量子计算初学笔记

李冠余

目录

第 一 章　预备知识

§ 1　基础假设

量子力学的数学理论首先要承认下面四条假设, 这些假设目前并没有被严格的推导证明, 只是从反复多次的实验结果中分析总结得到的, 目前所有的实验结果都可以很好的遵循量子力学当前的理论.

1.1　状态空间假设

量子系统的所有量子态构成希尔伯特空间, 称为状态空间.

如果状态空间是有限维的, 则它与 $\mathbb{C}^N$ 同构. 非负整数 n 称为量子比特数, 设 $N = 2^n$, 那么此时量子态可以表示为:

$$\psi = \begin{pmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{N-1} \end{pmatrix},$$

它的共轭转置表示为 $\psi^\dagger = (\psi_0^*, \psi_1^*, \ldots, \psi_{N-1}^*)$, 其中 c^* 是 $c \in \mathbb{C}$ 的复共轭. 在量子计算中还通常使用 Dirac 符号, 用 $|\psi\rangle$ 表示一个量子态, $\langle\psi|$ 表示其共轭转置, 内积定义为 $\langle\phi|\psi\rangle = \sum_{i=0}^{N-1} \phi_i^* \psi_i$, 不过要写成这种量子态的形式还是需要满足归一化, 也就是 $\langle\phi|\psi\rangle = 1$.

所以任何一个 $|\psi\rangle$ 都可以在一个给定的正交归一基 $\{|e_i\rangle\}$ ($\langle e_i|e_j\rangle = \delta_{ij}$) 中展开为: $|\psi\rangle = \sum_i c_i|e_i\rangle$, 其中 $c_i = \langle e_i|\psi\rangle$ 是复系数, 称为量子态 $|\psi\rangle$ 在基态 $|e_i\rangle$ 上的概率振幅. 通常也把状态 $|\psi\rangle$ 在位置 x 上的概率振幅定义为波函数:

$$\varphi(x) = \langle x|\psi\rangle, \tag{1.1}$$

$|c_i|^2$ 表示在基态 $|e_i\rangle$ 中被发现的概率.

由归一化条件有: $\langle\psi|\psi\rangle = \sum_i |c_i|^2 \coloneqq \sum_i |\varphi(e_i)|^2 = 1$.

考虑 $|+\rangle$ 和 $|-\rangle$, 很自然的有这样一个疑问, 那就是他们的概率是相同的, 那为什么还要区分这两个量子态. 这个问题 section 1.2中可以得到解释.

如果状态空间是无限维的, 例如考虑一个量子在一维空间中的行为, 那么其状态空间是无限维的, 并且基底是连续的, 也就是说所可观测量 (在后面量子测量中会提到) 填满了整个数轴. 此时

$$|\psi\rangle = \int_{-\infty}^{\infty} \varphi(x)|x\rangle\, dx. \tag{1.2}$$

其中 $\langle x|x'\rangle = \delta(x - x')$.

同样的, 由归一化条件有:

$$\langle\psi|\psi\rangle = \int_{-\infty}^{\infty} \delta(x-x')\langle\psi|x'\rangle\langle x|\psi\rangle dx \ = \int_{-\infty}^{\infty} |\langle x|\psi\rangle|^2 dx \coloneqq \int_{-\infty}^{\infty} |\varphi(x)|^2 dx = 1.$$

常用到的符号还有: $|\pm\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, $\overline{|0\rangle} = |1\rangle$, $\overline{|1\rangle} = |0\rangle$, $\{0,1\}^n$ 表示长度为 n 的所有二进制字符串的集合.

注 1.1 (经典状态以及概率向量) 在经典问题中, 例如骰子, 经典状态为 (可能出现的结果)*1,2,3,4,5,6;* 抛硬币, 经典状态为正面和反面. 在这里可以把经典状态集记为 Σ, 比特则是 Σ=$\{0,1\}$ 的系统. 我们也可以为每个经典状态分配概率来表示对其了解的程度, 例如抛硬币, 记正面为 *0,* 背面为 *1,* 那么我们相信在次数足够多的时候会有 $Pr(X=0) = \dfrac{1}{2}$, $Pr(X=1) = \dfrac{1}{2}$, 一个更简洁的写法是通过一个向量的形式: $\begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$.

注 1.2 为了方便, 可以使用 $|N\rangle$ 来描述标准基 $\{|e_i\rangle\}$, 这是一个二进制表示, 例如对于 $N=4$, 基态 $|y\rangle$ 的值可以是 $|0\rangle, |1\rangle, |2\rangle, |3\rangle$, 分别对应二进制表示:

$$|0\rangle = |00\rangle, \quad |1\rangle = |01\rangle, \quad |2\rangle = |10\rangle, \quad |3\rangle = |11\rangle$$

对于 $N=8$, 基态 $|y\rangle$ 的值可以是 $|0\rangle, |1\rangle, \ldots, |7\rangle$, 分别对应二进制表示:

$$|0\rangle = |000\rangle, \quad |1\rangle = |001\rangle, \quad |2\rangle = |010\rangle, \quad |3\rangle = |011\rangle, \quad |4\rangle = |100\rangle, \quad |5\rangle = |101\rangle, \quad |6\rangle = |110\rangle,$$

1.2　演化算子假设

以 N 量子位为例, 量子态的演化总是通过一个酉矩阵 $U \in \mathbb{C}^{N\times N}$ 实现, 即

$$|\psi'\rangle = U|\psi\rangle,\ UU^\dagger = U^\dagger U = I_N.$$

其中 $U^\dagger$ 是 U 的共轭转置, I_N 是 N 维单位矩阵.

可以定义范数:

$$\||\psi\rangle\| = \sqrt{\langle\psi \mid \psi\rangle},\ \|A\| := \max_{|\psi\rangle} \|A|\psi\rangle\|. \tag{1.3}$$

在定义了范数之后自然就有了距离可以用来衡量误差, 在这个基础上, 由于实际应用中一个算法可能会涉及到很多量子门, 接下来考察多个量子门产生的误差.

引理 1.3 *U_i, V_i 是酉矩阵, 满足 $\|U_i - V_i\| \le \epsilon (i = 1, 2, 3...)$, 则 $\|U_t \dots U_2 U_1 - V_t \dots V_2 V_1\| \le t\epsilon$.*

证明

$$\begin{aligned}
&\|U_{t+1}U_t \dots U_1 - V_{t+1}V_t \dots V_1\| \\
&\quad = \|U_{t+1}U_t \dots U_1 - U_{t+1}V_t \dots V_1 + U_{t+1}V_t \dots V_1 - V_{t+1}V_t \dots V_1\| \\
&\quad \le \|U_{t+1}U_t \dots U_1 - U_{t+1}V_t \dots V_1\| + \|U_{t+1}V_t \dots V_1 - V_{t+1}V_t \dots V_1\| \\
&\quad = \|U_{t+1}\left(U_t \dots U_1 - V_t \dots V_1\right)\| + \|\left(U_{t+1} - V_{t+1}\right)V_t \dots V_1\| \\
&\quad = \|U_t \dots U_1 - V_t \dots V_1\| + \|U_{t+1} - V_{t+1}\| \\
&\quad \le (t+1)\epsilon.
\end{aligned}$$

□

例 1.4 *在量子计算中, 习惯于把演化算子所对应的酉矩阵称为量子门, 以下是几个常见的量子门:*

- *Hadamard 门 (H 门):*

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

通过计算可以得到 $H|+\rangle = |0\rangle$, $H|-\rangle = |1\rangle$, 这也就解释了为什么要区分 $|+\rangle$ 和 $|-\rangle$.

- *Phase* 门 *(S* 门*):*

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

- $\pi/8$ 门 *(T* 门*):* $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

- *CNOT* 门*:*

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

- 泡利矩阵*:*

$$\sigma_x(NOT\ 门) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

定义 1.5 行列式的模为 *1* 的 $n \times n$ 酉矩阵以矩阵乘法作为运算构成一个李群*,* 记作 $\mathrm{SU}(n)$.

如果将这个群中的一个元素写做 e^{iA} , 那么因为 $e^{iA}e^{-iA^\dagger} = I$, 有 $e^{-iA^\dagger} = e^{-iA}$. 因此, 就有 $A = A^\dagger$, 也就是 A 是 Hermite 矩阵. 又因为 $\det(e^{iA}) = e^{i\mathrm{Tr}A} = 1$, 所以 $\mathrm{Tr}A = 0$, 任意一个零迹二阶 Hermite 矩阵都可以用三个泡利矩阵**例** 1.4的线性组合给出. 于是可以把任意一个 SU(2) 的群元素写做

$$U = e^{i\alpha\boldsymbol{\sigma}}, \tag{1.4}$$

其中 $\vec{a} \in \mathbb{R}^3$, $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$.

根据**引理** 1.3可以知道, 想要保证 t 个门误差控制在 ϵ 以内, 只需保证每一个门误差控制在 ϵ/t 以内. 对于任意一个单个的门, 为了设计方便, 通过类比经典的通用门, 我们也想构造通用量子门集, 这就需要考虑利用群对易子 $[\![U, V]\!] := UVU^{-1}V^{-1}$ 来构建一个网格, 覆盖整个以 I 为圆心的小球上 (对于其它的酉矩阵平移到 I 即可). 令

$$S_\epsilon := \{U \in \mathrm{SU}(2) : \|I - U\| \leq \epsilon\}. \tag{1.5}$$

对于集合 $\Gamma, S \subseteq \mathrm{SU}(2)$, 如果对于 S 中的任意一个 A, 在 Γ 中有一个 U, 使得 $\|A - U\| \leq \epsilon$, 我们就说 Γ 是 S 的一个 ϵ-网.

引理 1.6 如果 Γ 是 S_ϵ 的 ϵ^2-网, 那么 $[\![\Gamma,\Gamma]\!] := \{[\![U,V]\!] : U,V \in \Gamma\}$ 是 S_{ϵ^2} 的一个 $O(\epsilon^3)$-网.

证明 由 SU(2) 群的性质可知

$$\begin{aligned}
&\text{(i)}\ \left\|I - e^{i\vec{a}\cdot\vec{\sigma}}\right\| = 2\sin\frac{\|\vec{a}\|}{2} = \|\vec{a}\| + O\left(\|\vec{a}\|^3\right);\\
&\text{(ii)}\ \left\|e^{i\vec{b}\cdot\vec{\sigma}} - e^{i\vec{c}\cdot\vec{\sigma}}\right\| \le \|\vec{b}-\vec{c}\|;\\
&\text{(iii)}\ [\vec{b}\cdot\vec{\sigma}, \vec{c}\cdot\vec{\sigma}] = 2i(\vec{b}\times\vec{c})\cdot\vec{\sigma};\\
&\text{(iv)}\ \left\|[\![e^{i\vec{b}\cdot\vec{\sigma}}, e^{i\vec{c}\cdot\vec{\sigma}}]\!] - e^{-[\vec{b}\cdot\vec{\sigma},\vec{c}\cdot\vec{\sigma}]}\right\| = O(\|\vec{b}\|\|\vec{c}\|(\|\vec{b}\|+\|\vec{c}\|)).
\end{aligned}$$

其中,$[A,B]$ 在物理中表示对易子 $AB-BA$.

对于 $A \in S_{\epsilon^2}$, 往证存在 $U,V \in \Gamma$ 中, 使得 $\|A - [\![U,V]\!]\| = O(\epsilon^3)$. 选取 $\vec{a} \in \mathbb{R}^3$, 使得 $A = e^{i\vec{a}\cdot\vec{\sigma}}$. 由于 $A \in S_{\epsilon^2}$, 根据（i）, 可以选取 $\vec{a}$, 使得 $\|\vec{a}\| = O(\epsilon^2)$. 然后选取 $\vec{b},\vec{c} \in \mathbb{R}^3$ 使得 $2\vec{b}\times\vec{c} = \vec{a}$. 不妨设这些向量是正交且等长的, 这样 $\|\vec{b}\| = \|\vec{c}\| = \sqrt{\|\vec{a}\|/2} = O(\epsilon)$. 令 $B = e^{i\vec{b}\cdot\vec{\sigma}}$ 并且 $C = e^{i\vec{c}\cdot\vec{\sigma}}$. 那么由 (iv) 可知 A 被 $[\![B,C]\!]$ 模拟所产生的误差为 $O(\epsilon^3)$.

然后, 需要从网 Γ 中选择点. 让 $U = e^{i\vec{u}\cdot\vec{\sigma}}$ 成为 Γ 中离 B 最近的元素, 让 $V = e^{i\vec{v}\cdot\vec{\sigma}}$ 成为 Γ 中离 C 最近的元素. 由于 Γ 是 S_ϵ 的 ϵ^2 网, 有 $\|U-B\| \le \epsilon^2$,$\|V-C\| \le \epsilon^2$, 即 $\|\vec{u}-\vec{b}\| = O(\epsilon^2)$ 和 $\|\vec{v}-\vec{c}\| = O(\epsilon^2)$.

根据三角形不等式,

$$\|A - [\![U,V]\!]\| \le \left\|A - e^{2i(\vec{u}\times\vec{v})\cdot\vec{\sigma}}\right\| + \left\|e^{2i(\vec{u}\times\vec{v})\cdot\vec{\sigma}} - [\![U,V]\!]\right\|.$$

对于第一项, 使用（ii）, 我们得到

$$\begin{aligned}
\left\|A - e^{2i(\vec{u}\times\vec{v})\cdot\vec{\sigma}}\right\| &= \left\|e^{2i(\vec{b}\times\vec{c})\cdot\vec{\sigma}} - e^{2i(\vec{u}\times\vec{v})\cdot\vec{\sigma}}\right\|\\
&\le 2\|\vec{b}\times\vec{c} - \vec{u}\times\vec{v}\|\\
&= 2\|(\vec{b}-\vec{u}+\vec{u})\times(\vec{c}-\vec{v}+\vec{v}) - \vec{u}\times\vec{v}\|\\
&= 2\|(\vec{b}-\vec{u})\times(\vec{c}-\vec{v}) + (\vec{b}-\vec{u})\times\vec{v} + \vec{u}\times(\vec{c}-\vec{v})\|\\
&= O\left(\epsilon^3\right).
\end{aligned}$$

对于第二项, 使用（iii）和（iv）可以得出

$$\left\|e^{2i(\vec{u}\times\vec{v})\cdot\vec{\sigma}} - [\![U,V]\!]\right\| = \left\|e^{-[\vec{u}\cdot\vec{\sigma},\vec{v}\cdot\vec{\sigma}]} - [\![U,V]\!]\right\| = O\left(\epsilon^3\right).$$

□

定理 1.7 (Solovay-Kitaev) 如果一组单量子位量子门生成 SU(2) 的稠密子群, 那么对于任意 $\epsilon > 0$, 存在一个正整数 t, 使得任意单量子比特上的演化算子 U 都可以被这组量子门及其逆中最多 t 个门的乘积近似, 误差在 ϵ 以内. 如果有两组这样的量子门集, 那么使用其中一组实现的任何 t 门电路都可以使用另一组中 $t \cdot poly\log(t/\epsilon)$ 个门的电路来实现, 且精度为 ϵ. 并且存在一个经典算法可以在时间 $t \cdot poly\log(t/\epsilon)$ 内找到这个电路.[1]

证明 只需考虑如何通过来自给定通用门集 Γ 的门序列, 将任意 $U \in \mathrm{SU}(2)$ 近似到精度 ϵ. 首先, 取 Γ 元素的乘积构成一个新的通用门集 Γ_0, 对于某个足够小的常数 ϵ_0, 这个新的通用门集是 SU(2) 的 ϵ_0^2 网. 由于 ϵ_0 是一个常数, 所以构造 Γ_0 的开销是恒定的.

取 $V_0 \in \Gamma_0$, 使得 $\|U - V_0\| \leq \varepsilon_0^2$. 因为 $\|U - V_0\| = \left\|UV_0^\dagger - I\right\|$, 所以有 $UV_0^\dagger. \in S_{\epsilon_0^2}$. 如果 ϵ_0 足够小, 那么 $\epsilon_0^2 < k\epsilon_0^{3/2} = \epsilon_1$, 所以 $UV_0^\dagger \in S_{\epsilon_1}$.

因为 Γ_0 是 SU(2) 的 ϵ_0^2 网, 所以它是 S_{ϵ_0} 的 ϵ_0^2 网. 因此, Γ_1 是 S_{ϵ_1} 的 ϵ_1^2 网, 所以有 $V_1 \in \Gamma_1$, 使得 $\left\|UV_0^\dagger - V_1\right| \leq \epsilon_1^2 < k\epsilon_1^{3/2} = \epsilon_2$, 即 Γ_1 是一个 ϵ_1^2 网. 也就是说 $UV_0^\dagger V_1^\dagger - I \in S_{\epsilon_2}$.

一般来说, 假设可以得到 $V_0, V_1, \ldots, V_{i-1}$, 那么 $UV_0^\dagger V_1^\dagger \ldots V_{i-1}^\dagger \in S_{\epsilon_i}$. 由于 Γ_i 是 S_{ϵ_i} 的 ϵ_i^2 网, 就可以找到 $V_i \in \Gamma_i$, 使得 $\left\|UV_0^\dagger V_1^\dagger \ldots V_{i-1}^\dagger - V_i\right\| \leq \epsilon_i^2$. 反过来, 这也就意味着 $UV_0^\dagger V_1^\dagger \ldots V_i^\dagger \in S_{\epsilon_{i+1}}$.

重复这个过程 t 次, $V_t \ldots V_1 V_0$ 就能很好地近似 U: 有 $\|U - V_t \ldots V_1 V_0\| \leq \epsilon_t^2$. 如果认为来自 Γ_0 的门是基本的[1]. 实现一个来自 Γ_i 的门所需的基本门数是 5^i, 所以实现近似中用到的门的总数是 $\sum_{i=0}^{t} 5^i = \left(5^{t+1} - 1\right)/4 = O\left(5^t\right)$. 为了使总体误差不超过 ϵ, 需要让 $\epsilon_t^2 = \left(\frac{k^2\epsilon_0}{k^2}\right)^{(3/2)^t} \leq \epsilon$, 即:

$$\left(\frac{3}{2}\right)^t > \frac{\frac{1}{2}\log\left(k^2\epsilon\right)}{log\left(k^2\epsilon_0\right)}. \tag{1.6}$$

因此, 使用的门数是

$$O\left(\log^\nu \frac{1}{6}\right),$$

其中 $\nu = \log 5/\log\frac{3}{2}$.

□

[1]为了实现这些门, 只需要使用来自 Γ 集合的一定数量的门. 因此, 如果我们将 Γ 中的门作为基本门来考虑, 那么实现这些基本门所需的额外成本只是一个常数因子.

Solovay‐Kitaev 定理也说明了任何一组量子门都可以被通用量子门集合所近似, 后续的研究发现了不同的通用量子门集集合没有好坏之分, 并且也证明了寻找近似值所需要的时间是 $poly(log1/\epsilon)$ 的[1][2], 下面给出通用量子门集合的例子.

例 1.8 任何 2×2 的酉矩阵都可以被表示成

$$\begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{pmatrix} \cdot \begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix} \cdot \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \cdot \begin{pmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{pmatrix},$$

其中 δ, α, θ, β 都是实数, 并且对任何的 $W\in \mathrm{SU}(2)$ 都可以表示为

$$\begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix} \cdot \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \cdot \begin{pmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{pmatrix}.$$

对于量子算法来说, 设 n 是输入的量子比特数, 如果量子电路中的门的数量是 $O(poly(n))$, 那么可以认为这个量子算法是高效的.

1.3　张量积假设

对于一个由 m 个比特构成的量子态, 其状态空间是各个量子比特状态空间的张量积, 记为 $H=\bigotimes_{i=0}^{m-1} H_i$. 设 $|\psi_i\rangle$ 是 H_i 中的状态向量, 则整体的量子态可表示为

$$|\Psi\rangle = |\psi_0\rangle\otimes|\psi_1\rangle\otimes\cdots\otimes|\psi_{m-1}\rangle. \tag{1.7}$$

然而, 并非所有 H 中的量子态都可以以这种形式表示, 因为如果是纠缠态的量子比特, 那么就分不开成单独的量子比特的张量积.

设 $\{|e_j^{(i)}\rangle\}_{j\in[N_i]}$ 是 H_i 的基, 则 H 中的一个一般的量子态可以表示为

$$|\Psi\rangle = \sum_{j_0,\cdots,j_{m-1}} c_{j_0,\ldots,j_{m-1}} |e_{j_0}^{(0)}\rangle\otimes\cdots\otimes|e_{j_{m-1}}^{(m-1)}\rangle. \tag{1.8}$$

一般为了方便也可以这样写: $|0\rangle\otimes|0\rangle{=}|00\rangle{=}|0,0\rangle{=}\,|0\rangle\,|0\rangle$, $|0\rangle^{\otimes n}=|0^{\otimes n}\rangle$.

张量积的运算也满足:

$$\langle u\otimes v|w\otimes x\rangle = \langle u|w\rangle\langle v|x\rangle,$$

这是容易验证的.

对于矩阵 $A \in \mathbb{C}^{M\times N}, B \in \mathbb{C}^{p\times q}, C \in \mathbb{C}^{N\times M}, DB \in \mathbb{C}^{q\times p}$. 有:

$$\begin{aligned}(A\otimes B)(C\otimes D) &= \begin{bmatrix} a_{11}B & \cdots & a_{1N}B \\ \vdots & \ddots & \vdots \\ a_{M1}B & \cdots & a_{MN}B \end{bmatrix} \begin{bmatrix} c_{11}D & \cdots & c_{1M}D \\ \vdots & \ddots & \vdots \\ c_{N1}D & \cdots & c_{NM}D \end{bmatrix} \\ &= \begin{bmatrix} \sum_{j=1}^{N} a_{1j}c_{j1}BD & \cdots & \sum_{j=1}^{N} a_{1j}c_{jM}BD \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^{N} a_{Mj}c_{j1}BD & \cdots & \sum_{j=1}^{N} a_{Mj}c_{jM}BD \end{bmatrix} \\ &= (AC)\otimes(BD)\end{aligned}$$

1.4　量子测量假设

投影测量

一个满足

$$1.\ H = H^{\dagger},$$

$$2.\ H^2 = H.$$

的矩阵被称为投影矩阵.

取投影矩阵 H 的特征值 m 对应的一个特征向量 $|v_m\rangle$, 那么有 $H|v_m\rangle = m|v_m\rangle$. 考虑矩阵 $\sum\limits_m m|v_m\rangle\langle v_m|$, 注意到 $m|v_m\rangle\langle v_m||v_m\rangle = m|v_m\rangle = H|v_m\rangle$, 并且特征向量不可能为 0, 有 $H = \sum\limits_m m|v_m\rangle\langle v_m|$, 结合 $H^2 = H$, 得出 $H = \sum\limits_m |v_m\rangle\langle v_m|$.

投影测量是由一组投影矩阵 $\{H_0, \ldots, H_{m-1}\}$ 集合描述的测量, 如果 $H_0 + \cdots + H_{m-1} = I$. 那么, 这样的测量应用在系统 X 的某个状态 $|\psi\rangle$ 上时, 有:

对于每个 $k \in \{0, \ldots, m-1\}$, 测量结果是 k, 概率等于

$$\Pr(\text{结果是}k) = \|H_k|\psi\rangle\|^2 = \langle\psi|H_k|\psi\rangle \tag{1.9}$$

此时 X 的量子态变为

$$\frac{H_k\left|\psi\right\rangle}{\|H_k\left|\psi\right\rangle\|}. \tag{1.10}$$

从数学的角度来看, 这就是在已经固定了某种态的前提下, 按照预先得到这些态的可能性重新分配一下量子态而已. 除此之外, 我们也可以选择除 $\{0,\ldots,m-1\}$ 之外的其他结果进行投影测量. 换句话说, 对于任何有限非空集 Σ, 如果我们有一组满足 $\sum\limits_{a\in\Sigma}H_a=I$, 的投影矩阵集合 $\{H_a:a\in\Sigma\}$, 那么对于 $a\in\Sigma$, 测量结果是 a, 概率等于 $\Pr(\text{结果是}a)=\|H_a\left|\psi\right\rangle\|^2$, 对于测量产生的任何结果 a, X 的状态变为 $\frac{H_a|\psi\rangle}{\|H_a|\psi\rangle\|}$, 这与前面是类似的.

例 1.9 标准基测量, 选取的投影矩阵集是 $\{|a\rangle\langle a|:a\in\Sigma\}$, 其中 Σ 是系统 X 的经典状态集.

例如测量 $|+\rangle$, 他对应的可能结果是 *0,1.*

$$Pr(\text{结果为 } 0)=\||0\rangle\langle 0|\,|+\rangle\|^2=\left|\frac{1}{\sqrt{2}}\right|^2=\frac{1}{2},$$

$$Pr(\text{结果为 } 1)=\||1\rangle\langle 1|\,|+\rangle\|^2=\left|\frac{1}{\sqrt{2}}\right|^2=\frac{1}{2}.$$

例 1.10 假设一个由三个量子比特构成的系统处于量子态:

$$|a_0\rangle=\frac{|0\rangle|+\rangle|-\rangle+|1\rangle|0\rangle|0\rangle-|1\rangle|1\rangle|1\rangle}{\sqrt{3}}$$

在中间位置上执行标准基测量, 问测量结果为 *0* 的概率, 以及该结果对应塌缩后的量子态是什么.

显然中间量子位测量后为 *0* 的概率是 $\frac{1}{2}$, 可能出现 *0* 的情况量子位是 $-\frac{|0\rangle|0\rangle|1\rangle}{2\sqrt{3}}+\frac{|0\rangle|0\rangle|0\rangle}{\sqrt{3}}+\frac{|1\rangle|0\rangle|0\rangle}{2\sqrt{3}}$, 塌缩后结果为 $\frac{|0\rangle|0\rangle|-\rangle+\sqrt{2}|1\rangle|0\rangle|0\rangle}{\sqrt{3}}$.

假设我们有两个系统 X,Y 处于量子态 $|\psi\rangle$, 并且在系统 X 上描述的集合 $\{H_a:a\in\Sigma\}$ 执行了投影测量, 而对 Y 什么也没做, 这就是相当于对联合系统进行了由集合 $\{H_a\otimes I:a\in\Sigma\}$ 描述的投影测量. 测量结果 a 出现的概率是 $\|(H_a\otimes I)\left|\psi\right\rangle\|^2$, 并且在结果 a 出现的情况下, (X,Y) 的量子态变为 $\frac{(H_a\otimes I)|\psi\rangle}{\|(H_a\otimes I)|\psi\rangle\|}$.

使用标准基集合的投影测量

任意的投影测量都可以使用酉操作, 标准基测量和一个额外的工作空间系统来代替, 下面是证明.

假设 X 是一个系统, 集合 $\{H_0, \ldots, H_{m-1}\}$ 是对 X 的投影测量. 为了方便, 假设我们测量的可能结果集是 $\{0, \ldots, m-1\}$. 不过在这里的 m 不一定等于 X 对应的经典结果数量—, 另外设 n 是 X 对应的经典结果数量, 这意味着每个矩阵 H_k 是一个 $n \times n$ 投影矩阵. 由于 $\{H_0 \ldots, H_{m-1}\}$ 代表一次投影测量, 因此满足 $\sum_{k=0}^{m-1} H_k = I_n$.

我们的目标是执行一个过程, 其效果与在 X 上执行这次投影测量相同, 但只使用酉操作和标准基测量来完成.

设额外的工作空间系统为 Y, Y 的经典状态集设为 $\{0, \ldots, m-1\}$, 这与投影测量的结果集相同. 想法是在 Y 上执行一个标准基测量, 并通过一些变换使得这次测量的结与在 X 上的投影测量结果等效. 首先假设 Y 初始化为某个固定状态, 不妨设为 $|0\rangle$.

为了让 Y 的标准基测量能够和 X 的信息产生联系, 考虑在系统 (Y, X) 上执行一个酉变换. 选取矩阵:

$$M = \sum_{k=0}^{m-1} |k\rangle \langle 0| \otimes H_k = \begin{pmatrix} H_0 & 0 & \cdots & 0 \\ H_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ H_{m-1} & 0 & \cdots & 0 \end{pmatrix}. \tag{1.11}$$

(这是一个分块矩阵, 矩阵中的每个 0 表示一个完全由零填充的 $n \times n$ 矩阵.)

在这里, M 显然不是一个酉矩阵 (除非 $m = 1$, 在这种情况下,$H_0 = I,\ M = I$). 不过由于 $\{H_0, \ldots, H_{m-1}\}$ 是一次投影测量, 显然 M 的前 n 列是正交的. 也可以通过计算来验证, 对于 $j \in \{0, \ldots, n-1\}$, M 中的第 j 列可以表示为:

$$|\psi_j\rangle = \sum_{k=0}^{m-1} |k\rangle \otimes H_k |j\rangle. \tag{1.12}$$

取 $i,j\in\{0,\ldots,n-1\}$, 那么有:

$$\begin{aligned}\langle\psi_i|\psi_j\rangle &= \left(\sum_{k=0}^{m-1}|k\rangle\otimes H_k|i\rangle\right)^{\dagger}\left(\sum_{l=0}^{m-1}|l\rangle\otimes H_l|j\rangle\right)\\ &= \sum_{k=0}^{m-1}\sum_{l=0}^{m-1}\langle k|l\rangle\langle i|H_kH_l|j\rangle\\ &= \sum_{k=0}^{m-1}\langle i|H_kH_k|j\rangle = \sum_{k=0}^{m-1}\langle i|H_k|j\rangle\\ &= \langle i|I|j\rangle = \begin{cases}1 & i=j\\ 0 & i\neq j\end{cases}.\end{aligned}$$

由于前面是正交的, 后面都是 0. 接下来, 可以用一些不同的复数项替换所有剩余的零项, 使得整个矩阵是酉矩阵:

$$U=\begin{pmatrix}H_0 & ? & \cdots & ?\\ H_1 & ? & \cdots & ?\\ \vdots & \vdots & \ddots & \vdots\\ H_{m-1} & ? & \cdots & ?\end{pmatrix}. \tag{1.13}$$

(对于具体的矩阵 $\{H_0,\ldots,H_{m-1}\}$, 可以使用 Schmidt 正交化计算出来.)

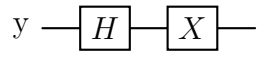
最后测量过程如下: 首先初始化 Y 为 $|0\rangle$, X 的初始状态是 ϕ. 在联合系统 (Y,X) 上执行 U, 即:

$$U(|0\rangle\times|\phi\rangle)=\sum_{k=0}^{m-1}|k\rangle\langle 0|\otimes H_k|0\rangle\times|\phi\rangle=\sum_{k=0}^{m-1}|k\rangle\otimes H_k|j\rangle. \tag{1.14}$$

当我们在 Y 上做标准基测量时, 获得每个结果 k 的概率 $\|H_k|\phi\rangle\|^2$, 此时, (Y,X) 的状态塌缩为 $|k\rangle\otimes\frac{H_k|\phi\rangle}{\|H_k|\phi\rangle\|}$. 因此, Y 测量结果和在 X 上直接执行由 $\{H_0,\ldots,H_{m-1}\}$ 描述的投影测量一样.

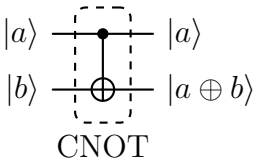
§ 2　量子电路

首先可以考虑这样一个简单的例子:



左侧代表量子比特, 名为 y, 由于一般来说基态较为容易制备, 因此通常都是以 $|0\rangle$ 作为初始. 电路从左到右执行, 第一个操作是通过 H 门 (见**例** 1.4), 第二个操作是通过泡利 X 门, 注意到 $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$, 因此也被称为量子非门, 在量子电路中也表示为  .

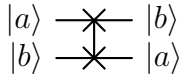
接下来是另一个例子:



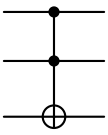
量子电路 *2.1:* 受控非门

意思是如果输入的控制量子比特 $|a\rangle$ 是 $|1\rangle$, 那么对目标比特 $|b\rangle$ 进行非门操作, 如果是 $|0\rangle$ 那么将不执行非门操作, 其中 $a \oplus b = (a + b) \mod 2$.

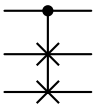
除此之外, 还有:



量子电路 *2.2:* 交换门

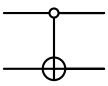


量子电路 *2.3: Toffoli* 门



量子电路 *2.4: Fredkin* 门

其中, 多控制的意思是当控制量子比特全是 $|1\rangle$ 时, 才会激活下面的操作. 相对于受 $|1\rangle$ 控制的量子电路, 我们自然而然的也会考虑受 $|0\rangle$ 控制的量子电路, 在电路图中记为空心圆点, 下面是一个例子:



量子电路 *2.5:* 零控制非门

电路中门的总数称为电路的大小. 因此, 假设电路中的门代表基本运算, 那么电路的大小就代表它所需的基本运算数量, 也就是计算成本. 不过电路的大小也不一定直

接对应运行时间, 比如一些操作之前相互不影响, 那么几个门也可以同时进行.

另一种衡量电路效率的方法是电路的深度, 表示从输入线路到输出线路的任何路径上遇到的最大门数, 这种方法考虑到了并行化的可能性, 不过在目前的算法中考虑较少.

事实上, 我们也可以为不同的逻辑门分配不同的成本, 例如当我们在查询模型中工作并计算电路对输入函数 (以黑盒的形式) 进行的查询次数时, 实际上将成本分给了查询门, 其它的门则是零成本.

§ 3　量子信息限制

3.1　不可克隆定理

定理 3.1 (不可克隆定理) *: 设 X 和 Y 是对应同一经典状态集 Σ(注 1.1) 的两个量子系统, 且 Σ 至少有两个元素. 不存在 Y 中的一个量子态 $|\phi\rangle$ 和量子门 U, 使得对于 X 的每一个量子态 $|\psi\rangle$, 都有 $U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle$.*

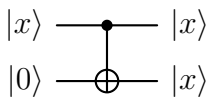
证明 取 $a, b \in \Sigma$ 且 $a \neq b$. 假设存在 $|\phi\rangle \in Y$ 和一个量子门 U , 使得 $U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle$ 对 X 中的每一个量子态 $|\psi\rangle$ 成立, 那么有 $U(|a\rangle \otimes |\phi\rangle) = |a\rangle \otimes |a\rangle$, $U(|b\rangle \otimes |\phi\rangle) = |b\rangle \otimes |b\rangle$.

由张量积运算的线性有: $U\left(\left(\frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle\right) \otimes |\phi\rangle\right) = \frac{1}{\sqrt{2}}|a\rangle \otimes |a\rangle + \frac{1}{\sqrt{2}}|b\rangle \otimes |b\rangle$. 由于 $U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle$ 对每一个量子态 $|\psi\rangle$ 成立, 那么也有

$$
\begin{aligned}
& U\left(\left(\frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle\right) \otimes |\phi\rangle\right) \\
=& \left(\frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle\right) \\
=& \frac{1}{\sqrt{2}}|a\rangle \otimes |a\rangle + \frac{1}{\sqrt{2}}|a\rangle \otimes |b\rangle + \frac{1}{\sqrt{2}}|b\rangle \otimes |a\rangle + \frac{1}{\sqrt{2}}|b\rangle \otimes |b\rangle \\
\neq& \frac{1}{\sqrt{2}}|a\rangle \otimes |a\rangle + \frac{1}{\sqrt{2}}|b\rangle \otimes |b\rangle .
\end{aligned}
$$

因此, 不存在一个状态 $|\phi\rangle$ 和一个酉操作 U, 使 $U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle$ 对每一个量子态向量 $|\psi\rangle$ 都成立. □

不过单纯想复制一个已知量子态 $|x\rangle$, 还是可以简单的通过 CNOT 门来实现的.



量子电路 *3.1:* 复制已知量子态

3.2　全局相位的无关性

设 $|\psi\rangle$ 和 $|\phi\rangle$ 是表示某系统的量子态的单位向量, 假设存在一个复数 $\alpha(|\alpha| = 1)$, 使得 $|\phi\rangle = \alpha|\psi\rangle$. 我们将 α 称为全局相位.

对于 $|\psi\rangle$, 任意的标准基 x 出现概率是 $|\langle x|\psi\rangle|^2$.

对于 $|\phi\rangle$, 任意的标准基 x 出现概率是 $|\langle x|\phi\rangle|^2 = |\alpha\langle x|\psi\rangle|^2 = |\alpha|^2|\langle x|\psi\rangle|^2 = |\langle x|\psi\rangle|^2$.

由于 $|\alpha| = 1$, 这两种量子态标准基测量结果相同.

下面考虑对这两个量子态都应用任意酉操作 U . 第一个量子态变为 $U|\psi\rangle$, 第二个量子态变为 $U|\phi\rangle = \alpha U|\psi\rangle$. 也就是说, 通过任意量子门后, 两个量子态仍然只相差同一个全局相位 α.

因此, 无论这两个量子态应用什么操作, 也总是只会相差一个全局相位, 无法通过量子测量来区分.

3.3　非正交量子态不能完美区分

如果我们有两个非正交量子态 $|\psi\rangle$ 和 $|\phi\rangle$, 即 $\langle\phi|\psi\rangle \neq 0$, 那么就不能完美区分它们.

一个量子电路如果能够说它完美地区分了 $|\psi\rangle$ 和 $|\phi\rangle$, 那么需要最后测量结果中一个状态为 0 , 而另一个状态为 1. 也就是要做到这样:

其中,U 代表电路中所有量子门的组合.

现在, 考虑 $|\psi\rangle$ 在电路上运行. 在测量刚要执行之前的状态可以写为 $U(|0\ldots0\rangle|\psi\rangle) = |\gamma_0\rangle|0\rangle + |\gamma_1\rangle|1\rangle$.$|\gamma_0\rangle$ 和 $|\gamma_1\rangle$, 表示除了顶部量子比特之外的所有量子比特. 顶部量子比特产生结果 0 和 1 的概率如下:

$\Pr(\text{结果为 } 0) = \||\gamma_0\rangle\|^2$, $\Pr(\text{结果为 } 1) = \||\gamma_1\rangle\|^2$.

量子态 $|\psi\rangle$ 通过量子电路后输出 0, 故有 $|\gamma_1\rangle = 0$, 即

$$U(|0\ldots0\rangle|\psi\rangle) = |\gamma_0\rangle|0\rangle.$$

等式两边左乘 $U^\dagger$ 得到:

$$|0\ldots0\rangle|\psi\rangle = U^\dagger(|\gamma_0\rangle|0\rangle). \tag{3.15}$$

类似地有

$$U(|0\ldots0\rangle|\phi\rangle) = |\delta_1\rangle|1\rangle$$

以及,

$$|0\ldots0\rangle|\phi\rangle = U^\dagger(|\delta_1\rangle|1\rangle). \tag{3.16}$$

(3.15) 式, (3.16) 式做内积有:

$$\text{右边} = (U^\dagger(|\gamma_0\rangle|0\rangle))^\dagger U^\dagger(|\delta_1\rangle|1\rangle) = (\langle\gamma_0|\langle 0|)UU^\dagger(|\delta_1\rangle|1\rangle) = (\langle\gamma_0|\langle 0|)(|\delta_1\rangle|1\rangle) = \langle\gamma_0|\delta_1\rangle\langle 0|1\rangle = 0,$$

$$0 = \text{左边} = (|0\ldots0\rangle|\psi\rangle)^\dagger(|0\ldots0\rangle|\phi\rangle) = \langle 0\ldots\ 0|0\ldots0\rangle\langle\psi|\phi\rangle = \langle\psi|\phi\rangle.$$

也就是说这样的电路能够实现, 需要 $|\psi\rangle$ 和 $|\phi\rangle$ 是正交, 不妨代入试一下.

假设量子态 $|\phi\rangle$ 和 $|\psi\rangle$ 正交 ($\langle\phi|\psi\rangle = 0$). 可以通过执行例如 $\{|\phi\rangle\langle\phi|, I - |\phi\rangle\langle\phi|\}$, 这些投影测量来完美地区分.

对于量子态 $|\phi\rangle$, 会得到:

$$\||\phi\rangle\langle\phi||\phi\rangle\|_2 = \||\phi\rangle\langle\phi|\phi\rangle\|_2 = \||\phi\rangle\|_2 = 1,$$

$$\|(I - |\phi\rangle\langle\phi|)|\phi\rangle\|_2 = \||\phi\rangle - |\phi\rangle\langle\phi|\phi\rangle\|_2 = \||\phi\rangle - |\phi\rangle\|_2 = 0.$$

对于状态 $|\psi\rangle$, 会得到:

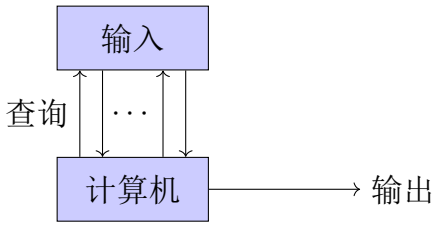
$$\||\phi\rangle\langle\phi||\psi\rangle\|_2 = \||\phi\rangle\langle\phi|\psi\rangle\|_2 = \|0\|_2 = 0,$$

$$\|(I - |\phi\rangle\langle\phi|)|\psi\rangle\|_2 = \||\psi\rangle - |\phi\rangle\langle\phi|\psi\rangle\|_2 = \||\psi\rangle\|_2 = 1.$$

第 二 章　量子查询算法

传统的计算机基本就是按照下面这个图的形式进行:

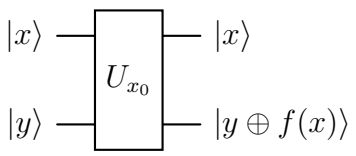
不同于上述这种过程, 下面要介绍的查询模型, 输入不是直接提供给计算机的. 而是以函数的形式提供, 计算机通过查询来访问输入.



在查询模型的计算中, 输入通常由一个 oracle 或 blackbox 提供. 这两个词语的意思就是说, 输入的完整描述对于计算来说是隐藏的, 我们无法看见函数的内部结构或理解它的工作机制, 唯一的访问方式就是提出问题.

§ 1　Deutsch 算法

考虑实现这样功能的一个量子电路:



量子电路 *1.1:* 相位返还

以 $f : \{0,1\} \to \{0,1\}$ 为例, 不妨带入 $|-\rangle$:

$$|x\rangle|-\rangle \xrightarrow{U_{x_0}} |x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - \overline{|f(x)\rangle}) = |x\rangle \otimes (-1)^{f(x)}|-\rangle .$$

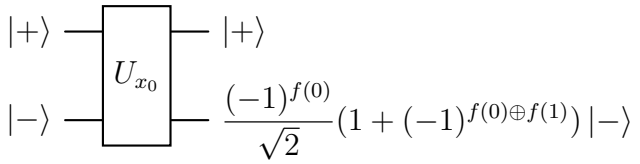
也就是实现了

$$|x\rangle|-\rangle \mapsto (-1)^{f(x)}|x\rangle|-\rangle \tag{1.1}$$

这个过程称为相位返还, 这里的 U_{x_0} 实际上就是前文提到的 oracle, 对于具体问题我们目前不考虑物理上构造它的难度, 只是定义了一个理论模型, 有助于阐明量子计算的潜在优势而已.

有两个盒子, 每个盒子里可能装着一个苹果或一个橙子. 我们想知道: 这两个盒子是否装着同样类型的水果. 考虑映射 $f:\{0,1\}\to\{0,1\}$. f 可以看作是打开盒子后观察水果类型的操作, 那么问题转化为对于映射 $f:\{0,1\}\to\{0,1\}$, 判断 $f(0)$ 是否 $=f(1)$, 这便是 Deutsch 问题.

显然直接查询两次可以直接回答 $f(0)$ 是否等于 $f(1)$. 但是通过量子电路 1.1, 考虑将 $|x\rangle$ 换为 $|+\rangle$, 那么可以构造出 $f(1)\otimes f(1)$:

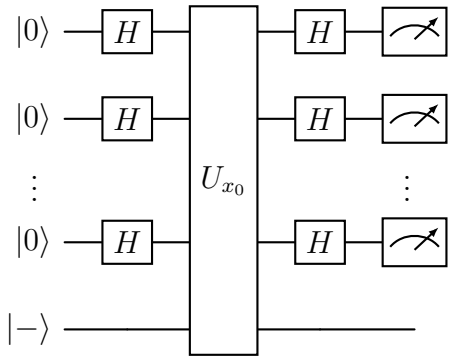


.

这样就可以通过一次操作来判断 $f(0)$ 是否等于 $f(1)$, 称为 Deutsch 算法.

该算法的多量子比特版本称为 Deutsch-Jozsa 算法, 即给定函数 $f:\{0,1\}^n\to\{0,1\}$, 需要满足要么 f 是一个常数函数 (即所有输入得到相同输出), 要么 f 是一个平衡函数 (一半输入得到 0, 另一半得到 1), 希望确定是哪一种函数.

事实上, 在前文 Deutsch 问题中, 也就是 $n=1$ 的情况下, $f(0)=f(1)$ 是常数函数, $f(0)\neq f(1)$ 是平衡函数, 现在根据 Deutsch 问题的经验考虑如下的电路图:



量子电路 *1.2: Deutsch-Jozsa* 算法

注意到:

$$(H|0\rangle)^{\otimes n}|-\rangle = |+\rangle^{\otimes n}|-\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|-\rangle \xrightarrow{U_{x_0}} \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle|-\rangle.$$

并且,

$$H|x\rangle = \frac{|0\rangle + (-1)^x|1\rangle}{\sqrt{2}}, \quad x\in\{0,1\}. \tag{1.2}$$

代入之后有:

$$H^{\otimes n}|x\rangle = \bigotimes_{j=1}^{n}\frac{|0\rangle+(-1)^{x_j}|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}\prod_{j=1}^{n}(-1)^{x_jy_j}|y\rangle. \tag{1.3}$$

其中 x_j, y_j 为第 j 个分量, 假设 y_j 要取 0, 那么前面对应位置就需要是 $|0\rangle$ 做的张量积, 如果让这个位置的系数为 1, 那么等号满足; 同样的, 要是 y_j 取 1, 那么这个部位的系数也为 $(-1)^{x_j}$, 因此从每一位来看等号是成立的, 整体上来看等号是成立的. 值得注意的是, 首先使用 H 门对输入的 $|0\rangle$ 作用, 在量子算法中是很常用的操作.

原式转化为,

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle|-\rangle \xrightarrow{H^{\otimes n}\otimes I} \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle|-\rangle = \sum_{y\in\{0,1\}^n}a_y|y\rangle|-\rangle$$

其中:

$$a_y = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x\cdot y}. \tag{1.4}$$

如果是常数函数, 记为 $f(x)=a$, 此时

$$a_y = \frac{(-1)^a}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot y},\ a_{0,\dots,0} = (-1)^a,\ a_y = 0(y\neq 0,\dots,0).$$

其余情况为平衡函数, 有:

$$a_{0,\dots,0} = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)} = \frac{1}{2^n}(2^{n-1}-2^{n-1}) = 0.$$

综上测量结果为全 $|0\rangle$ 的时候为常数函数, 其余情况为平衡函数.

§ 2　非结构化搜索问题

2.1　Grover 算法

接着上一节的例子, 现在我们的目标是找到含有橙子的盒子. 问题转化为, 对于 $f:\{0,1\}^n\to\{0,1\}$, 并且存在一个唯一的标记状态 x_0 使得 $f(x_0)=1$, 我们希望找到 x_0. 这是典型的非结构化搜索问题, 因为我们对于 f 的内在结构 (如何从输入得到输出) 是不清楚的, 无法直接构建一个结构化的查询来寻找 x_0, 而是挨个盒子打开检查, 需要经历 $N-1$ 次的穷举. 结构化搜索指的, 是例如有一个包含运动员信息的数据库, 记录包含姓名、国籍、项目和成绩. 如果需要找到所有参加“100 米跑”且来自“中国”的运动员的记录, 根据“项目”和“国籍”字段进行过滤, 这就是结构化搜索.

针对上述非结构化搜索问题, 考虑使用第一节的相位返还算子 U, 将本节研究的问题带入之后就是

$$\begin{cases}|x\rangle\mapsto|x\rangle\,,f(x)=0;\\ |x\rangle\mapsto-|x\rangle\,,f(x)=1.\end{cases}\tag{2.5}$$

设

$$|\psi\rangle=\frac{1}{\sqrt{N}}\sum_{x\in[N]}|x\rangle.\tag{2.6}$$

可以改写为:

$$|\psi\rangle=\frac{1}{\sqrt{N}}|\omega\rangle+\sqrt{1-\frac{1}{\sqrt{N}}}\,|\omega^{\perp}\rangle=\sin(\theta)|\omega\rangle+\cos(\theta)|\omega^{\perp}\rangle,\tag{2.7}$$

其中:

$$|\omega^{\perp}\rangle=\frac{1}{\sqrt{N-1}}\sum_{x\in[N],\langle x_0||x\rangle=0}|x\rangle,\ \theta=\arcsin\frac{1}{\sqrt{N}}.$$

考虑酉矩阵 $V_\psi=2\,|\psi\rangle\langle\psi|-I$, 有

$$\begin{cases}V\,|\psi\rangle=|\psi\rangle\,,\\ V\,|\omega\rangle=\dfrac{2}{\sqrt{n}}\,|\psi\rangle-|\omega\rangle\,.\end{cases}$$

注意到:

$$\begin{cases} VU\left|\omega\right\rangle = (2\left|\psi\right\rangle\left\langle\psi\right| - I)(-\left|\omega\right\rangle) = (1-2\sin^2\theta)\left|\omega\right\rangle + 2\sin\theta\cos\theta\left|\omega^\perp\right\rangle, \\ VU\left|\omega^\perp\right\rangle = (2\left|\psi\right\rangle\left\langle\psi\right| - I)(\left|\omega^\perp\right\rangle) = -2\sin\theta\cos\theta\left|\omega\right\rangle + (2\cos^2\theta-1)\left|\omega^\perp\right\rangle. \end{cases} \tag{2.8}$$

为了表示方便可以将这个变换整理成矩阵:

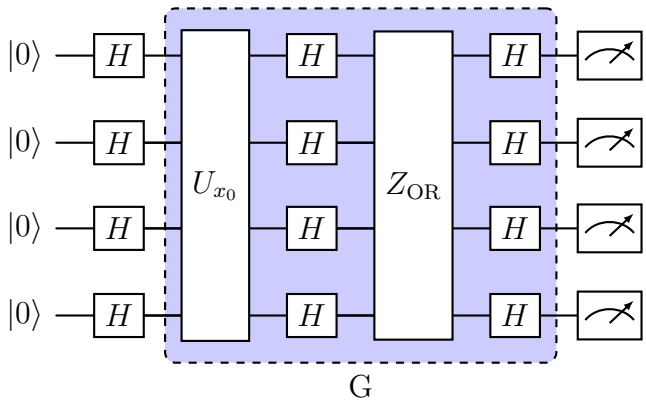
$$\begin{pmatrix} 1-2\sin^2\theta & -2\sin\theta\cos\theta \\ 2\sin\theta\cos\theta & 2\cos^2\theta-1 \end{pmatrix} = \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^2 \tag{2.9}$$

这也就说明进行一次 $G = VU$ 相当于做两次角度为 θ 的旋转变换, 则 $G^k|\psi\rangle = \sin((2k+1)\theta)|\omega\rangle + \cos((2k+1)\theta)|\omega_0^\perp\rangle$. 想让 $\sin((2k+1)\theta/2) \approx 1$, 需要 $k \approx \frac{\pi}{2\theta} \approx \frac{\pi}{4}\sqrt{N}$, 也就是说 Grover 算法可以通过 $O(\sqrt{N})$ 次查询解决无结构搜索问题.

接下来考虑量子电路, 考虑 $Z_{\mathrm{OR}} = 2\left|0^n\right\rangle\left\langle 0^n\right| - I$, 对两边做 H 门有:

$$H^{\otimes n} Z_{\mathrm{OR}} H^{\otimes n} = 2\left|\psi\right\rangle\left\langle\psi\right| - I = V \tag{2.10}$$

在这里我们得到了 V 的量子电路, 则该算法通过以下电路实现:



量子电路 *2.1: Grover 算法*

当 x_0 不唯一时, 该方法也同样使用, 令 $A_0 = \{x \in \Sigma^n : f(x) = 0\}$, $A_1 = \{x \in \Sigma^n : f(x) = 1\}$. 则有:

$$\left|\omega\right\rangle = \frac{1}{\sqrt{|A_0|}} \sum_{x\in A_0} \left|x\right\rangle, \ \left|\omega^\perp\right\rangle = \frac{1}{\sqrt{|A_1|}} \sum_{x\in A_1} \left|x\right\rangle. \tag{2.11}$$

$$|\psi\rangle = \sqrt{\frac{|A_0|}{N}}\,|\omega\rangle + \sqrt{\frac{|A_1|}{N}}\,|\omega^{\perp}\rangle\,. \tag{2.12}$$

维持算子不变, 进行运算有:

$$\begin{cases} G\,|\omega\rangle = \frac{|A_0|-|A_1|}{N}\,|\omega\rangle + \frac{2\sqrt{|A_0|\cdot|A_1|}}{N}\,|\omega^{\perp}\rangle\,, \\ G\,|\omega^{\perp}\rangle = -\frac{2\sqrt{|A_0|\cdot|A_1|}}{N}\,|\omega\rangle + \frac{|A_0|-|A_1|}{N}\,|\omega^{\perp}\rangle\,. \end{cases} \tag{2.13}$$

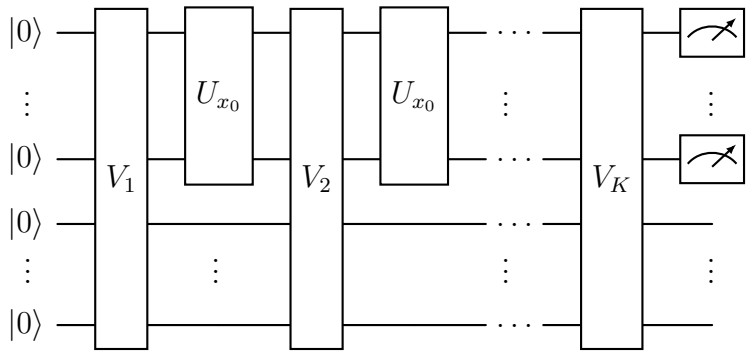
整理成矩阵为:

$$\begin{pmatrix} \frac{|A_0|-|A_1|}{N} & \frac{2\sqrt{|A_0|\cdot|A_1|}}{N} \\ -\frac{2\sqrt{|A_0|\cdot|A_1|}}{N} & \frac{|A_0|-|A_1|}{N} \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{|A_0|}{N}} & -\sqrt{\frac{|A_1|}{N}} \\ \sqrt{\frac{|A_1|}{N}} & \sqrt{\frac{|A_0|}{N}} \end{pmatrix}^2 = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^2 \tag{2.14}$$

其中 $\theta = \sin^{-1}\left(\sqrt{\frac{|A_1|}{N}}\right)$.

2.2　查询算法复杂度下限

前一节我们得出 Grover 算法可以通过 $O(\sqrt{N})$ 次查询 U_{x_0}, 以较高的概率找到 x_0. 事实上, 这是渐近最优的, 即没有量子算法可以使用少于 $O(\sqrt{N})$ 的访问次数来完成这项任务.



量子电路 *2.2:* 非结构化搜索算法示意图

任何以 $|0\rangle$ 为初始状态并访问 U_{x_0} k 次的量子搜索算法可以被写成以下形式:

$$|\psi_k^{x_0}\rangle = V_k^{x_0}\psi_0 = V_k U_{x_0} V_{k-1} U_{x_0} \ldots V_1 U_{x_0}\,|0\rangle\,. \tag{2.15}$$

上标 x_0 表示状态依赖于标记量子态 x_0, 解决这个问题等价于存在 k, 使得对于每

个标记 x_0, 都有 $|\langle\psi_k^{x_0}|x_0\rangle^2| \geq C$. 也就是说, 以 $|\psi_k^{x_0}\rangle$ 作为基, 测量 x_0 结果为 k 的概率至少为 1/2.

为了证明下界, 不妨定义一个假算法 V_k: $|\psi_k\rangle = V_k|0\rangle = V_kV_2V_1|0\rangle$. 这个算法不涉及解决方案 x_0 的任何信息, 并不能解决搜索问题. 因此真实解和假解是可以区分的量子态, 也就是说 $\| |\psi_k^{x_0}\rangle - |\psi_k\rangle \| \geq C,\ C > 0$. 则:

$$\sum_{x_0\in[n]} \| |\psi_k^{x_0}\rangle - |\psi_k\rangle \| \geq CN. \tag{2.16}$$

特别的有,

$$\sum_{x_0\in[n]} \| |\psi_1^{x_0}\rangle - |\psi_1\rangle \| = 0. \tag{2.17}$$

这是由于此时还未通过 U_{x_0} 门, 另一方面来考虑差的范数:

$$\begin{aligned}
\| |\psi_k^{x_0}\rangle - |\psi_k\rangle \| &= \|V_kU_{x_0}|\psi_{k-1}^{x_0}\rangle - V_k|\psi_{k-1}\rangle \| \\
&= \|U_{x_0}|\psi_{k-1}^{x_0}\rangle - |\psi_{k-1}\rangle \| \\
&= \| |\psi_{k-1}^{x_0}\rangle - U_{x_0}|\psi_{k-1}\rangle \| \\
&= \| |\psi_{k-1}^{x_0}\rangle - |\psi_{k-1}\rangle + |\psi_{k-1}\rangle - U_{x_0}|\psi_{k-1}\rangle \| \\
&\leq \| |\psi_{k-1}^{x_0}\rangle - |\psi_{k-1}\rangle \| + \| |\psi_{k-1}\rangle - U_{x_0}|\psi_{k-1}\rangle \|
\end{aligned} \tag{2.18}$$

在这里, 定义 $|\psi_k\rangle = \sum_{y=1}^n \alpha_{y,t}|y\rangle|\phi_y\rangle$. 也就是专注于第一个系统是量子态 $|y\rangle$(即抛掉了下面辅助量子比特), 这样可以更清楚的看到 U_{x_0} 对结果的影响. 此时,

$$U_{x_0}|\psi_k\rangle = \sum_{y\neq x_0} \alpha_{y,t}|y\rangle|\phi_y\rangle - \alpha_{x_0,t}|x_0\rangle|\phi_{x_0}\rangle = |\psi_k\rangle - 2\alpha_{x_0,t}|x_0\rangle|\phi_{x_0}\rangle.$$

因此

$$\|U_{x_0}|\psi_k\rangle - |\psi_k\rangle \| = 2|\alpha_{x_0,t}|.$$

结合(2.18) 式, 有:

$$\| |\psi_k\rangle - |\psi_k^{x_0}\rangle \| \leq 2\sum_{j=1}^{k-1} |\alpha_{x_0,j}|, \quad \forall x \in \{1,\ldots,n\}.$$

$$\sum_{x=1}^{n} \| \, |\psi_k\rangle - |\psi_k^{x_0}\rangle \, \| \leq 2 \sum_{x=1}^{n} \sum_{j=1}^{k-1} |\alpha_{x,j}| = 2 \sum_{j=1}^{k-1} \sum_{x=1}^{n} |\alpha_{x,j}|.$$

$$\leq 2\sqrt{n} \sum_{j=1}^{k-1} \sqrt{\sum_{x=1}^{n} |\alpha_{x,j}|^2} = 2(k-1)\sqrt{n}. \tag{2.19}$$

结合(2.17) 式, (2.18) 式, (2.19) 式, 可以得出

$$cn \leq 2(k-1)\sqrt{n} \implies k \geq \frac{c\sqrt{n}}{2} + 1 = \Omega(\sqrt{n}). \tag{2.20}$$

第 三 章　相位近似及其应用

§ 1　量子相位近似

定理 1.1 (谱分解) 设 M 是一个 $N \times N$ 的正规矩阵. 设 λ_j 是矩阵 M 的特征值, 而 $|\psi_j\rangle$ 是对应的特征向量, 那么有

$$M = \lambda_1 |\psi_1\rangle \langle\psi_1| + \cdots + \lambda_N |\psi_N\rangle \langle\psi_N| . \tag{1.1}$$

即

$$M = \sum_{k=1}^{N} \lambda_k |\psi_k\rangle \langle\psi_k| \tag{1.2}$$

证明 由于正规矩阵属于不同特征根的特征向量正交, 则对于任意的归一化向量 $|v\rangle$

$$M|v\rangle = \sum_{k=1}^{N} M \langle\psi_k|v\rangle |\psi_k\rangle = \sum_{k=1}^{N} \langle\psi_k|v\rangle \lambda_k |\psi_k\rangle = \sum_{k=1}^{N} \lambda_k |\psi_k\rangle \langle\psi_k|v\rangle .$$

□

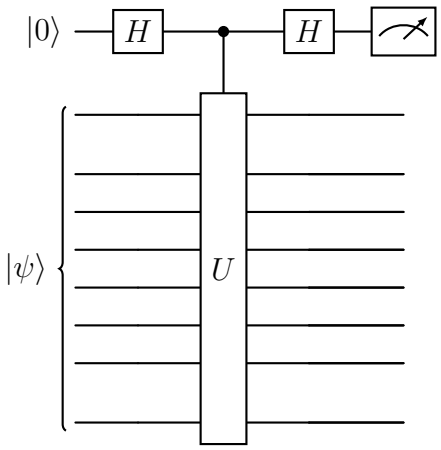
在相位估计问题中, 给定 n 个量子位的量子态 $|\psi\rangle$ 和作用在 n 个量子位上的量子电路. 假设 $|\psi\rangle$ 是该电路中酉矩阵 U 的特征向量, 目标是识别或近似其对应的特征值 λ.

由于是酉矩阵所以 λ 位于复数单位圆上, 可以写成 $\lambda = e^{2\pi i\theta}$, 其中 θ 是满足 $0 \leq \theta < 1$ 的唯一实数. 问题的目标是计算或近似这个实数 θ.

注 1.2 在相位估计问题中, 随着 $\theta = 0$ 到 $\theta = 1$, 也就是在单位圆上绕一圈. 因此, 当考虑近似的精确性时, 接近 $\theta = 1$ 的值应该被视为接近 $\theta = 0$. 例如, 若近似值为 $\theta = 0.999$, 则视为在 $\theta = 0$ 附近的 0.001 处.

1.1　低精度相位近似

解答这个问题, 先从一个简单版本开始, 考虑问题的低精度解:



量子电路 *1.1:* 低精度相位近

初始状态为

$$|\pi_1\rangle = |\psi\rangle|0\rangle, \tag{1.3}$$

通过第一个 H 门后:

$$|\pi_2\rangle = |\psi\rangle|+\rangle = \frac{1}{\sqrt{2}}|\psi\rangle|0\rangle + \frac{1}{\sqrt{2}}|\psi\rangle|1\rangle. \tag{1.4}$$

通过受控 U 门:

$$|\pi_3\rangle = \frac{1}{\sqrt{2}}|\psi\rangle|0\rangle + \frac{1}{\sqrt{2}}U|\psi\rangle|1\rangle. \tag{1.5}$$

根据假设 $|\psi\rangle$ 是 U 的特征向量, 且其特征值为 $\lambda = e^{2\pi i\theta}$, 进一步有:

$$|\pi_3\rangle = \frac{1}{\sqrt{2}}|\psi\rangle|0\rangle + \frac{e^{2\pi i\theta}}{\sqrt{2}}|\psi\rangle|1\rangle. \tag{1.6}$$

最后, 为了区分开 $|0\rangle$, $|1\rangle$ 对应的概率, 通过第二个 H 门, 状态变为:

$$|\pi_4\rangle = |\psi\rangle \otimes \left(\frac{1+e^{2\pi i\theta}}{2}|0\rangle + \frac{1-e^{2\pi i\theta}}{2}|1\rangle\right). \tag{1.7}$$

测量后会得到 0 和 1 的结果, 其概率分别为:

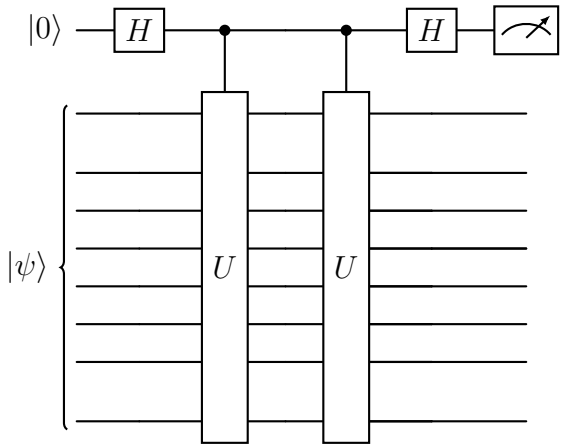
$$p_0 = \left|\frac{1+e^{2\pi i\theta}}{2}\right|^2 = \cos^2(\pi\theta), \tag{1.8}$$

$$p_1 = \left|\frac{1-e^{2\pi i\theta}}{2}\right|^2 = \sin^2(\pi\theta). \tag{1.9}$$

显然这个概率和为 1, 测量结果总是 0 时, $\theta = 0$. 而当测量结果总是 1 时, $\theta = 1/2$. 并且越接近这两个测量结果, 越可以知道 θ 的近似值. 因此, 虽然测量结果不能精确反映 θ 的值 (显然 p_0 和 p_1 取其它值的时候, 无法确定 θ 具体是什么), 但它确实提供了关于 θ 的一些信息.

1.2　二量子位相位近似

首先考虑两个受控 U 门的结果：



量子电路 *1.2:* 双相位

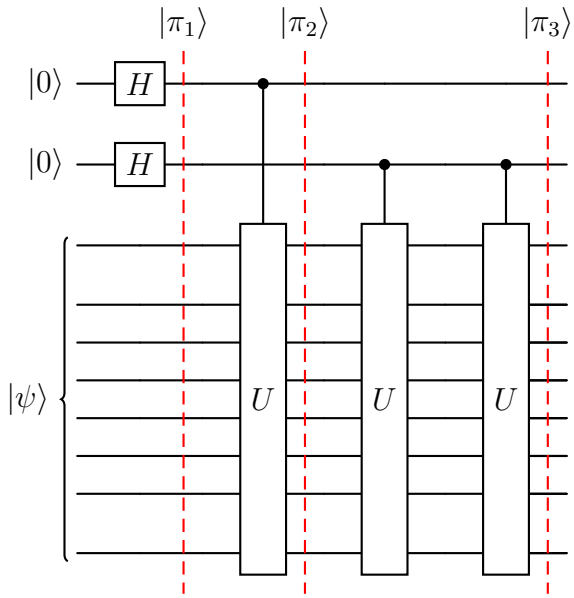
此时, 我们考虑的就是 U^2 的相位近似, 如果 $|\psi\rangle$ 是 U 的特征向量, 且其特征值为 $\lambda = e^{2\pi i\theta}$, 那么他也是 U^2 的特征向量, 对应特征值为 $\lambda = e^{2\pi i(2\theta)}$. 为此我们考虑结合双相位矩阵以及使用两个初始量子位, 这样的话或许可以获得更多关于目标 θ 的信息.

量子电路 1.3中后面的 H 门已被移除, 并且没有测量. 我们将随着探讨如何从电路中尽可能多地挖掘 θ 的信息来继续完善电路.

如果我们运行这个电路, 底部量子位的状态在整个电路中都会保持为 $|\psi\rangle$(由于这是特征向量), 相位将会被收集到顶部两个量子位的状态中.

$$|\pi_1\rangle = |\psi\rangle \otimes \frac{1}{2}\sum_{a_0=0}^{1}\sum_{a_1=0}^{1}|a_1a_0\rangle\,. \tag{1.10}$$

经过第一个受控 U 门, 当且仅当 $a_0 = 1$ 时生效, 而当 $a_0 = 0$ 时不生效.



量子电路 *1.3:* 双相位双量子位相位近似

$$|\pi_2\rangle = |\psi\rangle \otimes \frac{1}{2} \sum_{a_0=0}^{1} \sum_{a_1=0}^{1} e^{2\pi i a_0 \theta} |a_1 a_0\rangle . \tag{1.11}$$

第二和第三个受控 U 门的作用类似, 但变成了对 a_1 进行操作, 并将 θ 替换为 2θ. 可以将结果写成如下形式：

$$|\pi_3\rangle = |\psi\rangle \otimes \frac{1}{2} \sum_{a_0=0}^{1} \sum_{a_1=0}^{1} e^{2\pi i (2a_1 + a_0) \theta} |a_1 a_0\rangle . \tag{1.12}$$

令 $x = 2a_1 + a_0$, 我们可以将状态重新表达为：

$$|\pi_3\rangle = |\psi\rangle \otimes \frac{1}{2} \sum_{x=0}^{3} e^{2\pi i x \theta} |x\rangle . \tag{1.13}$$

我们的目标还是从这个状态中尽可能多地提取有关 θ 的信息. 考虑一个特殊情况, 假设 $\theta = \frac{y}{4}$, 其中 $y \in \{0, 1, 2, 3\}$. 换句话说, 我们有 $\theta \in \{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}\}$, 因此我们可以使用两个二进制位精确表示这些值, 分别为 00、01、10 和 11. 虽然一般情况下 θ 可能不是这四个值中的一个, 但通过考虑这一特殊情况, 我们可以了解如何最有效地提取这个值的信息.

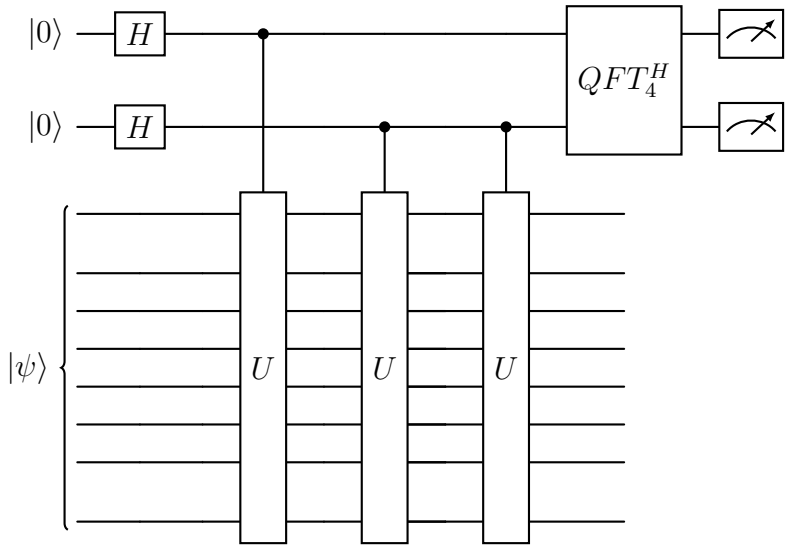
我们为每个可能的 $y \in \{0, 1, 2, 3\}$ 定义一个两量子位的状态向量：

$$|\phi_y\rangle = \frac{1}{2} \sum_{x=0}^{3} e^{2\pi i x \frac{y}{4}} |x\rangle . \tag{1.14}$$

写开就是：

$$\begin{aligned}
|\phi_0\rangle &= \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle + \frac{1}{2}|3\rangle, \\
|\phi_1\rangle &= \frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle - \frac{1}{2}|2\rangle - \frac{i}{2}|3\rangle, \\
|\phi_2\rangle &= \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle - \frac{1}{2}|3\rangle, \\
|\phi_3\rangle &= \frac{1}{2}|0\rangle - \frac{i}{2}|1\rangle - \frac{1}{2}|2\rangle + \frac{i}{2}|3\rangle.
\end{aligned} \tag{1.15}$$

容易验证这些向量是正交并且每个向量也是单位向量, 这意味着 $\{|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle\}$ 是一个正交且归一化的基, 因此存在一个测量可以完美区分它们.



量子电路 *1.4:* 双相位相位近似

为了使用量子电路进行这种区分, 可以选取酉矩阵 V, 使得:

$$\begin{aligned}
V|00\rangle &= |\phi_0\rangle, \\
V|01\rangle &= |\phi_1\rangle, \\
V|10\rangle &= |\phi_2\rangle, \\
V|11\rangle &= |\phi_3\rangle.
\end{aligned} \tag{1.16}$$

整理成矩阵形式:

$$V = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \tag{1.17}$$

由于这个矩阵还与四维离散傅里叶变换相关, 鉴于这一事实, 不妨称其为 QFT_4.

QFT_4 将标准态映射到上述四个可能的状态, 那此时我们也可以反向执行此操作, 将 $|\phi_0\rangle, \ldots, |\phi_3\rangle$ 转换为标准基态 $|0\rangle, \ldots, |3\rangle$. 也就是可以通过测量来确定哪个值 $y \in \{0,1,2,3\}$ 对应着 θ, 即 $\theta = \frac{y}{4}$.

也就是说, 如果有 $\theta = \frac{y}{4}$ $(y \in \{0,1,2,3\})$ 这样的限定条件, 之后运行此电路, 则进行测量前的量子态为 $|\psi\rangle|y\rangle$, 这里的 y 是二进制数字, 也就是说这个测量将毫无误差地得到 y 的值. 这个量子电路与前面的单量子位版本相比, 是一个明显的改进, 不过还是需要 θ 接近于 $\frac{y}{4}$, 才能得到较为准确的结果. 不过这提供了一个思路, 那就是可以通过增加更多的量子位, 来把 θ 分成更多份来实现更精确的近似.

自然的, 现在我们考虑 $U^{2^{m-1}}$ 门:

$$U^{2^{m-1}}|\psi\rangle = e^{2\pi i 2^{m-1}}|\psi\rangle.$$

也就是此时 $\theta = \frac{x_{m-1}}{2^{m-1}}$, 近似结果精准. 现在考虑初始使用 m 个量子位, 有:

$$\theta = \sum_{j=1}^{m} \frac{x_j}{2^j} = 0.x_1x_2\ldots x_m.$$

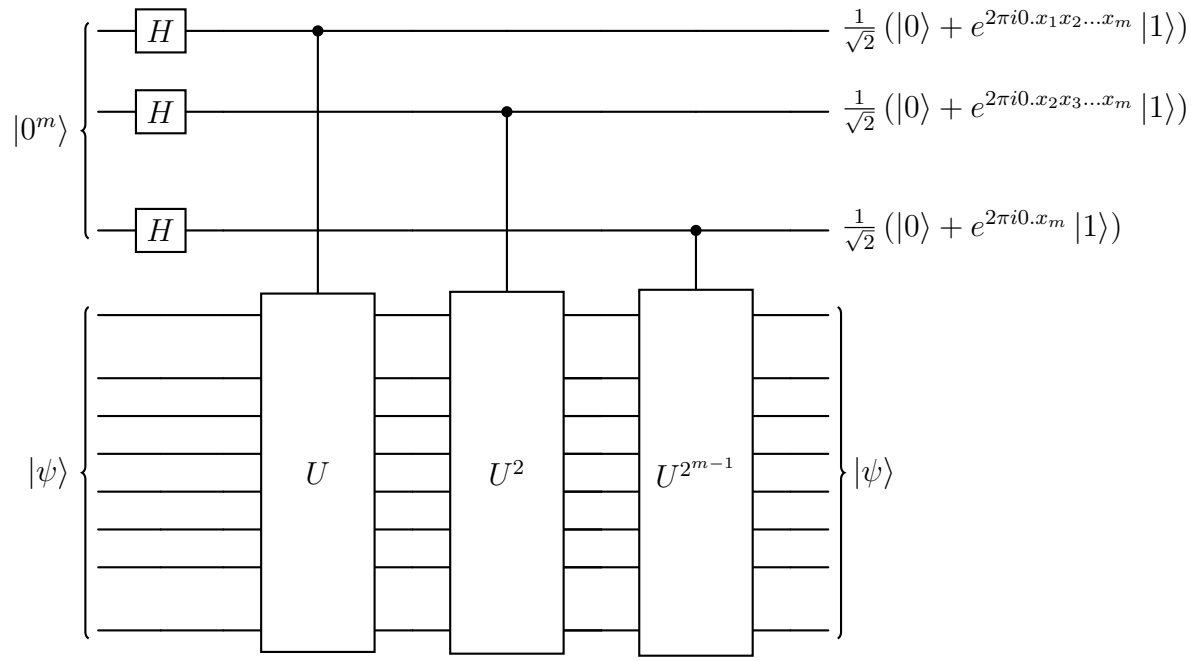
则

$$U^{2^k}|\psi\rangle = e^{2\pi i 2^k\theta} = e^{2\pi i 0.x_{k+1}x_{k+2}\ldots x_n}|\psi\rangle.$$

注意到, 输出的量子态为:

$$\begin{aligned}
&\bigotimes_{i=1}^{m} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\cdot 0.x_{m+1-i}\cdots x_m}|1\rangle\right) \\
&= \frac{1}{\sqrt{2^m}}(e^{\frac{2\pi i 2^{m-1}xy_{m-1}}{2^m}}|y_{m-1}\rangle + e^{\frac{2\pi i 2^{m-2}xy_{m-2}}{2^m}}|y_{m-2}\rangle + \cdots + e^{\frac{2\pi i x y_0}{2^m}}|y_0\rangle) \qquad (1.18)\\
&= \frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1} e^{\frac{2\pi i x y}{2^m}}|y\rangle.
\end{aligned}$$

这是我们所熟悉的形式, 看起来就像傅里叶变换的表达式, 所以我们来考虑量子傅立叶变换变换, 从而使用逆变换得到正交的标准基 $|x\rangle$ 从而通过测量得到对应的结果.



量子电路 *1.5:* 精确相位近似

§ 2　量子傅立叶变换

首先, 考虑一个 2^n 维数组 $\{x_j\}(j = 0, \cdots, 2^n - 1)$, 离散傅立叶变换 $\{y_k\}(k = 0, \cdots, 2^n - 1)$ 为:

$$y_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} x_j e^{\frac{2\pi ikj}{2^n}}. \tag{2.19}$$

实际上量子傅立叶变换算法相当于把这个数组整理成向量再规定归一化条件成为量子态, 这样就可以定义 N 维的量子傅里叶变换:

$$|\phi_y\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{\frac{2\pi ixy}{N}} |x\rangle \tag{2.20}$$

我们把 ϕ_y 当成矩阵的列, 则这个变换可以整理成一个 $N \times N$ 的矩阵:

$$QFT_N = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{\frac{2\pi ixy}{N}} |x\rangle \langle y| \tag{2.21}$$

下面是一些量子傅里叶变换矩阵：

$$QFT_1 = \begin{pmatrix} 1 \end{pmatrix}$$

$$QFT_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$QFT_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \frac{-1+i\sqrt{3}}{2} & \frac{-1-i\sqrt{3}}{2} \\ 1 & \frac{-1-i\sqrt{3}}{2} & \frac{-1+i\sqrt{3}}{2} \end{pmatrix}$$

$$QFT_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

特别的,QFT_2 也就是我们常用的 H 门. 下面来验证 QFT_N 是酉矩阵, 往证 $\{|\phi_0\rangle, \ldots, |\phi_{N-1}\rangle\}$ 是正交的.

$$\langle \phi_z | \phi_y \rangle = \frac{1}{N} \sum_{x=0}^{N-1} e^{\frac{2\pi i x(y-z)}{N}} \tag{2.22}$$

令 $\alpha = e^{\frac{2\pi i(y-z)}{N}}$, 原式变为 $\frac{1}{N}\sum_{x=0}^{N-1} \alpha^x$. 注意到:

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{N-1} = \begin{cases} \frac{\alpha^N - 1}{\alpha - 1}, & 若\alpha \neq 1 \\ N, & 若\alpha = 1 \end{cases} \tag{2.23}$$

特别地, 当 $\alpha = e^{\frac{2\pi i(y-z)}{N}}$, 且当 $y = z$ 时,$\alpha = 1$, 因此内积为：

$$\langle \phi_y | \phi_y \rangle = 1 \tag{2.24}$$

当 $y \neq z$ 时,$\alpha^N = 1$, 所以

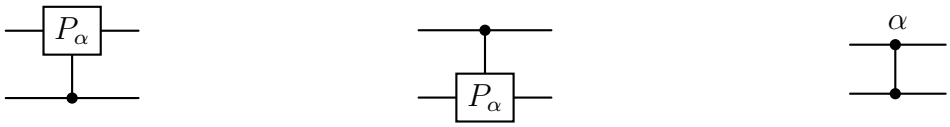
$$\langle \phi_z | \phi_y \rangle = 0 \tag{2.25}$$

这表明 $\{|\phi_0\rangle, \ldots, |\phi_{N-1}\rangle\}$ 是一个正交归一集, 因此 QFT_N 是酉矩阵.

为了在量子电路中实现量子傅里叶变换, 需要使用受控相位门, 形式如下：

$$P_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \tag{2.26}$$

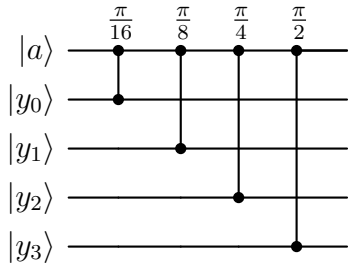
我们可以用这样的量子电路来表示受控相位门：



受控相位门可以实现如下变换:

$$|y\rangle\,|a\rangle \mapsto e^{\frac{2\pi iay}{2^m}}\,|y\rangle\,|a\rangle \tag{2.27}$$

其中 a 是某一个比特,$y \in \{0,\ldots,2^m-1\}$ 是一个用二进制表示的 m 位数字. 以 $m=5$ 为例, 有:



量子电路 *2.1:* 双相位相位近似

对 $m \geq 2$ 的情况下, 我们可以执行以下操作：

首先, 对底部 $m-1$ 个量子比特执行 2^{m-1} 维的量子傅里叶变换, 得到：

$$(QFT_{2^{m-1}}\,|x\rangle)\,|a\rangle = \frac{1}{\sqrt{2^{m-1}}}\sum_{y=0}^{2^{m-1}-1} e^{\frac{2\pi ixy}{2^{m-1}}}\,|y\rangle\,|a\rangle\,. \tag{2.28}$$

使用顶部量子比特作为控制位, 向其余 $m-1$ 个量子比特中的每个标准基态 $|y\rangle$ 加入相位, 得到：

$$\frac{1}{\sqrt{2^{m-1}}}\sum_{y=0}^{2^{m-1}-1} e^{\frac{2\pi ixy}{2^{m-1}}}e^{\frac{2\pi iay}{2^m}}\,|y\rangle\,|a\rangle\,. \tag{2.29}$$

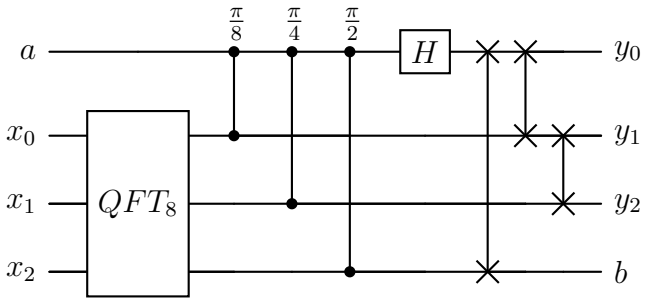
顶部量子比特执行 H 门, 为了方便表示可以写作:

$$\frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^{m-1}-1}\sum_{b=0}^{1}(-1)^{ab}e^{\frac{2\pi ixy}{2^{m-1}}}e^{\frac{2\pi iay}{2^m}}\,|y\rangle\,|b\rangle\,. \tag{2.30}$$

对量子比特的顺序进行重排：

$$\frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^{m-1}-1} \sum_{b=0}^{1} (-1)^{ab} e^{\frac{2\pi i x y}{2^{m-1}}} e^{\frac{2\pi i a y}{2^m}} |b\rangle |y\rangle . \tag{2.31}$$

接下来我们举一个 $N = 2^4$ 的例子:



量子电路 *2.2:* 双相位相位近似

这种实现方法实际上就是经典的快速傅里叶变换算法在量子电路中的实现, 在这里可能会有这样的疑问, 为什么要使用控制相位门, 进行迭代的操作, 而不是直接用 QFT 矩阵. 这和前面提到过的通用量子门集有关, 不是所有的酉矩阵都可以方便的拿来作为量子门的, 通常还是习惯使用通用量子门, 这和硬件是有关系的.