基于多目标扩展通用 Toffoli 门的量子比较器设计

王 冬[1,2] 刘志昊[2] 朱皖宁[2] 李善治[1]

(河南大学复杂智能网络系统研究所 开封 475004)[1] (东南大学计算机科学与工程学院 南京 211189)[2]

摘 要 利用多目标扩展通用 Toffoli 门,提出了经典量子信息比较器的设计构造方法,并对其正确性进行了理论证明,在此基础之上,给出了量子比较器在简单搜索问题中的一个应用。与其它同类量子比较器相比,此比较器通过减少使用辅助位来节约相关量子资源;通过设置多目标扩展通用 Toffoli 门的控制条件,使得在比较出结果后剩余的门不再起作用,从而提高了运行效率,降低了出错率,增强了比较器的鲁棒性。

关键词 量子计算,多目标扩展通用 Toffoli 门,量子比较器

中图法分类号 TP387,TN911.73 **文献标识码** A

Design of Quantum Comparator Based on Extended General Toffoli Gates with Multiple Targets

WANG Dong[1,2] LIU Zhi-hao[2] ZHU Wan-ning[2] LI Shan-zhi[1]

(Institute of Complex Intelligent Network System, Henan University, Kaifeng 475004, China)[1]

(School of Computer Science and Engineering, Southeast University, Nanjing 211189, China)[2]

Abstract By employing extended general Toffoli gates with multiple targets, a constructive method of classical quantum information comparator was presented. Further its correctness was proved theoretically. Based on which an application of quantum comparator working in the quantum search algorithm was given. Compared with the other like quantum comparators, our comparator uses less ancilla qubits so that the required related quantum resources can be saved. By setting the control conditions of the extended general Toffoli gates with multiple targets, the subsequent gates can not work any longer after obtaining the comparison result in our comparator. Thus the efficiency is improved, and the error rate is reduced and the robustness of comparator is enhanced.

Keywords Quantum computation, Extended general Toffoli gate with multiple targets, Quantum comparator

1 引言

量子计算和量子信息科学是研究利用量子力学理论进行信息处理的一门科学。其利用微观粒子的量子态作为信息的载体,凭借着量子力学所特有的一些性质和物理现象(如量子叠加性、纠缠性和相干性及量子隐形传态等)进行有效的信息处理,被认为是最具前景的研究领域之一[1]。早在 20 世纪 60 年代初,人们已发现不可逆计算产生的能耗会导致计算机芯片发热,从而影响芯片的集成度,限制了经典计算机的运行速度和计算能力[2]。解决以上问题的一个可能办法是,采用不同的电路设计理念。可逆性是量子计算的特征,量子可逆电路要求其输入和输出之间存在一一映射的关系,理论上不丢失输入信息,不存在热耗散问题,从而可将芯片的运行速度和计算能力发挥到极致[2]。在众多考虑取代当今经典计算机的研究中,利用量子效应建立量子计算机的方案脱颖而出,量子计算机在计算能力通信能力、存储能力和现实世界的仿真能力上具有潜在的、更加出色的表现。量子计算机可等效为一个量子图灵机,理论上已证明,量子图灵机可等效为一个量子逻辑电路[1]。量子逻辑门均可逆,其实现的操作可用酉矩阵来描述,利用量子逻辑门级联构建一些实际可行的专用电路是重要的,专用电路的设计实现及应用可加速运行算法,并可对量子寄存器或量子芯片等的设计实现做出贡献[3]。自 1996 年 Vedral 等人[4]在 Physical Review A 上发表了量子全加器的电路后,专用量子电路的设计成为量子计算中的另一个研究热点,之后量子全减器、计数器及受控集成加减电路[5]设计完成,它们是构建量子计算机的基本电路模块。

1997 年 Grover[6]提出的量子搜索算法对经典算法进行了二次加速,使其成为量子计算中最为著名的结果之一[1],其中比较器电路是 Grover 算法的重要组成部分。2006 年 Cheng 等人[7]设计出量子归并排序算法电路,得益于量子比较器的大量并行使用,使得归并排序算法的时间复杂度降低至 $\Theta((\log n)^2)$。量子比较器不仅应用于量子搜索和排序算法,还应用在量子条件语句设计、求解逆函数的算法设计、量子运算器和控制器设计等多个领域,对量子计算机[3]的进一

到稿日期:2011-11-14 返修日期:2012-02-20 本文受国家自然科学基金项目(61070240,60873101),河南省自然科学基金项目(102300410175),江苏省高校自然科学基金(10KJB520021),河南大学自然科学基金(09YBZR043)资助。

王 冬(1977—),女,博士生,副教授,主要研究方向为量子计算、量子可逆逻辑电路综合,E-mail:juliawdd@qq.com;刘志昊(1982—),男,博士生,主要研究方向为量子通信、量子信息处理;朱皖宁(1983—),男,博士生,主要研究方向为量子算法、量子可逆逻辑电路综合;李善治(1966—),实验师,主要研究方向为量子算法。

步研究将会做出一些贡献。然而目前对量子比较器的设计与优化的研究还较少，Oliveira 等人[8,9]给出基于二进制数的比较方法、使用标准 Toffoli 门实现的量子比较器；Nascimento 等人[10]给出基于二进制减法器的量子比较器设计方法；Shigeru 等人[11]给出 Grover 算法的一个应用框架，并简单描述了一个量子比较器电路；Khan 等人[12]提出在四元域上设计量子四值逻辑比较器，并给出复杂的电路图；这些设计或基于已有的解决方案和技术、或基于成熟的数学理论抽象问题并进行形式化推导和验证，都取得了良好效果，但给出的比较器电路均较繁琐。

本文提出利用多目标扩展通用 Toffoli 门(extended general Toffoli gate with multiple targets)设计构造量子比较器的方法。与其它同类量子比较器相比，所构造的量子比较器使用更少的辅助位，节约了电路所需的量子资源，通过设置多目标扩展通用 Toffoli 门的控制条件，使得在比较出结果后剩余的门不再起作用，可提高运行效率，降低出错率，增强比较器的鲁棒性，其电路结构清晰，易于理解、推导和验证。

2 预备知识

定义 1 量子比特(qubit)的两个可能状态$|0\rangle$和$|1\rangle$是正交基态，分别对应经典比特的 0 和 1。量子比特可以是$|0\rangle$和$|1\rangle$的线性组合，称为叠加态(superposition)。

$$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$$

式中，α和β是复数，满足归一化条件：$|\alpha|^2+|\beta|^2=1$。即在对量子比特进行测量时，得到$|0\rangle$的概率为$|\alpha|^2$，得到$|1\rangle$的概率为$|\beta|^2$[1]。

非正交量子态是不能被比较和排序的[13]。为在量子计算中进行经典的算术和逻辑运算，可利用量子的正交基态$|0\rangle$和$|1\rangle$对数字进行编码，从而可以用量子态有效表示一个 n 位数。编码方法类似于十进制数的二进制表示。例如：十进制数 15，可用量子态编码成$|1111\rangle$。用正交基态编码后的数字可以进行比较[13]。

定义 2 Toffoli 量子门中通常有 4 种线型，如图 1 所示。

(1)肯定控制线(见图 1(a))：如果在这条线上的输入为 0，则受控线的值将不改变；如果输入为 1，则其它的肯定/否定控制线确定受控线上的值是否被反转。通过肯定控制线的值不变。

(2)否定控制线(见图 1(b))：如果在这条线上的输入为 1，则受控线的值将不改变；如果输入为 0，则其它的肯定/否定控制线确定受控线上的值是否被反转。通过否定控制线的值不变。

(3)受控线(见图 1(c))：也叫目标线，每个门至少有一条受控线，通过受控线的值，受肯定/否定控制线的控制。

(4)无关线(见图 1(d))：通过无关线的值不变，也不对其它线产生影响。

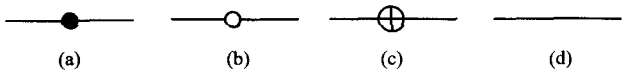

图 1 Toffoli 门 4 种线型

传统 Toffoli 量子门[14-16]，记为 $TOF(C,T)$，其中输入变量集合 $In=\{x_0,x_1,\cdots,x_{n-1}\}$，控制线集合 $C=\{x_{i_2},x_{i_3},\cdots,x_{i_n}\}$，则受控线集合 $T=\{x_{i_1}\}$，且 $C\cap T=\varnothing$，$C\cup T\subset In$。输出变量集合映射为$\{x_0,x_1,\cdots,x_{i_1-1},x_{i_1}\oplus\prod_{k=2}^{n}x_{i_k},x_{i_1+1},\cdots,x_{n-1}\}$。若$\exists m\in\{2,3,\cdots,n\}$，$x_{i_m}=0\Rightarrow\prod_{k=2}^{n}x_{i_k}=0$，则受控线$x_{i_1}$的输出为$x_{i_1}\oplus\prod_{k=2}^{n}x_{i_k}=x_{i_1}\oplus 0=x_{i_1}$；若$\forall m\in\{2,3,\cdots,n\}$，$x_{i_m}=1\Rightarrow\prod_{k=2}^{n}x_{i_k}=1$，则受控线$x_{i_1}$的输出为$x_{i_1}\oplus\prod_{k=2}^{n}x_{i_k}=x_{i_1}\oplus 1=\bar{x}_{i_1}$。控制线的数量决定了不同的 Tottoli 门，如图 2 所示[15]。

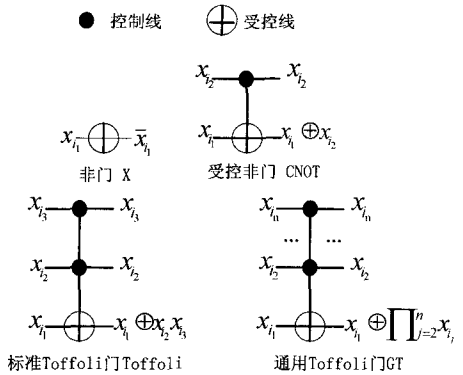

图 2 Toffoli 量子门

定义 3 传统的通用 Toffoli 门(General Toffoli gate，GT 门)只有肯定控制线。然而 1 并没有任何特殊之处，控制线置 0 控制受控线信号反转是合理的[1]。增加了否定控制线的 GT 门称为扩展通用 Toffoli 门(extended general Toffoli gate)，记为 $EGT(C,T)$。图 3(a)是 GT 门：$w_0=w,x_0=x,y_0=y,z_0=z\oplus wxy$，图 3(b)是 EGT 门：$w_0=w,x_0=x,y_0=y,z_0=z\oplus w\bar{x}y$，图 3 (c)是与 EGT 门等价的用 GT 门和非门组成的电路，否定控制线等价于在肯定控制线的两侧各加一个非门(X 门)。

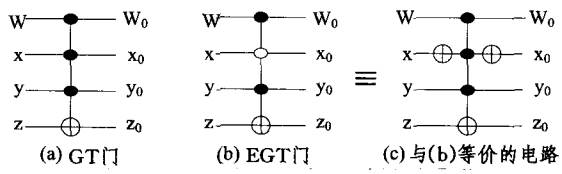

图 3

定义 4 多目标扩展通用 Toffoli 门是具有多个目标线的 EGT 门，其中每个目标线的控制条件均相同，如图 4(a)所示。图 4(b)为与多目标扩展通用 Toffoli 门等价的 EGT 门电路[1]。

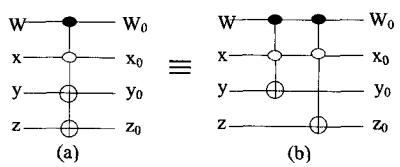

图 4 多目标扩展通用

定义 5 图 5 是描述测量运算的符号。封闭量子系统按

西算子演化，但在某一时刻，实验者和实验设备要观察系统，以了解系统内部的情况，这个观测作用使系统不再封闭，也就不再服从酉演化，这个观测作用即为量子测量。量子测量由一组测量算子$\{M_m\}$描述，这些算子作用在被测系统状态空间上，指标 m 表示实验中可能的测量结果[1]。

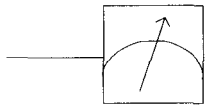

图 5　测量符号

3　量子比较器的构造

由于两个数 a 与 b 的大小关系有 $a>b$，$a=b$，$a<b$ 这 3 种情况，因此在二进制量子计算中需使用两个量子位 c_1，c_2 来记录比较结果。对 c_1，c_2 进行测量的结果用来说明 a，b 的大小关系：如果 c_1，c_2 的测量结果为 10，则 $a>b$；如果 c_1，c_2 的测量结果为 01，则 $a<b$；如果 c_1，c_2 的测量结果为 00，则 $a=b$。

3.1　一位量子比较器

若 a，b 均是一位二进制数，依据定义 1 其可表示成量子态：$|a\rangle$，$|b\rangle$，首先将 c_1c_2 初始状态设置为$|00\rangle$，当$|a\rangle$，$|b\rangle$中仅有一个为$|1\rangle$时，就将此状态$|1\rangle$重置到 c_1 或 c_2 上，其余情况下不改变 c_1，c_2 的状态。对一位数 a，b 进行比较的电路如图 6 所示。

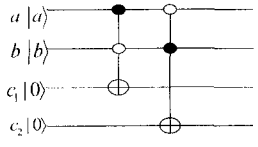

图 6　一位量子比较器

依据 EGT 门的定义，分析图 6 可知，若$|a\rangle=|1\rangle$，$|b\rangle=|0\rangle$，通过两个 EGT 门，c_1 的状态变为$|1\rangle$，c_2 的状态仍为$|0\rangle$，若$|a\rangle=|0\rangle$，$|b\rangle=|1\rangle$，通过两个 EGT 门，c_1 的状态仍为$|0\rangle$，c_2 的状态变为$|1\rangle$，其余情况 c_1，c_2 的状态均保持$|0\rangle$不变。最后，通过 c_1，c_2 的测量结果，即可准确判断出 a，b 的大小关系。

3.2　n 位量子比较器

3.2.1　n 位量子比较器的构造

n 位量子比较器是在 1 位量子比较器基础上的扩充。两个 n 位二进制数 a 与 b 的比较是从最高位向最低位依次按位进行的，若在比较过程中 a，b 第一次在某一位不相等，则这一位的大小关系就是 a，b 的大小关系，比较过程结束。即若 a，b 的第 n，…，$y+1$ 位（高位）均相等，则对它们的第 y 位进行比较，若在第 y 位上不相等，则此位上的大小关系即为 a，b 的大小关系，比较过程到此结束；若 a，b 在第 y 位上仍然相等，就要对它们的第 $y-1$ 位进行比较。按此方法继续，若直到第 1 位比较过程仍未结束，就比较 a，b 的第 1 位，若不同，则两个数在第 1 位上的大小关系即为 a，b 的大小关系，比较过程结束；若相同，则 $a=b$，比较过程结束。

首先依据定义 1 将 a，b 两个 n 位二进制数分别表示成量子态：$|a_na_{n-1}\cdots a_1\rangle$，$|b_nb_{n-1}\cdots b_1\rangle$，再依据上述两个 n 位数的比较方法，利用多目标扩展通用 Toffoli 门，构造 n 位量子比较器，如图 7 所示。

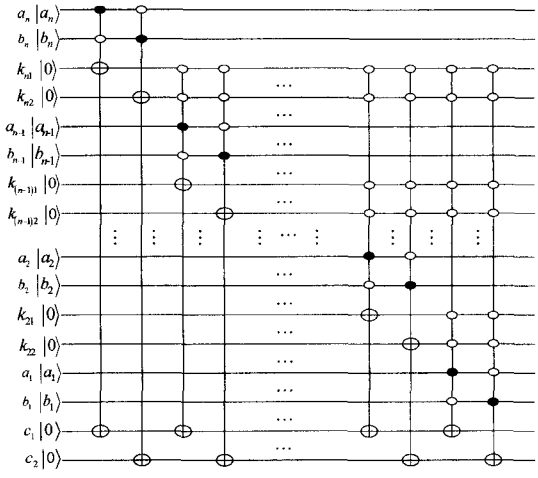

图 7　n 位量子比较器

显然图 7 所示的 n 位量子比较器代表一个酉算子。c_1，c_2 的初态均被设置为$|0\rangle$，用以记录 a，b 的比较结果。每一对 a_i，b_i（$i\in(2\cdots n)$）的下方均有初态为$|0\rangle$的两个辅助位 k_{i1}，k_{i2}，用以在 a，b 两个数的 n，$n-1$，…，$y+1$ 位都相等的情况下，记录第 y 位$|a_y\rangle$，$|b_y\rangle$的比较结果。

分析图 7 可知，比较是从两个数的最高位即第 n 位开始的，每一位的比较都依次用到相邻的两个多目标扩展通用 Toffoli 门。若$|a_n\rangle$，$|b_n\rangle$不同，则其中必有一个状态为$|1\rangle$，另一个状态为$|0\rangle$，这必将满足图 7 中最左边的两个多目标扩展通用 Toffoli 门之一的控制条件，因此这两个门之一将起作用，这样就会把$|a_n\rangle$，$|b_n\rangle$重置到其下的两个辅助位 k_{n1}，k_{n2}及 c_1，c_2 上，即比较出 a，b 的大小。由于此时 k_{n1}，k_{n2}中有一个的状态从$|0\rangle$变为$|1\rangle$，而其余的多目标扩展通用 Toffoli 门在这两个辅助位上的控制条件都为$|0\rangle$，因此这些门将不再起作用，故 c_1，c_2 的状态在此后将保持不变。若$|a_n\rangle$，$|b_n\rangle$相同，或都为$|0\rangle$或都为$|1\rangle$，这不满足图 7 中最左边的两个门的作用条件，因此 k_{n1}，k_{n2}及 c_1，c_2 的状态都将保持$|0\rangle$不变，也就意味着在此位上两个数没有比较出大小，此时第 3 和第 4 个门在 k_{n1}，k_{n2}上的控制条件得到满足，因此将按照第 n 位的比较方法继续比较第 $n-1$ 位。依此，从高位向低位逐位进行比较，一旦 a，b 在某一位上的状态不同，它们的状态就会被设置到其下的两个辅助位和 c_1，c_2 上，此时两个辅助位之一的状态被置为$|1\rangle$，剩余的门由于在这一位上不满足控制条件，因此都将不再起作用，c_1，c_2 之一的状态也被置为$|1\rangle$，即比较出 a，b 的大小，比较过程结束。最后，通过 c_1，c_2 的测量结果即可准确判断 a，b 的大小关系：如果 c_1，c_2 的测量结果为 10，则 $a>b$；如果 c_1，c_2 的测量结果为 01，则 $a<b$；如果 c_1，c_2 的测量结果为 00，则 $a=b$。

3.2.2　量子比较器正确性的理论证明

求证：图 7 所示的 n 位量子比较器是正确的。

证明：由于图 7 中每一条辅助线 k_{i1}，k_{i2}（$i=n,n-1,\cdots,2$）以及 c_1，c_2 的初态均被设置为$|0\rangle$，依据定义 4，排序为奇数的每一个多目标扩展通用 Toffoli 门（如第 1，3，5 个门）在 k_{i1}（$i=n,n-1,\cdots,2$）和 c_1 上的输出一样，为式(1)：

$\bigwedge_{g=n}^{i+1}\bar{k}_{g1}\bar{k}_{g2}a_i\bar{b}_i$（$i=n$ 时，$\bigwedge_{g=n}^{i+1}\bar{k}_{g1}\bar{k}_{g2}a_i\bar{b}_i=a_n\bar{b}_n$） (1)

由合取范式的定义可知，当某一个 $k_{g1}=1(g=n\cdots i+1)$ 时（即 $\bar{k}_{g1}=0$），式(1)的运算结果为 0，即相当于此门没有起作用。

c_1 的最终输出为排序为奇数的每一个多目标扩展通用 Toffoli 门在 c_1 上的输出的异或和，可由式(2)表示。

$$c_1=a_n\bar{b}_n\oplus\bar{k}_{n1}\bar{k}_{n2}a_{n-1}\bar{b}_{n-1}\oplus\cdots\oplus\bar{k}_{n1}\bar{k}_{n2}\cdots\bar{k}_{21}\bar{k}_{22}a_1\bar{b}_1$$
$$=\bigoplus_{i=n}^{1}\bigwedge_{g=n}^{i+1}\bar{k}_{g1}\bar{k}_{g2}a_i\bar{b}_i \quad (2)$$

同理，排序为偶数的每一个多目标扩展通用 Toffoli 门（如第 2,4,6 个门）在 $k_{i2}(i=n,n-1,\cdots,2)$ 和 c_2 上的输出一样，为式(3)：

$\bigwedge_{g=n}^{i+1}\bar{k}_{g1}\bar{k}_{g2}\bar{a}_i b_i$（$i=n$ 时，$\bigwedge_{g=n}^{i+1}\bar{k}_{g1}\bar{k}_{g2}\bar{a}_i b_i=\bar{a}_n b_n$） (3)

c_2 的最终输出为排序为偶数的每一个多目标扩展通用 Toffoli 门在 c_2 上的输出的异或和，由式(4)表示。

$$c_2=\bar{a}_n b_n\oplus\bar{k}_{n1}\bar{k}_{n2}\bar{a}_{n-1}b_{n-1}\oplus\cdots\oplus\bar{k}_{n1}\bar{k}_{n2}\cdots\bar{k}_{21}\bar{k}_{22}\bar{a}_1 b_1$$
$$=\bigoplus_{i=n}^{1}\bigwedge_{g=n}^{i+1}\bar{k}_{g1}\bar{k}_{g2}\bar{a}_i b_i \quad (4)$$

若 $a>b$，不失一般性，假设 a 和 b 的最高 $n\cdots y+1$ 位相同（或都为 0 或都为 1）且 $a_y>b_y$，则有 $a_y=1,b_y=0$。因为 k_{i1}，$k_{i2}(i=n,n-1,\cdots,2)$ 以及 c_1,c_2 的初态均被设置为 $|0\rangle$，计算式(1)和式(3)得：$k_{i1}=0,k_{i2}=0(i=n,\cdots,y+1)$，图 7 中前 $2(n-y)$ 个门的输出均为 0，因此，计算式(2)和式(4)可知：到此时为止，c_1,c_2 的输出均为 0。此后，经过第 $2(n-y)+1$ 个门，此门的控制条件为：$k_{i1}=0,k_{i2}=0(i=n,\cdots,y+1),a_y=1,b_y=0$，因此由式(1)得：$k_{y1}=1$。之后，再经过第 $2(n-y)+2$ 个门，此门的控制条件为：$k_{i1}=0,k_{i2}=0(i=n,\cdots,y+1),a_y=0,b_y=1$，由式(3)得：$k_{y2}=0$。至此，由式(2)和式(4)可知：

$$c_1=a_n\bar{b}_n\oplus\bar{k}_{n1}\bar{k}_{n2}a_{n-1}\bar{b}_{n-1}\oplus\cdots\oplus\bar{k}_{n1}\bar{k}_{n2}\cdots\bar{k}_{(y+1)1}\bar{k}_{(y+1)2}$$
$$a_1\bar{b}_1=\underbrace{0\oplus\cdots\oplus 0}_{n-y\text{个}0}\oplus 1=1$$
$$c_2=\bar{a}_n b_n\oplus\bar{k}_{n1}\bar{k}_{n2}\bar{a}_{n-1}b_{n-1}\oplus\cdots\oplus\bar{k}_{n1}\bar{k}_{n2}\cdots\bar{k}_{(y+1)1}\bar{k}_{(y+1)2}$$
$$\bar{a}_1 b_1=\underbrace{0\oplus\cdots\oplus 0}_{n-y+1\text{个}0}=0$$

由于 $k_{y1}=1,\bar{k}_{y1}=0$，则计算式(1)可知：①$k_{h1}=0(h=y-1\cdots2)$；②此后的每个门在 c_1 上的输出均为 0，所以 c_1 的最终输出为 $c_1=\underbrace{0\oplus\cdots\oplus 0}_{n-y\text{个}0}\oplus 1\oplus\underbrace{0\oplus\cdots\oplus 0}_{y-1\text{个}0}=1$。计算式(3)可知：①$k_{h2}=0(h=y-1\cdots2)$；②此后的每个门在 c_2 上的输出也为 0，所以 c_2 的最终输出仍为 0。故最终 c_1,c_2 的测量结果为 10。

同理可证：若 $a<b$，c_1,c_2 的测量结果为 01；若 $a=b$，c_1,c_2 的测量结果为 00。

在比较两个 n 位二进制数时，我们的比较器使用了 $2n-2$ 个辅助位，而文献[9]使用了 $3n-1$ 个辅助位，文献[10]使用了 $2n$ 个辅助位。由于对多个量子的同时操作是困难的，因此辅助位的减少有助于在节约量子资源的同时提高电路的鲁棒性。同时，我们的比较器采用 $2n$ 个多目标扩展通用 Toffoli 门级联的形式，通过将辅助位上的多目标扩展通用 Toffoli 门的条件动态设置为置 0 受控，使得在比较出结果后，其余的门将不再起作用，这有助于降低电路出错的概率，进一步提高电路的鲁棒性。近年来，多目标扩展通用 Toffoli 门在文献中常被使用[1]，是因为它的使用有助于电路的化简和理解。

4 量子比较器在简单搜索问题上的一个应用

量子比较器应用广泛，如可应用在量子搜索算法的设计、量子条件语句的设计、量子算法中逆函数求解问题的设计，量子运算器、控制器及交换机等的设计中。为便于表示和应用，将量子比较器简化为如图 8 所示的形式。

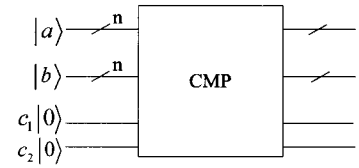

图 8 简化的量子比较器表示

我们的任务是在一个从 0 到 2^n-1 的连续自然数空间中，搜索比指定数大，或比指定数小，或与指定数相等的所有数。例如：在 0 到 31 中搜索比 15 小或大或相等的所有数。问题解决框架如图 9 所示。

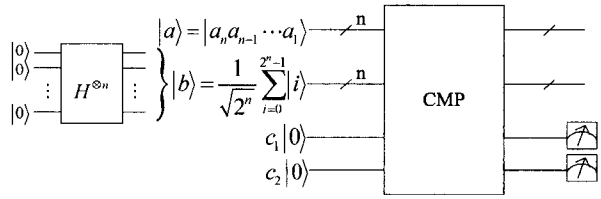

图 9 简单搜索问题解决方案的电路框架

图 9 中，$|a\rangle=|a_n a_{n-1}\cdots a_1\rangle$ 为一个确定的乘积态，并作为比较基。$|b\rangle=\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle$ 为 n 量子位的均匀叠加态，代表问题的整个搜索空间。如在例题中 $|a\rangle=|01111\rangle$，$|b\rangle=\frac{1}{4\sqrt{2}}\sum_{i=0}^{31}|i\rangle$。

由量子比较器的功能描述得出其酉演化过程可由式(5)表示：

$$U_{cmp}|a\rangle|b\rangle|c_1\rangle|c_2\rangle=|a\rangle\frac{|a\rangle}{\sqrt{2^n}}|0\rangle|0\rangle+|a\rangle\frac{\sum_{i=a+1}^{2^n-1}|i\rangle}{\sqrt{2^n}}|0\rangle$$
$$|1\rangle+|a\rangle\frac{\sum_{i=0}^{a-1}|i\rangle}{\sqrt{2^n}}|1\rangle|0\rangle \quad (5)$$

分析式(5)知，使用计算基对 c_1,c_2 进行测量，若测量结果为 10，则测量后 $|b\rangle$ 代表比 a 小的所有数的叠加；若测量结果为 01，则测量后 $|b\rangle$ 代表比 a 大的所有数的叠加；若测量结果为 00，则测量后 $|b\rangle$ 塌缩到 a。

结束语 本文首先给出了一位量子比较器，之后对其进行扩充，设计出 n 位量子比较器，并对其正确性进行证明，最后给出了量子比较器在简单搜索问题中的一个应用。与其它同类量子比较器相比，我们的比较器使用了更少的辅助位，节

约了相关量子资源；通过将多目标扩展通用 Toffoli 门的条件动态设置为 0 和门电路的顺序级联设计方式，提高了比较器的运行效率，降低了出错率，增强了比较器的鲁棒性。

进一步的工作为：①进一步研究并优化量子比较器电路。②深化量子比较器的应用，将量子比较器应用到更多更复杂的算法中，利用量子计算的并行运算模式提高算法的性能。③设计更多的包括算术运算及逻辑运算在内的基本的专用量子电路，探讨量子计算机系统的构建模式。

参 考 文 献

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

[2] Landauer R. Irreversibility and heat generation of the computing process [J]. IBM Journal of Research and Development, 1961, 5 (3): 183-191

[3] Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer [J]. Proceedings of the Royal Society, 1985, 400(1818): 97-101

[4] Vedral V, Barenco A, Ekert A. Quantum networks for elementary arithmetic operations [J]. Physical Review A, 1996, 54(1): 147-153

[5] Bomble L, Lauvergnat D, Remacle A, et al. Controlled full adder or subtractor by vibrational quantum computing [J]. Physical Review A, 2009, 80(2): 022332/ 1-8

[6] Grover L K. Quantum mechanics helps in searching for a needle in a haystack [J]. Physical Review Letters, 1997, 79(2): 325-328

[7] Cheng S T, Wang C Y. Quantum switching and quantum merge sorting [J]. IEEE Transactions on Circuits and Systems, 2006, 53(2): 316-325

[8] Oliveira D S, Sousa P B, Ramos R V. Quantum search algorithm using quantum bit string comparator [C]// Proceedings of 2006 International Telecommunications Symposium. 2006: 582-585

[9] Oliveira D S, Ramos R V. Quantum bit string comparator: circuits and applications [J]. Quantum Computers and Computing, 2007, 7(1): 17-26

[10] Nascimento A L, Kowada L A B, Oliveira W R. A reversible ULA [C]// WECIQ: First Workshop-school in Quantum Information and Computation. Brazil, 2006

[11] Shigeru Y, Masaki N. An efficient framework to utilize Grover search [J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science), 2011, 31(2): 49-58

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

[13] Arul A J. Impossibility of comparing and sorting quantum states [OL]. http://arxiv.org/abs/quant-ph/0107085, 2001

[14] Barcnco A, Bennett C, et al. Elementary gates for quantum computation [J]. Physical Review A, 1995, 52(5): 3457-3467

[15] Song Xiao-yu, Yang Guo-wu, Perkowski M, et al. Algebraic characteristics of reversible gates [J]. Theory of Computing Systems, 2005, 39(2): 311-391

[16] 李志强，陈汉武，徐宝文，等. 基于 Hash 表的量子可逆逻辑电路综合的快速算[J]. 计算机研究与发展，2008，45(12)：2162-2171

(上接第 295 页)

可见，在 RTX 中间语言级能够正确处理机器模式，并能正确分配伪寄存器。在 GCC 完成寄存器分配后，该指令的 RTL 描述如图 4(b)所示。可见，GCC 能够正确进行寄存器分配。最终生成的对应汇编指令为：fvaddd %v1，%v0，%v0。

```
(insn 89 88 90 6 example .c:21 (set (reg/v:V4DF 199 [ res3 ]) (plus:V4DF
(reg/v:V4DF 195 [ res1 ]) (reg/v:V4DF 198 [ res2 ]))) -1 (nil))
```

(a)

```
(insn 89 87 97 example .c:21 (set (reg/v:V4DF 103 %v0 [orig:199 res3 ]
[199])
    (plus:V4DF (reg:V4DF 104 %v1 [212])
        (reg:V4DF 103 %v0 [218]))) 504 {vpu_fvadd} (expr_list:REG_DEAD
(reg:V4DF 104 %v1 [212]) (nil)))
```

(b)

图 4 向量操作指令的 RTL 形式

结束语 GCC 编译器是一套非常庞大而复杂的软件系统。面向新目标机的指令集体系结构，在 GCC 后端中实现对该目标机的支持，是非常复杂的编译器工程实现工作。微软亚洲研究院的张亚勤博士说过“工程的能力决定创新的水平”。对具体的编译器所做的实现工作，在编译器工程技术领域非常重要。

基于 GCC 的 Sparc 后端，本文实现了支持四路双精度 SIMD 指令的四路双精度短向量寄存器描述。在此过程中，完成了新的目标机定义，扩充了一类向量模式，定义了一类新的寄存器约束，实现了四路双精度寄存器的描述。本文的工作对基于 GCC 进行的研究和开发工作有很大的参考价值。

参 考 文 献

[1] GCC, GNU Compiler Collection[OL]. http://gcc.gnu.org/

[2] The GNU General Public License[OL]. http://www.gnu.org/licenses/licenses.html#GPL

[3] OpenSPARC™ T2 Core Microarchitecture Specification[Z]. Revision A, Sun Microsystems, Inc., December 2007

[4] Firasta N, Buxton M, Jinbo P, et al. Intel AVX: New Frontiers in Performance Improvements and Energy Efficiency[Z]. Intel white paper, 2008

[5] The VIS™ Instruction Set V1.0[Z]. White paper, Sun Microsystems Inc., June 2002

[6] Makarov V N. The Integrated Register Allocator for GCC[C]// Proceedings of the GCC Developers' Summit. Ottawa, Ontario, Canada, July 2007: 77-90

[7] Stallman R M. The GCC Developer Community. GNU Compiler Collection Internals. For GCC version 4.6[Z]. Free Software Foundation, 2010