量子三值全加器设计

王 冬[1,2],朱长江[2],张晓蕾[2]
(1.武汉大学软件工程国家重点实验室,湖北武汉 430072;2.河南大学软件学院,河南开封 475004)

摘 要: 量子多值加法器是构建量子多值计算机的基本模块.通过认真分析三元域上加法的运算规则及带进位加法的真值表,通过设置扩展三值 Toffoli 门的控制条件有效实现一位加法在各种情况下的进位,利用三值 Feynman 门实现一位加法的求和运算,由此设计出一位量子三值全加器,再利用进位线将各位量子全加器连接起来构造出 n 位量子三值全加器.与同类电路相比,此量子全加器所使用的辅助线及量子代价都有所减少.

关键词: 多值逻辑; 全加器; 扩展三值 Toffoli 门; 三值 Feynman 门
中图分类号: TP387; TN911.73 **文献标识码:** A **文章编号:** 0372-2112 (2014)07-1452-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.07.033

The Design of Quantum Ternary Full Adder

WANG Dong[1,2], ZHU Chang-jiang[2], ZHANG Xiao-lei[2]
(1. *State Key Laboratory of Software Engineering, Wuhan University, Wuhan, Hubei* 430072, *China*;
2. *Software College, Henan University, Kaifeng, Henan* 475004, *China*)

Abstract: Quantum multiple-valued adder is the basic module to construct quantum multiple-valued computer. By analyzing addition operation rules and truth table of addition with carry in ternary field, setting control conditions of quantum generalized ternary Toffoli gates to realize the addition carry in all cases and making use of ternary Feynman gates to realize sum, one qutrit full adder is given. At last, nqutrit ternary full adder is constructed by using carry bit to connect all one qutrit full adders. Compared with other same type circuits, the ancilla qubits and quantum costs of this quantum full adder have been decreased.

Key words: multiple-valued logic; full adder; generalized ternary Toffoli gate; ternary Feynman gate

1 引言

量子内在固有的叠加、纠缠和不可克隆等自然属性使得量子计算具有并行、可逆及理论上无条件安全等特性,在复杂计算和安全通信等领域被证明具有超越经典计算的潜力,被认为是最具前景的计算模式之一[1].基于二值逻辑的经典量子计算可以胜任诸如复杂性集类和可计算性等基础问题,然而从量子的自然属性的角度来看,一个量子系统具有多于两个的非简并状态是正常的,即多层系统(multilevel system)更自然,而多值逻辑正是描述多层量子系统所负载信息的理想数学工具[2].目前,量子多值逻辑在量子纠错编码、容错技术及量子安全通信中都有较好的应用[3,4].

量子多值 oracle 电路(特定类型的专用电路)借助多值逻辑量子位(qudit)更大的计算空间,完成相同的计算任务可以使用更少的量子位,从而进一步增强电路的鲁棒性,因此更具优势[5].2005 年 Khan 等人[6]给出量子三值编码器和解码器电路,2006 年 Miller 等人[7]利用量子可逆逻辑电路综合算法给出三值全加器电路,2008 年 Khan[8]利用四元域上的受控 M – S[5]门给出量子四值比较器电路.2011 年 Wang 等人[9]给出针对图着色问题的三值量子搜索算法中的 oracle 电路,并详细讨论了电路的复杂性及质量.各种量子多值 oracle 电路的实现对于构建量子多值计算机,设计复杂的量子多值算法,改善电路质量起到了推动作用.

加法运算是计算机的基本运算之一,加法器常用作计算机的算术逻辑部件,执行逻辑操作、移位及指令调用等.本文通过有效设置量子受控门的控制条件,利用量子扩展三值 Toffoli 门及 Feynman 门,设计出一种新型量子三值全加器.与其它同类电路[7,10]相比,该加法器的量子代价和所使用的辅助线更少,这有利于降低量子加法器的构造成本及物理实现的难度[5,11],并可有效增强其可靠性[12].

收稿日期:2013-01-15;修回日期:2013-10-08;责任编辑:李勇锋
基金项目:国家自然科学基金(No.61004006,No.61103235);软件工程国家重点实验室开放基金(No.SKLSE2012-09-41)

2　预备知识

定义 1　三值量子位(qutrit, quantum ternary digit)的状态可以用三维复向量空间中的向量表示,特殊的$|0\rangle$,$|1\rangle$和$|2\rangle$状态称为计算基态(computational basis state),是构成这个向量空间的一组正交基. qutrit 的状态可以用计算基态$|0\rangle$,$|1\rangle$,$|2\rangle$的线性组合来表示:

$$|\psi\rangle = \sum_{m=0}^{2} c_m |m\rangle \tag{1}$$

其中 c_m 为概率幅(amplitude),测量结果 $m \in \{0,1,2\}$出现的概率是$|c_m|^2$,满足归一化条件:$|c_0|^2 + |c_1|^2 + |c_2|^2 = 1$. 当有两个或三个 $c_m \neq 0$ 时,称$|\psi\rangle$为叠加态.

量子门负责处理量子信息,将量子信息从一种形式转换为另一种形式. 酉性限制是对量子门的惟一限制,每个酉矩阵都可以定义一个有效的量子门[13]. 2000 年 Muthukrishan 和 Stroud[5]设计并实现了在线性离子阱中构建一位和两位多值(d-valued)量子基本门(quantum primitive gate)的方案,其中两位门是一位门的受控门,控制条件为$|d-1\rangle$,这些门也被统称为 M-S 门,它们的量子代价被指定为 1[7]. Muthukrishan 和 Stroud 还证明了 M-S 门的通用性,即任意量子多值门均可由 M-S 门组合而成,这表明任意量子多值门物理实现上的可行性[5]. 由量子基本门构建的门称为量子宏观门(quantum macro-level gate). 量子宏观门也可以被解析成由量子基本门级联组合而成的电路,常用电路中所包含的量子基本门的数量作为电路的量子代价[13].

定义 2　在多值逻辑空间中实现置换函数功能的量子门称为量子多值置换门. 三元域上的每一个置换均可表示一个一位量子三值置换门,记作:$g_3(\cdots)$,括号中的数字列表代表门所完成的三元域上的一个置换,括号中的运算代表门施加在三值量子位上的运算. 为方便,也可用 g 代表这些门,用数字列表或运算代表其中的某一个门. 这些一位量子三值置换门中,$g_3(120)$,$g_3(201)$,$g_3(012)$分别对应三元域上的 +1, +2 运算及 +0 或 ×1 运算,$g_3(120)$与 $g_3(201)$互逆[1,12]. 它们的酉矩阵如下所示.

$$g_3(120) = g_3(+1) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$g_3(12) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$g_3(201) = g_3(+2) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

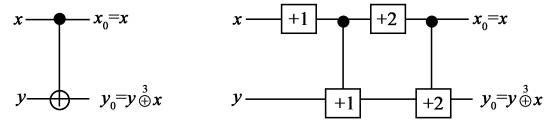
$$g_3(01) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$g_3(02) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$$g_3(012) = g_3(+0) = g_3(\times 1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

两位三值 M-S 门可以由一位门和一个控制位组合而成,控制条件为$|2\rangle$.

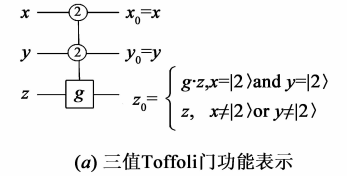
定义 3　三值 Feynman 门(常被称为 CNOT 门)是两位门,第一量子位(控制位)的输出状态始终不变,第二量子位(受控位)的输出状态等于第一、二量子位的输入之和(模 3 加运算)[12],如图 1a 所示. 三值 Feynman 门是量子宏观门,可由定义 2 给出的 M-S 门级联构建,如图 1b 所示. 由图 1b 知,三值 Feynman 门的量子代价为 4.



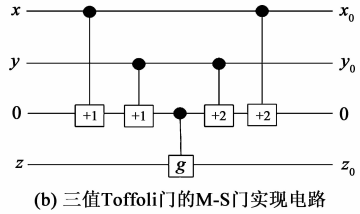
(*a*) 三值Feynman门　　(*b*) 三值Feynman门的M-S门实现电路

图1　三值Feynman门

定义 4　三值 Toffoli 门是三位门,第一、二量子位(控制位)的输出状态分别等于其输入状态,当两个控制位的输入状态均为$|2\rangle$时,第三量子位(受控位)上的基本门(这里我们只考虑定义 2 中的 g 门)进行作用,否则第三量子位上的基本门不作用,如图 2a 所示. 三值 Toffoli 门是量子宏观门,可由定义 2 给出的 M-S 门级联而成,如图 2b 所示. 由图 2b 知,三值 Toffoli 门中有一条隐含的辅助线,其量子代价为 5.



(*a*) 三值Toffoli门功能表示



(b) 三值Toffoli门的M-S门实现电路

图2　三值Toffoli门

定义 5　当三值 Toffoli 门的控制条件为$|0\rangle$,$|1\rangle$,$|2\rangle$中的任意值时,称其为扩展三值 Toffoli 门(generalized ternary Toffoli gate),如图 3 所示. 其中门(+1)和(+2)互逆. 从图 3 可知,扩展三值 Toffoli 门可由三值

Toffoli 门和一位 M-S 门级联构建,其量子代价为 2×(非 2 控制点个数)+5.

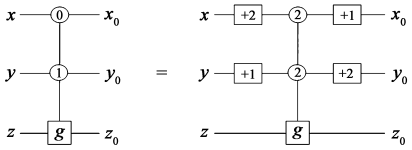


图3 扩展三值Toffoli门的一个实例

3 量子三值全加器

3.1 量子三值全加器电路设计

在每一位加法运算中,加数、被加数与低位的进位作为输入,和数与向高位的进位作为输出的装置为全加器.依据带进位加法的运算规则,和数与向高位的进位的计算公式如式(2).

$$S_i = X_i \overset{3}{\oplus} Y_i \overset{3}{\oplus} C_i$$
$$C_{i+1} = \mathrm{int}\left[\frac{X_i + Y_i + C_i}{3}\right] \tag{2}$$

依据式(2),并考虑到实际带进位加法运算中,低位向高位的进位最多为 1,可构造出每一位三值全加器的真值表,如表 1 所示.

表 1 三值全加器的真值表

X_i	Y_i	C_i	X_i+Y_i	C_{i+1}	S_i
0	0	0	0	0	0
0	1	0	1	0	1
0	2	0	2	0	2
1	0	0	1	0	1
1	1	0	2	0	2
1	2	0	0	1	0
2	0	0	2	0	2
2	1	0	0	1	0
2	2	0	1	1	1
0	0	1	0	0	1
0	1	1	1	0	2
0	2	1	2	1	0
1	0	1	1	0	2
1	1	1	2	1	0
1	2	1	0	1	1
2	0	1	2	1	0
2	1	1	0	1	1
2	2	1	1	1	2

由表 1 知,当 $X_iY_i \in \{12, 21, 22\}$ 时,无论 C_i 为 0 或 1,都有 $C_{i+1}=1$;当 $C_i=1$ 并且 $X_i+Y_i=2$ 时,$C_{i+1}=1$.其余情况下 $C_{i+1}=0$.和数 $S_i = X_i \overset{3}{\oplus} Y_i \overset{3}{\oplus} C_i = (X_i \overset{3}{\oplus} Y_i) \overset{3}{\oplus} C_i$,依据定义 3,可用三值 Feynman 门实现三元域上的加法.因此,利用三值 Feynman 门和扩展三值 Toffoli 门可生成如图 4 所示的一位量子三值全加器电路.

图 4 中,无论 C_i 为 0 或 1,当 $X_iY_i \in \{12, 21, 22\}$ 时,最左边的三个扩展三值 Toffoli 门中的某一个将起作用,使得 C_{i+1} 从 0 变为 1,之后的 Feynman 门将 X_i 与 Y_i 的和置于 Y_i 上,由于当 $X_iY_i \in \{12, 21, 22\}$ 时,$X_i \overset{3}{\oplus} Y_i \neq 2$,这不满足最右边的扩展三值 Toffoli 门的控制条件,此门不会起作用,因此最终 C_{i+1} 最多为 1.如果在第一个三值 Feynman 门之后 $Y_i=2$ 并且 $C_i=1$,此时一定有 $X_iY_i \notin \{12, 21, 22\}$,则最左边的三个扩展三值 Toffoli 门一定都不会发生作用,而 $Y_i=2$,$C_i=1$ 满足最右边的扩展三值 Toffoli 门的控制条件,因此该门将起作用,使得 C_{i+1} 从 0 变为 1 并保持到最后.其余情况下电路的输入不会满足四个扩展三值 Toffoli 门中任意一个的控制条件,因此四个门均不发生作用,C_{i+1} 的值保持 0 不变,即没有产生向高位的进位.在一位的全加运算中,我们将产生进位的各种条件进行归类,通过有效设置扩展三值 Toffoli 门的控制条件来实现各种情况下的进位.

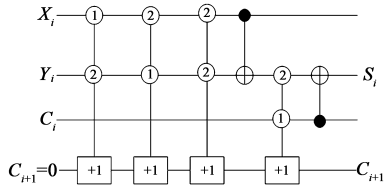


图4 一位三值全加器

由定义 3 知,第一个三值 Feynman 门将 X_i 与 Y_i 的和置于 Y_i 上,第二个三值 Feynman 门又将 C_i 的值叠加到 $X_i \overset{3}{\oplus} Y_i$ 之上,所以最终 Y_i 的输出为 X_i, Y_i, C_i 的和数.

通过以上分析可知,图 4 所示的全加器电路可以正确计算出三个输入的和数及向高位的进位,是正确的一位全加器电路.

依据加法的运算规则,n 位全加器是一位全加器的 n 次迭代过程.因此利用向高位的进位作为连接线,连接每一位全加器即构造出 n 位全加器,如图 5 所示,其中 FA 代表一位量子三值全加器电路.

3.2 量子代价分析与比较

由于量子电路的量子代价是组成它的所有门的量子代价之和,所以图 4 给出的一位量子三值全加器的代价是三个扩展三值 Toffoli 门、一个三值 Toffoli 门及两个

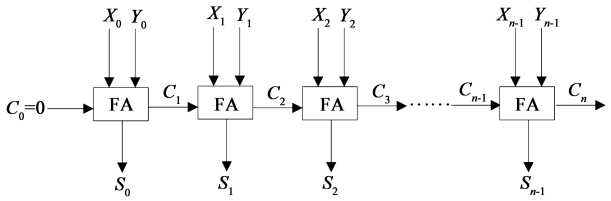


图5　n位三值全加器

三值 Feynman 门的量子代价之和.依据定义 3、4、5 分别给出的三值 Feynman 门、三值 Toffoli 门及扩展三值 Toffoli 门的量子代价计算公式,图 4 给出的一位量子三值全加器电路的量子代价为:$3\times(2\times1+5)+5+2\times4=21+5+8=34$.由于 n 位全加器电路是一位全加器电路的 n 次迭代,所以图 5 给出的 n 位全加器电路的量子代价为 $34n$.

文献[10]在分析一位加法运算时完全使用数学公式的结论,计算出向高位的进位的可能值有 0,1,2 三种情况,它忽略了实际上带进位的加法运算中向高位的进位只有 0,1 两种情况的事实.我们在给出电路时,充分考虑了加法的运算规则和实际运算中的进位情况,并且细致地分析了一位三值全加器的真值表,总结出产生进位的各种情况,将它们进行分类,通过设置扩展三值 Toffoli 门的控制条件在电路中实现进位.正是由于这个原因,使得我们的一位量子三值全加器电路比文献[10]给出的同类电路少使用两个扩展三值 Toffoli 门和一个 Feynman 门,量子代价减少 16(文献[10]给出的同类电路的量子代价为 50).因此我们的 n 位全加器电路比文献[10]的同类电路的量子代价减少 $16n$.

文献[7]是利用多值逻辑可逆电路综合算法,通过在有限范围内进行搜索的方法给出一位量子三值全加器电路,其量子代价为 96,比我们的电路多 62.因此我们的 n 位全加器电路的量子代价比文献[7]的同类电路减少 $62n$.

在辅助线的使用上,因为每一个扩展三值 Toffoli 门的实现都隐含一条辅助线,我们的量子一位全加器电路比文献[10]给出的同类电路少使用两个扩展三值 Toffoli 门,所以少使用两条隐含辅助线.此外,我们的量子一位全加器电路中再没有使用任何其它的辅助线,而文献[10]给出的量子一位全加器电路中还使用了一条贯穿电路的辅助线,因此我们共少使用 3 条辅助线,所以,我们的 n 位全加器电路比文献[10]的同类电路共少使用 $3n$ 条辅助线.由于多量子的相干操作是困难的,所以辅助线的减少可有效降低电路物理实现的难度,增强电路的鲁棒性.

4　结论

从信息处理及量子的自然属性的观点来看,对于未来的计算系统,多值量子技术在理论上是理想的选择之一[5].量子加法器是构建量子计算机的关键模块.利用扩展三值 Toffoli 门及 Feynman 门,通过分析一位三值全加器的真值表得到能够产生进位的各种情况,结合三值加法的运算规则,本文给出了量子三值全加器的设计思想及其电路.与文献[10]的同类电路相比,我们的 n 位量子全加器的量子代价减少 $16n$,所使用的辅助线减少 $3n$.与文献[7]的同类电路相比,我们的 n 位量子全加器的量子代价减少 $62n$.相比之下,我们的量子三值全加器的量子代价更小,所使用的辅助线更少,并因此有效降低了物理实现的难度,增强了电路的可靠性.

进一步的工作为,分析研究各种多值带进位加法的运算规则,在量子三值全加器的基础上,给出量子任意多值全加器的构建框架,利用此框架可以方便有效地构造量子任意多值全加器.

参考文献

[1] Plesch M, Brukner C. Quantum-state preparation with universal gate decompositions[J]. Physical Review A, 2011, 83(3): 032302/1 – 5.

[2] Bartlett S D, Guise H D, Sanders B C. Quantum encodings in spin systems and harmonic oscillators[J]. Physical Review A, 2002, 65(5): 052316/1 – 4.

[3] Ashikhmin A, Knill E. Nonbinary quantum stabilizer codes[J]. IEEE Transactions on Information Theory, 2001, 47(7): 3065 – 3072.

[4] Liu Z H, Chen H W, Xu J, et al. High-dimensional deterministic multiparty quantum secret sharing without unitary operations [J]. Quantum Information Processing, 2013, 12(1): 587 – 599.

[5] Muthukrishnan A, Stroud C R. Multivalued logic gates for quantum computation[J]. Physical Review A, 2000, 62(5): 052309/1 – 8.

[6] Khan M H A, Perkowski M A. Quantum realization of ternary encoder and decoder[A]. Proceedings of 7th International Symposium On Representations and Methodology of Future Computing Technologies (RM2005)[C]. Tokyo: IEEE, 2005. 5 – 6.

[7] Miller D M, Maslov D, Dueck G W. Synthesis of quantum multiple-valued circuits[J]. Journal of Multiple-Valued Logic Soft Computing, 2006, 12(5 – 6): 1 – 28.

[8] Khan M H A. Synthesis of quaternary reversible/quantum comparators[J]. Journal of Systems Architecture, 2008, 54(10): 977 – 982.

[9] Wang Y S, Perkowski M A. Improved complexity of quantum oracles for ternary grover algorithm for graph coloring[A]. Proceedings of 41st IEEE International Symposium on Multiple-

Valued Logic (ISMVL) [C]. Tusula: IEEE, 2011. 294 – 301.
[10] Khan M H A, Perkowski M A. Quantum ternry parallel adder/subtractor with partially-look-ahead carry[J]. Journal of Systems Architecture, 2007, 53(7): 453 – 464.
[11] Yang G W, Xie F, Song X Y, et al. Universality of 2-qudit ternary reversible gates[J]. Journal of Physics A, 2006, 39(24): 7763 – 7773.
[12] Khan M H A. Quantum realization of multiple – valued Feynman and Toffoli gates without ancilla input[A]. Proceedings of 39th International Symposium on Multiple-Valued Logic (ISMVL)[C]. Naha Okinawa: IEEE, 2009. 103 – 108.
[13] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information[M]. Cambridge, England: Cambridge University Press, 2000.

作者简介

王 冬 女. 1977 年 1 月出生, 河南焦作人. 副教授、硕士生导师. 1998 年, 2004 年和 2012 年分别在河南大学和东南大学获理学学士、理学硕士和工学博士学位. 主要从事量子计算、量子可逆逻辑综合等方面的研究工作.
E-mail: 122062815@qq.com

朱长江 男. 1978 年 9 月出生, 河南平顶山人. 讲师. 2002 年, 2011 年分别在河南大学获得工学学士、理学硕士学位. 主要从事数据挖掘方面的研究工作.
E-mail: kfzcj@163.com