Qubits
qubits.top

量子计算
—算法篇

Quantum Computing

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，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/qubits
https://gitee.com/mymagicpower/qubits

*** 版权声明：**
- 仅限用于个人学习
- 禁止用于任何商业用途

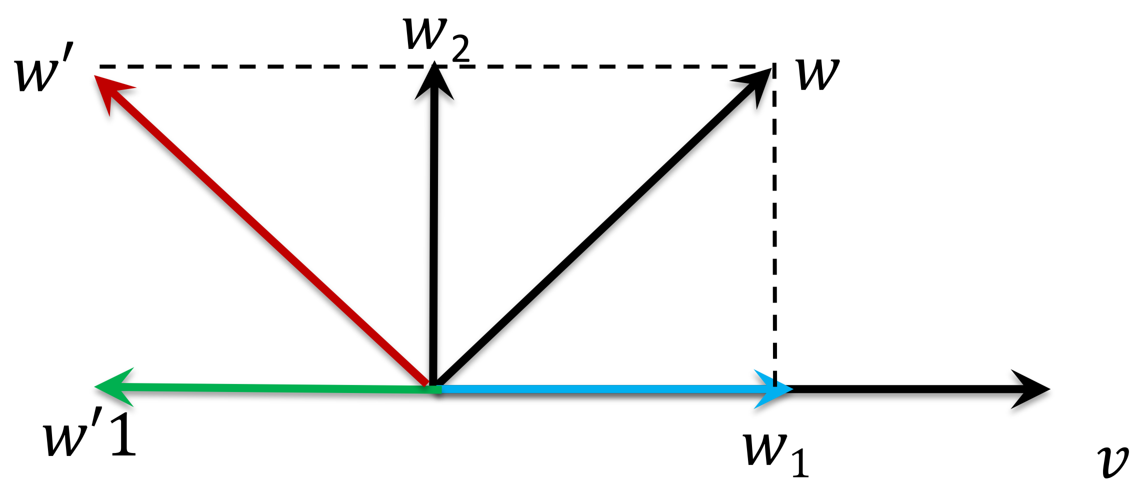
Calvin, QQ: 179209347 Mail: 179209347@qq.com

任意维度反射变换 – 实向量空间

线性代数，在任意维度空间中，有如下反射变换，对应的矩阵为：

$$R_n = I_n - 2vv^T$$

在公式中， I_n 为 nxn 的单位矩阵，v为长度为 1 的 n 维列向量， vv^T为 nxn 的矩阵。
R_n 可以实现**反射变换**：把任意向量 w 与 v 平行的分量 w_1 反向为 $w'1$，而与 v 垂直的分量 w_2保持不变。



R_n 作用于任何向量，相当于关于 v 的垂直分量 $w2$（法线）做镜像映射。

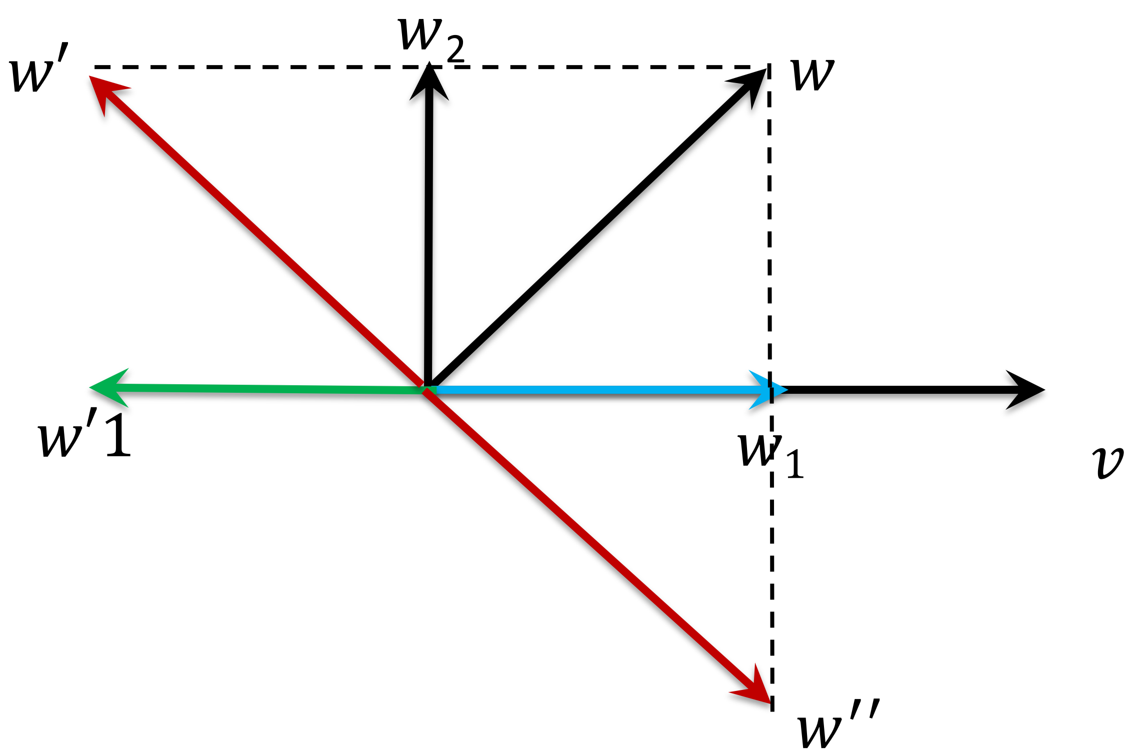
Calvin, QQ: 179209347 Mail: 179209347@qq.com

任意维度镜像变换 – 实向量空间

如果我们将公式改为下面的写法，也就是增加一个负号，我们看看它的几何性质：

$$R_n = 2vv^T - I_n$$

增加一个负号，相当于在任意维空间中，将 w' 翻转反向，至 w'' 的位置，显然，其与原向量关于 v 形成镜像映射关系。

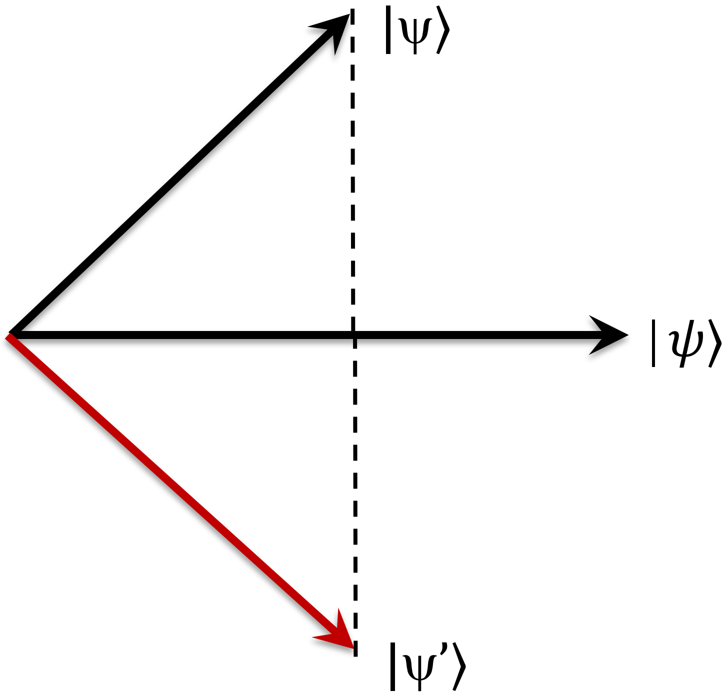


R_n 作用于任何向量，相当于关于 v 做镜像映射。

任意维度镜像变换 – 复向量空间

根据我们之前总结的实向量与复向量的变换关系，我们可以得到下面等价的公式：

$$R_n = 2|\psi\rangle\langle\psi| - I_n$$



- 连续两次镜像映射可以定义一次旋转，我们也可以通过两次反射定义旋转。

R_n 作用于任何量子态向量 $|\psi\rangle$，相当于关于 $|\psi\rangle$ 做镜像映射。
$$R_n = 2|\psi\rangle\langle\psi| - I_n$$

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, ……, $N-1$ } → {0,1}

找到 $f(x)$=1 的 x

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:

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

其中 $|q\rangle$ 是一个结果寄存器, ⊕ 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's Search Algorithm - 初态

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。
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 $|\beta\rangle$ 。

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = |\beta\rangle + |\alpha\rangle$$

假设有 M个解，则： $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_x |x\rangle$ $|\beta\rangle = \frac{1}{\sqrt{M}} \sum_x |x\rangle$

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:

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

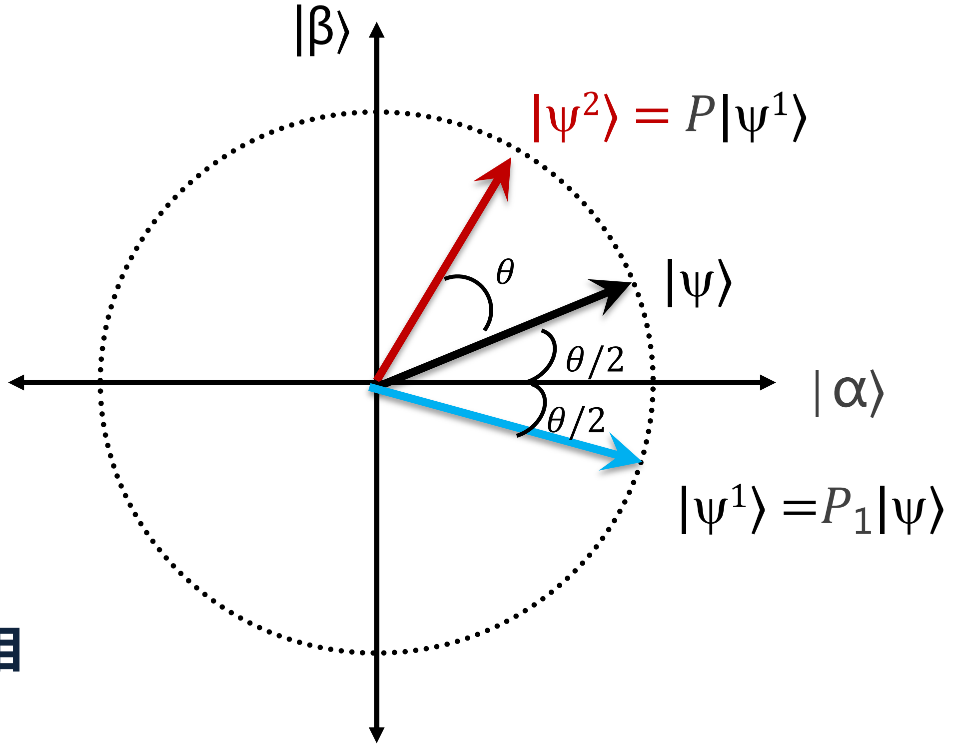
Grover's Search Algorithm - **相位翻转(镜像翻转)**

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:

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



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**）。

Grover's Search Algorithm - **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:

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

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

Grover's Search Algorithm - 旋转(连续两次镜像)

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:

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

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

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

实质上可以视为一个角度为 θ 的旋转量子门（ RY(θ) 门 ）操作。

Grover‘s Search Algorithm - **旋转 - Grover 迭代**

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's Search Algorithm - **旋转 - Grover 迭代次数 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。

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

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 $f(i) = 1$ ，

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

当我们需要搜所的值个数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。

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

迭代的次数 R 满足:

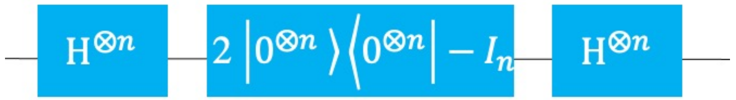
$$R \leq \frac{\pi}{4}\sqrt{\frac{N}{M}}$$

Calvin, QQ: 179209347 Mail: 179209347@qq.com

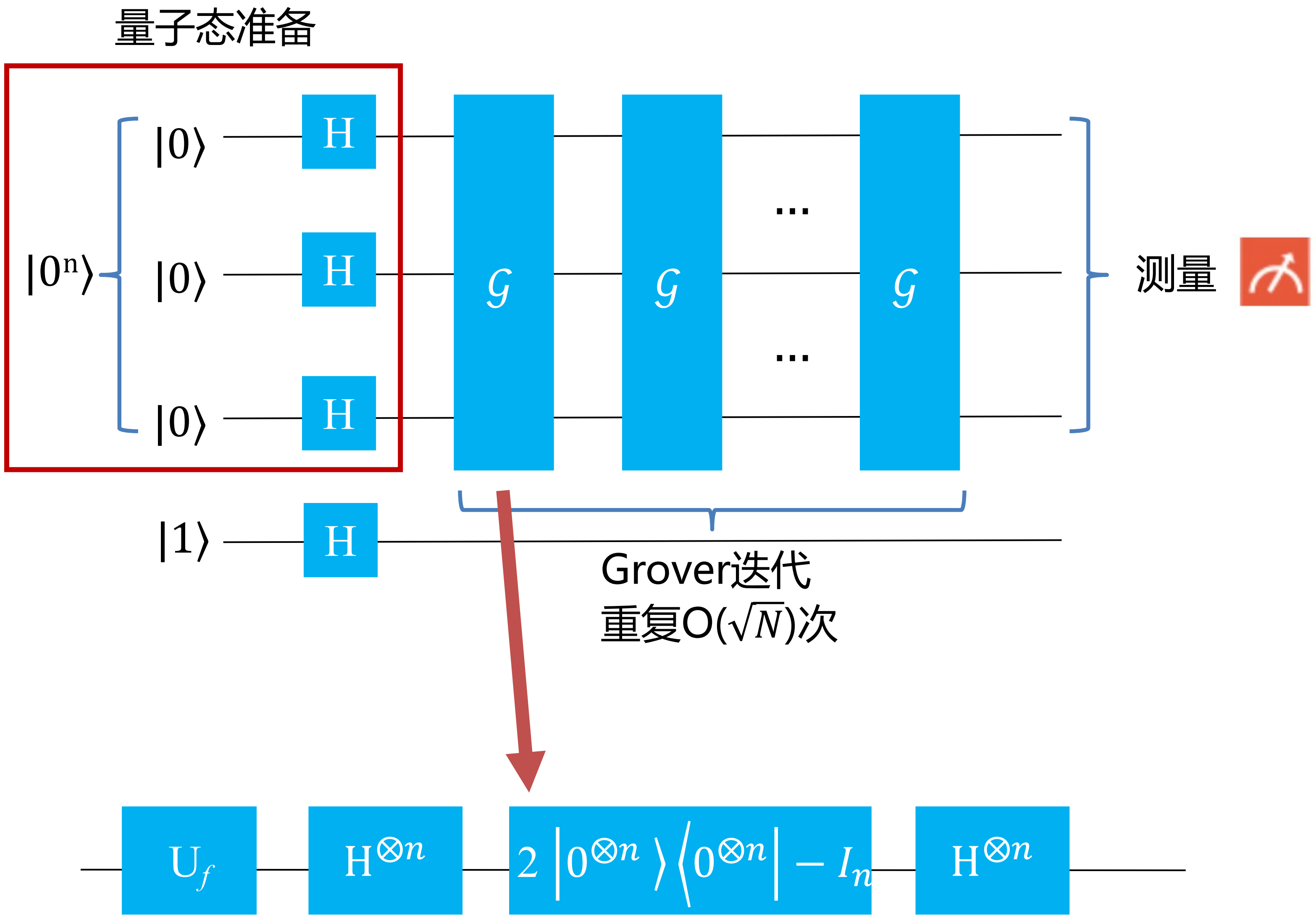
Grover算法量子线路

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

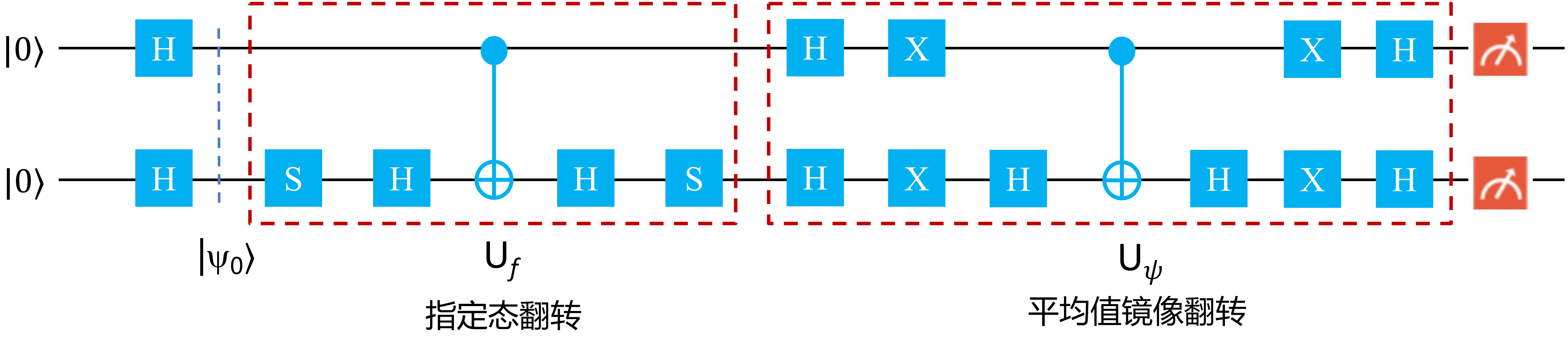
而每一次的Grover迭代，也可以分为两个部分：
- 一部分是指定态翻转U_f，这部分是为了实现指定态的相位翻转
- 另一部分 - 平均值翻转



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



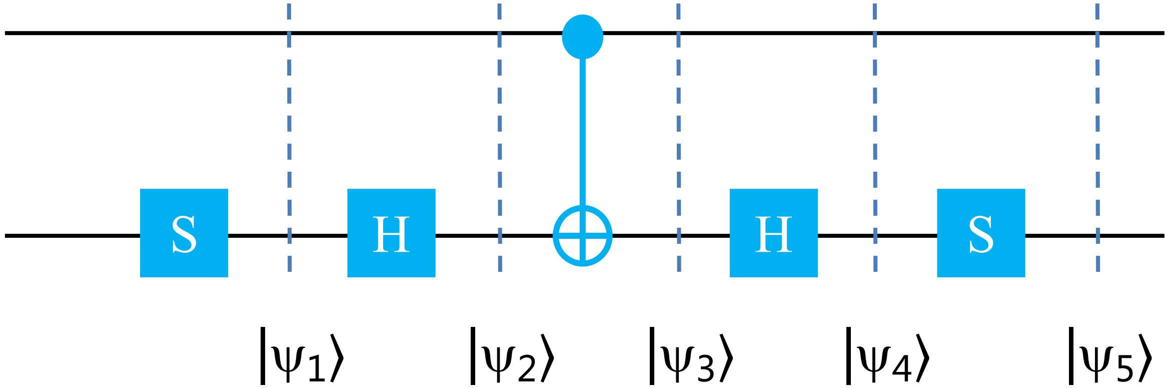
Grover算法量子线路 - 两比特例子



初态制备：

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

Grover算法量子线路 - 指定态翻转 U_f - 两比特例子



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

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

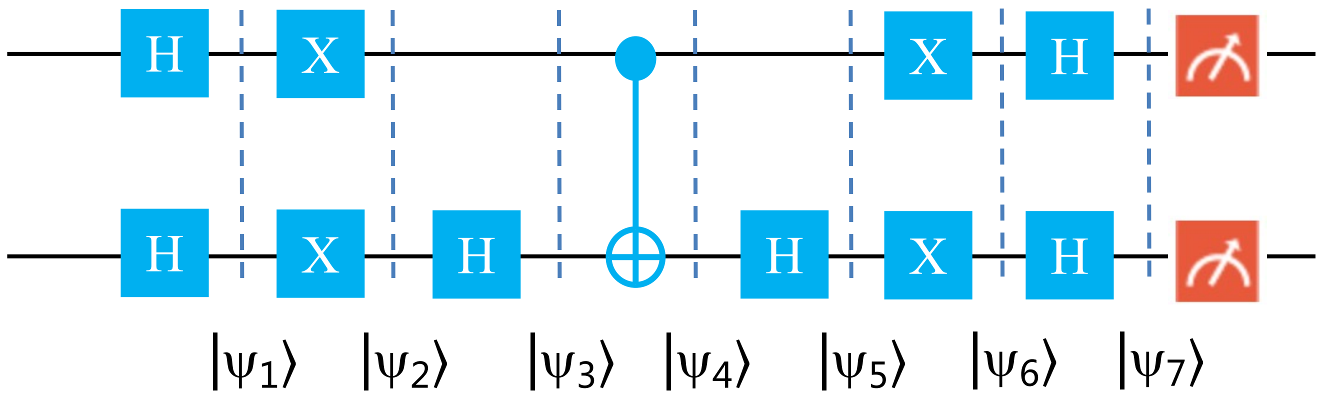
$$|\psi_3\rangle = \frac{\sqrt{2}}{4}\left((1+i)|00\rangle + (1-i)|01\rangle + (1-i)|10\rangle + (1+i)|11\rangle \right)$$

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

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

Calvin, QQ: 179209347 Mail: 179209347@qq.com

平均值镜像翻转 U_ψ - 两比特例子



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

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

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

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

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

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

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

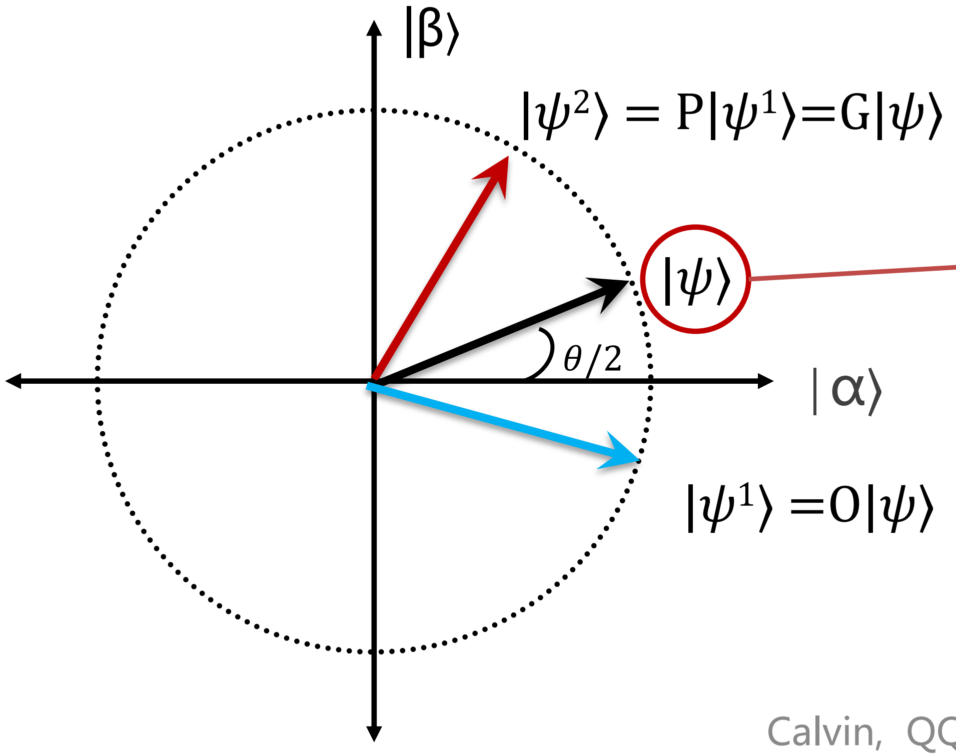
Calvin, QQ: 179209347 Mail: 179209347@qq.com

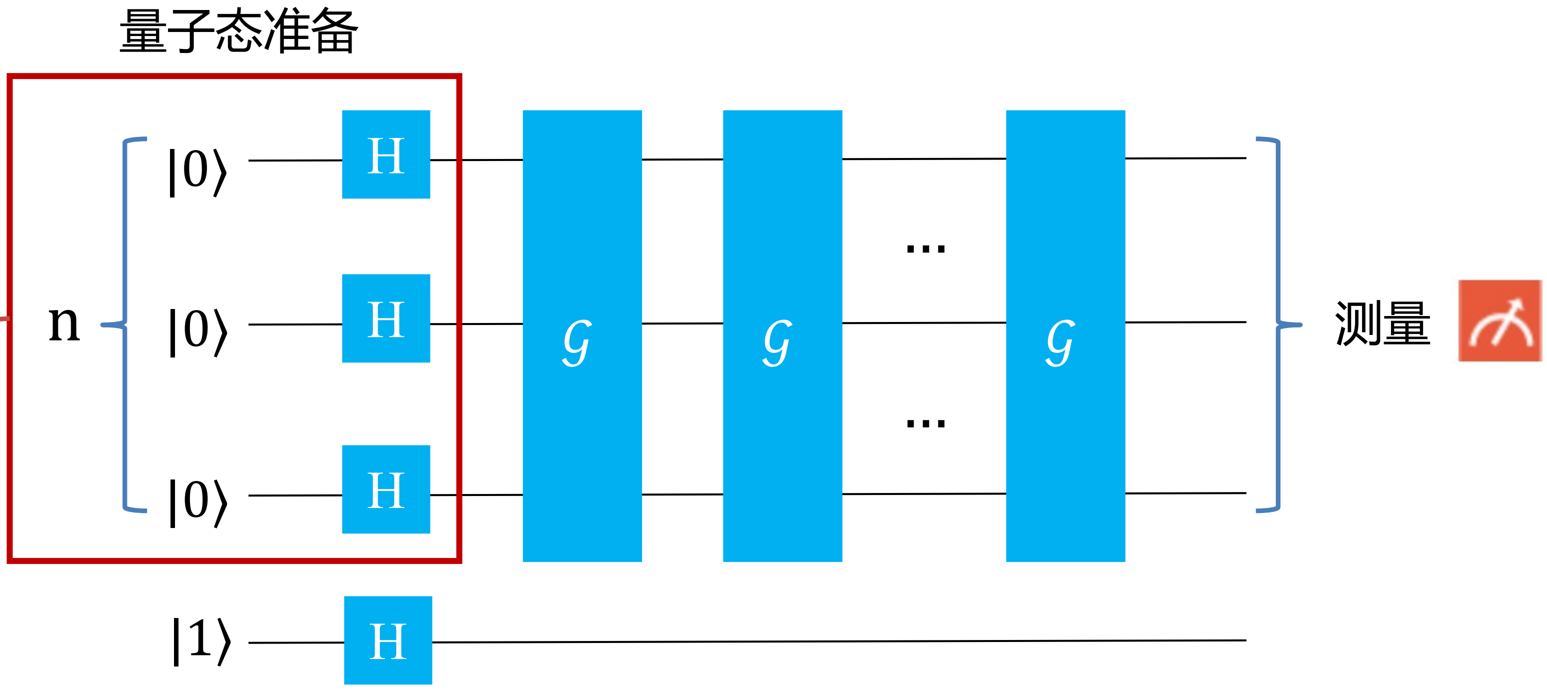
N量子比特 - Grover算法量子线路 – 初态制备

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





Calvin, QQ: 179209347 Mail: 179209347@qq.com

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：

$$\mathrm{O}_{\omega}|x\rangle = \begin{cases} |x\rangle \ (x \neq \omega) \\ -|x\rangle \ (x = \omega) \end{cases}$$

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。

$$\mathrm{O}_{\omega} = \begin{array}{c c} & \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

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：

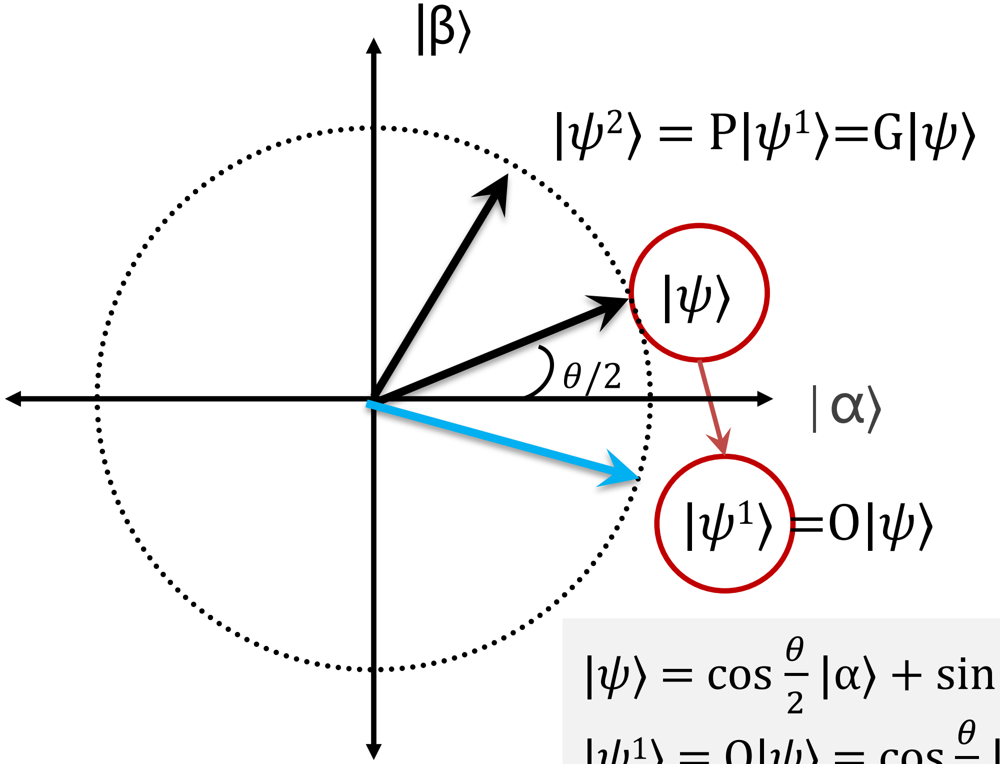
$$O_\omega=\begin{bmatrix}(-1)^{f(0)} & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & (-1)^{f(2^n)}\end{bmatrix}$$

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：

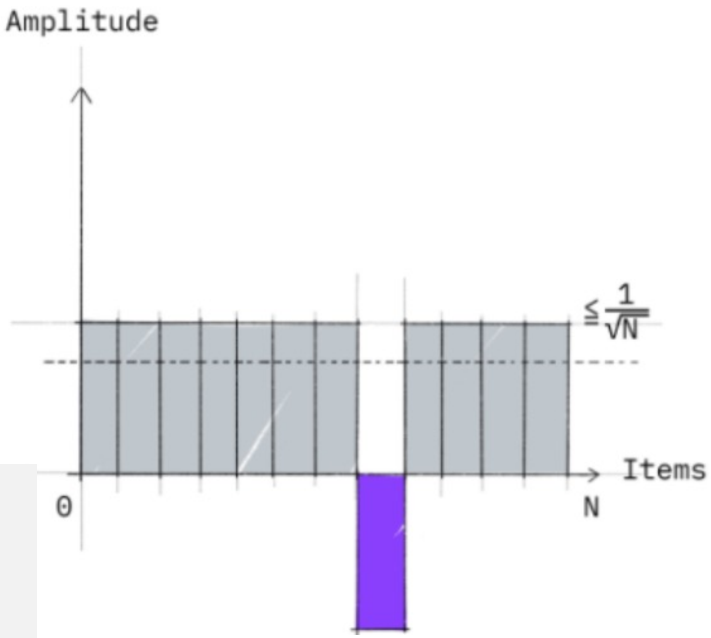
$$U_f \quad H^{\otimes n} \quad 2\left|0^{\otimes n}\right\rangle\left\langle 0^{\otimes n}\right| - I_n \quad H^{\otimes n}$$

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



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

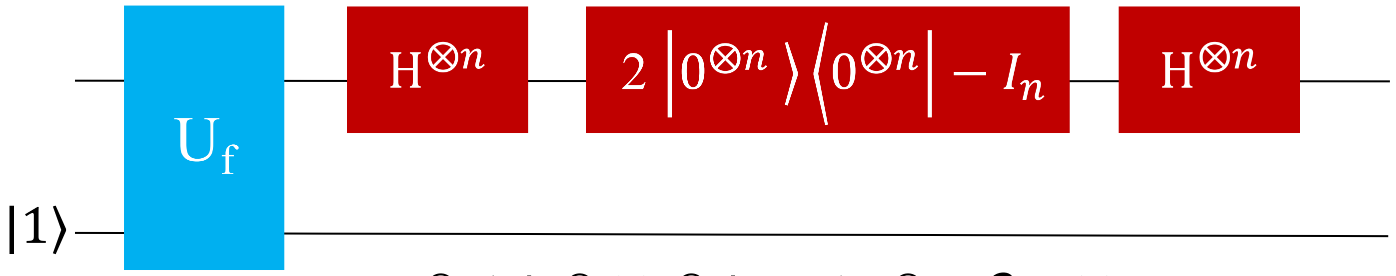
使用 O 算符作用之后，我们得到的结果为：



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。

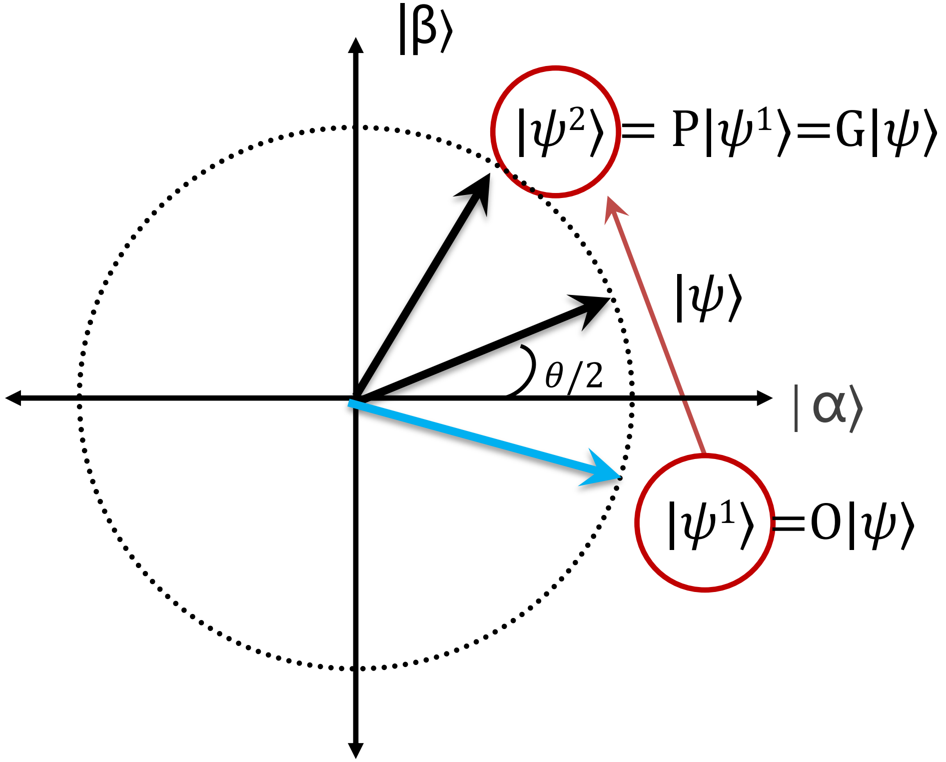
Grover算法量子线路 - 镜像翻转

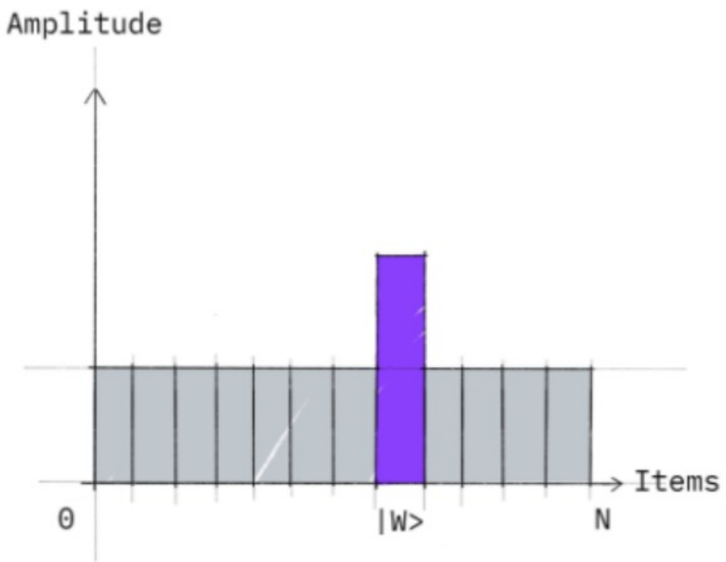
3、最后，可以根据各个基态的幅值计算出均值，然后按照这个均值镜像翻转各个基态的幅值，就可以得到如下图所示的结果。



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

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

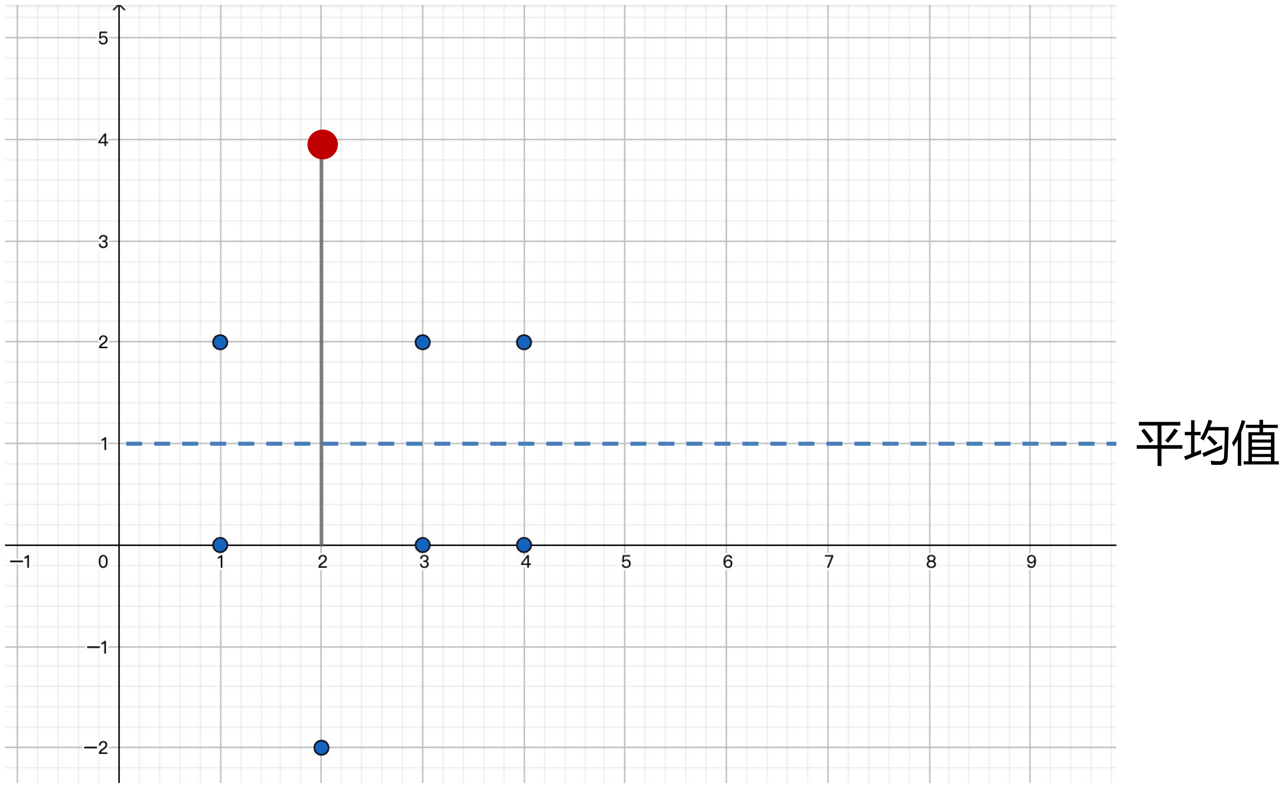
平均值翻转 (Inversion about the mean)

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：

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

$|s\rangle = H^{\otimes n}|0^{\otimes n}\rangle$

$\langle s| = \langle 0^{\otimes n}|\, H^{\otimes n}$

$I_n = H^{\otimes n} H^{\otimes n}$

则有：

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

$|s\rangle$ 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：

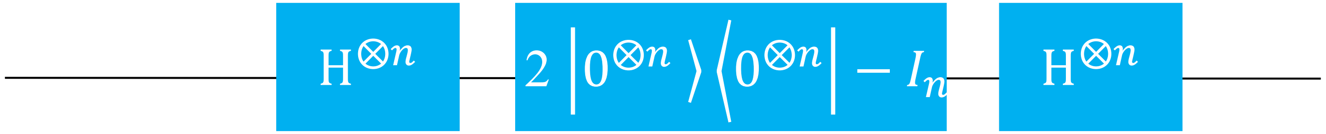
$$|s\rangle\langle s| = \frac{1}{\sqrt{N}}\begin{bmatrix}1\\ \dots\\ \dots\\ 1\end{bmatrix}\frac{1}{\sqrt{N}}\begin{bmatrix}1 & 1 & \dots & 1 & 1\end{bmatrix} = \frac{1}{N}\begin{bmatrix}1 & \cdots & 1\\ \vdots & \ddots & \vdots\\ 1 & \cdots & 1\end{bmatrix}$$

系数 $\frac{1}{N}$ 可用来计算均值，例如：

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

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

平均值镜像翻转



由于 $2\,|\,0^{\otimes n}><0^{\otimes n}|\ - I_n = 2\begin{bmatrix}1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & 0\end{bmatrix} - I_n = \begin{bmatrix}1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & -1\end{bmatrix}$

则有：

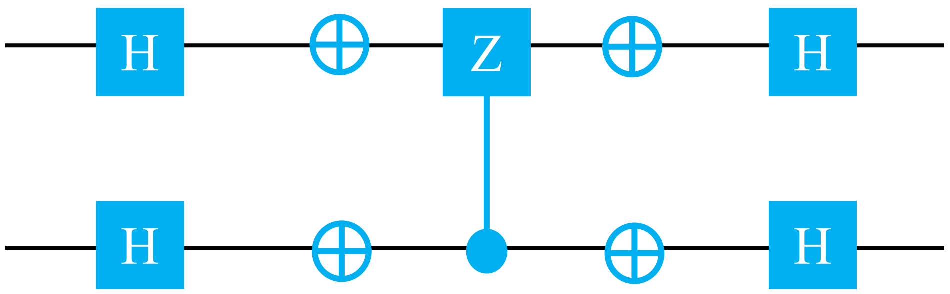
$$
\begin{aligned}
P = 2\,|s\rangle\langle s| - I_n &= 2\,H^{\otimes n}|\,0^{\otimes n}><0^{\otimes n}|\,H^{\otimes n} - I_n \\
&= H^{\otimes n}(2\,|\,0^{\otimes n}><0^{\otimes n}|\ - I_n\,)H^{\otimes n} \\
&= H^{\otimes n}\begin{bmatrix}1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & -1\end{bmatrix}H^{\otimes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

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

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

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



Calvin, QQ: 179209347 Mail: 179209347@qq.com

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。

Qubits
qubits.top

Thank You