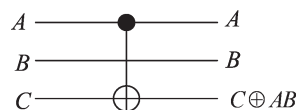


图2 Toffoli 门的线路符号图
Fig.2 Wiring symbols of Toffoli gate

3 一位数值比较器的设计

数值比较器是用来判断两个数的数值大小或相等的器件,是重要的量子电路逻辑部件之一。设比较两个一位的数值数据 A 和 B ,真值表如表1所示。

表1 比较两个一位数值数据大小的真值表

Tab.1 Table of comparing two one-bit numerical value

A	B	$A > B (GA)$	$A = B (EQ)$	$A < B (GB)$
0	0	0	1	0
0	1	0	0	1
1	0	1	0	0
1	1	0	1	0

用 GA 表示 $A > B$, EQ 表示 $A = B$, GB 表示 $A < B$,根据真值表得到逻辑表达式:

$$\left. \begin{aligned} GA &= A\bar{B} \\ EQ &= \bar{A}\bar{B} + AB \\ &= \overline{A \oplus B} \\ GB &= \bar{A}B \end{aligned} \right\} \quad (1)$$

将 Toffoli 门的3个输入设为 A 、 $\bar{B}$ 和0,可得到输出 A 、 $\bar{B}$ 和 $A\bar{B}$,同理将3个输入分别置为 $\bar{A}$ 、 B 、0可得到 $\bar{A}B$ 。 EQ 则可以先用一个受控非门得到 $A \oplus B$,再将该结果用一个 Pauli-X 门取反得到。用受控非门和 Toffoli 门实现的一位数值比较电路如图3所示。线路中用了5个 Pauli-X 门、1个受控非门和2个 Toffoli

门。有4个输入($A, B, 0, 0$)和4个输出(A, EQ, GA, GB)。

垃圾输出最小化是可逆逻辑电路设计的一个重要指标。受控非门 $|A, B\rangle \rightarrow |A, A \oplus B\rangle$ 具有一个垃圾输出 A , Toffoli 门 $|A, B, C\rangle \rightarrow |A, B, C \oplus AB\rangle$ 有两个垃圾输出 A 和 B 。在1位数值比较器的设计的过程中,兼顾了可逆和最少垃圾输出的原则,如果少于4个输出,则无法从输出知道输入的数据,违反可逆性,如果采用大于4个的输出,则可以减少 Pauli-X 门的使用,但相应的代价是垃圾输出增多。电路中具有1个垃圾输出 A ,其他3个输出 EQ, GA, GB 均为有效输出。

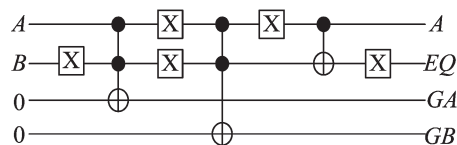


图3 1位数值比较电路

Fig.3 Comparing circuit of two one-bit numerical value

4 多位数值比较器的设计

根据模块化的设计原则,可以在1位可逆电路的设计基础上设计出多位数值比较器。将多位数分为高位和低位两部分,先分别比较高位部分和低位部分是否相等,再根据下面的公式2判断两个多位数值数据最终的大小。公式2中的 A 和 B 表示要比较大小的两个多位数, A_1 和 A_0 分别为 A 的高位部分和低位部分, B_1 和 B_0 分别为 B 的高位部分和低位部分。

$$\left. \begin{aligned} GA &= GA_1 + EQ_1 GA_0 \\ GB &= GB_1 + EQ_1 GB_0 \\ EQ &= EQ_1 EQ_0 \end{aligned} \right\} \quad (2)$$

将上式的逻辑关系用 Toffoli 门和 CNOT 门表示,画出级联模块图,如图4所示。线路图中共有9个输入和9个输出,求 EQ 用了1个 Toffoli 门,求 GA 和 GB 分别用了1个 Toffoli 门和一个 CONT 门。模块共有3个有效输出和6个垃圾输出。3个有效输出 EQ, GA, GB 可按需要作为下一步级联的输入。

设将1位数值比较器线路(图3)称为NG门,比较器的级联模块线路(图4)称为CG门,则可将2位数值比较线路模块化为图5所示。4位数值比较可以将数值分为高2位和低2位分别进行比较,再将两个比较结果按图5级联比较。其他多位数值比较均可用NG模块和CG模块依此级联而成。

当需要比较的数值位数较多时,用1位比较电路直接级联实现多位数的比较需要用到多个NG模块和CG模块。实现 n 位数值比较需要 n 个NG门和 $n-1$ 个CG门,电路的级联层次多,需要的量子门总数较多,垃圾输出也多。下面将设计一个优化的4位数值比较器。

设比较两个4位二进制数($A_3A_2A_1A_0, B_3B_2B_1B_0$)的大小。用 EQ 表示两个数相等, GA 表示 $A > B$, GB 表示 $B > A$ 。则有

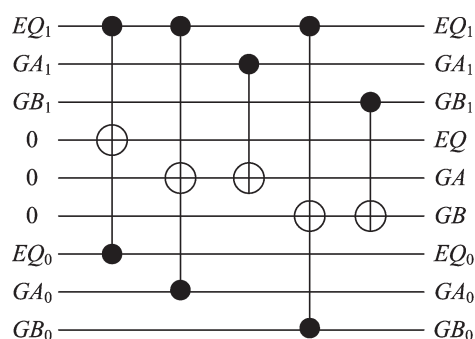


图4 比较器的级联模块线路图

Fig.4 Circuit of the cascading module used in the comparator

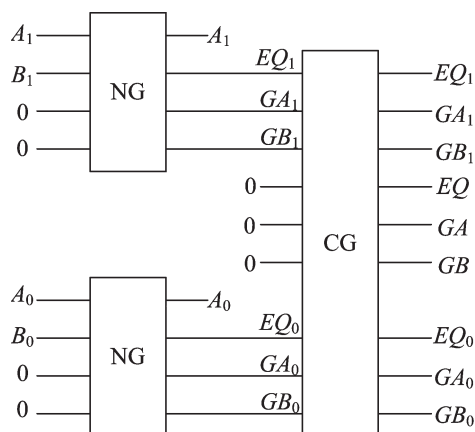


图5 级联实现两位数值比较

Fig.5 Comparing two-bit numerical value by cascading

$$\left. \begin{aligned}
 GA &= A_3 \overline{B_3} + \overline{A_3 \oplus B_3} A_2 \overline{B_2} + \overline{A_3 \oplus B_3} A_2 \oplus B_2 A_1 \overline{B_1} \\
 &\quad + \overline{A_3 \oplus B_3} A_2 \oplus B_2 A_1 \oplus B_1 A_0 \overline{B_0} \\
 &= A_3 \overline{B_3} + E_3 A_2 \overline{B_2} + E_3 E_2 A_1 \overline{B_1} \\
 &\quad + E_3 E_2 E_1 A_0 \overline{B_0} \\
 GB &= \overline{A_3} B_3 + \overline{A_3 \oplus B_3} A_2 B_2 + \overline{A_3 \oplus B_3} A_2 \oplus B_2 A_1 B_1 \\
 &\quad + \overline{A_3 \oplus B_3} A_2 \oplus B_2 A_1 \oplus B_1 A_0 B_0 \\
 EQ &= \overline{A_3 \oplus B_3} A_2 \oplus B_2 A_1 \oplus B_1 A_0 \oplus B_0 \\
 &= E_3 E_2 E_1 E_0
 \end{aligned} \right\} \quad (3)$$

根据公式可知,求 GA 和 GB 需要用到多个 Pauli-X 门、受控非门和 Toffoli 门,因此采取了间接求 GB 的方式,即采用公式(4)的方式:

$$GB = \overline{GA} \overline{EQ} = \overline{GA + EQ} \quad (4)$$

将公式(3)和公式(4)中的与关系用 Toffoli 门实现,或(异或)关系用 CNOT 门实现,经过优化设计的 4 位数值比较电路如图 6 所示。优化的 4 位数值比较线路共有 16 个输入和 16 个输出。线路图共用了 13 个 Pauli-X 门、12 个受控非门、10 个 Toffoli 门,具有 13 个垃圾输出。

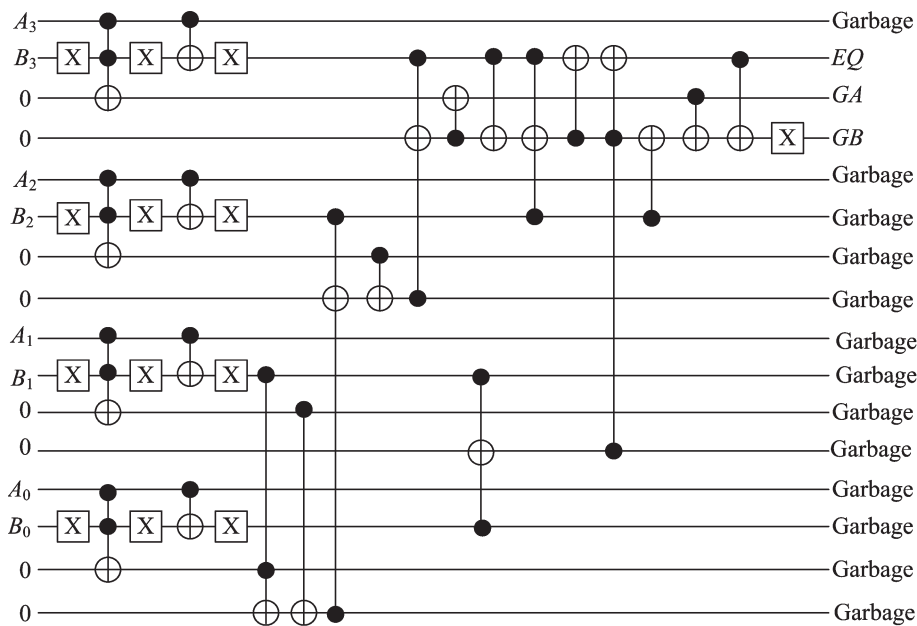


图 6 优化的 4 位数值比较电路
Fig.6 Comparing circuit of optimized four-bit numerical value

用 1 位的比较模块直接级联完成 8 位数的比较,需要将高 4 位和低 4 位级联比较得到结果,而高 4 位和低 4 位又需要分别分为两个 2 位数级联比较,每个 2 位再细分为两个 1 位进行比较。这种方式级联得到的电路共需要 8 个 NG 模块分别用于 8 个 1 位比较结果、4 个 CG 模块用于得到 4 个 2 位比较结果、2 个 CG 模块用于得到两个 4 位比较结果、1 个 CG 模块用于得到 1 个 8 位比较结果。每个 NG 模块有 1 个垃圾输出、用到 5 个 Pauli-X 门、1 个受控非门、2 个 Toffoli 门。CG 模块有 6 个垃圾输出、用到 2 个受控非门、3 个 Toffoli 门。用 1 位比较电路直接级联进行 8 位数的比较共有 $8 \times 1 + 7 \times 6 = 50$ 个垃圾输出、 $8 \times 5 = 40$ 个 Pauli-X 门、 $8 \times 1 + 7 \times 2 = 22$ 个受控非门、 $8 \times 2 + 7 \times 3 = 37$ 个 Toffoli 门。而用经过优化的 4 位比较模块完成 8 位数值比较只需要 2 个 4 位模块通过 1 个 CG 模块级联即可得到比较结果。用这种方法得到的 8 位的数值比较线路共有 $2 \times 13 + 6 = 32$ 个垃圾输出、用到 $2 \times 13 = 26$ 个 Pauli-X 门、 $2 \times 12 + 2 = 26$ 个受控非门、 $2 \times 10 + 3 = 23$ 个 Toffoli 门。和直接用 1 位比较电路级联得到的 8 位数值比较电路相比较,优化的电路产生的垃圾输出少

18 个,用到的 Pauli-X 门少 14 个,受控非门多 4 个,Toffoli 门少 14 个。总体线路比用 1 位级联简洁,垃圾输出减少了 36%,量子门总数减少了 24%,电路性能得到较好的提升。

5 结语

量子电路是量子模式识别^[7]、量子图像处理的具体逻辑实现,电路的功能可以进一步用底层的量子细胞自动机 QCA^[8]进行仿真。该文基于 Pauli-X 门、受控非门、Toffoli 门进行了可逆数值比较器的设计。详细阐述了 1 位数值比较器以及级联模块的设计与实现。文中所用的 3 种基本可逆门和 1 位比较电路均用 QCADesigner 进行了仿真模拟,仿真结果证实了所设计电路的正确性。因为垃圾输出是影响可逆电路性能最重要的因素,因此整个设计策略是尽量减少垃圾输出。为了进一步减少垃圾输出、减少量子门的使用,文章对 4 位数值比较器进行了优化。文中所设计比较器电路的策略是:不管多少位数值,均采用多位同时比较的方式进行,这与传统的比较方式(即先比较高位,如高位相等,再比较次高位,如又相等,再比较下一位)的方式不同。比较器的比较策略和线路中所用的可逆门等可作进一步研究和探讨,利用数值比较器实现更复杂的可逆电路系统也有待进一步研究。

参考文献:

- [1] LANDAUER R. Irreversibility and heat generation in the computing process[J]. IBM Journal of Research and Development, 1961(5):183-191.
- [2] 戴葵,宋辉,刘芸,等. 量子信息技术引论[M]. 长沙:国防科技大学出版社,2001:1-2.
- [3] 赵生妹,郑宝玉. 量子信息处理技术[M]. 北京:北京邮电大学出版社,2010:35-38.
- [4] GERALDO A. Barbosa.Quantum half-adder[J]. Physical Review A,2006(73):1-6.
- [5] ZHOU RIGUI, SHI YANG, WANG HUI'AN, et al. Transistor realization of reversible "ZS" series gates and reversible array multiplier[J]. Microelectronics Journal, 2011, 42(2):305-315.
- [6] REKHA K JAMES, K POULOSE JACOB, et al. Reversible binary coded decimal adders using toffoli gates[J]. Lecture Notes in Electrical engineering, 2009(14):117-131.
- [7] ZHOU RIGUI, DING QIULIN. Quantum pattern recognition with probability of 100%[J]. International Journal of Theoretical Physics, 2008, 47(5):1278-1285.
- [8] HEUMPI CHO, EARL E, SWARTZLANDER, JR. Adder and multiplier design in quantum-dot cellular automata[J]. IEEE Transactions on Computers, 2009, 58(6):721-727.

Design and Optimization of Reversible Numerical Comparator Based on Toffoli Gate

Li Mingcui

(School of Information Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: As one of the most important components of many complex quantum circuits, reversible numerical comparator has rarely been researched yet. Firstly, the circuits of one-bit comparator and the cascade module are proposed based on Pauli-X gate, CNOT gate and Toffoli gate. More complex comparator circuits can be achieved by constructing the one-bit module and the cascade module. Then, the four-bit numerical comparator is optimized in order to construct more efficiently n-bit numerical comparators. After optimization, the garbage output and the amount of quantum gate in the circuit are reduced by 36% and 24% respectively. And the circuit performance is improved.

Key words: quantum; reversible; Toffoli; comparator