

量子计算的原理、发展、实现

胡喜平 李廷龙

2019 年 10 月 7 日

1 引言

量子计算 (Quantum computing) 最早于 1969 年提出, 是指使用量子逻辑进行通用计算。与传统计算机不同, 量子计算使用量子比特 (quantum qubit) 进行数据的存储与操作, 使用量子算法进行数据操作。1982 年, 理查德·费曼在演讲中提出利用量子体系进行通用计算的想法, 但是当时对于量子计算如何实现依旧无人得知。量子计算机与传统计算机相比在一些特定的问题求解方面有独特的优势。例如, 在使用计算机模拟量子现象时, 使用传统计算机模拟计算时, 庞大的希尔伯特空间导致运算时间相当长, 使用量子体系计算机能大大缩短计算时间。在质因数分解时, 量子计算机的计算速度远高于传统计算机。这主要是因为量子计算机独特的构造。量子比特可以同时表示多种状态, 而传统计算机里半导体只能记录 0 和 1 两种状态。同时, 量子计算机对破解 RSA 加密算法等密码学领域有重大的意义, 因此变成了热门的话题。

2 量子计算的基本原理

2.1 量子比特模型的建立

传统的半导体计算机中比特只有两种状态, 即 0 和 1. 量子比特不同与半导体比特的特殊之处在于量子比特时刻处于 0 和 1 的叠加态中。关于 0 和 1 的定义可以有多种方式, 例如我们可以定义电子自旋向上为 1, 那么电子自旋向下就是 0. 因为叠加态的缘故, 量子比特的数值可以在 0 和 1 之间任意取值。即

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

其中 α 和 β 是复数, 且它们的模长平方和是 1, 量子比特在 0 状态和 1 状态的概率分别为 $|\alpha|^2$ 和 $|\beta|^2$ 为了方便, 我们用一个单位向量表示量子比特的状态

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad (2)$$

则逻辑运算时的 NOT 门表示为

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (3)$$

因为

$$X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \quad (4)$$

即量子比特状态向量左乘 X 后反转. 另一个量子计算时使用的逻辑门称为 Hadamard 门, 它可以根据系数分解量子态, 定义为:

$$H(\alpha|0\rangle + \beta|1\rangle) = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle \quad (5)$$

用矩阵来表示为

$$H = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (6)$$

同 NOT 门一样, 连续使用两次 Hadamard 门后量子回到原先的状态。

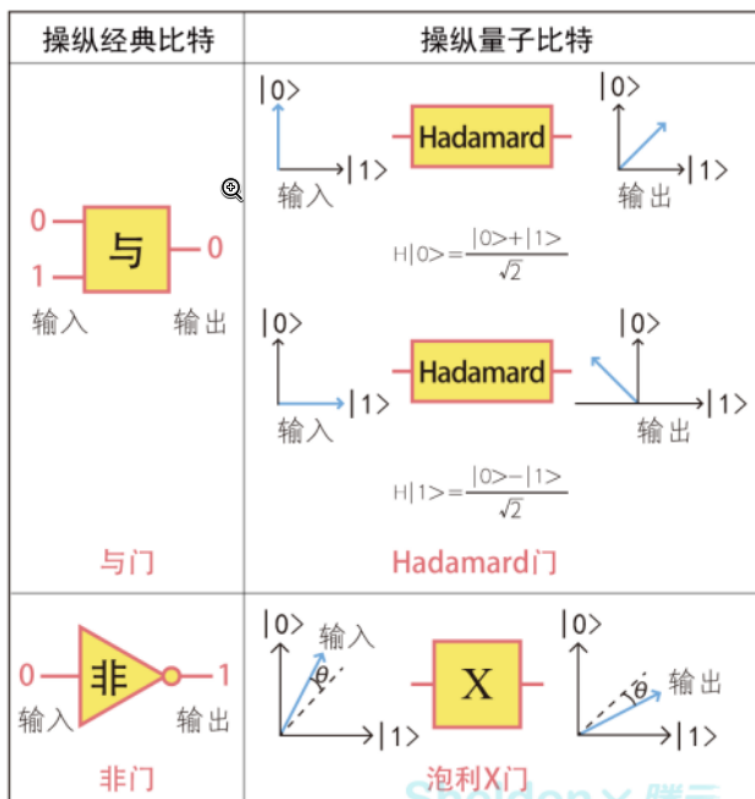


图 1: 操控一个量子比特的逻辑门

以上都是对于一个量子比特的逻辑门, 对于用来条件判断的两个量子的逻辑门, 在量子计算中由多输入多输出的受控 NOT 门实现。当第一个输入的量子比特是 0 时, 对保持第二个输入比特不变。当第一个输入的量子比特是 1 时, 则以 NOT 门作用于第二个比特。即:

$$CNOT(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \theta|11\rangle) = \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \theta|10\rangle \quad (7)$$

2.2 运用量子比特进行量子计算的原理

经典计算机的计算大致分为三个过程, 即输入数据, 使用若干量子门对数据进行逻辑运算, 输出数据。量子计算和经典计算机计算过程大致相同, 输入量子比特, 用量子门对量子比特进行操作, 观测操作后的量子比特获取结果。主要的不同就是量子有叠加态, 即一个量子比特可以表示 0, 同时也可以表示 1, 而在经典计算机中一个比特只能同时表示 0 或 1 中的一种情况。量子的叠加态在最后观察时才会坍塌到一种 0 或 1 的确定状态。因为量子的叠加特性, 量子计算可以并行。两个量子比特可以一次进行 4

次运算， n 个量子比特可以一次进行 2^n 次并行运算，而经典计算机一次只能进行一次计算。但是，由于量子比特本身及其不稳定，极容易和周围环境发成纠缠，微小的环境噪声都能对量子比特产生影响，导致计算错误。而且量子比特的数量越多，计算的错误率也就随之升高。在实际应用中需要一些手段来进行纠错。

2.3 量子计算的物理实现方法

以 D-wave 量子计算机为例，它主要是用约瑟夫森效应 (Josephson effect) 来构造量子比特进行计算。约瑟夫森效应是宏观量子效应的一种体现，当把两个超导体置于绝缘体的两侧时，由于量子隧穿效应，会产生一种超电流流过绝缘体，这种电流的产生不需要电压。中间的绝缘体称作约瑟夫森结。

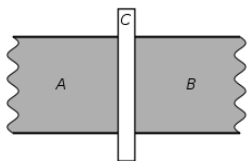


图 2: 约瑟夫森结



图 3: 约瑟夫森结的电路符号

约瑟夫森结中的超电流可能是正向，也可能是反向，且概率相等。因此可以作为量子比特来存储数据。



图 4: D-wave 一个量子比特组成

D-wave 量子计算机的一个量子比特由一个环组成，在这个环里电流可能顺时针流，可能逆时针流。同时，可以通过施加垂直于线框的磁场来改变里面的电流，达成对量子比特的控制。

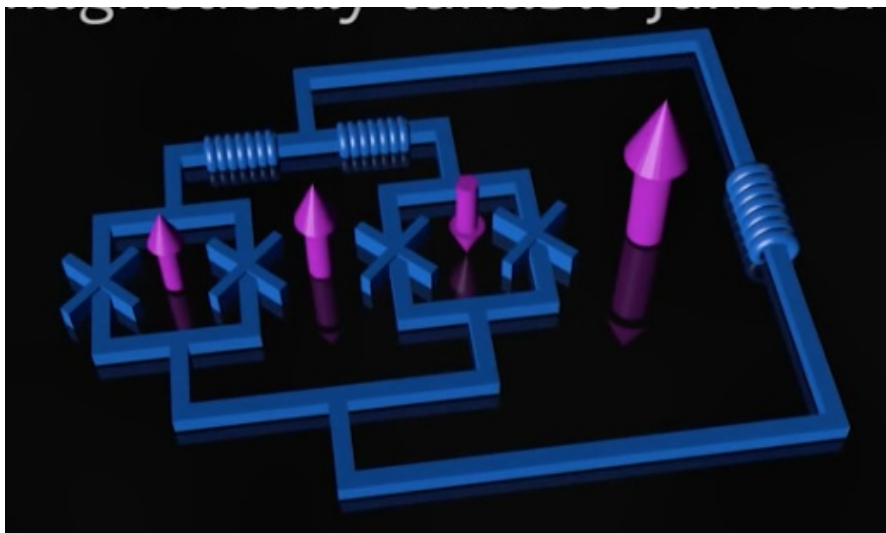


图 5: 最终量子比特设计

当然，这只是初级的设计。为了更精准地对量子比特进行控制，后续加入了势井和更多的磁场。除了使用超导约瑟夫森结实现量子运算的方案以外，还有应用离子阱、中性原子的能级、光的偏振等实现量子比特的方案，各中实现方案各有优劣。

参考文献

- [1] 量子计算的物理实现, 薛飞, 杜江峰, 周先意, 韩荣典, (中国科学技术大学近代物理系合肥)
- [2] Josephson effect, https://en.wikipedia.org/wiki/Josephson_effect
- [3] D-Wave Systems, https://en.wikipedia.org/wiki/D-Wave_Systems
- [4] 量子计算机的工作原理如何解释, <https://www.zhihu.com/question/30545465>
- [5] 10 分钟看懂量子比特、量子计算和量子算法 <https://zhuanlan.zhihu.com/p/27387032>
- [6] Quantum computation using quantum dots, Xin Wang, City University of Hong Kong