[基础数学与应用数学研究]

量子并行性及其应用

王晓晗[1]，曹怀信[2]，吴水艳[1]

(1.咸阳师范学院 数学系，陕西　咸阳　712000；2.陕西师范大学 数学与信息科学学院，陕西　西安　710062)

摘　要：量子并行性是许多量子算法的一个基本特征，本文主要从矩阵论的思想出发阐述了量子并行性的原理及其应用，利用矩阵方法证明两种量子线路的输出结果和 Deutsch 算法。

关键词：量子比特；逻辑门；量子线路；矩阵

中图分类号：O241.82　　文献标识码：A　　文章编号：1672-2914(2008)06-0012-03

量子最早出现在光量子理论中，是微观系统中能量的一个力学单位。量子信息的基本存储单元称为量子比特(Qubit)。量子比特被描述为具有特定属性的数学对象。量子状态的变化可以用量子计算的语言来描述，量子计算机是由包含连线和基本量子门[1] 排列起来、形成的处理量子信息的量子线路建造的。量子门就是一个酉算子[2]（相应矩阵 U 要满足的条件是酉性(unitary))，即 $U^{\dagger}U=I$ 。

量子并行性[3]是许多量子算法中的一个基本特征，简而言之，量子并行性使量子计算机可以同时计算函数 $f(x)$在许多不同的 处的值。

设 $f:\{0,1\}\to\{0,1\}$ 是具有一比特定义域和值域的函数。考虑初态为$|x,y\rangle$的双量子比特的量子计算机。通过适当的逻辑门序列可以把这个状态变换为$|x,y\oplus f(x)\rangle$，其中$\oplus$表示模 2 加法。第一个寄存器为数据寄存器，第二个为目标寄存器，映射$|x,y\rangle\to|x,y\oplus f(x)\rangle$叫做 U_f，可证明它是酉的[3]。在文献[1,3]中是利用量子线路来表示输入和输出的量子状态，以下我们将使用矩阵的方法得出量子线路的输出结果，Deutsch 问题是由 Deutsch 在文献[1,4]中提出的，本文也是利用矩阵方法证明其结果。

1　预备知识

设 $f:\{0,1\}\to\{0,1\}$ 是具有一比特定义域和值域的函数。考虑初态为$|x,y\rangle$的双量子比特的量子计算机。通过适当的逻辑门序列可以把这个状态变换为$|x,y\oplus f(x)\rangle$，其中$\oplus$表示模 2 加法。

$$|x,y\rangle\xrightarrow{U_f}|x,y\oplus f(x)\rangle$$

其中，f 函数共有如下四种形式：

(ⅰ)当 $f(x)=x$ 时，U_f 矩阵表示为

$$\boldsymbol{U}_f=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix};$$

(ⅱ)当 $f(0)=1,f(1)=0$ 时，U_f 矩阵表示为

$$\boldsymbol{U}_f=\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix};$$

(ⅲ)当 $f(0)=f(1)=0$ 时，U_f 矩阵表示为

$$\boldsymbol{U}_f=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}=\boldsymbol{I};$$

(ⅳ)当 $f(0)=f(1)=1$ 时，U_f 矩阵表示为

$$\boldsymbol{U}_f=\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&1&0\end{bmatrix}$$

其中 U_f 都是酉矩阵。

我们主要讨论在第二种情况下的作用。

2　量子并行性的运算

定理 1　在计算基下，图 1 线路的矩阵表示为

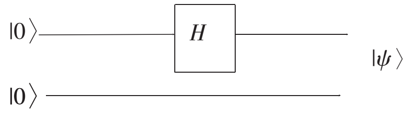

图 1

收稿日期：2008-09-21
作者简介：王晓晗(1977-)，女，陕西蓝田县人，咸阳师范学院数学系讲师，研究方向为算子代数与小波理论。

$$U_1=\frac{1}{\sqrt{2}}\begin{bmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{bmatrix}。$$

证明　在计算基态$|00\rangle,|01\rangle,|10\rangle,|11\rangle$下，记

$$U_1=\frac{1}{\sqrt{2}}\begin{bmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{bmatrix}$$

$$(\boldsymbol{H}\otimes\boldsymbol{I})|00\rangle=\boldsymbol{H}|0\rangle\otimes\boldsymbol{I}|0\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}=U|00\rangle,$$

$$(\boldsymbol{H}\otimes\boldsymbol{I})|01\rangle=\boldsymbol{H}|0\rangle\otimes\boldsymbol{I}|1\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}=U|01\rangle,$$

$$(\boldsymbol{H}\otimes\boldsymbol{I})|10\rangle=\boldsymbol{H}|1\rangle\otimes\boldsymbol{I}|0\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\-1\\0\end{bmatrix}=U|10\rangle,$$

$$(\boldsymbol{H}\otimes\boldsymbol{I})|10\rangle=\boldsymbol{H}|1\rangle\otimes\boldsymbol{I}|0\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\-1\end{bmatrix}=U|11\rangle,$$

且

$$U_1U_1^{+}=\frac{1}{\sqrt{2}}\begin{bmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{bmatrix}=\boldsymbol{I}。$$

考虑图 2 的线路，把 U_f 加到计算基以外的一个输入。数据寄存器中是叠加态 $(|0\rangle+|1\rangle)/\sqrt{2}$，这可由 Hadamard 门[3] 作用到$|0\rangle$上得到。于是应用 U_f 得到状态

$$\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$$

定理 2　输入初态为$|0\rangle\otimes|1\rangle$，通过图 2 的线路作用，则输出状态为

$$\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}。$$

证明　我们讨论 U_f 在第二种情况下的作用

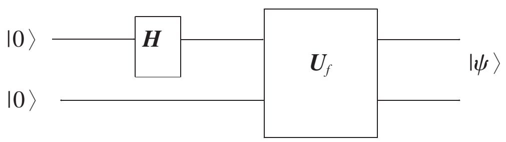

图 2

$$|\psi\rangle=U_fU(|0\rangle\otimes|0\rangle)=$$

$$\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}=$$

$$\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}。$$

在定理 2 中如果利用 Hadamard 变换，两个 Hadamard 门同时作用到双量子比特上，若初态全为$|0\rangle$的情况，输出结果是

$$\frac{|0,f(0)\rangle+|0,1\oplus f(0)\rangle+|1,f(1)\rangle+|1,1\oplus f(1)\rangle}{2}$$

定理 3　输入初态为 $|0\rangle\otimes|0\rangle$，通过图 3 的线路作用，则输出状态为$|0,f(0)\rangle+|0,1\oplus f(0)\rangle+|1,f(1)\rangle+|1,1\oplus f(1)\rangle$。

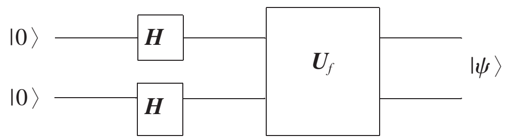

图 3

证明　利用定理 2 和函数 f 的第二种情况

$$|\psi\rangle=U_f\,E(|0\rangle\otimes|0\rangle)=$$

$$\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\frac{1}{2}\begin{bmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=$$

$$\frac{1}{2}\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}=\frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}=$$

$$\frac{|0,f(0)\rangle+|0,1\oplus f(0)\rangle+|1,f(1)\rangle+|1,1\oplus f(1)\rangle}{2}。$$

当进行 n 比特输入 x 和单比特输出 $f(x)$函数的量子并行性计算。制备 $n+1$ 量子比特的状态$|0\rangle^{\otimes n}|0\rangle$，对前 n 位应用 Hadamard 门变换，并连接 U_f 的量子线路，就产生状态

$$\frac{1}{\sqrt{2^n}}\sum_x|x\rangle|f(x)\rangle$$

在某种意义，表面上似乎只进行一次 f 计算，量子并行性却使 f 的所有可能值同时被计算出来。

如果我们把图 2 的线路稍加修改，就可以用 Deutsch 算法的实现来说明量子线路如何超越经典

线路。Deutsch 算法是把量子并行性和量子力学中称为干涉(interference)的性质结合起来，这样，通过测量第一量子比特，我们就可以确定出 $f(0)\oplus f(1)$。我们通过量子线路仅对 $f(x)$ 的一次计算，就能够确定 $f(x)$ 的全局性质。

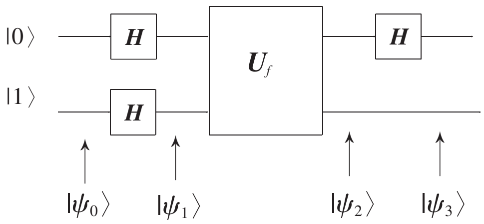

图 4

$$|\psi_0\rangle-|0\rangle\otimes|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix},$$

$$|\psi_1\rangle=\boldsymbol{E}|\psi_0\rangle=\frac{1}{2}\begin{bmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{bmatrix}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=\frac{1}{2}\begin{bmatrix}1\\-1\\1\\-1\end{bmatrix}=$$

$$\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right],$$

$$|\psi_2\rangle=U_f|\psi_1\rangle=\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\frac{1}{2}\begin{bmatrix}1\\-1\\1\\-1\end{bmatrix}=\frac{1}{2}\begin{bmatrix}-1\\1\\1\\-1\end{bmatrix}=$$

$$-\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

$$|\psi_3\rangle=U|\psi_2\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{bmatrix}\frac{1}{2}\begin{bmatrix}-1\\1\\1\\-1\end{bmatrix}=$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}0\\0\\-1\\1\end{bmatrix}=-|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]。$$

参考文献：

[1]D. Deutsch, A. Barenco , A. Ekert. Universality in quantum computation[M].London：Proc, R. Soc. A, 1995，669−667.

[2]A. Dvurecenskij ,S. Pulmannova. New Trends in Quantum Structures[M]. Dordrecht: Kluwer Academic publishers, 2000.

[3]尼尔森·庄.量子计算与量子信息(一)—量子计算部分[M].赵千川,译.北京：清华大学出版社，2004.

[4]D. Deutsch. Quantum computational networks[M]. London : Proc, R. Soc. A, 1989:425.

The Quantum Parallelism and Its Application

WANG Xiao-han[1], CAO Huai-xin[2] , WU Shui-yan[1]

(1. Department of Mathmatics, Xianyang Normal University, Xianyang, Shaanxi 712000;

2. College of Mathmatics and Information Scinece, Shaanxi Normal University, Xi'an, Shaanxi 710062, China)

Abstract：The quantum parallelism theorem is the basic characteristics of many quantum computations. In this paper, we expounded the principle and its application of the quantum parallelism theorem from the theory of matrices, and use it to prove that the output of two quantum circuits and Deutsch computation.

Key words：Qubit；quantum gate；quantum circuits；matrix