

量子计算与算法(简介)

March 23, 2016

lol

简单粗暴地讲一下这方面内容,其实挺简单的

简单粗暴地讲一下这方面内容,其实挺简单的
将用一些不是很科学但是易懂的语言讲述

简单粗暴地讲一下这方面内容,其实挺简单的

将用一些不是很科学但是易懂的语言讲述

本人比较SB,所以吐槽时手下留情

内容

内容

基本定义

内容

基本定义

量子门

内容

基本定义

量子门

量子测量

内容

基本定义

量子门

量子测量

基本量子算法

量子位

一个量子位是一个二维复向量,表示0和1状态的叠加

量子位

一个量子位是一个二维复向量,表示0和1状态的叠加

考虑一个黑盒子里面的硬币...

量子位

一个量子位是一个二维复向量,表示0和1状态的叠加

考虑一个黑盒子里面的硬币...

可以通过相位将 $|0\rangle$ 的分量变成实数

Bloch球

为了方便理解后面的内容,可以考虑一个球,其中 $y = -1$ 表示 $|1\rangle$, $y = 1$ 表示 $|0\rangle$,绕 y 轴转相当于 $|1\rangle$ 的分量在复平面的单位圆上面转

量子位对

两个量子位组成一对就是量子位对 :)

量子位对

两个量子位组成一对就是量子位对 :)

可以表示成 $|00\rangle$, $|01\rangle$, $|10\rangle$ 和 $|11\rangle$ 的线性组合

量子位对

两个量子位组成一对就是量子位对 :)

可以表示成 $|00\rangle, |01\rangle, |10\rangle$ 和 $|11\rangle$ 的线性组合

当然把这个东西表示成四维复空间中的一个点时,这个点在单位球上

量子位对

两个量子位组成一对就是量子位对 :)

可以表示成 $|00\rangle, |01\rangle, |10\rangle$ 和 $|11\rangle$ 的线性组合

当然把这个东西表示成四维复空间中的一个点时,这个点在单位球上

可以以此类推得到多个量子位复合的情况

量子位对

例
子: $(\frac{3}{5} |0\rangle + \frac{4}{5} |1\rangle) \otimes (\frac{4}{5} |0\rangle + \frac{3}{5} |1\rangle) = (\frac{12}{25} |00\rangle + \frac{9}{25} |01\rangle + \frac{16}{25} |10\rangle + \frac{12}{25} |11\rangle)$

量子位对

例

$$\text{子:} (\frac{3}{5} |0\rangle + \frac{4}{5} |1\rangle) \otimes (\frac{4}{5} |0\rangle + \frac{3}{5} |1\rangle) = (\frac{12}{25} |00\rangle + \frac{9}{25} |01\rangle + \frac{16}{25} |10\rangle + \frac{12}{25} |11\rangle)$$

可以将多个量子位用一个高维复向量表示(多个二维向量的张量积),这样在有多个输入的情况下比较方便

量子位对

可以通过某些手段将多个量子纠缠在一起

量子位对

可以通过某些手段将多个量子纠缠在一起

比如 $\frac{2}{3} |00\rangle + \frac{2}{3} |01\rangle + \frac{1}{3} |10\rangle$

量子位对

可以通过某些手段将多个量子纠缠在一起

比如 $\frac{2}{3} |00\rangle + \frac{2}{3} |01\rangle + \frac{1}{3} |10\rangle$

不能表示成独立的两个量子的张量积 :/

量子位对

可以通过某些手段将多个量子纠缠在一起

比如 $\frac{2}{3} |00\rangle + \frac{2}{3} |01\rangle + \frac{1}{3} |10\rangle$

不能表示成独立的两个量子的张量积 :/

后面还会提到纠缠相关的内容

单位门

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

没什么好说的.

轴转门

为了方便大家望文生意这里用通俗易懂的名字称呼这些门 :)

轴转门

为了方便大家望文生意这里用通俗易懂的名字称呼这些门 :)

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

轴转门

为了方便大家望文生意这里用通俗易懂的名字称呼这些门 :)

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

轴转门

为了方便大家望文生意这里用通俗易懂的名字称呼这些门 :)

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

轴转门

相当于在Bloch球上面绕着对应的轴转

轴转门

相当于在Bloch球上面绕着对应的轴转

特别的, σ_x 就是传统意义上的 NOT 门

叠加门

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

叠加门

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

为了更好地理解这东西,引入 $|+\rangle$ 和 $|-\rangle$

叠加门

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

为了更好理解这东西,引入 $|+\rangle$ 和 $|-\rangle$

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

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

叠加门

可以通过简单的观察发现 H 相当于把 $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ 变成 $|q\rangle = \alpha|+\rangle + \beta|-\rangle$

叠加门

可以通过简单的观察发现 H 相当于把 $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ 变成 $|q\rangle = \alpha|+\rangle + \beta|-\rangle$
注意 $|+\rangle$ 和 $|-\rangle$ 是一组新的基...

相位门

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

相位门

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

给量子一个 $|1\rangle$ 上的相位.

旋转门

上面的这些门实际上都是在Bloch球上面旋转,只是上面提到的有特殊性

旋转门

上面的这些门实际上都是在Bloch球上面旋转,只是上面提到的有特殊性

其实量子位本身的性质就决定了这些门都是在Bloch球上旋转.这类旋转变换可以用 $U(\text{Unitary})$ 来表示

旋转门

上面的这些门实际上都是在Bloch球上面旋转,只是上面提到的有特殊性

其实量子位本身的性质就决定了这些门都是在Bloch球上旋转.这类旋转变换可以用 U (Unitary)来表示

有个性质: $U\bar{U}^T = I$,其中 \bar{M} 表示将矩阵 M 的元素全部进行共轭

控制非门

现在开始讨论基本的多量子门,将请大家写出它们的矩阵形式加强理解 :)

控制非门

现在开始讨论基本的多量子门,将请大家写出它们的矩阵形式加强理解 :)

控制非门的作用是读入两个量子(其中一个是控制量子位),如果控制量子位是 $|1\rangle$ 则将目标量子位进行一次 NOT 变换.最后控制量子位不变.

控制非门

现在开始讨论基本的多量子门,将请大家写出它们的矩阵形式加强理解 :)

控制非门的作用是读入两个量子(其中一个控制量子位),如果控制量子位是 $|1\rangle$ 则将目标量子位进行一次 NOT 变换.最后控制量子位不变.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \text{第一位是控制量子位.}$$

交换门

交换门的作用是交换两个量子位.

交换门

交换门的作用是交换两个量子位.

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

交换门

交换门的作用是交换两个量子位.

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

注意到这东西其实可以用三个 *CNOT* 门来实现...

控制旋转门

作用类似控制非门...只是将非门中的 NOT 变换变成前面提到的任意的 U 变换.

控制旋转门

作用类似控制非门...只是将非门中的 NOT 变换变成前面提到的任意的 U 变换.

仔细观察前面的 $CNOT$ 门的矩阵表示就可以写出这个门的矩阵表示了.

控制旋转门

作用类似控制非门...只是将非门中的 NOT 变换变成前面提到的任意的 U 变换.

仔细观察前面的 $CNOT$ 门的矩阵表示就可以写出这个门的矩阵表示了.

$$CU = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

控制旋转门

作用类似控制非门...只是将非门中的 NOT 变换变成前面提到的任意的 U 变换.

仔细观察前面的 $CNOT$ 门的矩阵表示就可以写出这个门的矩阵表示了.

$$CU = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

实际上是一个 4×4 矩阵...采用以上写法进行简化 :)

控制交换门

这里直接先给出矩阵表示:

控制交换门

这里直接先给出矩阵表示:

$$CSWAP = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

控制交换门

这里直接先给出矩阵表示:

$$CSWAP = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

作用是如果控制量子位为 $|1\rangle$ 时交换第二和第三个量子位.

控制交换门

这里直接先给出矩阵表示:

$$CSWAP = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

作用是如果控制量子位为 $|1\rangle$ 时交换第二和第三个量子位.

为什么是 8×8 矩阵呢?因为三个量子位的张量积是一个八维复向量(以 $|000\rangle, |001\rangle, |010\rangle, \dots, |111\rangle$ 为基).

双重控制旋转门

作用是如果第一个和第二个量子位均为 $|1\rangle$ 时对第三个量子位进行一次 U 的变换.

双重控制旋转门

作用是如果第一个和第二个量子位均为 $|1\rangle$ 时对第三个量子位进行一次 U 的变换.

$$CCU = \begin{pmatrix} I_6 & 0 \\ 0 & U \end{pmatrix} (I_6 \text{指的是} 6 \times 6 \text{的单位矩阵}).$$

双重控制旋转门

作用是如果第一个和第二个量子位均为 $|1\rangle$ 时对第三个量子位进行一次 U 的变换.

$$CCU = \begin{pmatrix} I_6 & 0 \\ 0 & U \end{pmatrix} (I_6 \text{指的是} 6 \times 6 \text{的单位矩阵}).$$

如同控制旋转门的情况一样,双重控制非门($CCNOT$ 或 $TOFOLLI$ 门)有其特殊的意义,所以需要在这里提一提.

$$H^{\otimes n}$$

这种神奇的门是 H 门自张量乘若干次以后的结果, 矩阵形式同标题上.

$$H^{\otimes n}$$

这种神奇的门是 H 门自张量乘若干次以后的结果, 矩阵形式同标题上.

因为在某些算法中有用到, 所以也需要提一提.

有了以上几种量子门,就可以运用经典信息论当中的电路来设计量子电路了,非常简单.

有了以上几种量子门,就可以运用经典信息论当中的电路来设计量子电路了,非常简单.

然而,这样做并不能充分利用量子位是叠加态这一特性进行计算.

有了以上几种量子门,就可以运用经典信息论当中的电路来设计量子电路了,非常简单.

然而,这样做并不能充分利用量子位是叠加态这一特性进行计算.

为了更好的进行计算,需要对量子进行测量以及使用专门的量子算法来优化量子电路.

Bra-ket

讲一些前置知识...

Bra-ket

讲一些前置知识...

这篇课件一直在用Dirac记号($|\rangle$).实际上这个记号还有左半边 $\langle|$.

Bra-ket

讲一些前置知识...

这篇课件一直在用Dirac记号($|\rangle$).实际上这个记号还有左半边 $\langle|$.

$$\langle x| = |\bar{x}\rangle^T$$

Bra-ket

讲一些前置知识...

这篇课件一直在用Dirac记号($|\rangle$).实际上这个记号还有左半边($\langle|$).

$$\langle x| = |\bar{x}\rangle^T$$

用这套记号的好处就是向量的点积表示起来非常简单: $\langle q|q'\rangle$

Bra-ket

讲一些前置知识...

这篇课件一直在用Dirac记号($|\rangle$).实际上这个记号还有左半边($\langle|$).

$$\langle x| = |\bar{x}\rangle^T$$

用这套记号的好处就是向量的点积表示起来非常简单: $\langle q|q'\rangle$

假设 $|x\rangle$ 是一个单位向量,那么将一个任意向量投影到这个单位向量上的算子是 $|x\rangle \langle x|$ (可以去验证一下).

特征向量,特征值和谱分解

相信大家都只到特征值和特征向量是什么.这里就不多说了.

特征向量,特征值和谱分解

相信大家都只到特征值和特征向量是什么.这里就不多说了.

如果一个算子是自伴随(后面会提到什么是自伴随)的,那么它的特征向量组成正交单位基(即其特征向量两两点积均为0而且都是单位向量).

特征向量,特征值和谱分解

相信大家都只到特征值和特征向量是什么.这里就不多说了.

如果一个算子是自伴随(后面会提到什么是自伴随)的,那么它的特征向量组成正交单位基(即其特征向量两两点积均为0而且都是单位向量).

因为这是一组基,所以可以理所当然地把这个矩阵在这组基上面进行表示.这种表示方法叫做谱分解(有些地方亦称作对角化).

量子测量

使用一组算子 $\{M_m\} (1 \leq m \leq n(P * p))$ 进行测量. 这组算子必须满足 $M_m = \bar{M}_m^T$ 以及 $\sum_{m=1}^n M_m = I$.

量子测量

使用一组算子 $\{M_m\} (1 \leq m \leq n(P * p))$ 进行测量. 这组算子必须满足 $M_m = \bar{M}_m^T$ 以及 $\sum_{m=1}^n M_m = I$.

一种非常平凡的构造方法是乱取几个满足第一个条件的算子, 然后最后一个等于 I 减去前面所有的算子 =.=

量子测量

使用一组算子 $\{M_m\} (1 \leq m \leq n(P * p))$ 进行测量. 这组算子必须满足 $M_m = \bar{M}_m^T$ 以及 $\sum_{m=1}^n M_m = I$.

一种非常平凡的构造方法是乱取几个满足第一个条件的算子, 然后最后一个等于 I 减去前面所有的算子 $=.$

一个量子态 (进行测量的所有量子) 通过一个测量会得到成功或者不成功的结果. 成功的概率是 $p_m(x) = \langle x | M_m | x \rangle$.

量子测量

使用一组算子 $\{M_m\} (1 \leq m \leq n(P * p))$ 进行测量. 这组算子必须满足 $M_m = \bar{M}_m^T$ 以及 $\sum_{m=1}^n M_m = I$.

一种非常平凡的构造方法是乱取几个满足第一个条件的算子, 然后最后一个等于 I 减去前面所有的算子 $=.$

一个量子态(进行测量的所有量子)通过一个测量会得到成功或者不成功的结果. 成功的概率是 $p_m(x) = \langle x | M_m | x \rangle$.

如果成功测量, 这个量子态就会坍缩到 $\frac{1}{\sqrt{p_m(x)}} M_m | x \rangle$. 否则坍缩到 $\frac{1}{\sqrt{1-p_m(x)}} (|x\rangle - M_m | x \rangle)$

量子测量

使用一组算子 $\{M_m\} (1 \leq m \leq n(P * p))$ 进行测量. 这组算子必须满足 $M_m = \bar{M}_m^T$ 以及 $\sum_{m=1}^n M_m = I$.

一种非常平凡的构造方法是乱取几个满足第一个条件的算子, 然后最后一个等于 I 减去前面所有的算子 $=.$

一个量子态 (进行测量的所有量子) 通过一个测量会得到成功或者不成功的结果. 成功的概率是 $p_m(x) = \langle x | M_m | x \rangle$.

如果成功测量, 这个量子态就会坍缩到 $\frac{1}{\sqrt{p_m(x)}} M_m | x \rangle$. 否则坍缩到 $\frac{1}{\sqrt{1-p_m(x)}} (|x\rangle - M_m | x \rangle)$

下面介绍三种常用的而且物理上能实现 (此处不讨论具体物理实现) 构造方式.

在纯态基上的投影

测量一个量子态的时候可以选择其纯态基上的投影.

在纯态基上的投影

测量一个量子态的时候可以选择其纯态基上的投影.

例子:测量 $\frac{2}{3} |00\rangle + \frac{2}{3} |01\rangle + \frac{1}{3} |10\rangle$ 时选择 $\{|00\rangle \langle 00|, |01\rangle \langle 01|, |10\rangle \langle 10|, |11\rangle \langle 11|\}$.

在纯态基上的投影

测量一个量子态的时候可以选择其纯态基上的投影.

例子:测量 $\frac{2}{3} |00\rangle + \frac{2}{3} |01\rangle + \frac{1}{3} |10\rangle$ 时选择 $\{|00\rangle\langle 00|, |01\rangle\langle 01|, |10\rangle\langle 10|, |11\rangle\langle 11|\}$.

因为是一组基,所以满足作为一组观测算子条件.

在纯态基上的投影

测量一个量子态的时候可以选择其纯态基上的投影.

例子:测量 $\frac{2}{3} |00\rangle + \frac{2}{3} |01\rangle + \frac{1}{3} |10\rangle$ 时选择 $\{|00\rangle\langle 00|, |01\rangle\langle 01|, |10\rangle\langle 10|, |11\rangle\langle 11|\}$.

因为是一组基,所以满足作为一组观测算子条件.

在以上例子中,用 $|00\rangle\langle 00|$ 和 $|01\rangle\langle 01|$ 观测成功的概率是 $\frac{4}{9}$, 用 $|10\rangle\langle 10|$ 观测成功的概率是 $\frac{1}{9}$.

在自伴随算子的特征空间的基上的投影

标题很长...自伴随算子就是转置并且对矩阵中元素求共轭以后和自己相同的算子(令 $A^+ = \bar{A}^T$,则自伴随可表示成 $A = A^+$).

在自伴随算子的特征空间的基上的投影

标题很长...自伴随算子就是转置并且对矩阵中元素求共轭以后和自己相同的算子(令 $A^+ = \bar{A}^T$,则自伴随可表示成 $A = A^+$).

自伴随算子的特征值都是实数!所以自伴随算子可能会与某些物理量有关联 :)

在自伴随算子的特征空间的基上的投影

标题很长...自伴随算子就是转置并且对矩阵中元素求共轭以后和自己相同的算子(令 $A^+ = \bar{A}^T$,则自伴随可表示成 $A = A^+$).

自伴随算子的特征值都是实数!所以自伴随算子可能会与某些物理量有关联 :)

前面提到了这种算子的特征向量组成一组正交单位基.所以说可以用类似上一页的方法进行测量.

在自伴随算子的特征空间的基上的投影

标题很长...自伴随算子就是转置并且对矩阵中元素求共轭以后和自己相同的算子(令 $A^+ = \bar{A}^T$,则自伴随可表示成 $A = A^+$).

自伴随算子的特征值都是实数!所以自伴随算子可能会与某些物理量有关联 :)

前面提到了这种算子的特征向量组成一组正交单位基.所以说可以用类似上一页的方法进行测量.

其实这里还可以推出"测不准"原理,有兴趣可以去查阅相关资料.

对于张量空间的测量

量子态实际上是一个向量,那么就可以选取其中一维中的纯态进行测量.

对于张量空间的测量

量子态实际上是一个向量,那么就可以选取其中一维中的纯态进行测量.
结果是这一位坍缩成对应于所用算子的状态.

对于张量空间的测量

量子态实际上是一个向量,那么就可以选取其中一维中的纯态进行测量.

结果是这一位坍缩成对应于所用算子的状态.

例子:测量 $\frac{2}{3} |00\rangle + \frac{2}{3} |01\rangle + \frac{1}{3} |10\rangle$ 时选择第一个量子位的 $|0\rangle \langle 0|$ 进行测量,测量成功概率是 $\frac{8}{9}$,成功时该量子态坍缩成 $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$.

量子测量的简单应用

很多量子算法的结果都是需要进行测量的,否则即使输出了量子也是没有实际用途的(除非可以作为其他算法的输入).

量子测量的简单应用

很多量子算法的结果都是需要进行测量的,否则即使输出了量子也是没有实际用途的(除非可以作为其他算法的输入).

量子测量门如同前面所讲的门一样,是有专门的记号的...

量子测量的简单应用

很多量子算法的结果都是需要进行测量的,否则即使输出了量子也是没有实际用途的(除非可以作为其他算法的输入).

量子测量门如同前面所讲的门一样,是有专门的记号的...

下面讲一些简单应用.

制备纯态

只需要对一大堆量子进行对应的测量,发现成功即制备完毕.

制备纯态

只需要对一大堆量子进行对应的测量,发现成功即制备完毕.

这正好说明了量子测量还可以用于将量子态进行坍缩来达到一些目的.

EPR-Bell量子态

有四种非常神奇的纠缠量子对状态:

EPR-Bell量子态

有四种非常神奇的纠缠量子对状态:

$$\begin{cases} |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{cases}$$

EPR-Bell量子态

有四种非常神奇的纠缠量子对状态:

$$\begin{cases} |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{cases}$$

因为它们无法被表示成两个独立量子位张量积,所以是纠缠态.以上这些纠缠态叫做EPR-Bell态.

EPR-Bell量子态

有四种非常神奇的纠缠量子对状态:

$$\begin{cases} |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{cases}$$

因为它们无法被表示成两个独立量子位张量积,所以是纠缠态.以上这些纠缠态叫做EPR-Bell态.

接下来讲的高压缩编码和量子传送就是在EPR-Bell量子态上进行操作的.

制备EPR-Bell量子位对

以制备 $|\beta_{00}\rangle$ 为例:

制备EPR-Bell量子位对

以制备 $|\beta_{00}\rangle$ 为例:

读入纯态 $|00\rangle$,将第一个量子位进行一次 H ,然后执行一次 $CNOT$ 即可.

制备EPR-Bell量子位对

以制备 $|\beta_{00}\rangle$ 为例:

读入纯态 $|00\rangle$,将第一个量子位进行一次 H ,然后执行一次 $CNOT$ 即可.

若要制备其他的EPR-Bell态,则可将 $|\beta_{00}\rangle$ 的第一位进行一次 $X(|\beta_{01}\rangle)$, $Z(|\beta_{10}\rangle)$, $iY(|\beta_{11}\rangle)$ 变换.

测量EPR-Bell量子态

首先说明一下用纯态基上投影算子测量纯态量子位时可以确定性地知道是 $|0\rangle$ 或 $|1\rangle$. 比如说用 $|0\rangle\langle 0|$ 进行测量, 如果成功说明待测量子就是 $|0\rangle$, 失败则说明待测量子是 $|1\rangle$.

那么如何用纯态基上投影算子确定性地测量EPR-Bell量子态呢?

测量EPR-Bell量子态

首先说明一下用纯态基上投影算子测量纯态量子位时可以确定性地知道是 $|0\rangle$ 或 $|1\rangle$. 比如说用 $|0\rangle\langle 0|$ 进行测量, 如果成功说明待测量子就是 $|0\rangle$, 失败则说明待测量子是 $|1\rangle$.

那么如何用纯态基上投影算子确定性地测量EPR-Bell量子态呢?

想法是转化成非纠缠态并单独测量.

测量EPR-Bell量子态

首先说明一下用纯态基上投影算子测量纯态量子位时可以确定性地知道是 $|0\rangle$ 或 $|1\rangle$. 比如说用 $|0\rangle\langle 0|$ 进行测量, 如果成功说明待测量子就是 $|0\rangle$, 失败则说明待测量子是 $|1\rangle$.

那么如何用纯态基上投影算子确定性地测量EPR-Bell量子态呢?

想法是转化成非纠缠态并单独测量.

利用一个 *CNOT* 门和第一个量子位上的 *H* 门就可以变成两个独立的纯态量子了. 分别测量即可.

高压压缩编码

现在小明有一对01信息.他可以通过给小鸣一个量子位来告诉他这个信息.

高压压缩编码

现在小明有一对01信息.他可以通过给小鸣一个量子位来告诉他这个信息.

实现方法:两个人事先先共享一对 $|\beta_{00}\rangle$.在传输时,小明可以用前面的方法将 $|\beta_{00}\rangle$ 通过 I, X, Z, iY 变成与那对01信息相对应的状态.然后小鸣只需要使用上一页测量EPR-Bell量子态的方法进行测量就可以提取信息了.

高压缩编码

现在小明有一对01信息.他可以通过给小鸣一个量子位来告诉他这个信息.

实现方法:两个人事先先共享一对 $|\beta_{00}\rangle$.在传输时,小明可以用前面的方法将 $|\beta_{00}\rangle$ 通过 I, X, Z, iY 变成与那对01信息相对应的状态.然后小鸣只需要使用上一页测量EPR-Bell量子态的方法进行测量就可以提取信息了.

可以扩展到用 n 个量子位传送 2^n 个01位.

量子传送

现在小明有一个量子.他可以通过给小鸣一对01信息来传送这个量子(虽然小明的那个量子的信息会被破坏)

量子传送

现在小明有一个量子.他可以通过给小鸣一对01信息来传送这个量子(虽然小明的那个量子的信息会被破坏)

注意到这实际上是高压缩编码的逆过程 :)

量子传送

现在小明有一个量子.他可以通过给小鸣一对01信息来传送这个量子(虽然小明的那个量子的信息会被破坏)

注意到这实际上是高压压缩编码的逆过程 :)

实现方法: 见图...

量子传送原理

计算一下.

量子传送原理

计算一下.

最初系统状态是 $|q\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle)$

量子传送原理

计算一下.

最初系统状态是 $|q\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle)$

经过一次 $CNOT$ 以后变成 $\frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle)$.

量子传送原理

计算一下.

最初系统状态是 $|q\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle)$

经过一次 $CNOT$ 以后变成 $\frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle)$.

经过 H 以后变成 $\frac{1}{2}(\alpha|000\rangle + \alpha|100\rangle + \beta|010\rangle - \beta|110\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|001\rangle - \beta|101\rangle)$.

量子传送原理

计算一下.

最初系统状态是 $|q\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle)$

经过一次 $CNOT$ 以后变成 $\frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle)$.

经过 H 以后变成 $\frac{1}{2}(\alpha|000\rangle + \alpha|100\rangle + \beta|010\rangle - \beta|110\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|001\rangle - \beta|101\rangle)$.

整理以后变成 $\frac{1}{2}(|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) + |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle))$

量子传送原理

然后小明分别对第一和第二个量子位进行观测,并将结果(一对01信息)发给小鸣.

量子传送原理

然后小明分别对第一和第二个量子位进行观测,并将结果(一对01信息)发给小鸣.

小鸣根据信息进行变换:

00: 状态坍缩成 $|00\rangle \otimes (\alpha |0\rangle + \beta |1\rangle)$,做一次 I 变换.

01: 状态坍缩成 $|01\rangle \otimes (\alpha |1\rangle + \beta |0\rangle)$,做一次 X 变换.

10: 状态坍缩成 $|10\rangle \otimes (\alpha |1\rangle - \beta |0\rangle)$,做一次 Z 变换.

11: 状态坍缩成 $|11\rangle \otimes (\alpha |0\rangle - \beta |1\rangle)$,做一次 X 变换和一次 Z 变换.

量子传送原理

然后小明分别对第一和第二个量子位进行观测,并将结果(一对01信息)发给小鸣.

小鸣根据信息进行变换:

00: 状态坍缩成 $|00\rangle \otimes (\alpha |0\rangle + \beta |1\rangle)$,做一次 I 变换.

01: 状态坍缩成 $|01\rangle \otimes (\alpha |1\rangle + \beta |0\rangle)$,做一次 X 变换.

10: 状态坍缩成 $|10\rangle \otimes (\alpha |1\rangle - \beta |0\rangle)$,做一次 Z 变换.

11: 状态坍缩成 $|11\rangle \otimes (\alpha |0\rangle - \beta |1\rangle)$,做一次 X 变换和一次 Z 变换.

然后就完成了.

量子传送原理

然后小明分别对第一和第二个量子位进行观测,并将结果(一对01信息)发给小鸣.

小鸣根据信息进行变换:

00: 状态坍缩成 $|00\rangle \otimes (\alpha |0\rangle + \beta |1\rangle)$,做一次 I 变换.

01: 状态坍缩成 $|01\rangle \otimes (\alpha |1\rangle + \beta |0\rangle)$,做一次 X 变换.

10: 状态坍缩成 $|10\rangle \otimes (\alpha |1\rangle - \beta |0\rangle)$,做一次 Z 变换.

11: 状态坍缩成 $|11\rangle \otimes (\alpha |0\rangle - \beta |1\rangle)$,做一次 X 变换和一次 Z 变换.

然后就完成了.

同样可以扩展到高维情况,利用 2^n 个01位同时传送 n 个量子位.然而如果不需要同时的话,就只需要制备足够多的 $|\beta_{00}\rangle$ 就能完成多次传送了.

QFT

开始讨论量子算法.由于篇幅关系,只讲非常关键的Shor算法.别的算法(如量子游走,Grover算法,量子加密等等)可以去查阅相关资料.

QFT

开始讨论量子算法.由于篇幅关系,只讲非常关键的Shor算法.别的算法(如量子游走,Grover算法,量子加密等等)可以去查阅相关资料.

Shor算法中有用到QFT,所以需要讲QFT.

QFT

开始讨论量子算法.由于篇幅关系,只讲非常关键的Shor算法.别的算法(如量子游走,Grover算法,量子加密等等)可以去查阅相关资料.

Shor算法中有用到QFT,所以需要讲QFT.

相信大家都知道DFT.QFT类似,就是将一个给定量子态 $|q\rangle$ (由 n 个量子位表示,可能存在纠缠)乘上相应的矩阵:

QFT

开始讨论量子算法.由于篇幅关系,只讲非常关键的Shor算法.别的算法(如量子游走,Grover算法,量子加密等等)可以去查阅相关资料.

Shor算法中有用到QFT,所以需要讲QFT.

相信大家都知道DFT.QFT类似,就是将一个给定量子态 $|q\rangle$ (由 n 个量子位表示,可能存在纠缠)乘上相应的矩阵:

$$\frac{1}{N} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix} \quad (\text{其})$$

中 $\omega = e^{\frac{2i\pi}{N}}$, $N = 2^n$)

QFT实现

并不能直接用一个门直接实现QFT.

QFT实现

并不能直接用一个门直接实现QFT.

如图.其中 $R_x = \begin{pmatrix} 1 & 0 \\ 0 & e^{2i\frac{\pi}{2^x}} \end{pmatrix}$

QFT实现

并不能直接用一个门直接实现QFT.

如图.其中 $R_x = \begin{pmatrix} 1 & 0 \\ 0 & e^{2i\frac{\pi}{2^x}} \end{pmatrix}$

因为没有办法对于任意一个输入制备其相应的量子态,所以QFT并没有什么单独的使用价值 =.=

Shor算法

Shor算法的步骤:

Shor算法

Shor算法的步骤:

1. N 是质数的情况下直接返回 N .
2. 如果 $N = a^b$, 做平凡的分解(有现成的多项式算法).
3. 反复随机在 $[2, N - 2]$ 中取一个 x 直到 x 与 N 互质.
4. 寻找 r 使得 $x^r \bmod N = 1$. (!?!?!?!?)
5. 如果 r 是奇数或者 $x^{\frac{r}{2}} \bmod N \neq -1$, 重新选 x (回到第3步).
6. $N_1 = \gcd(r + 1, N)$ 和 $N_2 = \gcd(r - 1, N)$ 是因子.
7. 分解 N_1, N_2 和 $\frac{N}{N_1 N_2}$.

Shor算法

Shor算法的步骤:

1. N 是质数的情况下直接返回 N .
2. 如果 $N = a^b$, 做平凡的分解(有现成的多项式算法).
3. 反复随机在 $[2, N - 2]$ 中取一个 x 直到 x 与 N 互质.
4. 寻找 r 使得 $x^r \bmod N = 1$. (!?!?!?!?)
5. 如果 r 是奇数或者 $x^{r/2} \bmod N \neq -1$, 重新选 x (回到第3步).
6. $N_1 = \gcd(r + 1, N)$ 和 $N_2 = \gcd(r - 1, N)$ 是因子.
7. 分解 N_1, N_2 和 $\frac{N}{N_1 N_2}$.

第四步在经典计算机上面尚无多项式算法, 可以在量子计算模型中寻找解决方案.

相位估计

先不管前面的内容. 现有一个Unitary算子 U 和其一个特征向量 $|u\rangle$ (Unitary算子就是那些 $U^\dagger U = UU^\dagger = I$ 的算子 U).

相位估计

先不管前面的内容. 现有一个Unitary算子 U 和其一个特征向量 $|u\rangle$ (Unitary算子就是那些 $U^\dagger U = UU^\dagger = I$ 的算子 U).

可以发现其特征值的表示形式是 $\lambda_u = e^{2i\pi\phi}$ ($0 \leq \phi < 1$). 这个 ϕ 就是需要去估计的相位.

相位估计

先不管前面的内容. 现有一个Unitary算子 U 和其一个特征向量 $|u\rangle$ (Unitary算子就是那些 $U^\dagger U = UU^\dagger = I$ 的算子 U).

可以发现其特征值的表示形式是 $\lambda_u = e^{2i\pi\phi}$ ($0 \leq \phi < 1$). 这个 ϕ 就是需要去估计的相位.

如图.

相位估计

先不管前面的内容. 现有一个Unitary算子 U 和其一个特征向量 $|u\rangle$ (Unitary算子就是那些 $U^\dagger U = UU^\dagger = I$ 的算子 U).

可以发现其特征值的表示形式是 $\lambda_u = e^{2i\pi\phi}$ ($0 \leq \phi < 1$). 这个 ϕ 就是需要去估计的相位.

如图.

做iQFT之前的状态非常近似 $\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2i\pi k\phi} |k\rangle \otimes |u\rangle$ ($N = 2^K$). 这里用整数表示纯态量子位的张量积, 比如 $|3\rangle = |000 \cdots 0011\rangle$, $|7\rangle = |000 \cdots 0111\rangle$.

相位估计

先不管前面的内容. 现有一个Unitary算子 U 和其一个特征向量 $|u\rangle$ (Unitary算子就是那些 $U^\dagger U = UU^\dagger = I$ 的算子 U).

可以发现其特征值的表示形式是 $\lambda_u = e^{2i\pi\phi}$ ($0 \leq \phi < 1$). 这个 ϕ 就是需要去估计的相位.

如图.

做iQFT之前的状态非常近似 $\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2i\pi k\phi} |k\rangle \otimes |u\rangle$ ($N = 2^K$). 这里用整数表示纯态量子位的张量积, 比如 $|3\rangle = |000 \cdots 0011\rangle$, $|7\rangle = |000 \cdots 0111\rangle$.

iQFT怎么做呢? 因为量子门都是可逆的, 所以把QFT的线路倒过来, 门都求逆就行了.

相位估计

先不管前面的内容. 现有一个Unitary算子 U 和其一个特征向量 $|u\rangle$ (Unitary算子就是那些 $U^\dagger U = UU^\dagger = I$ 的算子 U).

可以发现其特征值的表示形式是 $\lambda_u = e^{2i\pi\phi}$ ($0 \leq \phi < 1$). 这个 ϕ 就是需要去估计的相位.

如图.

做iQFT之前的状态非常近似 $\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2i\pi k\phi} |k\rangle \otimes |u\rangle$ ($N = 2^K$). 这里用整数表示纯态量子位的张量积, 比如 $|3\rangle = |000 \cdots 0011\rangle$, $|7\rangle = |000 \cdots 0111\rangle$.

iQFT怎么做呢? 因为量子门都是可逆的, 所以把QFT的线路倒过来, 门都求逆就行了.

测量结果就是 ϕ 的非常近似的二进制表示的前 K 位.

相位估计

如果不知道特征向量 $|u\rangle$, 可以把 $|u\rangle$ 换成任意向量 $|u^*\rangle$, 这样的话输出就变成了含 $|u\rangle$ 的叠加态.

相位估计

如果不知道特征向量 $|u\rangle$, 可以把 $|u\rangle$ 换成任意向量 $|u^*\rangle$, 这样的话输出就变成了含 $|u\rangle$ 的叠加态.

这样进行测量就只有 $|\langle u | (|u\rangle \langle u|) |u^*\rangle|^2$ 的概率得到正确的输出了.

相位估计

如果不知道特征向量 $|u\rangle$,可以把 $|u\rangle$ 换成任意向量 $|u^*\rangle$,这样的话输出就变成了含 $|u\rangle$ 的叠加态.

这样进行测量就只有 $|\langle u | (|u\rangle \langle u|) |u^*\rangle|^2$ 的概率得到正确的输出了.

然而,在 U 特殊的情况下,即使没有得到这组特定的输出也是有用的(或者说一样有用).

相位估计

如果不知道特征向量 $|u\rangle$, 可以把 $|u\rangle$ 换成任意向量 $|u^*\rangle$, 这样的话输出就变成了含 $|u\rangle$ 的叠加态.

这样进行测量就只有 $|\langle u | (|u\rangle \langle u|) |u^*\rangle|^2$ 的概率得到正确的输出了.

然而, 在 U 特殊的情况下, 即使没有得到这组特定的输出也是有用的(或者说一样有用).

接下来就给出这个特殊的 U .

求 x 的度数 r

现在回到Shor算法的第4步(求 r 使得 $x^r \bmod N = 1$).

求 x 的度数 r

现在回到Shor算法的第4步(求 r 使得 $x^r \bmod N = 1$).

可以把 U 定义成 $U|y\rangle = |yx \bmod N\rangle$ (这里还是使用整数来表示纯态张量积).显然 U 是Unitary的.

求 x 的度数 r

现在回到Shor算法的第4步(求 r 使得 $x^r \bmod N = 1$).

可以把 U 定义成 $U|y\rangle = |yx \bmod N\rangle$ (这里还是使用整数来表示纯态张量积).显然 U 是Unitary的.

U 的特征向量

是 $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2i\pi ks}{r}} |x^k \bmod N\rangle$ ($s = 0, 1, \dots, r-1$), 对应的特征值是 $\lambda_s = e^{\frac{2i\pi s}{r}}$, 其中 s/r 是相位.

求 x 的度数 r

现在回到Shor算法的第4步(求 r 使得 $x^r \bmod N = 1$).

可以把 U 定义成 $U|y\rangle = |yx \bmod N\rangle$ (这里还是使用整数来表示纯态张量积).显然 U 是Unitary的.

U 的特征向量

是 $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2i\pi ks}{r}} |x^k \bmod N\rangle$ ($s = 0, 1, \dots, r-1$), 对应的特征值是 $\lambda_s = e^{\frac{2i\pi s}{r}}$, 其中 s/r 是相位.

可以验证 $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2i\pi ks}{r}} |u_s\rangle = |x^k \bmod N\rangle$.

求 x 的度数 r

现在回到Shor算法的第4步(求 r 使得 $x^r \bmod N = 1$).

可以把 U 定义成 $U|y\rangle = |yx \bmod N\rangle$ (这里还是使用整数来表示纯态张量积).显然 U 是Unitary的.

U 的特征向量

是 $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2i\pi ks}{r}} |x^k \bmod N\rangle$ ($s = 0, 1, \dots, r-1$), 对应的特征值是 $\lambda_s = e^{\frac{2i\pi s}{r}}$, 其中 s/r 是相位.

可以验证 $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2i\pi ks}{r}} |u_s\rangle = |x^k \bmod N\rangle$.

特别的, 当 $k = 0$ 时, $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$.

求 x 的度数 r

用这个 U 算子和 $|u^*\rangle = |1\rangle$ 作为输入进行相位估计(因为我们不知道 r ,所以自然不知道 $|u_s\rangle$).

求 x 的度数 r

用这个 U 算子和 $|u^*\rangle = |1\rangle$ 作为输入进行相位估计(因为我们不知道 r ,所以自然不知道 $|u_s\rangle$).

结果是 $|q\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\phi_s\rangle \otimes |u_s\rangle$, 其中 ϕ_s 是 $|u_s\rangle$ 的相位, $|\phi_s\rangle$ 是 ϕ_s 的近似二进制小数表示.

求 x 的度数 r

用这个 U 算子和 $|u^*\rangle = |1\rangle$ 作为输入进行相位估计(因为我们不知道 r ,所以自然不知道 $|u_s\rangle$).

结果是 $|q\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\phi_s\rangle \otimes |u_s\rangle$, 其中 ϕ_s 是 $|u_s\rangle$ 的相位, $|\phi_s\rangle$ 是 ϕ_s 的近似二进制小数表示.

因为这些 ϕ_s 都是分母为 r 的有理数的近似值, 所以都是有用的!

求 x 的度数 r

用这个 U 算子和 $|u^*\rangle = |1\rangle$ 作为输入进行相位估计(因为我们不知道 r ,所以自然不知道 $|u_s\rangle$).

结果是 $|q\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\phi_s\rangle \otimes |u_s\rangle$, 其中 ϕ_s 是 $|u_s\rangle$ 的相位, $|\phi_s\rangle$ 是 ϕ_s 的近似二进制小数表示.

因为这些 ϕ_s 都是分母为 r 的有理数的近似值, 所以都是有用的!

进行测量, 可以随机得到一组01信息, 表示一个相位的近似值.

求 x 的度数 r

用这个 U 算子和 $|u^*\rangle = |1\rangle$ 作为输入进行相位估计(因为我们不知道 r ,所以自然不知道 $|u_s\rangle$).

结果是 $|q\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\phi_s\rangle \otimes |u_s\rangle$, 其中 ϕ_s 是 $|u_s\rangle$ 的相位, $|\phi_s\rangle$ 是 ϕ_s 的近似二进制小数表示.

因为这些 ϕ_s 都是分母为 r 的有理数的近似值,所以都是有用的!

进行测量,可以随机得到一组01信息,表示一个相位的近似值.

取 $L = \lceil 2 \log_2 N \rceil, K = 2L + 1 + \lceil \log_2(2 + \frac{1}{2\epsilon}) \rceil$ 就能保证 $1 - \epsilon$ 的概率测量成功.

求 x 的度数 r

用这个 U 算子和 $|u^*\rangle = |1\rangle$ 作为输入进行相位估计(因为我们不知道 r ,所以自然不知道 $|u_s\rangle$).

结果是 $|q\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\phi_s\rangle \otimes |u_s\rangle$, 其中 ϕ_s 是 $|u_s\rangle$ 的相位, $|\phi_s\rangle$ 是 ϕ_s 的近似二进制小数表示.

因为这些 ϕ_s 都是分母为 r 的有理数的近似值, 所以都是有用的!

进行测量, 可以随机得到一组01信息, 表示一个相位的近似值.

取 $L = \lceil 2 \log_2 N \rceil$, $K = 2L + 1 + \lceil \log_2(2 + \frac{1}{2\epsilon}) \rceil$ 就能保证 $1 - \epsilon$ 的概率测量成功.

知道了近似值以后, 就可以利用连分数表示近似成一个有理数 $\frac{s}{r}$ 了. 其分母 r 很有可能是 x 的度数, 但是需要进行验算以确保正确性(如果失败了, 就要回到Shor算法第3步).

参考文献

Desurvire, Emmanuel. Classical and quantum Information theory: an introduction for the telecom scientist. Cambridge University Press, 2009.

?!

有Linux上面模拟量子计算机的工具:libquantum.

?!

有Linux上面模拟量子计算机的工具:libquantum.

谢谢大家.