

量子纠错与经典纠错的比较

赵红敏

(北京交通大学理学院, 北京 100044)

摘要: 量子计算机利用其量子位态特有的相干叠加和纠缠性, 使得在某些问题的处理上优于经典计算机, 同时也导致量子计算过程中的出错图样不同于经典计算。讨论了二者的区别, 在此基础上详细介绍了量子计算机中开发的量子纠错方案。

关键词: 量子计算; 纠错; 纠缠; 退相干

中图分类号: TP3-05 **文献标识码:** A

Comparison of quantum error correction and classical error correction

ZHAO Hong-min

(School of Sciences, Beijing Jiaotong University, Beijing 100044, China)

Abstract: The quantum computer can deal with some kinds of problems better than the classical computer by using its special coherence and entanglement. Additionally, the types of error that happened during quantum computing are different from those in classical computing. The differences between them are discussed, and the quantum error correction methods developed in quantum computer are also introduced in detail.

Key words: quantum computing; error correction; entanglement; decoherence

传统计算机就是现在通用的硅芯片计算机。近 30 多年来, 制造工艺的进步使硅芯片的集成度提高了 10 万倍, 这一发展规律验证了 Moore 定律, 即大约每 18 个月, 计算机芯片的集成度就增加 1 倍^[1]。如果 Moore 定律还继续适用, 要不了多久, 芯片的布线间隔就会达到分子或原子数量级。这就涉及到许多问题: 其中, 高密度布线会引起芯片的耗能和散热剧增, 如果这个问题解决不了, 计算机进行大量运算所产生的热量有可能会使芯片材料出现局部融化。另一个很严重的问题是在高集成度下, 独立的电子器件只有几个原子那么大的时候, 在这个原子量级上支配电路中电子行为的物理规律将不再是经典物理规律, 而是量子力学, 所以, 传统的硅芯片计算机将不可避免地遭遇这个发展极限。

为了消除计算机中的能耗, 必须设法把计算过程中的不可逆运算转变成可逆运算, 减少信息数量的增减 (一个位操作所需最小能量为 $\Theta = kT \ln 2$, k 是 Boltzman 常数)。对可逆计算机的研究引出了量子计算机的概念。因为量子力学表明: 任何一个隔离的量子系统都可以作为一个可逆的计算系统。1982 年, FEYNMAN 最早就敏锐地发现原子是个非凡的“计算天才”, 并提出了量子计算的构想^[2]。1985 年, DEUTSCH 进一步阐述了 FEYNMAN 的思想, 给出了量子计算机的理论计算模型^[3]。关于量子计算机原理及算法等问题已有一些文章介绍, 本文仅就量子计算中的纠错问题作分析。

众所周知, 比特是经典计算机中信息存储的最小单元。一个比特只能取 0 或者 1 这样一个二进制数。

在量子计算机中,量子信息的最小单元是量子比特(qubit)。就像经典计算机有一个状态(或0或1)一样,量子比特也有一个状态。量子比特可能的状态是 $|0\rangle$ 和 $|1\rangle$,分别对应经典比特的0和1。量子比特和经典比特最大的区别就在于量子比特的状态不仅可以处在 $|0\rangle$ 或者 $|1\rangle$ 态上,还可以处于这些状态的线性组合(常称为相干叠加态)中 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (其中 α, β 为任意的复常数)。也就是说,量子比特可以同时存储 $|0\rangle$ 和 $|1\rangle$ 两个状态。对于由 N 个比特组成的经典存储器来说,在某一个时刻,它只能存储 2^N 个二进制数中的一个;而对于由 N 个量子比特组成的量子存储器来说,在某一个时刻,它能同时存储这 2^N 个二进制数。所以,量子计算机存储的信息量要远远大于经典计算机。此外,不同的量子比特状态之间还可以发生纠缠。比如,一对粒子除了可以处在 $|00\rangle, |01\rangle, |10\rangle$ 和 $|11\rangle$ 态外,还可以处在它们的纠缠态,比如 $\gamma|01\rangle + \delta|10\rangle$ 中。纠缠态是一种特殊(复合系统)的相干叠加态,处在纠缠态的一对粒子相互纠缠在一起,对其中一个粒子的测量,必然会同时影响到另外一个粒子。正是由于纠缠态的相干叠加性,量子计算机才得以实现不同于经典计算机上的并行计算,使量子计算从根本上超越经典计算。

量子计算机的优越性主要体现在量子并行计算上,不论是量子并行计算还是对量子系统进行模拟,都利用了量子系统最本质的特性——量子态的相干叠加和纠缠。但是在实际系统中,量子态的这种相干叠加和纠缠很脆弱、很难保持。因为量子计算机不是一个孤立的量子系统,它必然要同外部环境,包括测量仪器发生相互作用,结果就会出现量子态相干性的丢失,使量子态退化为经典态。这就是退相干效应。退相干效应的存在使量子计算的优越性丢失,运算结果出现错误。除了退相干不可避免地导致量子错误外,其他一些技术原因,比如量子门操作中的误差也会导致量子错误。为了实现有价值的量子计算,首要的任务就是克服退相干效应,对量子计算过程中出现的错误及时加以监控并纠正。为实现这一目的,量子纠错编码应运而生。由于经典计算与量子计算有本质区别,导致量子纠错完全不同于经典纠错。

1 经典纠错

经典计算机作为一个复杂的计算系统,在运行过程中噪声不可避免,所以同样也面临着门运算错误和计算不精确等问题。但是人们现在并不怀疑计算结果的正确性。因为在经典计算机中,已经发展了一套很完善的纠错理论,成功地运用在了计算机中。只要机器出错的概率不超过某个阈值,借助于纠错技术,依然可以获得可靠的计算结果。线性分组码是一类经典纠错码。不论是奇偶校验还是Hamming校验,其基本原理就是冗余校验。即除了基本的有效信息码外,还增加校验的冗余码。将有效的信息位与校验位一起按某种规则编码,并一起写入存储器或向外发送。当从存储器或从外部接收到编码信息的代码时,按约定规则译码,取出有效部分,同时利用校验信息位判断接受到的代码是否有错,若有错,则自动恢复正确的代码。举个最简单的重复码的例子,比如用3个比特编码1个比特的信息,可以将信号0编码为000,信号1编码为111,这样如果最多有一个比特发生错误,比如000变成了001,那么通过观测每一个比特值并两两对比的方法,按照少数服从多数的原则,找出出错的第3个比特,并恢复第3个比特值为0,从而纠正这个错误。

2 量子纠错

在量子纠错刚刚开始的时候,人们很想把经典计算机中这套完善的纠错理论直接照搬过来。但是由于量子位不同于经典位,人们很快发现存在着许多困难。首先就是在经典编码中,为了引入信息冗余,需要将单比特的态复制到多比特的态上去。但在量子力学中,根据著名的量子态不可克隆原理,禁止未知量子态的复制^[4]。其次,经典编码在纠错的时候,需要将经典位的态进行测量,以确定错误的图样。但在量子情况下,对量子态的测量会引起量子态的坍塌,破坏了量子相干性。测量后的状态已不再是原来的状态,导致量子信息的丢失。所以不能采用经典的办法,通过运算期间的检测判定中间数据的正确性来保证量子计算机最后运算结果不出错。第三,经典纠错码中的错误只有一种 $0 \leftrightarrow 1$,即0,1之间的跃迁。但量子错误的自由度要大得多,除了位翻转错误 $|0\rangle \leftrightarrow |1\rangle$,还有可能发生位相错误 $|1\rangle \rightarrow -|1\rangle$ 。第四,经典信息的错误是分立的,而量子位态取值于一个二维的Hilbert空间的任意态矢,所以量子信息的错误可以是连续的。比如在一个量子门操作下,一个量子位态应由 $\alpha|0\rangle + \beta|1\rangle$ 变为 $\alpha|0\rangle + \beta e^{i\phi}|1\rangle$ 态,但是由于门操作中的误差,使得量子位态变成了 $\alpha|0\rangle + \beta e^{i(\phi + \delta)}|1\rangle$, δ 是一个小量,实际的这个量子态虽然很接近正确的量子态,但它依然是错的。可怕的是如果不采取措施纠正这些小错误,随着时间的推移,这些小错会慢慢积累起来,最终变成大

错。最后为了诊断和纠正错误,必须观察几个量子位,但是量子测量必然会扰乱被测量子态,从而引入新的错误。由于这些原因,量子纠错比经典纠错困难得多。事实上,直到 1995 年,SHOR 才在此方向取得一个本质性的进展,提出了第 1 个量子纠错编码方案^[5]。

3 量子纠错方案

3.1 纠随机错的量子码

通常量子纠错码是指纠随机错的量子码。量子纠错码可以看成是 k 个量子位(Hilbert 空间的维数是 2^k)到 n 个量子位(Hilbert 空间的维数是 2^n)的映射。这里 $n > k$ 。要保护的信息就是存储在这 k 个量子位中,被称做逻辑量子位或编码量子位。附加的 $n - k$ 个量子位以冗余的方式存储这 k 个逻辑量子位,目的是保护编码信息免遭破坏。从这点上来看,量子纠错码实际上是经典纠错码的量子类比。

比如,最初,SHOR 采用 1 组($n = 9$)量子位来编码 1 个($k = 1$)量子位纠一位错。根据 SHOR 的理论, $|0\rangle, |1\rangle$ 被编码后的态 $|\bar{0}\rangle$ 和 $|\bar{1}\rangle$ 分别被称作“逻辑 0”和“逻辑 1”,

$$|0\rangle \rightarrow |\bar{0}\rangle \equiv 2^{-\frac{3}{2}}(|1000\rangle + |1111\rangle)(|1000\rangle + |1111\rangle)(|1000\rangle + |1111\rangle),$$

$$|1\rangle \rightarrow |\bar{1}\rangle \equiv 2^{-\frac{3}{2}}(|1000\rangle - |1111\rangle)(|1000\rangle - |1111\rangle)(|1000\rangle - |1111\rangle).$$

$|\bar{0}\rangle$ 和 $|\bar{1}\rangle$ 每个都包括 3 个三量子位的团簇。每一个团簇都置于相同的量子态。每个团簇都有三重位的冗余。利用这个冗余编码,不仅可以纠正位翻转错误,还可以改正位相错误。

考虑一个团簇中发生了位翻转错误,即状态由 $|000\rangle \pm |111\rangle$ 比如说变成了 $|010\rangle \pm |101\rangle$ 。因为不能对单个量子位进行测量(这会破坏量子态),而是对这个量子位的状态进行集体测量。测量任意 2 个量子位态的模 2 加值(比如以 x, y, z 表示这 3 个量子位态,则分别测量量子位态 $x \oplus y, y \oplus z, x \oplus z$),如果测得的值均为 0,则没有发生位翻转,否则,如果 3 个量子位之一发生了翻转,则测量值中必有一个 1。通过比较,便可以知道哪一个出了错,并将它及时纠正过来。这样就纠正了位翻转错误。对于量子位发生的小错误,这种方法同样适用。

现在假设在其中的一个团簇中发生了位相错误,这个错误改变了这个团簇中 $|000\rangle$ 和 $|111\rangle$ 的相对符号,以至于

$$|000\rangle + |111\rangle \rightarrow |000\rangle - |111\rangle,$$

$$|000\rangle - |111\rangle \rightarrow |000\rangle + |111\rangle.$$

这样,这个团簇中的相对位相就不同于其他 2 个团簇中的相对位相,通过比较一对团簇中的位相(6 个量子位的集体测量),而不是测量每一个团簇中的相对位相(这会改变编码信息),就可以找出位相改变的团簇,检测的结果允许断定哪一个团簇中的符号不同于其他 2 个团簇,从而,可以把么正位相变换应用到那个团簇中的量子位之一,改变其符号,纠正错误。

九位编码在概念上是简单的,但它不是最有效的量子编码,为了一位量子位而引入了 9 个量子位,其代价太大了。1996 年 STEANE 提出的用 7 个比特编码 1 个比特来纠一位错的量子码对后来的量子纠错方案的改进影响很大^[6]。目前被证明最有效的纠一位错的编码方案是利用 5 个比特编码 1 个比特来完成^[7,8]。GOTTESMAN 及 CALDERBANK 等人发现了量子纠错码的群理论结构^[9,10],引进了码“稳定子”的概念,使量子纠错码理论更为系统和完善。

3.2 防合作错的量子码

在实际情况下,量子计算机中所有的量子比特不仅都要经历退相干过程而且都要参与门运算。在这些过程中,每个比特都有可能出错。所以量子计算机中发生错误的量子比特数是不确定的,但是只要量子比特独立的发生退相干,即各个比特随机地出错,彼此毫不关联,那么前面介绍的量子纠错方案都会行之有效。但是实际中发生退相干的量子比特却相互关联,这就是合作消相干。合作消相干结果导致各个比特出错的概率也相互关联,即量子位发生合作量子错。研究人员证明,所有用来纠量子位独立消相干的量子纠错方案都可以用来克服一般的空间关联消相干,而且量子纠错的操作步骤不需要改变。

另外,已经发现更好的方案用来克服合作量子错,这就是 2 类非常重要的量子编码:量子避错码和量子防错码。它们重在防错而非纠错,所以与量子纠错方案有本质区别。量子防错码基于量子 Zeno 效应,在这

(下转第 226 页)

4 结 语

针对传统信息检索系统的不足,提出了一种基于药品本体的信息检索系统,并把相似度算法融入其中,提高了检索的查准率和查全率。当然还有很多工作需要进一步研究。例如:如何在 Web 资源上建立一个通用的本体库,现在还没有一个很好的理论支持,目前研究的很多方面都是基于领域本体而建立的;此外,关于文档的相似度算法仍是需要解决的问题。

参考文献:

- [1] 宋峻峰,张维明,肖卫东,等.基于本体的信息检索模型研究[J].南京大学学报(自然科学版),2005,41(2):189-196.
- [2] 陈 康,武港山.基于 Ontology 的信息检索技术研究[J].中文信息学报,2005,19(2):51-57.
- [3] 江克勤,张玉州,王一宾.基于语义的 Web 信息检索[J].计算机技术与发展,2007,17(1):36-39.
- [4] 李 明,王 丽.基于本体的信息检索系统模型[J].兰州理工大学学报,2007,33(2):90-93.
- [5] 王晓东,高宏卿.基于 Ontology 的智能系统开发[J].河南师范大学学报,2005,33(1):25-28.
- [6] 杨 芳,杨振山.基于语义网的电子政务文档智能检索[J].计算机应用,2005,25(10):2 434-2 438.
- [7] 焦玉英,张 璐.基于 Ontology 的语义检索模型架构[J].图书馆学刊,2006,(6):112-114.

(上接第 213 页)

个方案中,仅仅需要 2 个比特来对 1 比特信息进行编码,就可以克服量子位的独立消相干,也可以克服一般的空间关联消相干。而量子避错码本质性地利用了消相干过程中的集体效应。对于集体消相干,存在一类特殊的能在噪声环境中保持稳定的态——相干保持态。这个方案利用 2 个比特编码 1 个比特的量子信息,通过将任意的输入态编码为一个较高维空间的相干保持态,可以用来克服物理上很重要的一类消相干。

4 结 语

尽管量子纠错存在着许多困难,但是量子纠错码、量子避错和防错码的开发证明了执行可靠的量子计算并不是可望而不可及。最新的结果表明,在量子计算机中,只要门操作和线路传输中的错误率低于一定的阈值,就可以进行任意精度的量子计算。相信在众多物理学家、信息学家的共同努力下,实现可靠量子计算不再是个梦想。

参考文献:

- [1] BIRNBAUM J, WILLIAMS R S. Physics and the information revolution[J]. Phys Today, 2000, 53: 38-42.
- [2] FEYNMAN R P. Simulating physics with computer[J]. Int J Theor Phys, 1982, 21: 467-487.
- [3] DEUTSCH D. Quantum theory: The church-turing principle and universal quantum computer[J]. Proc R Soc A, 1985, 400: 97-117.
- [4] WOOTTERS W K, ZUREK W H. A single quantum cannot be cloned[J]. Nature, 1982, 299: 802.
- [5] SHOR P W. Scheme for reducing decoherence in quantum memory[J]. Phys Rev A, 1995, 52: 2 493-2 496.
- [6] STEANE A M. Multiple particles interference and quantum error correction[J]. Proc R Soc(London) A, 1996, 452: 2 551-2 557.
- [7] LAFLAMMER, MIGUEL C, PAZ J P, et al. Perfect quantum error correcting code[J]. Phys Rev Lett, 1996, 77: 198-201.
- [8] BENNETT C H, DIVINCENZO D P, SMOLIN J A, et al. Mixed-state entanglement and quantum error correction[J]. Phys Rev A, 1996, 54: 3 824-3 851.
- [9] GOTTESMAN D. An introduction to quantum error correction[J]. Proceedings of Symposia in Applied Mathematics, 2002, 58: 221-224.
- [10] CALDERBANK A R, SHOR P W. Good quantum error-correcting codes exist[J]. Phys Rev A, 1996, 54: 1 098-1 105.

科技引领,携手创新,共建和谐