第 37 卷 第 2 期 华侨大学学报(自然科学版) Vol. 37 No. 2
2016 年 3 月 Journal of Huaqiao University (Natural Science) Mar. 2016

文章编号:1000-5013(2016)02-0155-05 **doi**:10.11830/ISSN.1000-5013.2016.02.0155

量子 Fourier 变换在实现 Deutsch-Jozsa 算法中的应用

张洪涛[1,2], 熊红梅[1,2], 冷玲英[1,2], 舒军[2]

(1. 湖北工业大学 纳米电子技术与微系统实验室, 湖北 武汉 430068;
2. 湖北工业大学 电气与电子工程学院, 湖北 武汉 430068)

摘要: 提出利用量子 Fourier 变换解决 Deutsch-Jozsa 算法问题的观点. 结合量子 Fourier 变换和 Deutsch-Jozsa 算法的量子电路,找到一种利用量子 Fourier 变换解决 Deutsch-Jozsa 算法新的量子电路,并考察该量子电路中各个线路的量子状态,结合算法对该量子线路的状态进行研究. 结果表明:利用量子 Fourier 变换解决 Deutsch 问题,能够有效地提高运算速度,节省运算时间.

关键词: Deutsch-Jozsa 算法; 量子傅里叶变换; 量子电路; 量子算法

中图分类号: TP 306 **文献标志码**: A

近年来,随着量子计算机研究的发展,人们不断地探索新的实现量子计算机的方案和新的量子算法. Deutsch-Jozsa 算法是由 Deutsch 等[1]在 1992 年提出的第一个量子计算算法,并由 Cleve 等[2]在 1998 年提出改进. 1994 年,Shor[3]构造了大数质因子分解的量子算法,Shor 算法可以在多项式时间内,求解大整数分解和有限域上离散对数问题. 1996 年,Grover 给出了一种量子搜索算法[4],Grover 量子搜索算法可以平方根地加速无序数据库的搜索. 自 Shor 算法和 Grover 量子搜索算法提出以后,有研究者将量子理论原理与智能计算相结合提出了量子智能计算[5]. 有关 Deutsch-Jozsa 算法的研究也一直在继续向前,并取得相当不错的成绩. 罗军等[6]在核磁共振量子计算机上实验实现了 7 位 Deutsch-Jozsa 算法;Zheng[7]利用腔 QED 实现了 Deutsch-Jozsa 算法;Dasgupta 等[8]在原子系统中实现了 Deutsch-Jozsa 算法. 量子傅里叶变换[9]作为一种基本量子工具,它在 Shor 的大数质因子分解算法已经得到了有效的应用,而 Deutsch-Jozsa 算法提出后,却鲜有人将其与量子傅里叶变换结合. 因此,本文从 Deutsch-Jozsa 算法原理出发,把量子 Fourier 变换应用于 Deutsch-Jozsa 算法中.

1 Deutsch-Jozsa 算法

1.1 Deutsch 命题

函数 $f(x)\in\{0,1\}$,要么 $f(x)$对所有的 x 是常数,即 $f(x)$为常数;要么 $f(x)$是平衡函数,即对 x 的所有取值,函数取 1 的概率为 1/2,取 0 的概率也为 1/2. A,B 两人进行数据传送,A 从 0 到 2^n-1 中选择一个数 x,并发送给 B,B 利用 $f(x)$对数 x 进行计算,得到结果后告诉 A 计算结果,A 必须用最快的时间,确定 B 用的是常数还是平衡函数[6].

1.2 Deutsch-Jozsa 算法的量子线路和算法流程

实现一般 Deutsch-Jozsa 算法[10]的量子线路,如图 1 所示. 图 1 中:$|0\rangle$,$|1\rangle$为量子状态;$\boldsymbol{H}$ 表示 Had-amard 变换,$\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$;$\boldsymbol{H}^{\otimes n}$为 Hadamard 变换的张量积;$U_f$ 为一种幺正变换,$|x,y\rangle\xrightarrow{U_f}$

收稿日期: 2015-10-14

通信作者: 张洪涛(1963-),男,教授,博士,主要从事数字信号处理和数字图像处理、嵌入式系统、纳米器件集成和纳米半导体技术的研究. E-mail:zhanght@mail.hbut.edu.cn.

基金项目: 湖北省武汉市科技局"十城千辆新动力汽车计划"(2013011801010600)

$|x,y\oplus f(x)\rangle$.

Deutsch-Jozsa 算法计算过程有以下 5 个步骤.

步骤 1 状态初始化,$|0\rangle^{\otimes n}|1\rangle$.

步骤 2 利用 Hadamard 变换产生叠加,$\rightarrow\frac{1}{\sqrt{2^n}}\times\sum_{x=0}^{2^n-1}|x\rangle[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$.

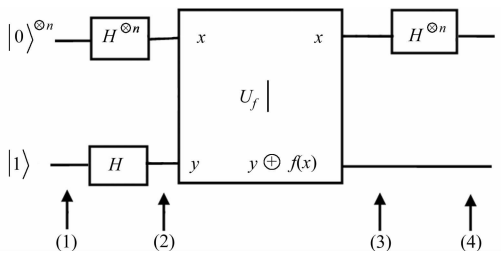

图 1 实现一般 Deutsch-Jozsa 算法的量子线路

Fig. 1 Quantum circuit of the general Deutsch-Jozsa algorithm

步骤 3 用 U_f 计算函数 $f(x)$,$\rightarrow\frac{1}{\sqrt{2^n}}\sum_x(-1)^{f(x)}|x\rangle[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$.

步骤 4 进行 Hadamard 变换,$\rightarrow\sum_z\sum_x\frac{(-1)^{x\otimes z+f(x)}|z\rangle}{2^n}[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$.

步骤 5 测量最终输出 z,$\rightarrow z$.

步骤 4 中,状态 $|0\rangle^{\otimes n}$ 的幅度是 $\sum\frac{(-1)^{f(x)}}{2^n}$. 函数 $f(x)$有以下 2 种可能:$f(x)$是常数函数,$|0\rangle^{\otimes n}$的幅度是+1 或−1,因为$|\varphi_3\rangle$具有单位长度,故所有其他幅度必须是 0,测量结果为 0;$f(x)$是平衡函数,对$|0\rangle^{\otimes n}$的正负幅度贡献抵消幅度为 0,测量结果至少有一位为非零. 归纳起来,如果 A 测量时 z 为 0,则函数是常数;否则,函数是平衡的.

2 量子 Fourier 变换

2.1 量子 Fourier 变换的定义

量子 Fourier 变换[11]定义:在一组标准正交基$|0\rangle,\cdots,|N-1\rangle$上的一个线性算子,其在基态上的作用,表示为

$$|j\rangle\rightarrow\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\exp(2\pi ijk/N)|j\rangle. \tag{1}$$

对任意状态的作用,可表示为

$$\sum_{j=0}^{N-1}f(j)|j\rangle\rightarrow\sum_{k=0}^{N-1}F(k)|k\rangle. \tag{2}$$

式(2)中:幅度 $F(k)$是幅度 $f(x)$的离散 Fourier 变换值,$F(k)=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}f(j)\exp(2\pi ijk/N)$.

取 $N=2^n$,其中,n 是某个正整数. 把状态 j 写成二进制形式 $j=j_1 2^{n-1}+j_2 2^{n-2}+\cdots+j_n 2^0$. 方便起见,用 $0.j_l j_{l+1}\cdots j_m$ 表示二进制分数$\frac{j_l}{2}+\frac{j_{l+1}}{4}+\cdots+\frac{j_m}{2^{m-l+1}}$. 则可给出量子 Fourier 变换的积形式,即

$$|j_1,\cdots,j_n\rangle\rightarrow\frac{(|0\rangle+\exp(2\pi i0.j_n)|1\rangle)}{2^{n/2}}\times\frac{(|0\rangle+\exp(2\pi i0.j_{n-1}j_n)|1\rangle)\cdots(|0\rangle+\exp(2\pi i0.j_1 j_2\cdots j_n)|1\rangle)}{2^{n/2}}. \tag{3}$$

2.2 量子 Fourier 变换的量子线路和算法流程

变换 $\boldsymbol{R}_k$ 表示酉变换 $\boldsymbol{R}_k\equiv\begin{pmatrix}1 & 0\\ 0 & \exp(2\pi i/2^k)\end{pmatrix}$. 首先,将输入状态$|j\rangle$写成二进制形式 $j=j_1 2^{n-1}+j_2 2^{n-2}+\cdots+j_n 2^0$,即输入为$|j_1 j_2\cdots j_n\rangle$,状态$|j\rangle$ 可用 n 个量子比特表示.

将 Hadamard 变换应用到第一量子比特得到状态$(|0\rangle+\exp(2\pi i0.j_1)|1\rangle)|j_2\cdots j_n\rangle/\sqrt{2}$. 应用受控 $\boldsymbol{R}_2$ 变换产生状态$(|0\rangle+\exp(2\pi i0.j_1 j_2)|1\rangle)|j_2\cdots j_n\rangle/\sqrt{2}$,继续应用受控 $\boldsymbol{R}_3$ 变换,$\boldsymbol{R}_4$ 直到 $\boldsymbol{R}_n$ 变换. 得到状态$(|0\rangle+\exp(2\pi i0.j_1 j_2\cdots j_n)|1\rangle)|j_2\cdots j_n\rangle/\sqrt{2}$.

接着，对第二量子比特执行类似过程，产生状态为

$$(|0\rangle+\exp(2\pi\mathrm{i}0.j_1j_2\cdots j_n)|1\rangle)(|0\rangle+\exp(2\pi\mathrm{i}0.j_2\cdots j_n)|1\rangle)|j_3\cdots j_n\rangle/\sqrt{2^2}.$$

对每个量子比特继续这样的操作，导出最终状态

$$(|0\rangle+\exp(2\pi\mathrm{i}0.j_1j_2\cdots j_n)|1\rangle)(|0\rangle+\exp(2\pi\mathrm{i}0.j_2\cdots j_n)|1\rangle)\cdots(|0\rangle+\exp(2\pi\mathrm{i}0.j_n)|1\rangle)/\sqrt{2^n}.$$

经过交换运算，量子比特状态为

$$(|0\rangle+\exp(2\pi\mathrm{i}0.j_n)|1\rangle)(|0\rangle+\exp(2\pi\mathrm{i}0.j_{n-1}j_n)|1\rangle)\cdots(|0\rangle+\exp(2\pi\mathrm{i}0.j_1j_2\cdots j_n)|1\rangle)/\sqrt{2^n}.$$

3　结合量子 Fourier 变换的 Deutsch-Jozsa 算法

3.1　算法的实现

在 Deutsch-Jozsa 算法的经典量子线路（图 1）中，过多地使用了 Hadamard 变换，使计算比较复杂. 量子 Fourier 变换的有效电路，如图 2 所示. 图 2 中，对输入状态的每一位进行变换，得到输入状态最终的量子 Fourier 变换. 将这两种量子线路结合，利用量子 Fourier 变换代替 Hadamard 变换，实现的方法，如图 3 所示.

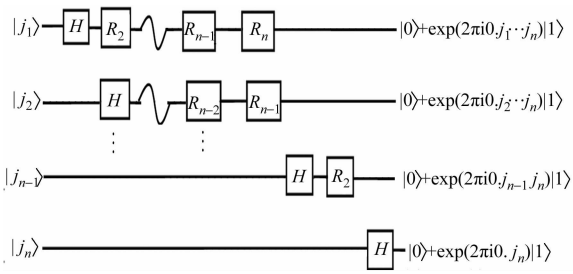

图 2　量子 Fourier 变换的有效电路

Fig. 2　Efficient circuit of quantum Fourier transform

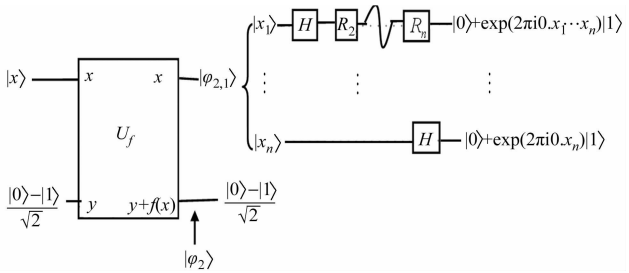

图 3　利用量子 Fourier 变换解决 Deutsch 问题的有效电路

Fig. 3　Efficient circuit of Deutsch problem by quantum Fourier transform

图 3 中，A 把从 $0\sim2^n-1$ 中选择的数 x 告诉 B，然后，B 对 A 传过来的数 x 进行函数 $f(x)$ 的运算. 对 x 使用幺正变换 $U_f:|x,y\rangle\rightarrow|x,y\oplus f(x)\rangle$，为了确保经过幺正变换后的计算结果仍存在 $f(x)$，此处的 y 选择由状态 $|1\rangle$ 经过 Hadamard 变换得到的叠加态 $(|0\rangle-|1\rangle)/\sqrt{2}$，它由 B 在计算时直接提供. B 得到计算结果后，将结果传回给 A，A 收到后，利用量子并行性对包含 x 的那部分量子比特进行量子 Fourier 变换，最后，根据量子 Fourier 变换的结果，分析确定函数 $f(x)$.

3.2　量子线路的分析

根据有效电路分析电路状态，初始状态为 A 选择的数 $|x\rangle$.

B 得到 A 发送的数 $|x\rangle$ 后，对其使用幺正变换 $U_f:|x,y\rangle\rightarrow|x,y\oplus f(x)\rangle$，可以得到 $|\varphi_2\rangle$，即

$$|\varphi_2\rangle=(-1)^{f(x)}|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}. \tag{4}$$

由式(4)可知：B 的函数计算结果保存在量子比特的幅度中. A 得到 B 的计算结果 $|\varphi_2\rangle$ 后，利用量子并行性对状态 $|\varphi_{21}\rangle=(-1)^{f(x)}|x\rangle$ 进行量子 Fourier 变换. 将状态 $|x\rangle$ 写成二进制形式 $x=x_12^{n-1}+x_22^{n-2}+\cdots+x_n2^0$. 图 3 中，$|\varphi_{2,1}\rangle$ 的幅值省略没有写出，即

$$|\varphi_{2,1}\rangle(-1)^{f(x)}|x\rangle=\sum_{x\in\{0,1\}^n}|x\rangle=\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle. \tag{5}$$

由量子 Fourier 变换的定义式(2)，有

$$|\varphi_{2,1}\rangle\rightarrow|\varphi_{2,2}\rangle=\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\Big[\sum_{x=0}^{2^n-1}(-1)^{f(x)}\exp(2\pi\mathrm{i}xk/2^n)\Big]|k\rangle. \tag{6}$$

对 $|\varphi_{2,2}\rangle$ 右边部分进行交换运算，可以得到

$$|\varphi_{2,3}\rangle=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}\Big[\sum_{k=0}^{2^n-1}(-1)^{f(x)}\exp(2\pi\mathrm{i}xk/2^n)|k\rangle\Big]. \tag{7}$$

最终,可以得到

$$|\varphi_{2,4}\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}[\sum_{k=0}^{2^n-1}\exp(2\pi ixk/2^n)\,|\,k\rangle]. \tag{8}$$

由式(1),(3),(20)可以得到

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}[\sum_{k=0}^{2^n-1}\exp(2\pi ixk/2^n)\,|\,k\rangle] = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(|\,0\rangle+\exp(2\pi i0.x_n)\,|\,1\rangle)\times$$
$$(|\,0\rangle+\exp(2\pi i0.x_{n-1}x_n)\,|\,1\rangle)\cdots(|\,0\rangle+\exp(2\pi i0.x_1\cdots x_n)\,|\,1\rangle). \tag{9}$$

即得到 $\varphi_{2,1}$ 的量子 Fourier 变换为

$$\varphi_{2,1}\rightarrow\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(|\,0\rangle+\exp(2\pi i0.x_n)\,|\,1\rangle)\times$$
$$(|\,0\rangle+\exp(2\pi i0.x_{n-1}x_n)\,|\,1\rangle)\cdots(|\,0\rangle+\exp(2\pi i0.x_1\cdots x_n)\,|\,1\rangle). \tag{10}$$

由式(10)可知:如果 $f(x)$是常数函数,$\varphi_{2,1}$进行量子 Fourier 变换后的 $\varphi_{2,4}$幅值为正数或负数;如果 $f(x)$是平衡函数,对 $\varphi_{2,4}$的正负幅度贡献抵消,幅度为 0.归纳起来,若最终测量结果是 0,则函数是平衡函数;否则,函数是常数函数.

3.3 算法的分析和比较

在图 1 的量子线路中,为了实现 Deutsch-Jozsa 算法,A 从 0 到 2^n-1 中选择一个数 x 后,将其存放在一个 n 量子比特的查询寄存器中.同时,还需要用一个单量子比特的寄存器给 B 存储答案,答案寄存器的初始状态为$|1\rangle$.开始,A 对 x 用 Hadamard 变换,使其处于 n 量子比特的叠加态.同时,使用 Hadamard 变换,使答案寄存器中的状态为$(|0\rangle-|1\rangle)/\sqrt{2}$.B 收到 A 的数据后,利用幺正变换 $U_f:|x,y\rangle\rightarrow|x,y\oplus f(x)\rangle$和量子并行性计算 $f(x)$,并把结果放在答案寄存器中传回给 A,A 用 Hadamard 变换干涉查询寄存器的状态,再通过适当的测量,确定 $f(x)$是平衡函数还是常数函数.

在图 3 的量子线路中,A 直接从 0 到 2^n-1 中选择的数 x 发送给 B,B 利用幺正变换 $U_f:|x,y\rangle\rightarrow|x,y\oplus f(x)\rangle$和量子并行性计算 $f(x)$,此处的 y 由 B 提供.A 得到 B 计算的结果后,利用量子并行性对前 n 位量子比特进行量子 Fourier 变换,再通过适当的测量,确定 $f(x)$是平衡函数还是常数函数.

对比图 1 和图 3 可知:在 Deutsch-Jozsa 算法中,减少对 Hadamard 变换的使用,改用量子 Fourier 变换也一样可以快速地判断出 $f(x)$是平衡函数还是常数函数,而且比使用 Hadamard 变换更简单、直接、快速.两种 Deutsch-Jozsa 算法的计算时间对比,如图 4 所示.图 4 中:t 为时间;B 为量子比特.由图 4 可知:同一个数 x 分别采用的两种 Deutsch-Jozsa 算法,利用量子傅里叶变换后的 Deutsch-Jozsa 算法比 Deutsch-Jozsa 算法耗时短,能更快地得到判断结果.

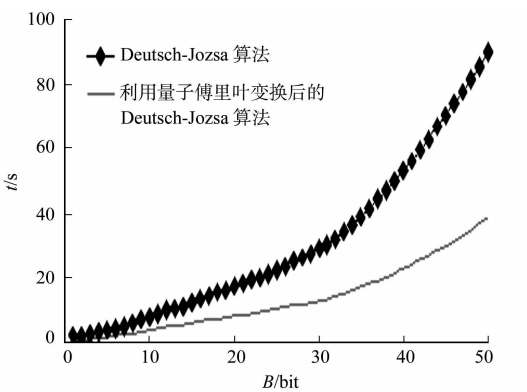

图 4 两种算法的计算时间对比图

Fig. 4 Comparison of two kinds of algorithm in computation time

4 结束语

文中介绍了 Deutsch 算法、量子线路算法和量子 Fourier 变换.在此基础上,推导并验证 Deutsch-Jozsa 算法可结合量子傅里叶变换进行快速计算,为解决 Deutsch-Jozsa 算法提供了新思路,这对"相对黑盒"指数加速的量子算法[12]的研究提供了新的方案,也为后面进行量子算法和量子计算机[13]的研究起着重要的作用.

参考文献:

[1] DEUTSCH D,JOZSA R. Rapid solution of problems by quantum computation[J]. Proceedings:Mathematical and Physical Sciences,1992,439(1907):553-558.

[2] CLEVE R,EKERT A,MACCHIAVELLO C,et al. Quantum algorithms revisited[J]. Proceedings of the Royal Society A Mathematical Physical and Enginneering Sciences,1997,454(1969):339-354.
[3] SHOR P W. Algorithms for quantum computation: Discrete logarithm factoring[C]// Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science. Los Alamitos:IEEE Press,1994:181-182.
[4] GROVER L. A fast quantum mechanical algorithm for database search[C]// Proceedings of the 28th Annual ACM Symposium on the Theory of Computing. New York:ACM,1996:212-219.
[5] 王蕴,黄德才,俞攸红. 量子计算及量子算法研究进展[J]. 计算机系统应用,2011,20(6):228-231,237.
[6] 魏达秀,杨晓冬,罗军,等. 七量子位 Deutsch-Jozsa 量子算法的核磁共振实验实现[J]. 原子核物理评论,2002,19(2):278-280.
[7] ZHENG Shibiao. Scheme for implementing the Deutsch-Jozsa algorithm in cavity QED[J]. Physical Review A,2004,70(3):034301(1-3).
[8] DASGUPTA S,BISWAS A,AGARWAL G S. Implementing Deutsch-Jozsa algorithm using light shifts and atomic ensembles [J]. Physical Review A,2005,71(1):012333(1-8).
[9] NIELSON M A,CHUANG I L. Quantum computation and quantum information[M]. Cambridge:Cambridge University Press,2000:32-35,217-219.
[10] BALLHYSA E. A generalization of Deutch-Jozsa algorithm[M]. Germany:LAMBERT Academic Publishing,2010:15-20.
[11] 付向群,鲍皖苏,王帅. ZN 上离散对数量子计算算法[J]. 计算机学报,2014,37(5):1058-1062.
[12] 龙桂鲁. 量子计算算法介绍[J]. 物理,2010,39(12):803-809.
[13] 张毅,卢凯,高颖慧. 量子算法与量子衍生算法[J]. 计算机学报,2013,36(9):1835-1842.

Application of the Quantum Fourier Transform in Deutsch-Jozsa Algorithm

ZHANG Hongtao[1,2], XIONG Hongmei[1,2],
TU Lingying[1,2], SHU Jun[2]

(1. Nanoelectron technology and microsystem Laboratory, Hubei University of Technology, Wuhan 430068, China;
2. School of Electrical and Electronic Engineering, Hubei University of Technology, Wuhan 430068, China)

Abstract: A new method to solve Deutsch-Jozsa algorithm by using quantum Fourier transform was presented. Combine the quantum circuits of quantum Fourier transform and Deutsch-Jozsa algorithm, then a new quantum circuit of solving Deutsch-Jozsa algorithm used quantum Fourier transform was found. And the quantum circuit processes were observed step by step, and states of the circuit was analyzed. The results showed that solving Deutstch problem by quantum Fourier transform can improve the operation speed and save the operation time.

Keywords: Deutsch-Jozsa algorithm; quantum Fourier transform; quantum circuit; quantum algorithms

（**责任编辑**：黄晓楠　　**英文审校**：吴逢铁）