计算机科学2001Vol. 28№. 9

浅释量子计算的计算能力

Simply Explain the computation Ability of Quantum Computation

匡春光

(总装装备指挥技术学院　北京101407)

Abstract Quantum computation is a new field of computer science. It is given attention to for its powerful computation ability. The paper explains the cause of its powerful computation ability by giving two typical quantum computation algorithms.

Keywords Quantum computiation, Computation ability

一、概述

量子计算机已被公认为是未来新型计算机的发展方向之一。尽管现在还没有研究出实用的量子计算机，但关于量子计算机的理论的研究已取得了很大进展。量子计算就是其中最主要的一个领域。量子计算机的强大计算能力是源于量子计算的计算能力。

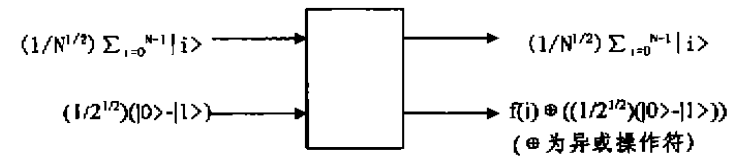
传统计算机以电位的高低表示为1和0来进行运算。计算的最小单位称为比特，用来描述一个电位。量子计算机以粒子的量子力学状态，如光子的极化状态和原子的自旋等表示为$|0\rangle$和$|1\rangle$来进行运算。$|0\rangle$即向量(1,0)，$|1\rangle$即向量(0,1)。计算的最小单位称为量子比特，用来描述一个粒子的量子力学状态。在传统计算机中，电位只能处于高状态(表示为1)或低状态(表示为0)，即电位处于一确定状态，在量子计算机中，情况就不是这样的了。粒子的量子力学状态并不是在$|0\rangle$和$|1\rangle$中择一。而是$|0\rangle$和$|1\rangle$的组合，即所谓的超态，表示为$c_0|0\rangle+c_1|1\rangle$，其中$c_0$,$c_1$为复数，$|c_0|^2+|c_1|^2=1$($|c_0|$为复数$c_0$的模)，如果测量这个量子比特，则由$|c_0|^2$的可能性得$|0\rangle$，由$|c_1|^2$的可能性得$|1\rangle$。在传统计算机中，当有多个比特在一起时，它们互不干涉。在量子计算机中，当多个量子比特在一起时，它们会相互干涉。它们的状态并不能分别表示为$c_0^1|0\rangle+c_1^1|1\rangle$和$c_0^2|0\rangle+c_1^2|1\rangle$，而是$|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$四种状态的组合，即它们的状态为：$(c_0^1|0\rangle+c_1^1|1\rangle)$张量乘$(c_0^2|0\rangle+c_1^2|1\rangle)=c_0^1c_0^2|00\rangle+c_0^1c_1^2|01\rangle+c_1^1c_0^2|10\rangle+c_1^1c_1^2|11\rangle$，简化表示为：$c_0|00\rangle+c_1|01\rangle+c_2|10\rangle+c_3|11\rangle$，其中$|00\rangle$即向量(1,0,0,0)，$|01\rangle$即向量(0,1,0,0)，$|10\rangle$即向量(0,0,1,0)，$|11\rangle$即向量(0,0,0,1)，$c_0$,$c_1$,$c_2$,$c_3$为复数，$|c_0|^2+|c_1|^2+|c_2|^2+|c_3|^2=1$，如果测量这两个量子比特，则由$|c_0|^2$的可能性得$|00\rangle$，$|c_1|^2$的可能性得$|01\rangle$，$|c_2|^2$的可能性得$|10\rangle$，$|c_3|^2$的可能性得$|11\rangle$。依次类推，如果有n个量子比特在一起，则它们的状态表示为：$\sum_{i=0}^{N-1}c_i|i\rangle$，(在本文中，$N=2^n$)，$i$是一个二进制数。$\sum_{i=0}^{N-1}|c_i|^2=1$。在此基础上，下面将举例说明量子计算的强大计算能力，量子计算的强大计算能力主要源于量子计算的并行性和干涉性。

二、Deutsch-Jozsa问题

Deutsch-Jozsa问题是这样的。f是一个由集合(1,2,…,N)到集合(0,1)的映射，或者$f(i)\equiv0$(常量)，或者有一半i使$f(i)=0$，另一半i使$f(i)=1$(平衡)，现要求判断f是哪一种情况。

如果用传统的办法来解决这个问题，需要查询$N/2+1$次才能确保得到正确答案，即随机取i值，查询相应的$f(i)$值，重复$N/2+1$次，如果每一次得到的$f(i)$都是0，则f是第一种情况，如果至少有一次$f(i)$是1，则f是第二种情况。

如果用量子计算方法解决这个问题，则可以这样做。设计一个量子电路实现以下功能：(这种量子电路是较容易实现的)



其输出为$(1/N^{1/2})\sum_{i=0}^{N-1}|i\rangle$张量乘$f(i)\oplus((1/2^{1/2})(|0\rangle-|1\rangle))$

$=(1/N^{1/2})\sum_{i=0}^{N-1}|i\rangle$张量乘$(-1)^{f(i)}\cdot((1/2^{1/2})(|0\rangle-|1\rangle))$

$=(1/N^{1/2})\sum_{i=0}^{N-1}(-1)^{f(i)}\cdot|i\rangle$张量乘$((1/2^{1/2})(|0\rangle-|1\rangle))$ (1)

如果f是第一种情况，则(1)式的前一部分

$(1/N^{1/2})\sum_{i=0}^{N-1}(-1)^{f(i)}\cdot|i\rangle$

$=(1/N^{1/2})\sum_{i=0}^{N-1}(-1)^{0}\cdot|i\rangle$

$=(1/N^{1/2})\sum_{i=0}^{N-1}|i\rangle$

$=(1/N^{1/2})((1,0,0,\cdots,0,0)+(0,1,0,\cdots,0,0)+\cdots+(0,0,0,\cdots,0,1))$

$=(1/N^{1/2})(1,1,1,\cdots,1,1)$

$=(1/N^{1/2})(1,1,1,\cdots,1,1)^{T}$ (2)

用N×N的矩阵H乘(2)式(H中的每一个元素的值为：$(-1)^{k\cdot l}$，其中k，l是H中的元素的行、列坐标，$k\cdot l=(\sum_{r=0}^{n-1}k_r\cdot l_r)\bmod 2$，$k_r$，$l_r$是k，$l$的二进制位)。

$H\cdot(1/N^{1/2})(1,1,1,\cdots,1,1)^{T}=(1,0,0,\cdots,0,0)^{T}$ (3)

如果f是第二种情况，则(1)式的前一部分

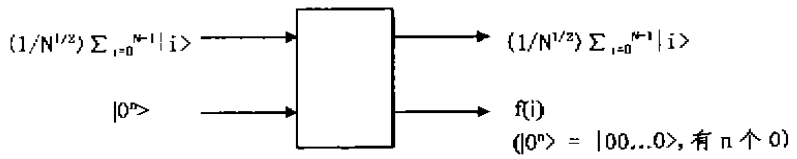
$(1/N^{1/2})\sum_{i=0}^{N-1}(-1)^{f(i)}\cdot|i\rangle$

$=(1/N^{1/2})(\pm1,\pm1,\pm1,\cdots,\pm1,\pm1)^{T}$ (4)

其中有一半元素是1，有一半元素是－1。用H乘(4)式，

$H\cdot(1/N^{1/2})(\pm1,\pm1,\pm1,\cdots,\pm1,\pm1)^{T}$

$=(0,0/1,0/1,\cdots,0/1,0/1)^{T}$ (5)



其输出为：$(1/N^{1/2})\sum_{i=0}^{N-1}|i\rangle$张量乘f(i) (6)

如果测量(6)式的前半部分，因为当$j=i\oplus s$时，$f(j)=f(i)$，所以得

$|i\rangle+|i\oplus s\rangle$ (7)

用H乘(7)式，得

$$(1/N^{1/2})\sum_{j=0}^{N-1}((-1)^{i\cdot j}+(-1)^{(i\oplus s)\cdot j})|j\rangle=\begin{cases}(1/N^{1/2})\sum_{j=0}^{N-1}\pm2|j\rangle & i\cdot j=(i\oplus s)\cdot j\\ 0 & i\cdot j\neq(i\oplus s)\cdot j\end{cases}\quad(8)$$

测量(8)式，如果得到$|j_1\rangle$，

则$i\cdot j_1=(i\oplus s)\cdot j_1$

$\Rightarrow i\cdot j_1=i\cdot j_1\oplus s\cdot j_1$

$\Rightarrow s\cdot j_1=0$

显然，(3)中的向量和(5)中的向量是不一样的，这样，根据结果向量就可以区分f是常量还是平衡。当N较小时，这两种办法相差不远，或者说量子计算的办法更麻烦，但N很大时，量子计算的办法就显出了它的优势。这个解决办法很好地利用了量子计算的并行性和干涉性。不管N有多大，问题一次解决，这就是量子计算的并行性。在用H乘(2)、(4)式后，结果向量中的任一维或者为1，或者为0，并不存在0，1之间的任何别的数，这正是量子计算干涉性的体现，多个量子比特在一起时，它们相互干涉，相互抵消不利情况(0，1之间的数)，构建有利情况(0或1)。

三、Simon问题

量子计算的强大计算能力除了体现于以上所说的并行性和干涉性外，还体现在量子计算算法中使用的一个观点。这个观点是，并不一定要以百分之百的正确性解决一个问题，解决问题时，可以允许存在极小的错误的可能性，下面这个例子就很好地说明了这一点。

Simon问题是这样的。f是一个从集合{1，2，…，N}到集合{1，2，…，N}的映射，f可能是一个一一映射，也可能是一个二一映射，二一映射，即存在一个不为0的s，当$j=1\oplus s$时，$f(j)=f(i)$，一一映射，即如果有$j=i\oplus s$，使$f(j)=f(i)$，则s必为0，现要判断f是哪一种情况。

如果用传统的算法，则要询问$N/2+1$次。下面详细讲述一下用量子计算方法怎么解决这个问题。

设计一个量子电路实现以下功能：

$=)(\sum_{r=0}^{n-1}s_r\cdot j_{1r})\bmod 2=0$

重复这种测量，得到$n+\delta$个不同的$|j_x\rangle$，得方程组

$$\begin{cases}(\sum_{r=0}^{n-1}s_r\cdot j_{1r})\bmod 2=0\\(\sum_{r=0}^{n-1}s_r\cdot j_{2r})\bmod 2=0\\\quad\vdots\\(\sum_{r=0}^{n-1}s_r\cdot j_{(n+\delta)r})\bmod 2=0\end{cases}$$

如果s只有0解，则认为f是一一映射，如果s有非0解，则f是二一映射。但这种判断还不是百分之百准确，如果s有非0解，则可以肯定f是第二种情况。但如果s只有0解，即找到的$n+\delta$个不同的$|j_x\rangle$中不存在一对

(下转第54页)

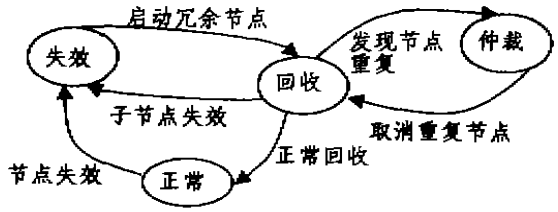


图5 系统恢复的状态转移图

仲裁算法的关键是优先权决定。通过集中分配会造成单点失效，分布式又存在一致性问题。我们采用计算机的地址，比如 IP 地址决定优先权。它具有唯一性，又不存在集中分配和分布式的缺陷。简述如下：恢复精灵监听根节点心跳(精灵和根节点在同一网段，根不知道精灵的位置，它的心跳是广播消息)，当没有心跳后，精灵广播自己 IP 地址表明要启动节点，收到消息的精灵比对自己的地址，如自己地址值大于消息中给出的就回送自己地址。发送者在时限内收到比自己地址值高的回复，就放弃启动企图。当产生重复节点时也是靠网络地址值高低分布式地决策出将关闭的节点。篇幅所限不能详述。

结论 本文研究了分布式入侵检测的问题和现状，提出了解决方案。可任意扩展的分布式结构，弥补了两层和三层模式伸缩性差及存在单点失效问题。基于消息和基于中间件的机制，使系统有良好开放性，方便集成第三方检测工具。文中提出的入侵免疫框架和抗毁框架在这一领域未见报道。入侵免疫框架通过模拟生物免疫机制自动发现共享新检测知识使系统自我进化。抗毁性框架针对安全系统的生存性要求提出，文献中广泛指出这一课题的重要性，但尚无专门研究。本文提出了框架并解决了系统重构中的若干问题。在这一领域有积极意义。

参 考 文 献

1 Allen J, Christie A. Sate of practice of intrusion detection technologies: [Technical report CMU/SEI-99-TR-028]. 1999
2 Janse W, Mell P. Applying Mobile Agents to Intrusion Detection and Response: [NIST Interim Report(IR)-6416 Oct]. 1999
3 Paxson V. Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks, 1999, 31(23-24): 2435～2463
4 Porras P A. Detecting Computer and Network Misuse Through the Production-based Expert System Toolset(P-Best). In: Proc. of 1999 IEEE Symposium on Security and Privacy, May 1999. 9～12
5 Spafford E. An Architecture for Intrusion Detection Using Autonomous Agents: [COAST Technical report]. June 1998
6 Lee W. A Data Mining Framework for Building Intrusion Detection Models. In: Proc. of 1999 IEEE Symposium on Security and Privacy, May, 1999
7 Jagannathan R. Lunt T. System Design Document: Next-Generation Intrusion Dectection Expert System (NIDES). System Design Document: A007, A012, A014 March 9, 1993
8 Ingram D J. Kremer H. Distributed Intrusion Detection for Computer Systems Using Communicating Agents. In: the Proc. of the 2000 Command and Control Research and Technology Symposium, June 2000
9 Helemer G G., Wong J S. K. Intelligent Agents for Intrusion Detection
10 Libicki L. Defending Cyberspace and Other Metaphors

(上接第129页)

$|j_{x1}\rangle$、$|j_{x2}\rangle$，使 $f(j_{x1})=f(j_{x2})$，但这并不排除存在一不为0的 s，使 $f(j_x)=f(i\oplus s)$，当然，$|i\rangle$不在所找的 $n+\delta$ 个不同的 $|j_x\rangle$中，这时 f 应是第二种情况，但我们会把它判断为第一种情况，出现判断失误。值得庆幸的是，这种可能性只有 $1/2^{n+\delta}$。这样小的可能性的错误在一般情况下是可以允许的。和前一个问题一样，当 N 很大时，量子计算的优越性是很显然的。

结束语 本文分三部分讲述了量子计算的计算能力，第一部分简单介绍了量子计算的基本概念及量子计算具有强大计算能力的原因。第二、三部分举例说明了量子计算具有强大计算能力的原因。量子计算还是计算机科学的一个新领域，希望本文的介绍能让读者建立一个量子计算的简单概念。

参 考 文 献

1 苏月琼. 量子计算机前途无量. 计算机世界，2000(17)
2 成就于后摩尔定律时代的量子计算. 计算机世界，2000(50)
3 Preskil J. Quantum Information and Computation. Lecture Notes