量子信息基础

第六章：量子计算

金潮渊
浙江大学信息与电子工程学院

浙江大学

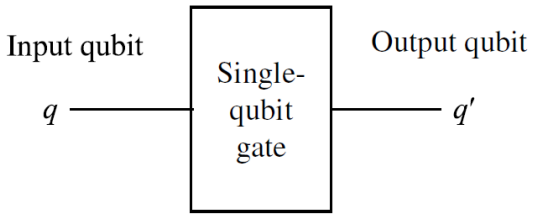
C6-2 量子算法和量子纠错

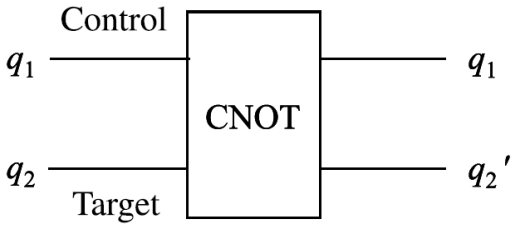
浙江大学

课程回顾

量子比特和量子逻辑：

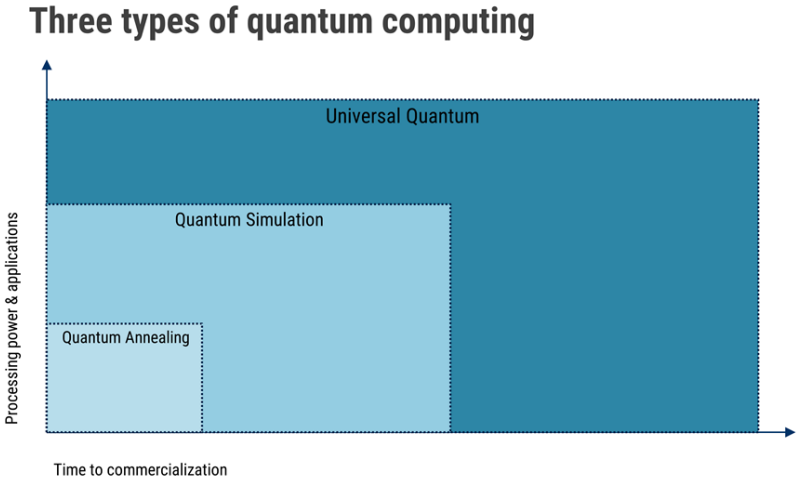
- 量子比特不是1或者0，而是1态和0态的量子叠加$|\psi\rangle = c_0|0\rangle + c_1|1\rangle$，其中$|c_0|^2 + |c_1|^2 = 1$。
- 量子寄存器存有N个量子比特。随着量子比特数的增加，量子信息呈指数增长。在计算过程中，共有2^N个线性叠加系数参与运算，但输入和输出是N个量子比特和N个经典比特。
- 量子计算机使用量子逻辑门（quantum logic gate）所组成的量子回路（quantum circuit）。单量子比特门是输入一个量子比特q输出另一个量子比特q'的逻辑器件。三种最为常见单量子比特门分别是X门、Z门和H门。最常见的双量子比特门是CNOT门。





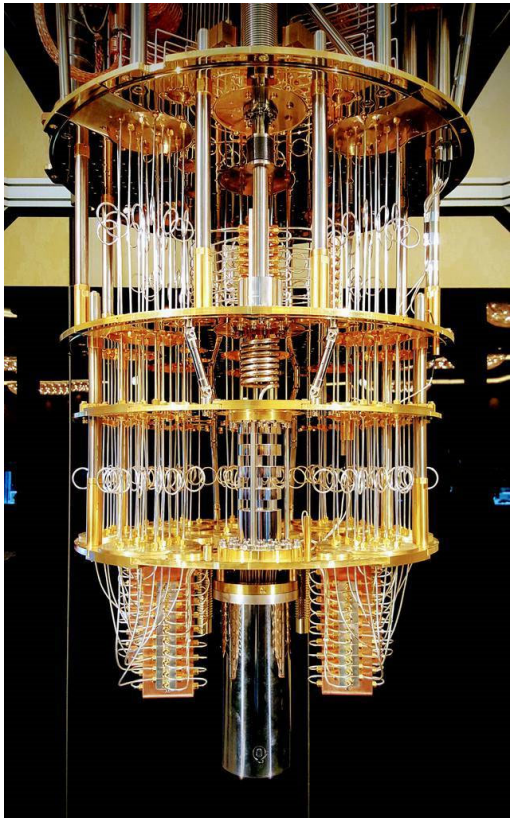
浙江大学

三种量子计算机



- 量子计算主要有三种类型。 每种类型的不同之处在于所需的处理能力(量子比特)的数量，可能的应用数量，以及实现商业可行性所需的时间：
  a. 量子退火机（quantum annealing）使用量子波动在给定的一组候选解（候选状态）上找目标函数的全局最小值。典型代表：D-Wave。
  b. 量子模拟机。利用可控的量子系统去模拟待研究的量子系统，它可以作为一种有效的实验手段用于研究经典计算机难以计算的问题 和 实验条件无法观测的现象。典型代表：Sycamore，九章。
  c. 通用量子计算机。可以进行任何复杂的计算，并快速得到解决方案。包括求解量子退火方程和模拟量子现象等。典型代表：QSystemOne。

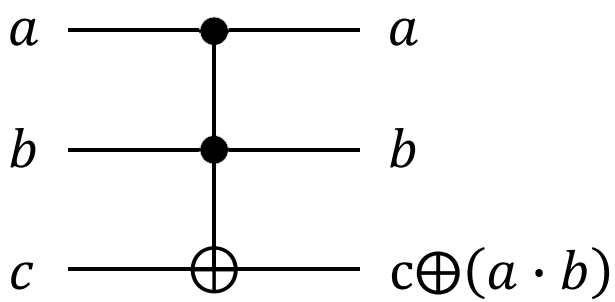
量子计算机能做什么？



- 量子计算机是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。
- 量子计算机在科学研究领域具有广泛应用前景。 学术界认为，在量子计算机达到大规模应用的比特数之前，将首先用于对量子体系的模拟。
- 量子计算主要运用在复杂度高的计算（比如NP问题）中，其潜在用途包括：（1）分子建模；（2）解密与加密；（3）金融建模；（4）数据搜索；（5）天气预报；（6）人工智能；等等。

可替代性和Toffoli门(1)

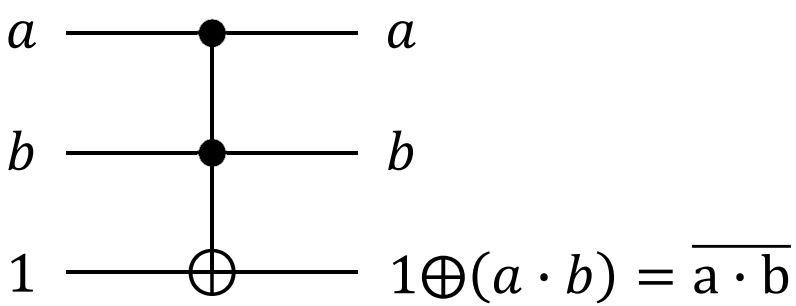
- 一个很重要但经常容易混淆的问题：量子计算机可否替代经典计算机？
- 从宏观角度考虑，我们的世界是由量子力学决定的。应该存在一条路径，基于量子原理的计算可以实现现实世界的仿真。
- 从量子逻辑门考虑，其幺正性决定了量子回路（1）较难实现循环；（2）较难实现扇入/扇出；（3）较难实现非可逆操作，如与非门。
- 但有一种逻辑门Toffoli门，有可能解决替代性问题。Toffoli门的量子回路和真值表如下所示

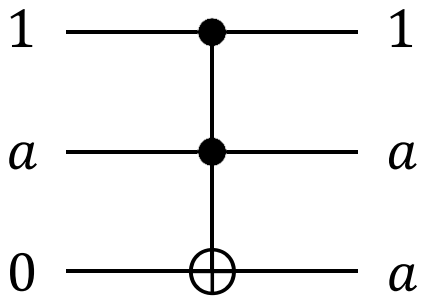


Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

浙江大学

可替代性和Toffoli门(2)





- 量子Toffoli门和经典Toffoli门类似，比如三量子比特|110⟩在量子Toffoli门的作用下可以变为|111⟩。我们可以写下这种操作所对应的8x8的幺正矩阵。
- 量子Toffoli门可以用来模拟经典逻辑门中的不可逆操作。比如与非门和扇出。
- 量子Toffoli门的扇出并不违反不可克隆原理，为什么？

$$\left[\begin{array}{cccc|cc|cc} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ \hline 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ \hline 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{array}\right]$$

量子算法

- 量子算法是在量子计算机上运行实际模型时使用的算法。经典算法是一个有限指令序列，类似地，量子算法也是一个有限指令序列。但是量子算法通常指那些具备量子特征的算法，比如量子叠加或量子纠缠。
- 量子分解算法是1994年贝尔实验室的应用数学家Peter Shor提出的，是迄今量子计算领域最著名的算法。
- 量子分解算法利用了量子计算的并行性，可以快速分解出大数的质因子。使量子计算机很容易破解广泛使用的密码如RSA公钥加密系统，严重威胁到银行、网络和电子商务等的信息安全以及国家安全。因此，Shor算法的提出迅速引起了世界各国对量子计算研究的高度关注。
- 2008年，中国科技大学的潘建伟、杨涛和陆朝阳等，与英国牛津大学的研究人员合作，在国际上首次利用光量子计算机实现了Shor量子分解算法。

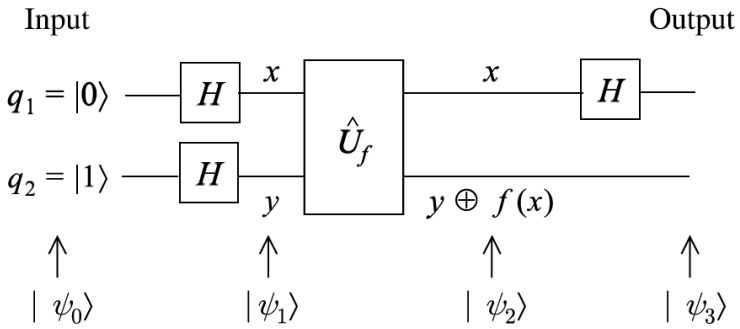
Deutsch算法(1)

	$f(0)$	$f(1)$	
f_1	0	0	Constant
f_2	1	0	Balanced
f_3	0	1	Balanced
f_4	1	1	Constant

- Deutsch算法是最早被提出的关于量子计算可以超越经典计算的算法。
- 假设我们有一个二进制函数$f(x)$。x的取值为0或者1，$f(x)$的结果也为0或者1。当$f(0)=f(1)$时，我们称$f(x)$是一个常函数（constant function）；当$f(0)\neq f(1)$时，我们称$f(x)$是一个对称函数（balanced function）。我们的任务是使用一个算法迅速判断$f(x)$是常函数还是对称函数。
- 完成这个任务，传统计算机需要两步，分别计算$f(0)$和$f(1)$，并做比较。而量子计算机只需要一步就可以完成。
- 处理该问题的量子算法称为Deutsch算法。当x的取值为一列二进制数时，处理问题的算法称为Deutsch-Jose算法

浙江大学

Deutsch算法(2)



Deutsch算法的量子回路如左图所示。量子回路的输入为$q_1 = |0\rangle$和$q_2 = |1\rangle$，即$|\psi_0\rangle = |01\rangle$。经过$H$门得到

$$x = H \cdot q_1 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$y = H \cdot q_2 = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

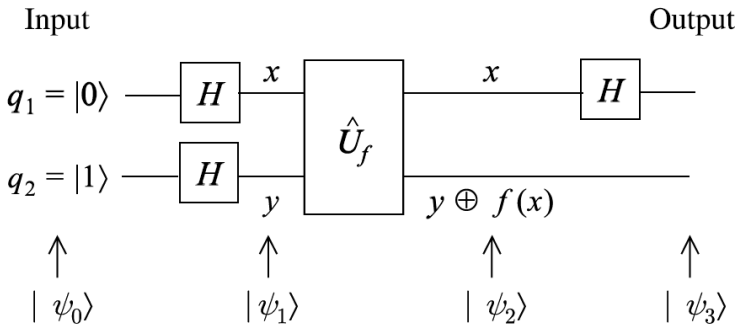
所以

$$|\psi_1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

对y进行异或$y \oplus f(x)$运算

$$|\psi_2\rangle = \frac{1}{2}(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle)$$

Deutsch算法(3)



- $q_1^{out} = 0$，$f(x)$是常函数
- $q_1^{out} = 1$，$f(x)$是对称函数

$$|\psi_2\rangle = \frac{1}{2}(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle)$$

- 如果$f(x)$是常函数$f(0) = f(1)$

$$|\psi_2\rangle^{constant} = \frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |1 \oplus f(0)\rangle)$$

$$|\psi_3\rangle^{constant} = \frac{1}{\sqrt{2}}|0\rangle(|f(0)\rangle - |1 \oplus f(0)\rangle)$$

- 如果$f(x)$是对称函数$f(0) \neq f(1)$，所以$f(0) = 1 \oplus f(1)$，$f(1) = 1 \oplus f(0)$

$$|\psi_2\rangle^{balanced} = \frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |1 \oplus f(0)\rangle)$$

$$|\psi_3\rangle^{constant} = \frac{1}{\sqrt{2}}|1\rangle(|f(0)\rangle - |1 \oplus f(0)\rangle)$$

Grover算法(1)


查询企业最新信息

光电器件 连接器 线路板 101

龙岗区(继续)

迈克光电子有限公司 2967 2490
优力大光电(深圳)有限公司 2805 6374
有为光电有限公司 2946 8736
灿嘉光电科技有限公司 2919 0062
陆百亿光电有限公司 2948 2458
国华光电科技有限公司 2941 5855
金星辉光电科技有限公司 2308 2983
金谷光电有限公司 2752 3299
鸣名光电技术有限公司 2946 2086
卓仪光电科技有限公司 2806 7178
卓明光电有限公司 8330 0011
美裕康光电照明有限公司 2376 1912
南星光电有限公司 2805 2133
威视特光电科技有限公司 8310 5909
星光宝光电科技有限公司 2904 3535
通鑫达光电有限公司 2811 3014
通达光电子有限公司 2760 2023
康盛光电科技有限公司 2798 0569

深圳市博川科技有限公司
深圳市宝安区观澜街道办樟坑及上围村金信达工业园1栋 2320 6558

深圳鑫的美光电有限公司
深圳市宝安区观澜街道办高尔夫大道国润工业区A栋3楼 2983 4023

奥佳光电(深圳)有限公司 2985 1789
晶弧达光电工程技术有限公司 2923 5798
联谊光电技术有限公司 8295 6511
联胜光电(深圳)有限公司 8527 6662
锐凌光电有限公司 2946 6316
斯伯锐光电有限公司 2310 3350
雅嘉美光电有限公司 2983 8602
紫源特光电科技有限公司 2803 2991
博辉光电有限公司 2310 2126
赛克斯康科技有限公司 8529 3393

连接器

福田区

振达电子有限公司 8395 7081
鸿兆科技有限公司 8279 4661
普仙电子(深圳)有限公司 8398 3425

南山区

嘉德信电子线材有限公司 2957 3887

宝安区

长江连接器有限公司 2995 9119
生兴连接器有限公司 2734 6880
合鑫连接器有限公司 2975 0677

光明新区

德益连接器有限公司 2945 9930
鑫明康精密电子有限公司 2996 5558

龙岗区

王氏欣科电源连接器加工厂 8409 2121
北鳌实业有限公司龙岗部 2834 6140
帝锋电子厂 2866 8999
信而昌电子有限公司 8407 8418

光明新区

合力兴科技有限公司 2349 4806
泰源科技(深圳)有限公司 2771 0581
通联技术有限公司 2909 0976
康力通连接器有限公司 2754 8916
嘉博兴电子科技有限公司 2715 7302

坪山新区

世耀精密工业(深圳)有限公司 8463 7402

龙华新区

正泰连接器有限公司 8179 7066

线路板

福田区

中盛大恒科技有限公司 8368 7270
向亿电路技术有限公司 8376 6058

南山区

昂鑫安贝电路科技(深圳)有限公司 2688 9378
爱析凯电子科技(深圳)有限公司 2682 4481
港粤线路板科技咨询(深圳)有限公司 8624 0033
魔诺科技有限公司 8615 7966
鑫茂隆电路有限公司 8629 3676

宝安区

广升科技有限公司 2370 0731
广德泰电路板有限公司 8173 7319
三基电科技有限公司 2308 6093
亿鑫达柔性电路有限公司 8259 8789
丰达兴线路板制造有限公司 2992 3200
中芯航科技有限公司 2790 6202
中兴新宇软电路有限公司 2768 2339
水捷镜台线路板(深圳)有限公司 2969 8971
邦基线路板厂 2723 4702
华讯达有限公司 2349 0831

昱永鑫精密电路有限公司 8821 5020
宏洋线路科技有限公司 8606 2567
宏大精密工业(深圳)有限公司 2768 5346
运丰电路板厂 2741 7101
宝昊电子科技有限公司 2759 5558
诚越电路有限公司 2935 8669
国电印刷电路板厂 2969 6919
凯升线路板有限公司 8529 6955
明哲诚实业有限公司宝安分部 2751 3111
协扬实业发展有限公司 2726 8991
欣迅达电路有限公司 2331 7334
视维兴电路有限公司 2335 7320
松微电子股份有限公司 2726 6956
恒宝士线路板有限公司 2730 0638
荣展电路技术有限公司 2960 6177
盈通恒翼科技有限公司 2643 7195
昱泰新电子科技(深圳)有限公司 2946 0029
贵达科技有限公司 2992 4238
溢达多层线路板有限公司 2606 8047
健创信电子有限公司 2778 5356
铭捷电路有限公司 2960 6060
深联电路有限公司 2738 8073
博宇线路板设备有限公司 2709 1611
辉煌线路板有限公司 2349 2543
联兴电路有限公司 2335 3837
联创电路有限公司 2349 1831
联路鑫电路板有限公司 2949 3876
骁艺电路有限公司 2724 4024
翔宇电路有限公司 2756 1863
新金典电路有限公司 2302 3441
精思维电路有限公司 2349 0993
德兴鸿科技(深圳)有限公司 2728 9028
鑫茂隆电路有限公司松岗分部 2349 0961

龙岗区

世纪科技(深圳)有限公司 8974 6631

光明新区

汉声光电有限公司 2916 8391
轩力电子厂 2962 5852
鑫宇通精密电路有限公司坪富裕工业园分部 2150 2566
雅亮科技(深圳)有限公司 2710 2625
嘉之宏电子有限公司 2716 5260

坪山新区

太平电路科技(深圳)有限公司 8409 9511
荣恩线路板(深圳)有限公司

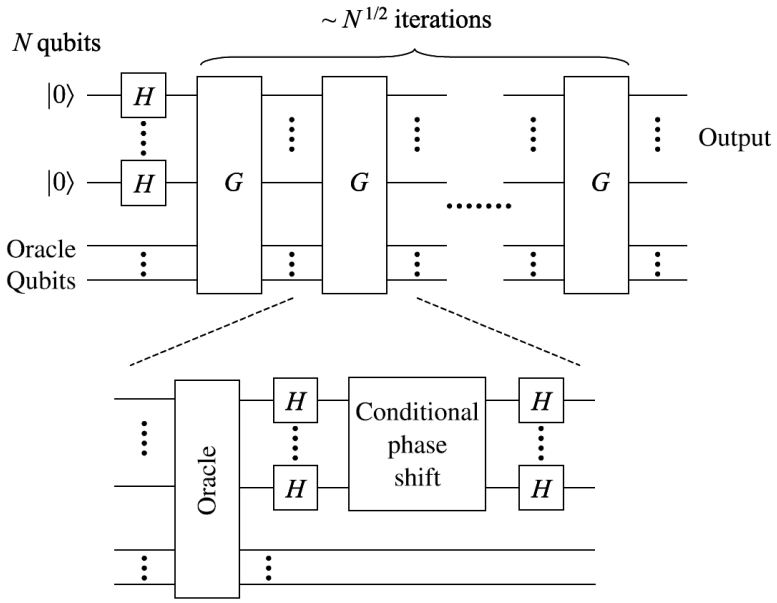
电子电工 电器 交通 汽车

电话黄页

- Grover算法是一种量子搜索算法，主要用于数据库检索。于1996年由计算机科学家 Lov Grover提出。
- 在处理从无序的D个数据中搜索出目标数这一问题时，它优于最好的经典算法，可做平方加速。也就是说，经典算法完成任务所需的时间正比于D，而量子算法则可在$\sqrt{D}$时间尺度内实现。如果D是一个非常大的数字，这将极大地节约时间。
- Grover算法的强大在于它的多功能性：它的公式是通用的，可适用于很多问题，比如：密码学、矩阵和图形问题、优化以及量子机器学习等。
- Grove算法的实现十分复杂，这里仅作简要介绍。

浙江大学 ZHEJIANG UNIVERSITY 1897

Grover算法(2)



- Grover算法的量子回路如左图所示。假设数据库中有N_{data}个条目，则算法需要调用N个量子比特的量子寄存器，使得$2^N \geq N_{data}$。简便起见，我们只考虑$2^N = N_{data}$的情况。

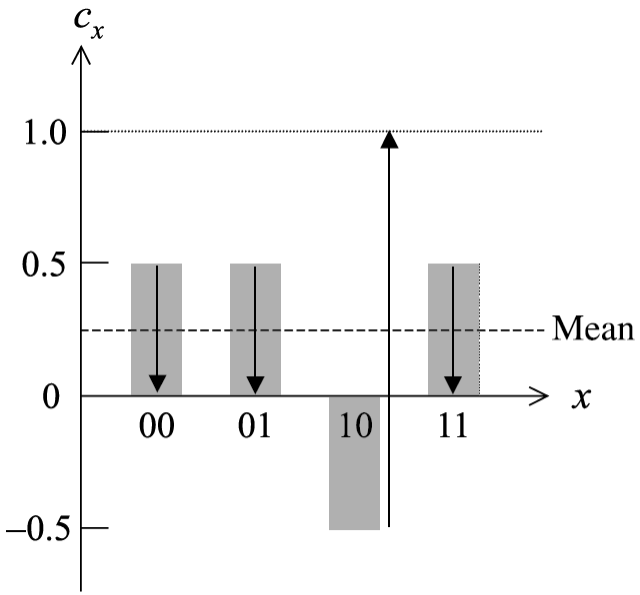
- 每一个量子比特起始都设为$|0\rangle$，然后经过一个H门

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2}}\right)^N (|0\rangle_1 + |1\rangle_1)(|0\rangle_2 + |1\rangle_2) \cdots\cdots (|0\rangle_N + |1\rangle_N)$$

$$= \frac{1}{\sqrt{N_{data}}} \sum_{x=0}^{N_{data}-1} |x\rangle$$

- 通过对$|\psi_1\rangle = (1,1,\ldots 1,\ldots 1)$的Grover操作直到它演化至某一个解的形式$|\psi_2\rangle = (0,0,\ldots 1,\ldots 0)$

Grover算法(3)



- 定义一个权威指令（oracle operation）

$$|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$$

当$|x\rangle$为解时，$f(x)=1$，否则$f(x)=0$。

- 以$N_{data}=4$为例，量子寄存器中储存$N=2$个量子比特

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2}}\right)^2 (|0\rangle_1 + |1\rangle_1)(|0\rangle_2 + |1\rangle_2)$$

$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$$

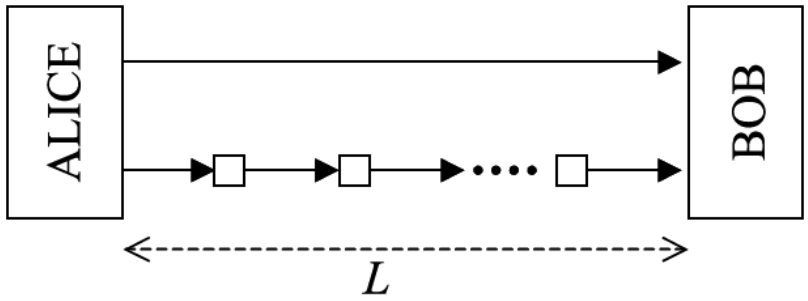
- 假设解为$|10\rangle$，使用权威指令后

$$|\psi\rangle = \left(\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2}\right)$$

- 通过计算出平均值$1/4$，通过Grover操作得到$|\psi_2\rangle = (0,0,1,0)$。

量子中继

- 量子计算的一个重要应用是提供量子通讯的中继设备。在传统通信系统中，中继设备主要是放大器，提供信号衰减后的放大。量子中继主要应用在量子密码学的量子信道中。
- 假设Alice和Bob之间量子信道的传输介质，一般是光纤，具有一定的损耗。那么Alice发出的光子送达到距离为L的Bob的几率为$\mathcal{P}(L) = e^{-L/L_0}$。如果Bob没有收到信号，那么他会要求Alice重复发出光子，重复率为e^{L/L_0}，以补偿信道内的损耗。
- 一种可替代的方案是在信道内设置N次传输，每段的长度为L/N，在每段传输中止处设置量子中继器。在量子信道内，无量子中继的衰减为e^{-L/NL_0}，所以每段的中继需求为e^{L/NL_0}。对于N次传输，中继需求为Ne^{L/NL_0}。假设$N = L/L_0$，中继次数为$\mathrm{e}L/L_0$。当$\mathrm{e}L/L_0 < e^{L/L_0}$时，量子中继变得有优势，即$L > L_0$。在光纤量子通讯系统中，对应大约几十公里的距离。



量子计算

退相干与纠错

- 量子计算面临的一个重大挑战是量子退相干过程。一切量子系统都不可避免地和环境耦合，因此变得脆弱和容易失效。
- 环境是大量原子和分子组成的系统，它们的个体遵从量子法则，集体遵从经典法则。量子体系和环境相互作用的过程一般称为退相干过程。如果量子体系的退相干时间记作T_2，量子门的操作时间记作T_{op}，量级计算系统可以容纳的操作数为$N_{op} = T_2/T_{op}$。
- 在量子计算过程中，需要设计检错和纠错的机制，补偿退相干过程造成的损失。具有纠错机制的量子计算称为容错量子计算。

System	T_2 (s)	T_{op} (s)	N_{op}
Nuclear spin	10^4	10^{-3}	10^7
Ion trap	10^0	10^{-6} (e)	10^6
Exciton (quantum dot)	10^{-9} (e)	10^{-12} (e)	10^3
Electron spin (quantum dot)	10^{-7}	10^{-12}	10^5
Superconducting flux qubit	10^{-8} (e)	10^{-10} (e)	10^2 (e)

浙江大学

参考文献

- 量子算法和应用主要参考：
  - Mark Fox, Quntum Optics – An Introduction, Oxford University Press (2006). 第13.5-13.6小节。