

量子计算 —算法篇

Quantum Computer

网址: www.qubits.top

作者: Calvin Tang

邮箱: 179209347@qq.com

介绍

教程简介：

- 面向对象：量子计算初学者
- 依赖课程：线性代数，解析几何，量子力学（非必需）

知乎专栏：

https://www.zhihu.com/column/c_1501138176371011584

Github & Gitee 地址：

<https://github.com/mymagicpower/quantum>

<https://gitee.com/mymagicpower/quantum>

* 版权声明：

- 仅限用于个人学习，或者大学授课使用
（大学授课如需ppt原件，请用学校邮箱联系我获取）
- 禁止用于任何商业用途

搜索算法

遍历搜寻问题的任务是从一个海量元素的无序集合中，找到满足某种要求的元素。因为这些元素并没有按要求进行有序的排列，并且数量又很大。在经典算法中，只能按逐个元素试下去，这也正是“遍历搜寻”这一名称的由来，一般情况下，算法复杂度为 $O(N)$ ， N 为数据规模。

而量子计算机中存在着量子搜索算法，也称为Grover算法，它的时间复杂度是 $O(\sqrt{N})$ 。在数据规模较大的情况下，量子搜索算法的优越性非常明显。

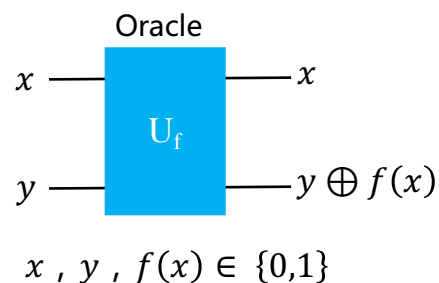
问题定义：

$f: \{0, 1, 2, 3, \dots, N-1\} \rightarrow \{0, 1\}$

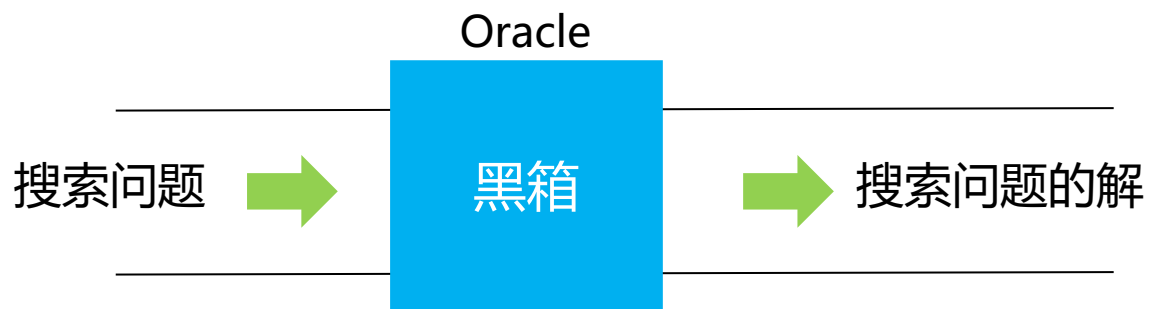
找到 $f(x)=1$ 的 x

Oracle的理解

- oracle 是一个酉算子，也就是线性代数里的矩阵，一般用 O 来表示
- oracle 的作用就是对量子状态做一个酉变换
- 可以识别搜索问题的解



$$|x\rangle |q\rangle \xrightarrow{\text{Oracle}} |x\rangle |q \oplus f(x)\rangle$$



通过Oracle，我们可以实现，当搜索问题的索引为我们的目标结果时，结果寄存器将翻转；反之结果寄存器值不变，从而我们可以通过判定结果寄存器的值，来确定搜索的时候对象是否是我们的目标值。

Grover 搜索算法介绍

首先，先化简一下搜索模型，将所有数据存在数据库中，假设有 n 个量子比特，用来记录数据库中的每一个数据的索引，一共可以表示 2^n 个数据，记为 N 个，希望搜索得到的数据有 M 个，为了表示一个数据是否是搜索的结果，建立一个函数：

$$f(x) \begin{cases} 0 & (x \neq x_0) \\ 1 & (x = x_0) \end{cases}$$

其中 x_0 为搜索目标的索引值，也即是说，当搜索到目标时，函数值 $f(x)$ 值为 1，如果搜索的结果不是目标时， $f(x)$ 值为 0。

假设有一个量子 Oracle 可以识别搜索问题的解，是别的结果通过 Oracle 的一个量子比特给出。可以将 Oracle 定义为：

$$|x\rangle |q\rangle \xrightarrow{\text{Oracle}} |x\rangle |q \oplus f(x)\rangle$$

其中 $|q\rangle$ 是一个结果寄存器， \oplus 是二进制加法。通过 Oracle 可以实现，当搜索的索引为目标结果时，结果寄存器翻转；反之，结果寄存器值不变；从而可以通过判断结果寄存器的值，来确定搜索的对象是否为目标值。

本源量子：<<量子计算与编程入门>>

Grover 搜索算法介绍 - 构造叠加态

假设被查找的集合为： $\{|x\rangle\} = \{|0\rangle, |1\rangle, \dots, |N-1\rangle\}$ ，在开始查找之前，要对系统进行初始化，即对每一个qubit 初态进行Hadamard 变换，使之处于

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \quad \leftarrow \quad (H|0\rangle)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

参考D-J算法章节推导过程

Grover 搜索算法介绍

同D-J算法类似，先讲初态制备在 $|0\rangle^{\otimes n} |1\rangle$ 态上， $|0\rangle^{\otimes n}$ 为查询寄存器， $|1\rangle$ 为结果寄存器。经过 Hardmard 门操作后，可以将查询寄存器的量子态，变为所有结果的叠加态；也即是说，经过了 Hardmard 门，就可以得到所有结果的索引，而结果寄存器则变为 $\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$ ，再使其通过 *Oracle*，可以对每一个索引都进行一次检验，如果是目标结果，则将答案寄存器的量子态进行 0、1 翻转，即答案寄存器变为：

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

而查询寄存器不变，但当检验的索引不是结果时，寄存器均不发生改变。因此，*Oracle* 可以换一种表示方式：

$$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{\text{Oracle}} (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

其中， $|x\rangle$ 是查询寄存器的等额叠加态中的一种情况。

如上述所知，*Oracle* 的作用，是通过改变了解的相位，标记了搜索问题的解。

Grover 搜索算法介绍

现在，将搜索问题的解通过相位标记区分出来，那么如何能够将量子态的末态变为已标记出的态呢？将问题换一种思路进行考虑，当查询寄存器由初态经过 Hardmard 门后，会变为所有可能情况的等额叠加态，也就是说，它包含着所有搜索问题的解与非搜索问题的解。可以将这个态标记为：

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = \frac{1}{\sqrt{N}} \sum_{\substack{j=0 \\ (j=x)}}^{N-1} |j\rangle + \frac{1}{\sqrt{N}} \sum_{\substack{i=0 \\ (i \neq x)}}^{N-1} |i\rangle = |\beta\rangle + |\alpha\rangle$$

将所有非搜索问题的解定义为一个量子态 $|\alpha\rangle$ ，搜索问题的解定义为一个量子态 $|\beta\rangle$ 。

假设有 M 个解，则：

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_x |x\rangle \quad |\beta\rangle = \frac{1}{\sqrt{M}} \sum_x |x\rangle$$

显然， $|\beta\rangle$ 为最终的量子态，而且 $|\alpha\rangle$ 和 $|\beta\rangle$ 相互正交。利用简单的代数运算，就可以将初态 $|\psi\rangle$ 重新表示为：

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$$

本源量子：<<量子计算与编程入门>>

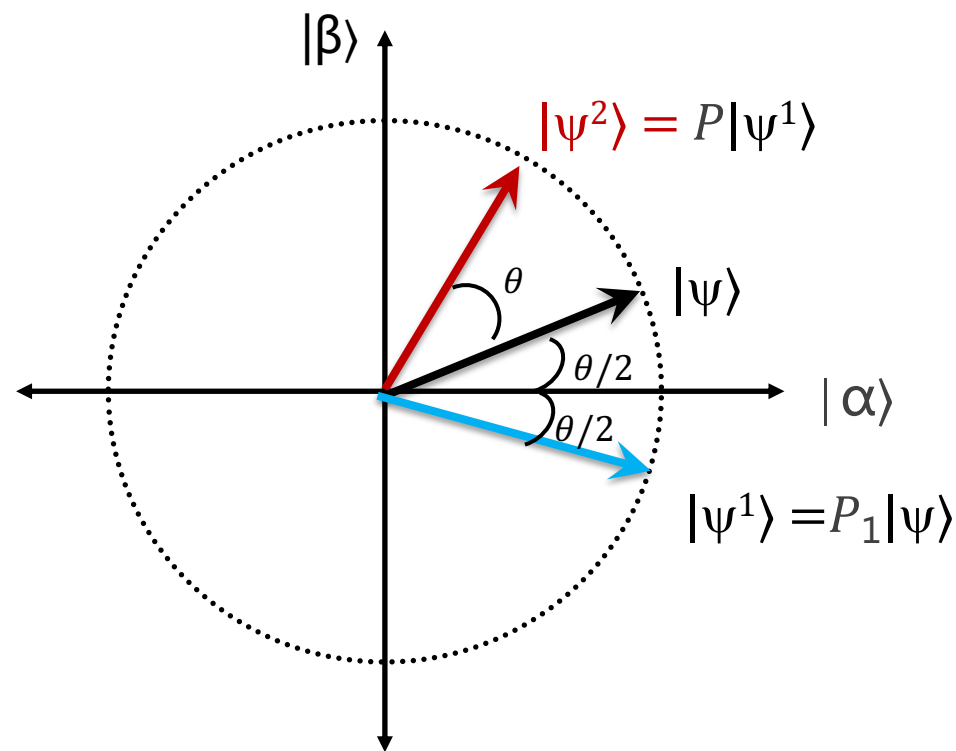
Grover 搜索算法介绍

初始态被搜索问题的解的集合和非搜索问题的解的集合重新定义，也就是说，初态属于 $|\alpha\rangle$ 与 $|\beta\rangle$ 张成的空间。因此，可以用平面向量来表示这三个量子态，如图：

那么，Oracle 作用在新的表示方法下的初态会产生怎样的影响呢？

Oracle 的作用是用负号标记搜索问题的解，所以，相当于将 $|\beta\rangle$ 内每一个态前均增加一个负号，将所有的负号提取出来，可以得到：

$$|\psi\rangle \xrightarrow{\text{Oracle}} \sqrt{\frac{N-M}{N}} |\alpha\rangle - \sqrt{\frac{M}{N}} |\beta\rangle$$



Grover 搜索算法介绍

对应在平面向量中，相当于将 $|\psi\rangle$ 做关于 $|\alpha\rangle$ 轴的对称（**相位翻转**），但仅有这一种操作是无法将量子态从 $|\psi\rangle$ 变为 $|\beta\rangle$ ，还需要另一种对称操作（**镜像翻转**）。

第二种对称操作，是将量子态关于 $|\psi\rangle$ 对称的操作，这个操作由三个部分构成：

1. 将量子态经过一个 Hardmard 门
2. 对量子态进行一个相位变换，将 $|0\rangle^{\otimes n}$ 态的系数保持不变，将其他的量子态的系数增加一个负号，相当于 $2|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I$ 酉变换算子；
3. 再经过一个 Hardmard 门。

这三步操作的数学表述为：

$$H^{\otimes n}(2|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I_n)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 \\ \dots \\ \dots \\ 1 \end{bmatrix}$$

本源量子：<<量子计算与编程入门>>

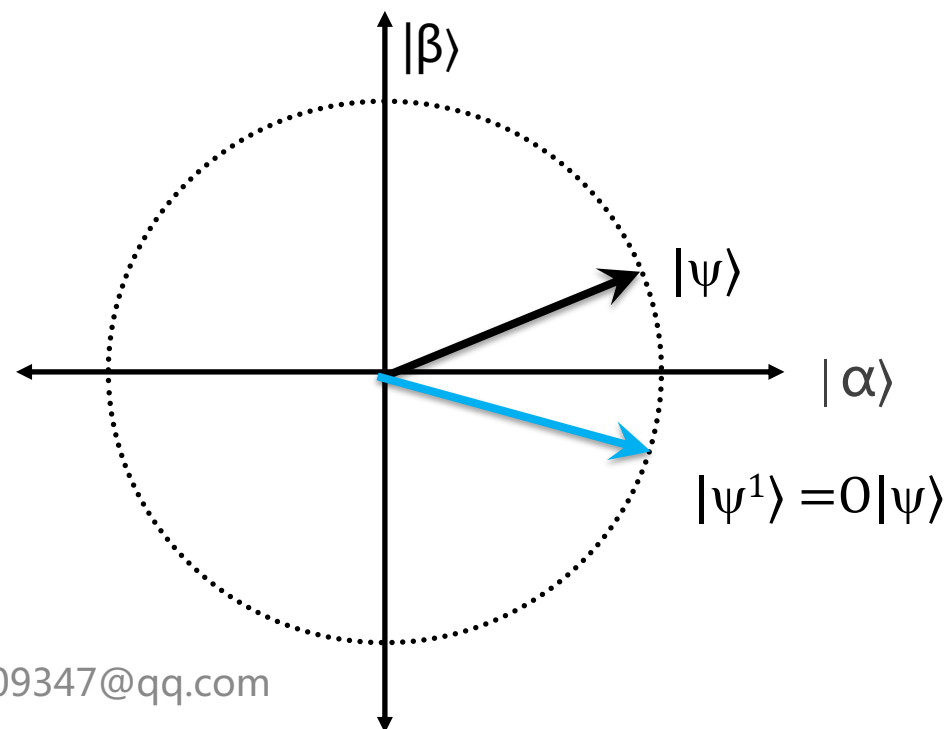
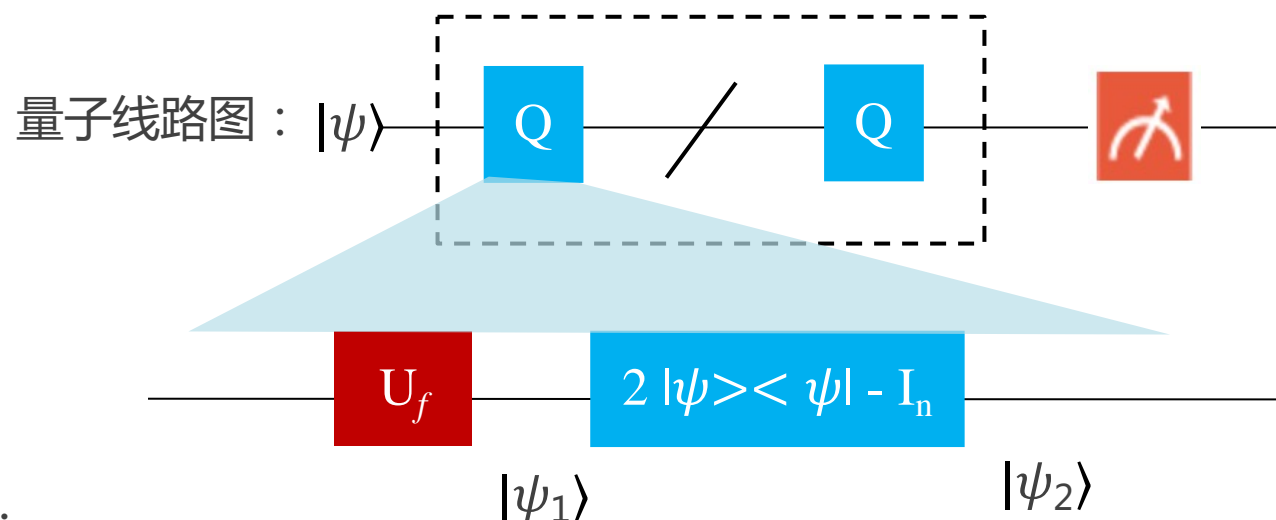
振幅放大 - 实现指定态的相位翻转（镜像）

指定态的**相位翻转**算子：

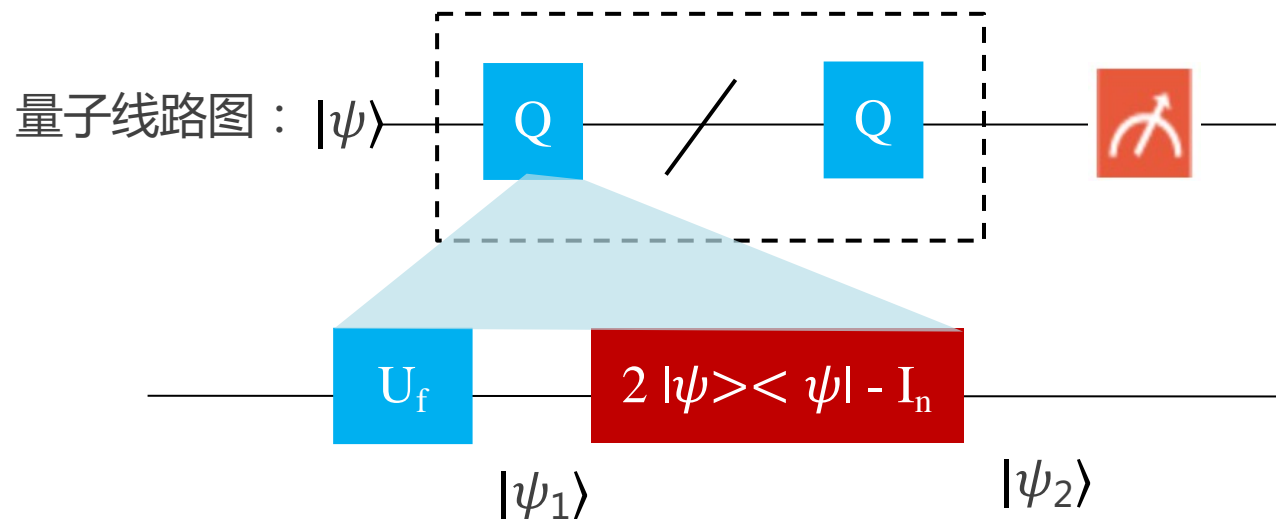
$$O = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix}$$

O 为关于横轴 $|\alpha\rangle$ 做镜像，那么 $\theta/2 = 0$ 所以有：

$$O = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



振幅放大 - 镜像翻转



➤ 振幅放大算子：

$$P = 2|\psi\rangle\langle\psi| - I$$

P 为关于 $|\psi\rangle$ 做**镜像翻转**，所以有：

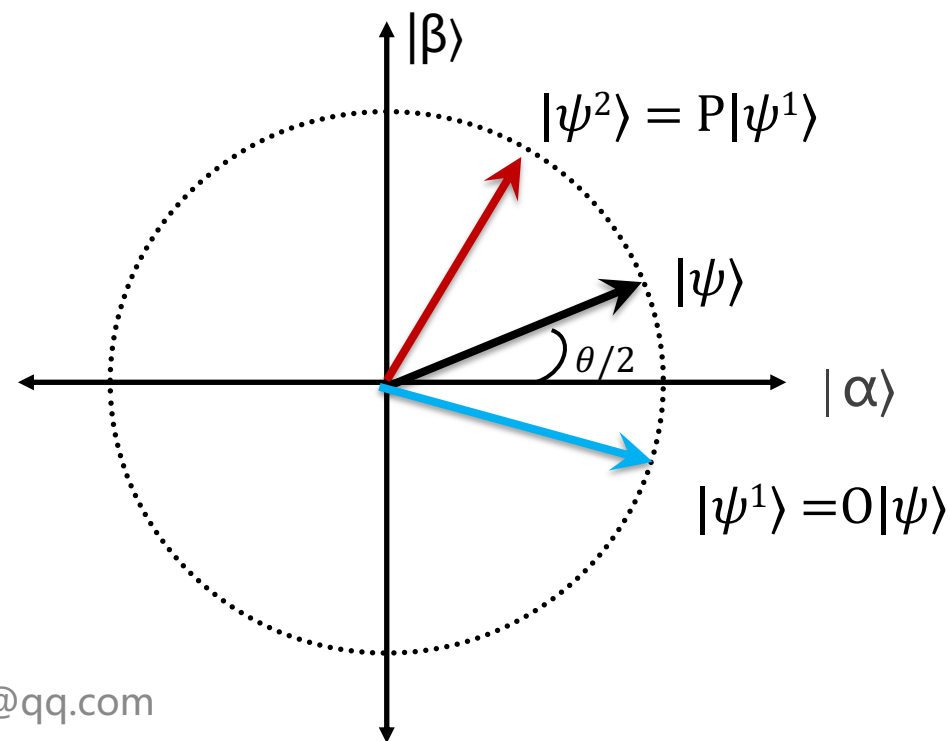
$$P = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix}$$

➤ 振幅放大算子：

$$G = PO$$

$$G = PO = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$



Grover 搜索算法介绍

前面介绍的两种对称操作，合在一起称为一次 Grover 迭代。假设初态 $|\psi\rangle$ 与 $|\alpha\rangle$ 可以表示为：

$$|\psi\rangle = \cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle$$

很容易得到：

$$\cos \frac{\theta}{2} = \sqrt{\frac{N-M}{N}} \quad \sin \frac{\theta}{2} = \sqrt{\frac{M}{N}}$$

由此可知在 $\{|\alpha\rangle, |\beta\rangle\}$ 张成的空间中算子 Q 可以表示为：

$$Q = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \text{ (让向量逆时针旋转 } \theta \text{)}$$

实质上可以视为一个角度为 θ 的旋转量子门（RY(θ) 门）操作。

算子 G - 性质

两角和与差的三角函数公式：

$$\begin{aligned}\sin(\alpha \pm \beta) &= \sin \alpha \cos \beta \pm \cos \alpha \sin \beta \\ \cos(\alpha \pm \beta) &= \cos \alpha \cos \beta \mp \sin \alpha \sin \beta\end{aligned}$$

$$G = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

$$\begin{aligned}G^2 &= \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} = \begin{bmatrix} \cos^2(\theta) - \sin^2(\theta) & -2\cos(\theta)\sin(\theta) \\ 2\cos(\theta)\sin(\theta) & \cos^2(\theta) - \sin^2(\theta) \end{bmatrix} \\ &= \begin{bmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{bmatrix}\end{aligned}$$

$$\begin{aligned}G^3 &= \begin{bmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{bmatrix} \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \\ &= \begin{bmatrix} \cos(2\theta)\cos(\theta) - \sin(2\theta)\sin(\theta) & -\cos(2\theta)\sin(\theta) - \sin(2\theta)\cos(\theta) \\ \sin(2\theta)\cos(\theta) + \cos(2\theta)\sin(\theta) & -\sin(2\theta)\sin(\theta) + \cos(2\theta)\cos(\theta) \end{bmatrix} \\ &= \begin{bmatrix} \cos(3\theta) & -\sin(3\theta) \\ \sin(3\theta) & \cos(3\theta) \end{bmatrix}\end{aligned}$$

....

$$G^n = \begin{bmatrix} \cos(n\theta) & -\sin(n\theta) \\ \sin(n\theta) & \cos(n\theta) \end{bmatrix}$$

矩阵几何意义：

每次作用于向量，相当于将向量逆时针旋转 θ

Grover 搜索算法介绍

可以从几何图像上看到，每一次 Grover 迭代，可以使量子态逆时针旋转 θ ，经历了 k 次 Grover 迭代，末态的量子态为：

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

选取合适的旋转次数 k 使得 $\sin^2\left(\frac{2k+1}{2}\theta\right)$ 最接近 1 即可完成振幅放大量子线路。
相比经典的遍历分类方法，振幅放大量子线路可以充分体现量子计算的优势。

Grover 搜索算法介绍 - 迭代的次数 R

因此，经过多次迭代操作，总可以使末态在 $|\beta\rangle$ 态上概率很大，满足精确度的要求。

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle - \sqrt{\frac{M}{N}} |\beta\rangle \quad G^k |\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right) |\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right) |\beta\rangle$$

其中 N 是确定的，不能更改，关键就在于 M ，先假设我们已经知道有 M 个 i 使得 $f(i) = 1$ ，

$$\cos \frac{\theta}{2} = \sqrt{\frac{N-M}{N}} \quad \sin \frac{\theta}{2} = \sqrt{\frac{M}{N}}$$

当我们需要搜索的值个数 M 远小于搜索空间 N 时：

$$\sqrt{\frac{M}{N}} = \sin \frac{\theta}{2} \approx \frac{\theta}{2}$$

当 θ 越小时，我们得到的搜索结果越准确。

$$\frac{2k+1}{2}\theta < \frac{\pi}{2}$$



$$k < \frac{\pi}{2\theta} - \frac{1}{2} \approx \frac{\pi}{4} \sqrt{\frac{N}{M}} - \frac{1}{2}$$



迭代的次数 R 满足：

$$R \leq \frac{\pi}{4} \sqrt{\frac{N}{M}}$$

Grover算法量子线路

Grover算法量子线路其实也就两个部分：

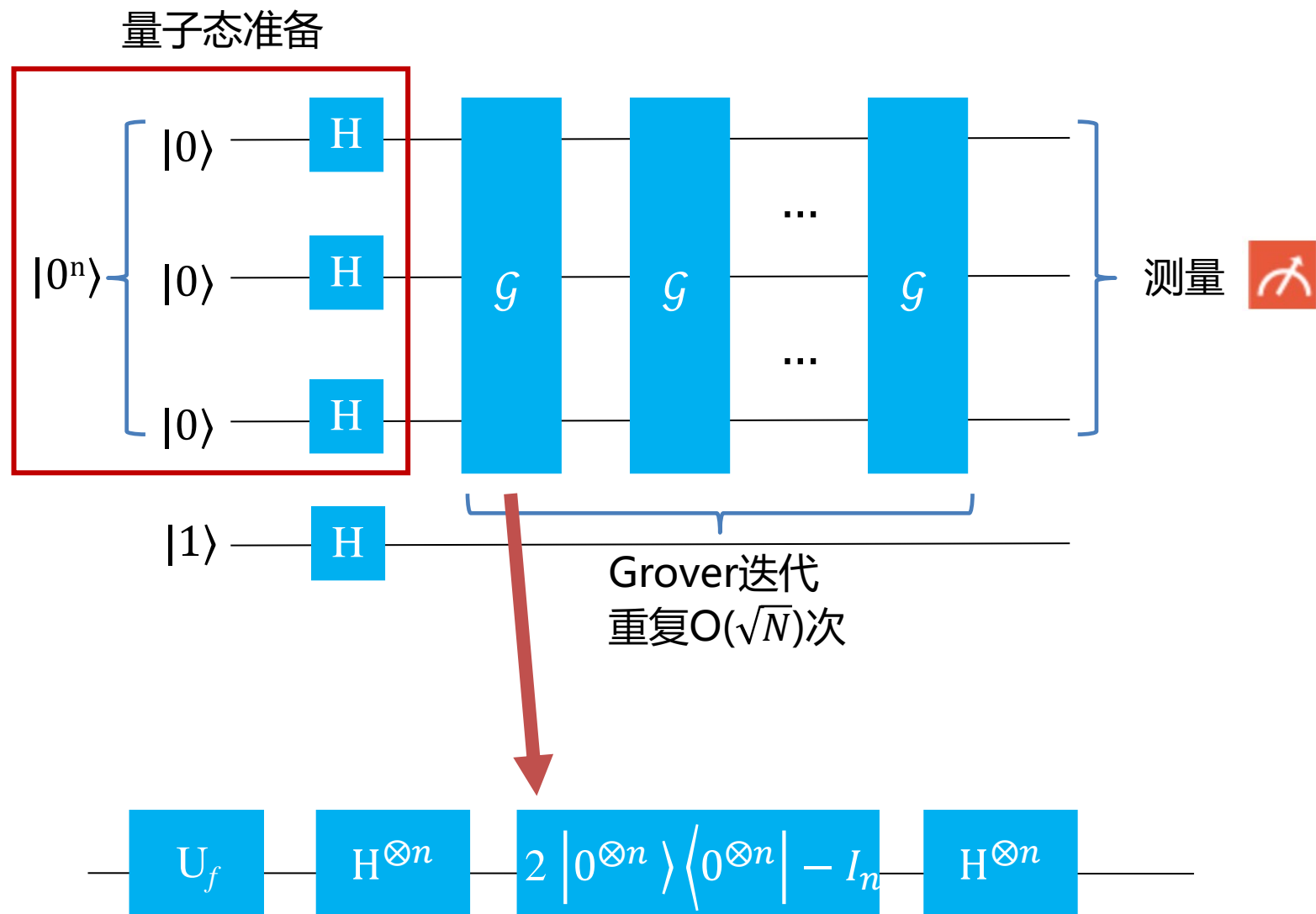
- 一个是量子态准备
- 另一个是多次Grover迭代

而每一次的Grover迭代，也可以分为两个部分：

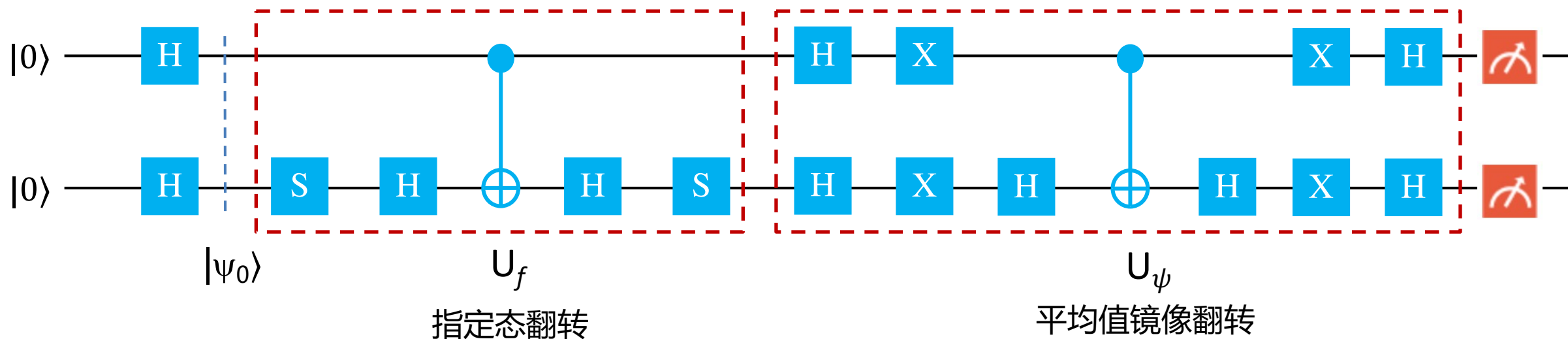
- 一部分是指定态翻转 U_f ，这部分是为了实现指定态的相位翻转
- 另一部分 - 平均值翻转



Grover diffusion operator，或者叫它 Inversion about the mean。



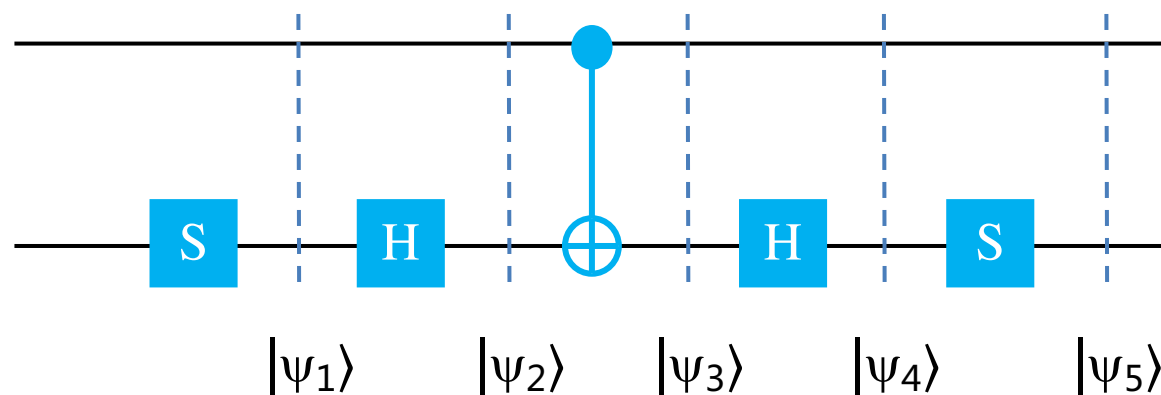
Grover算法量子线路 - 两比特例子



初态制备：

$$|\psi_0\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

指定态翻转 U_f - 两比特例子



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

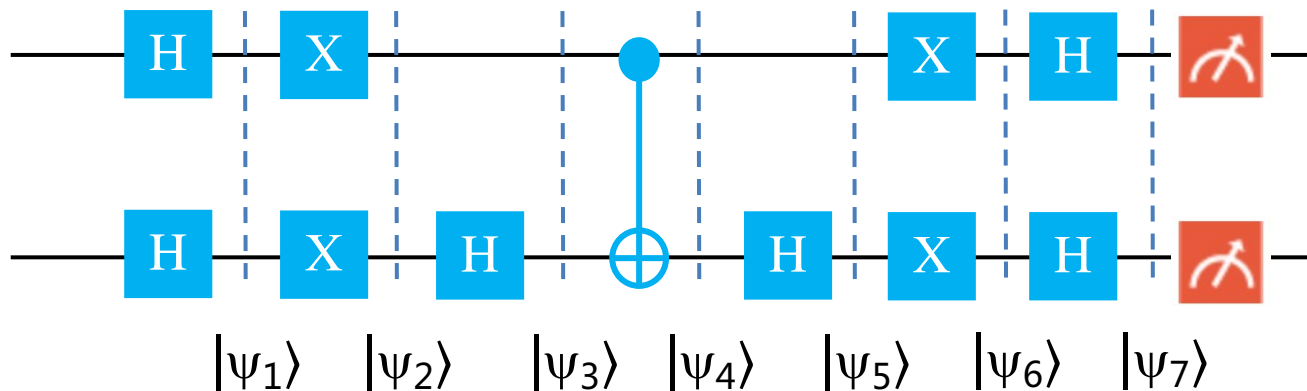
$$|\psi_2\rangle = \frac{\sqrt{2}}{4} ((1+i)|00\rangle + (1-i)|01\rangle + (1+i)|10\rangle + (1-i)|11\rangle)$$

$$|\psi_3\rangle = \frac{\sqrt{2}}{4} ((1+i)|00\rangle + (1-i)|01\rangle + (1-i)|10\rangle + (1+i)|11\rangle)$$

$$|\psi_4\rangle = \frac{1}{2} (|00\rangle + i|01\rangle + |10\rangle - i|11\rangle)$$

$$|\psi_5\rangle = \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle + |11\rangle)$$

平均值镜像翻转 U_ψ - 两比特例子



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

$$|\psi_2\rangle = \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle + |11\rangle)$$

$$|\psi_3\rangle = \frac{\sqrt{2}}{2} (|01\rangle + |10\rangle)$$

$$|\psi_4\rangle = \frac{\sqrt{2}}{2} (|01\rangle + |11\rangle)$$

$$|\psi_5\rangle = \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

$$|\psi_6\rangle = \frac{1}{2} (-|00\rangle + |01\rangle - |10\rangle + |11\rangle)$$

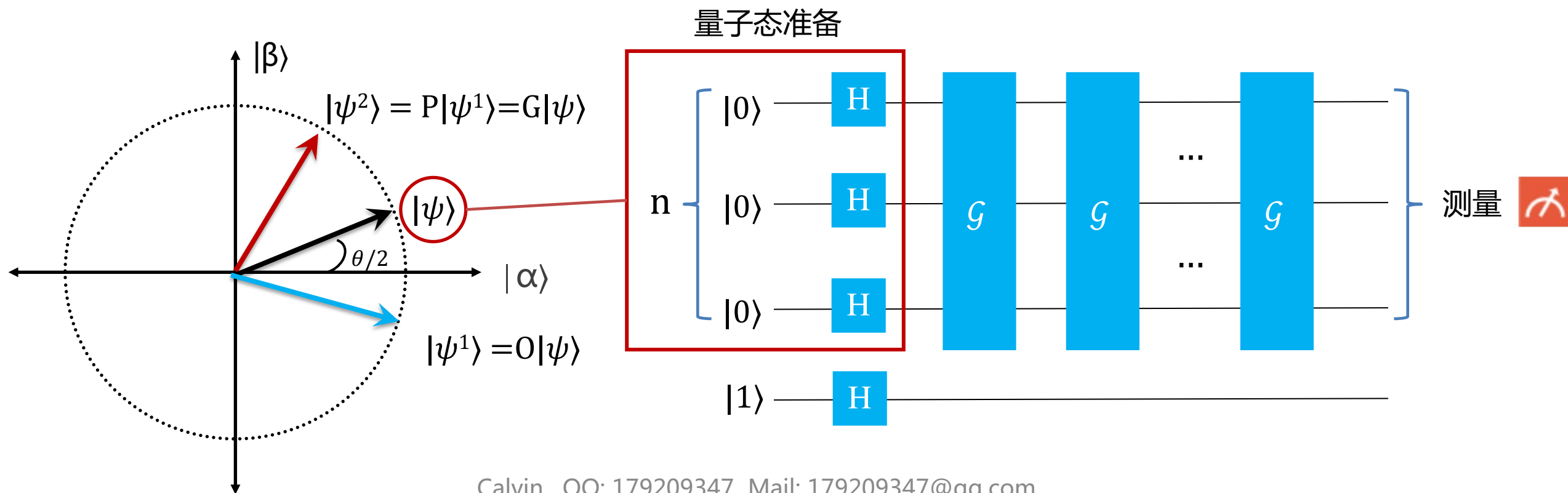
$$|\psi_7\rangle = -|01\rangle$$

Grover算法量子线路 – 初态制备

1、首先，假设假设Grover迭代单元的输入是很多态的均匀叠加，如下图所示：

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \leftarrow (H|0\rangle)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

参考D-J算法章节推导过程



Grover算法量子线路 - 实现指定态（想要搜索的态）的相位翻转

为了将我们需要寻找的数据和其他的数据分开，此时需要**构造一个Oracle**，将目标值变换相位，也就是增加一个负号，即：

$$O_{\omega}|x\rangle = \begin{cases} |x\rangle & (x \neq \omega) \\ -|x\rangle & (x = \omega) \end{cases}$$

两量子比特的矩阵形式：

这里我们需要找的是 $|10\rangle$ ，发现构成该矩阵的行和列都是对应的向量。

$$O_{\omega} = \begin{matrix} & \begin{matrix} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{matrix} \\ \begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{matrix}$$

Grover算法量子线路 - 实现指定态（想要搜索的态）的相位翻转

$f(x) = 1$ 时变号，等于 0 时不变，则：

$$O_{\omega}|x\rangle = \begin{cases} |x\rangle & (x \neq \omega) \\ -|x\rangle & (x = \omega) \end{cases} = (-1)^{f(x)} |x\rangle$$

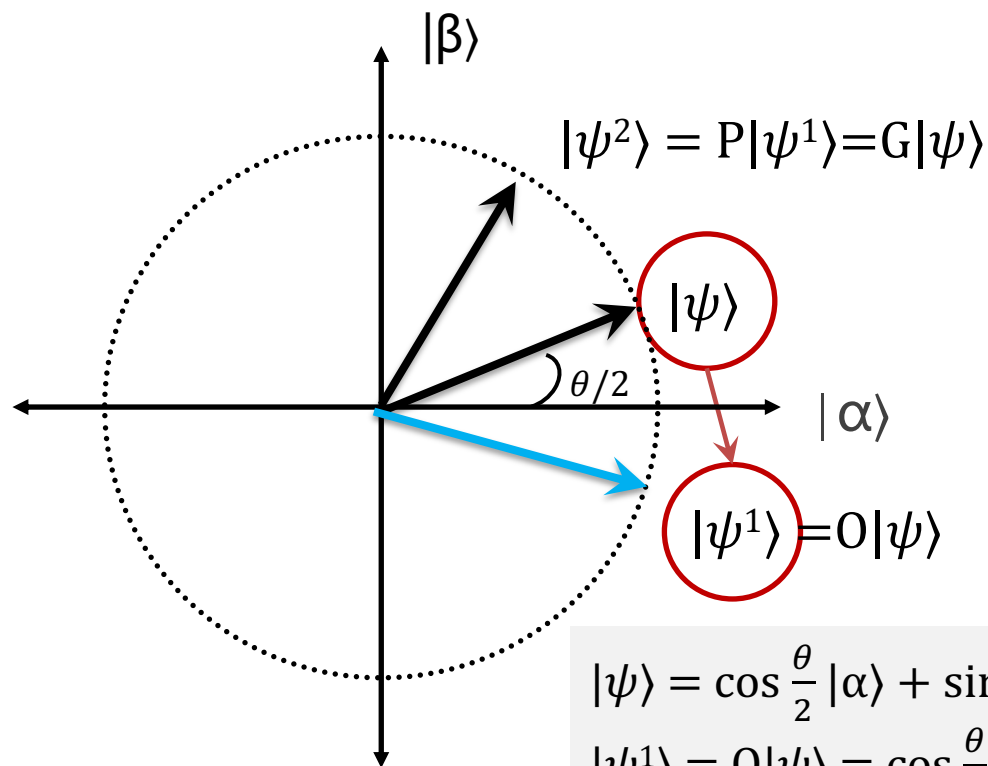
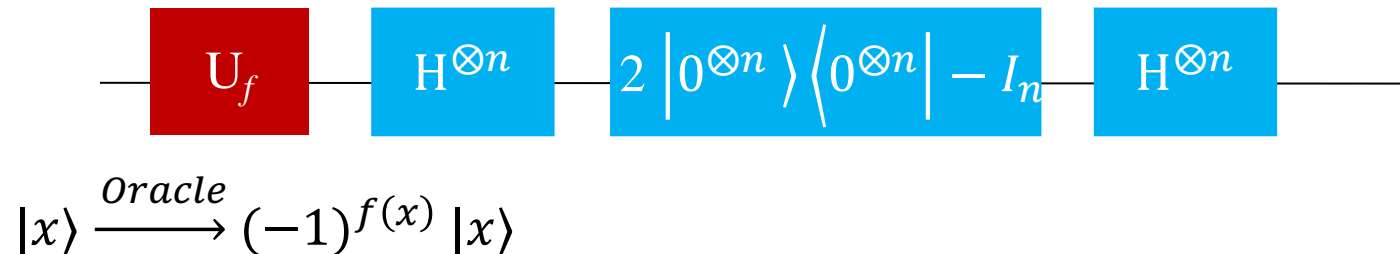
$$O_{\omega} = I - 2|x\rangle\langle x|$$

O_{ω} 矩阵形式：

$$O_{\omega} = \begin{bmatrix} (-1)^{f(0)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & (-1)^{f(2^n)} \end{bmatrix}$$

Grover算法量子线路 - 实现指定态（想要搜索的态）的相位翻转

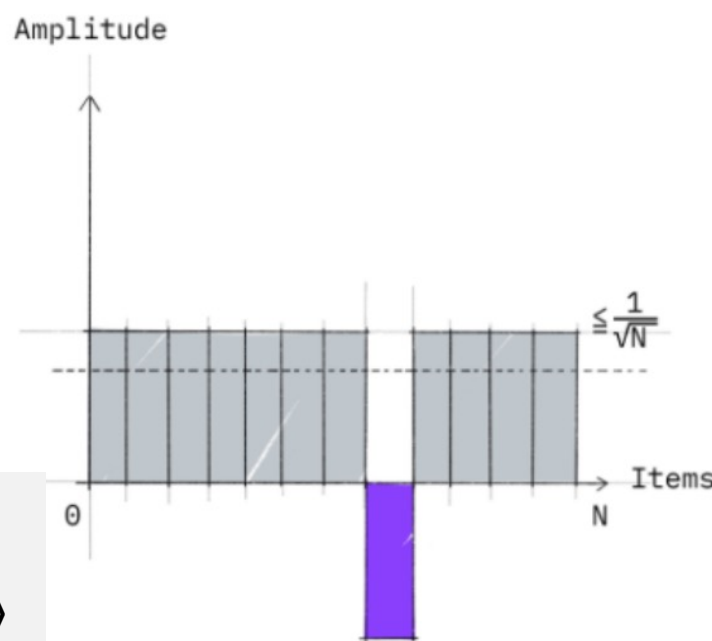
2、然后，我们可以通过 U_w 的作用，把想要搜索的态的幅值翻转过来，其他正交的态不变。然后可以得到下图的效果：



$$|\psi\rangle = \cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle$$

$$|\psi^1\rangle = O|\psi\rangle = \cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle$$

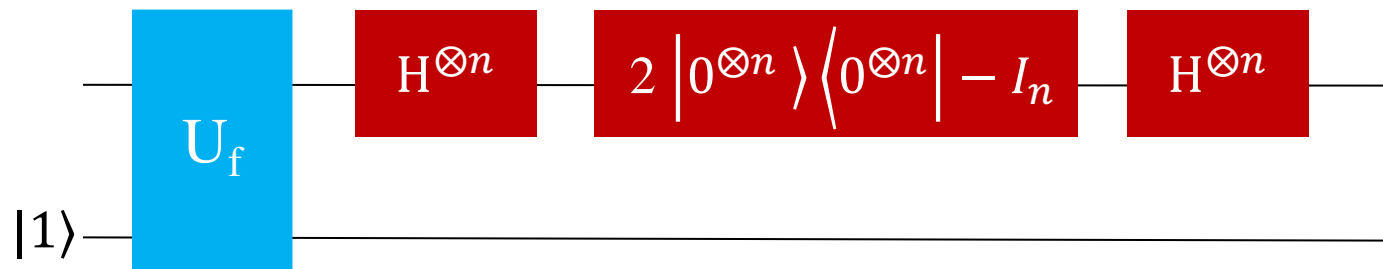
使用 O 算符作用之后，我们得到的结果为：



其中虚线代表振幅的平均值，相位变换以后，显然，振幅的平均值下降了一些。

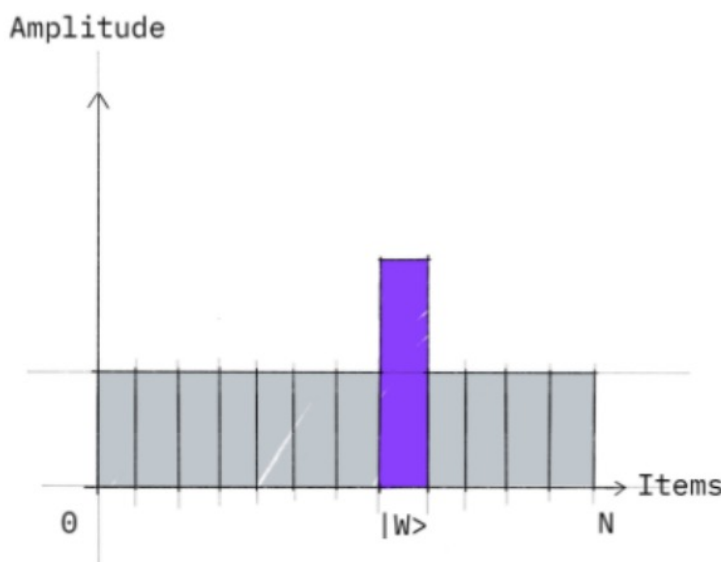
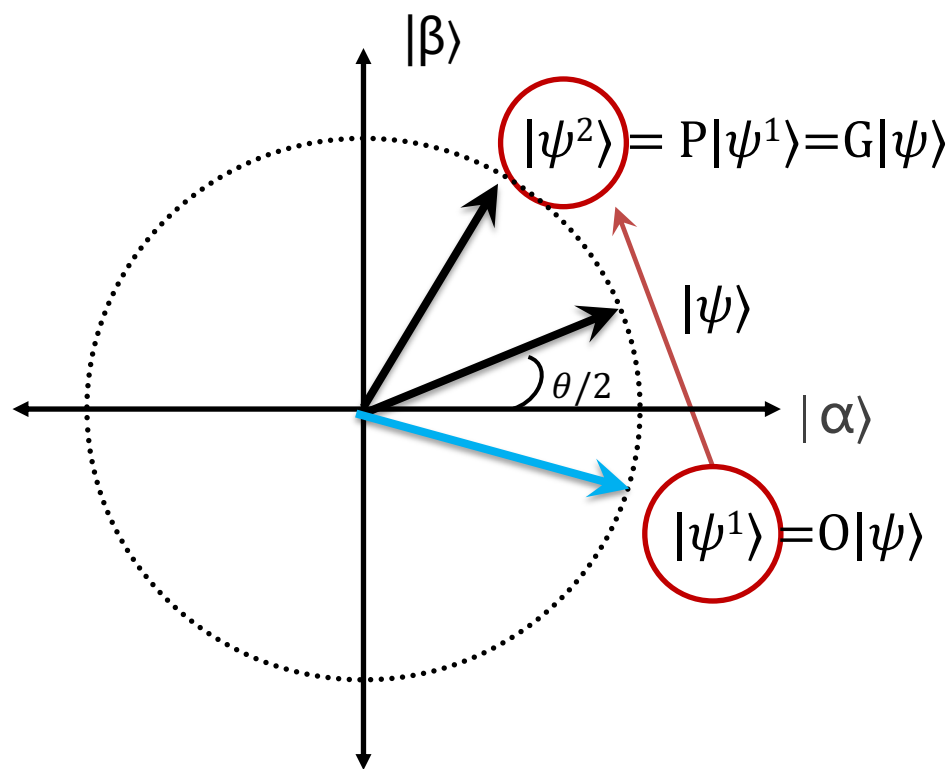
Grover算法量子线路 - 镜像翻转

3、最后，可以根据各个基态的幅值计算出均值，然后按照这个均值镜像翻转各个基态的幅值，就可以得到如下图所示的结果。



$$H^{\otimes n}(2|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I_n)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$$

$P = 2|\psi\rangle\langle\psi| - I$, $|\psi\rangle\langle\psi|$, 全1矩阵, 系数 $1/N$ 可用来计算均值



可以直观发现，通过上面三个步骤，**目标态的幅值增大了**。事实上，使用Grover迭代一定次数，目标态的幅值可以比较接近1。然后进行测量，可以大概率地测量到目标态，也就是说搜索到了目标态。

Grover算法量子线路 - 镜像翻转

$$|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$$

$$|\psi^1\rangle = O|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle - \sin\frac{\theta}{2}|\beta\rangle$$

$$P = 2|\psi\rangle\langle\psi| - I$$

$$= 2(\cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle)(\cos\frac{\theta}{2}\langle\alpha| + \sin\frac{\theta}{2}\langle\beta|) - I$$

$$= 2\cos\frac{\theta}{2}\cos\frac{\theta}{2}|\alpha\rangle\langle\alpha| + 2\cos\frac{\theta}{2}\sin\frac{\theta}{2}|\alpha\rangle\langle\beta| + 2\sin\frac{\theta}{2}\cos\frac{\theta}{2}|\beta\rangle\langle\alpha| + 2\sin\frac{\theta}{2}\sin\frac{\theta}{2}|\beta\rangle\langle\beta| - I$$

$$|\psi^2\rangle = P|\psi^1\rangle = P(\cos\frac{\theta}{2}|\alpha\rangle - \sin\frac{\theta}{2}|\beta\rangle)$$

$$= 2\cos\frac{\theta}{2}\cos\frac{\theta}{2}\cos\frac{\theta}{2}|\alpha\rangle\langle\alpha|\alpha\rangle + 2\cos\frac{\theta}{2}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|\alpha\rangle\langle\beta|\alpha\rangle + 2\sin\frac{\theta}{2}\cos\frac{\theta}{2}\cos\frac{\theta}{2}|\beta\rangle\langle\alpha|\alpha\rangle + 2\sin\frac{\theta}{2}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|\beta\rangle\langle\beta|\alpha\rangle - \cos\frac{\theta}{2}|\alpha\rangle$$

$$- 2\cos\frac{\theta}{2}\cos\frac{\theta}{2}\sin\frac{\theta}{2}|\alpha\rangle\langle\alpha|\beta\rangle - 2\cos\frac{\theta}{2}\sin\frac{\theta}{2}\sin\frac{\theta}{2}|\alpha\rangle\langle\beta|\beta\rangle - 2\sin\frac{\theta}{2}\cos\frac{\theta}{2}\sin\frac{\theta}{2}|\beta\rangle\langle\alpha|\beta\rangle - 2\sin\frac{\theta}{2}\sin\frac{\theta}{2}\sin\frac{\theta}{2}|\beta\rangle\langle\beta|\beta\rangle + \sin\frac{\theta}{2}|\beta\rangle$$

$$= (2\cos\frac{\theta}{2}\cos^2\frac{\theta}{2}|\alpha\rangle + 2\sin\frac{\theta}{2}\cos^2\frac{\theta}{2}|\beta\rangle - \cos\frac{\theta}{2}|\alpha\rangle) - (2\cos\frac{\theta}{2}\sin^2\frac{\theta}{2}|\alpha\rangle + 2\sin\frac{\theta}{2}\sin^2\frac{\theta}{2}|\beta\rangle - \sin\frac{\theta}{2}|\beta\rangle)$$

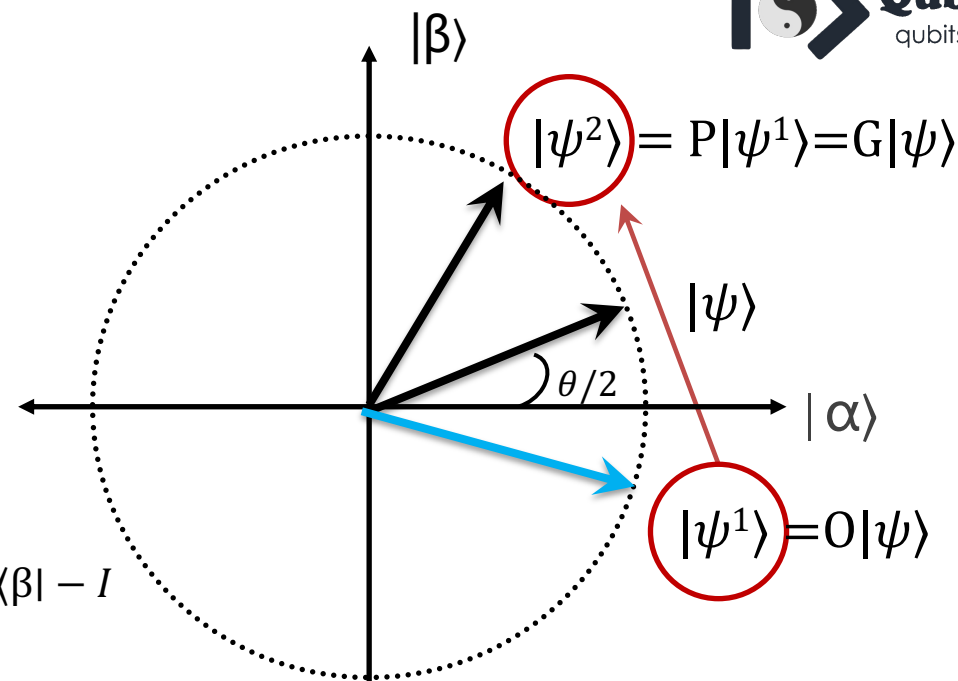
$$|\psi^1\rangle + |\psi^2\rangle = 2\cos\frac{\theta}{2}\cos^2\frac{\theta}{2}|\alpha\rangle + 2\sin\frac{\theta}{2}\cos^2\frac{\theta}{2}|\beta\rangle - 2\cos\frac{\theta}{2}\sin^2\frac{\theta}{2}|\alpha\rangle - 2\sin\frac{\theta}{2}\sin^2\frac{\theta}{2}|\beta\rangle$$

$$= 2\cos\frac{\theta}{2}(\cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2})|\alpha\rangle + 2\sin\frac{\theta}{2}(\cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2})|\beta\rangle$$

$$= 2(\cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2})(\cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle)$$

$$= 2(\cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2})|\psi\rangle = 2\cos\theta|\psi\rangle$$

由于 $|\psi^1\rangle, |\psi^2\rangle$ 为归一化向量，说明 $|\psi^1\rangle, |\psi^2\rangle$ 关于 $|\psi\rangle$ 镜像对称



平均值翻转 (Inversion about the mean)

令 $S = \{s_j\}$ ，实数集的有限集合，令 m 为其平均值，我们创建一个新的集合 T ，集合 T 中包含的数据为 $\{t_j = 2m - s_j\}$ ， T 具有如下性质：

- T 中元素平均值仍为 m
- $t_j - m = m - s_j$ ，且 $|t_j - m| = |s_j - m|$
- 如果 $s_j < m$ ，则 $t_j > m$ ，如果 $s_j > m$ ，则 $t_j < m$

令：

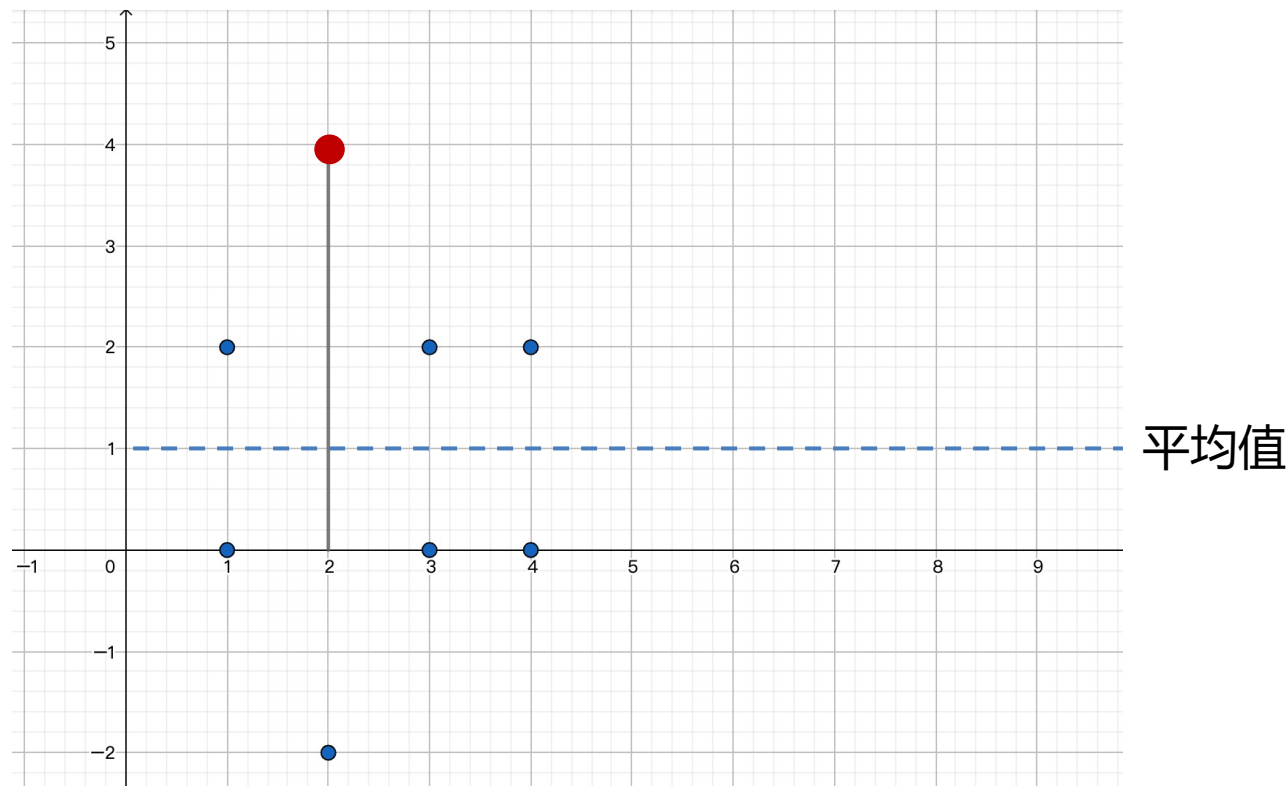
$$S = \{2, -2, 2, 2\}$$

则：

$$m = 1$$

$$T = \{0, 4, 0, 0\}$$

从例子中可以看出，唯一的负值经过平均值翻转，会显得非常突出。



平均值镜像翻转 - $2|s\rangle\langle s| - I_n$

因为：

$$\begin{aligned} |s\rangle &= (H|0\rangle)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \\ |s\rangle &= H^{\otimes n} |0^{\otimes n}\rangle \\ \langle s| &= \langle 0^{\otimes n}| H^{\otimes n} \\ I_n &= H^{\otimes n} H^{\otimes n} \end{aligned}$$

则有：

$$P = 2|\psi\rangle\langle\psi| - I = 2|s\rangle\langle s| - I_n = 2 H^{\otimes n} |0^{\otimes n}\rangle\langle 0^{\otimes n}| H^{\otimes n} - I_n = H^{\otimes n} (2 |0^{\otimes n}\rangle\langle 0^{\otimes n}| - I_n) H^{\otimes n}$$

$|s\rangle$ 为全 1 归一化向量，例如：

$$|s\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

平均值镜像翻转 - $2|s\rangle\langle s| - I_n$

$|s\rangle\langle s|$ 为全 1 矩阵：

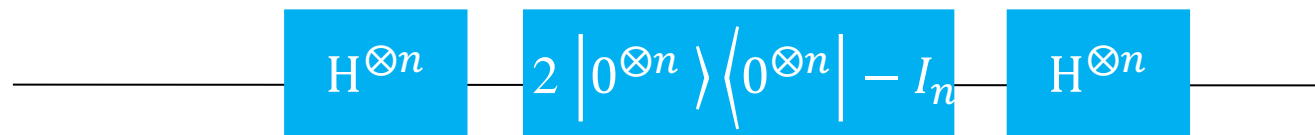
$$|s\rangle\langle s| = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 \\ \vdots \\ \vdots \\ 1 \end{bmatrix} \frac{1}{\sqrt{N}} [1 \ 1 \ \dots \ 1 \ 1] = \frac{1}{N} \begin{bmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{bmatrix}$$

系数 $\frac{1}{N}$ 可用来计算均值，例如：

$$|\psi\rangle = |\alpha\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{bmatrix}$$

$$|s\rangle\langle s||\alpha\rangle = \frac{1}{N} \begin{bmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{bmatrix} = \begin{bmatrix} \frac{\sum \alpha_{n-1}}{N} \\ \frac{\sum \alpha_{n-1}}{N} \\ \vdots \\ \frac{\sum \alpha_{n-1}}{N} \end{bmatrix} \rightarrow \bar{\alpha}$$

平均值镜像翻转



$$\text{由于 } 2|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I_n = 2 \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix} - I_n = \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -1 \end{bmatrix}$$

则有：

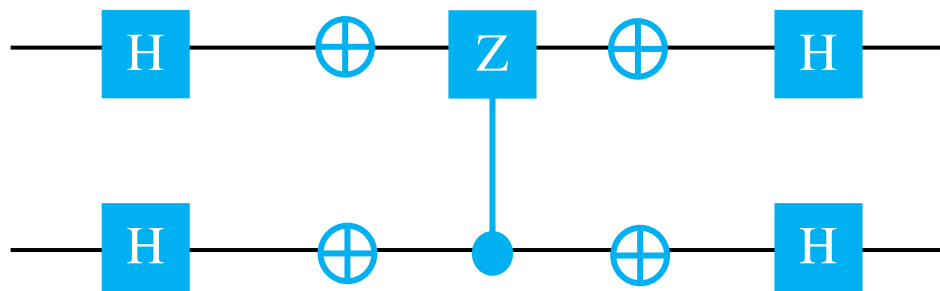
$$\begin{aligned} P &= 2|s\rangle\langle s| - I_n = 2 H^{\otimes n} |0^{\otimes n}\rangle\langle 0^{\otimes n}| H^{\otimes n} - I_n \\ &= H^{\otimes n} (2|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I_n) H^{\otimes n} \\ &= H^{\otimes n} \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -1 \end{bmatrix} H^{\otimes n} \\ &= \begin{bmatrix} \frac{2}{N} & -1 & \cdots & \frac{2}{N} \\ \vdots & & \ddots & \vdots \\ \frac{2}{N} & & \cdots & \frac{2}{N} & -1 \end{bmatrix} \end{aligned}$$

对角线为 $\frac{2}{N} - 1$ ，其余为 $\frac{2}{N}$

平均值镜像翻转其它分解

$$\begin{aligned}
 2 |s\rangle\langle s| - I_n &= 2 H^{\otimes n} |0^{\otimes n}\rangle\langle 0^{\otimes n}| H^{\otimes n} - I_n = H^{\otimes n} (2 |0^{\otimes n}\rangle\langle 0^{\otimes n}| - I_n) H^{\otimes n} \\
 &= H^{\otimes n} (X^{\otimes n} \text{Ctrl-Z } X^{\otimes n}) H^{\otimes n}
 \end{aligned}$$

$H^{\otimes n} X^{\otimes n}$ 代表张量积。Ctrl-Z 代表受控 Z 门：



平均值镜像翻转其它分解 – 例子

$$2 |00\rangle\langle 00| - I = 2 \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = -1 \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

最后的矩阵可以拆解为 XZX变换：

$$-1 \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = -1 X^{\otimes 2} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} X^{\otimes 2}$$

其中 $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$ 刚好是受控 Z门的变换矩阵。



Thank

You