Grover's Algorithm

参考资料：qiskit的官网文档。

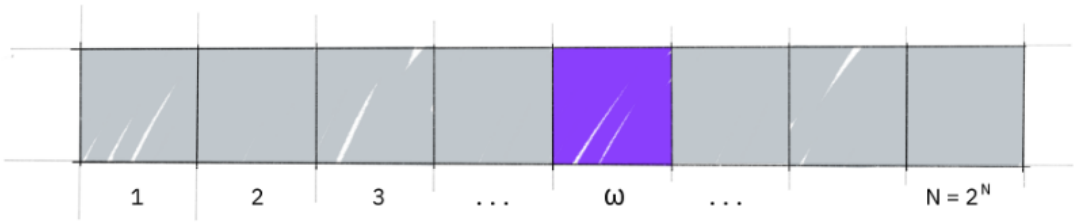
实现快速的非结构化搜索。

1. Introduction

您可能听说过，量子计算机相对于经典计算机的众多优势之一是其卓越的**搜索数据库速度**。Grover 的算法证明了这种能力。该算法可以**二次加速非结构化搜索问题**，但它的用途不止于此；它可以作为一种通用技巧或子程序来获得各种其他算法的二次运行时间改进。这称为幅度放大技巧。

非结构化搜索

假设给你一个包含 **N 个项目的大列表。** 在这些项目中，我们希望找到一个具有独特属性的项目； 我们称这个为获胜者 w。 将列表中的每个项目视为具有特定颜色的框。 假设列表中的所有项目都是灰色的，除了获胜者 w 是紫色的。



要使用经典计算找到紫色框（标记的项目），**必须平均检查 N/2 个这些框，在最坏的情况下，检查所有 N 个。** 然而，在量子计算机上，我们可以使用 **Grover 的幅度放大技巧(amplitude amplification trick)**以大约 **√N 步找到标记的项目。** 二次加速确实可以大大节省在长列表中查找标记项目的时间。 此外，该算法**不使用列表的内部结构**，这**使其具有通用性**； 这就是为什么它立即为许多经典问题提供了二次量子加速。

Creating an Oracle

对于本教科书中的示例，我们的“**数据库**”包含我们的**量子位可能处于的所有可能的计算基础状态。**例如，如果我们有 3 个量子位，我们的列表是状态 $|000\rangle$、$|001\rangle$、 ... ,$|111\rangle$，(即状态 $|0\rangle, \dots, |7\rangle$）。

Grover 的算法解决了为解决方案状态添加**负相位的预言机。**即对于计算基础中的任何状态 |x⟩：

$$U_\omega|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq \omega \\ -|x\rangle & \text{if } x = \omega \end{cases}$$

该**预言机将是一个对角矩阵**，其中**与标记项对应的条目将具有负相位。** 例如，如果我们有三个量子位并且 w=101，我们的预言机将有矩阵：

$$U_\omega = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \leftarrow \omega = 101$$

Grover 的算法如此强大的原因在于将**问题转换为这种形式的预言机是多么容易。** 有许多计算问题很难找到解决方案，但**验证解决方案相对容易。** 例如，我们可以通过检查所有规则是否满足来轻松验证数独的解决方案。 对于这些问题，我们可以创建一个函数 f，它采用建议的解 x，如果 **x 不是解 (x != w)**，则返回 **f(x)=0**，对于**有效解 (x=w)**，**返回 f(x)=1。** 我们的预言机可以描述为：

$$U_\omega |x\rangle = (-1)^{f(x)} |x\rangle$$

预言机的矩阵将是以下形式的对角矩阵：

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

在本章的下一部分，我们旨在教授算法的核心概念。 我们将**创建预先知道 ω 的示例预言机**，而**不用担心这些预言机是否有用。** 在本章的最后，我们将介绍一个简短的例子，我们**创建一个预言机来解决一个问题（数独）。**

幅度放大（Amplitude Amplification）

那么算法是如何工作的呢？ 在查看项目列表之前，**我们不知道标记的项目在哪里。** 因此，**对其位置的任何猜测都与其他任何猜测一样好，这可以用均匀叠加来表示**：

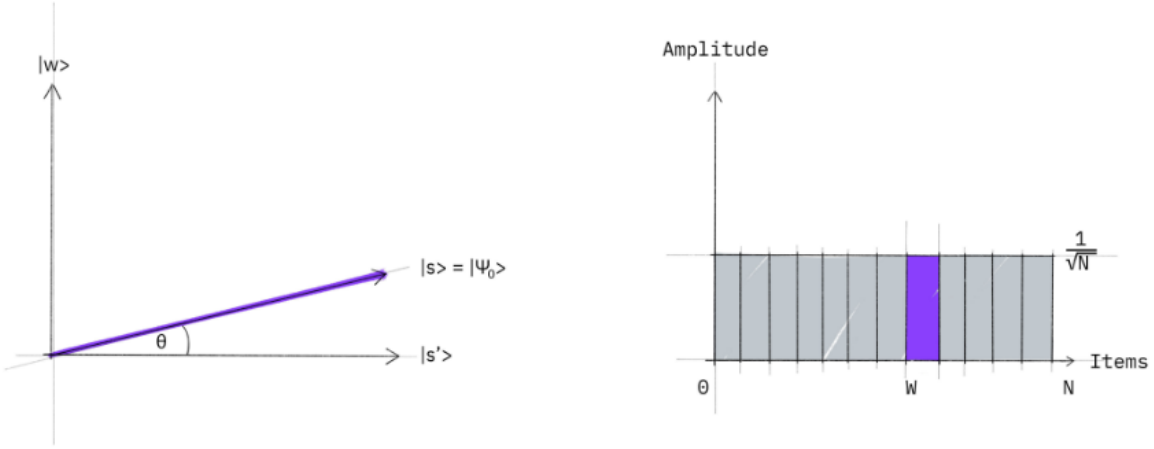
$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

如果此时我们要在标准基础上进行测量$|x\rangle$，根据第五量子定律，这种叠加将坍缩为具有相同概率的任何一个基态$\frac{1}{2^n} = \frac{1}{N}$. 因此，我们猜测正确 w 值的机会1在$2^n$，正如所料。因此，平均而言，我们需要尝试$N/2 = \frac{1}{2^{n-1}}$次猜测正确的项目。

进入称为**幅度放大的程序**，这是**量子计算机显着提高这种概率的方式。**此过程**拉伸（放大）标记项目的幅度**，从而**缩小其他项目的幅度**，以便测量最终状态将返回几乎确定的正确项目。

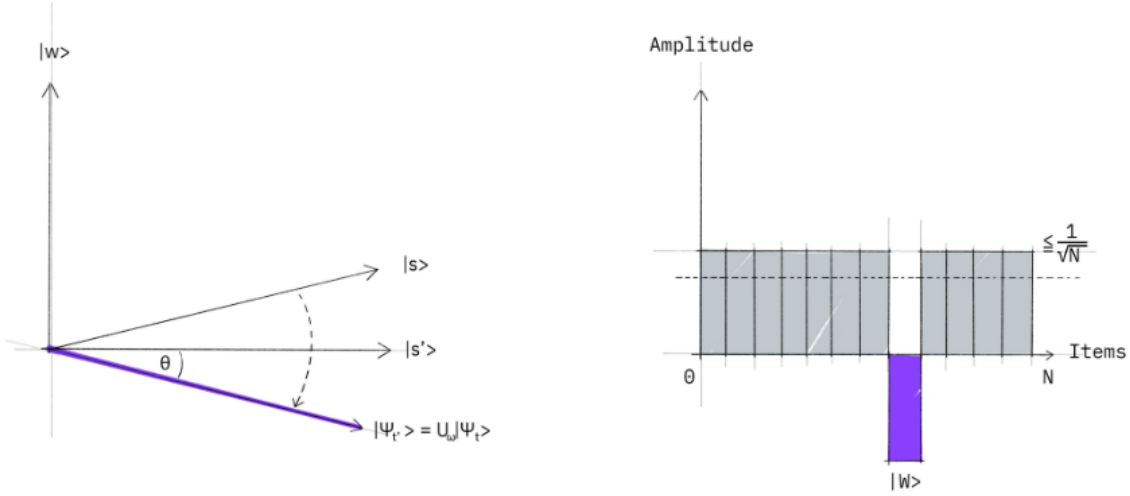
该算法在两次反射方面具有很好的几何解释，这会在二维平面中产生旋转。 我们需要考虑的唯一两个特殊状态是获胜者$|w\rangle$和均匀叠加$|s\rangle$。 这两个向量跨越向量空间 C^N 中的一个二维平面。 它们不是完全垂直的，因为 $|w\rangle$ 也出现在振幅为 $N^{-1/2}$ 的叠加中。 然而，我们可以在这两个向量的跨度中引入**一个额外的状态** $|s'\rangle$，它垂直于 $|w\rangle$ 并且通过移除 $|w\rangle$ 和重新缩放从 $|s\rangle$ 获得。

第 1 步：幅度放大过程从均匀叠加开始$|s\rangle$, 它很容易由$|s\rangle = H^{\otimes n}|0\rangle^{\otimes n}$得到。



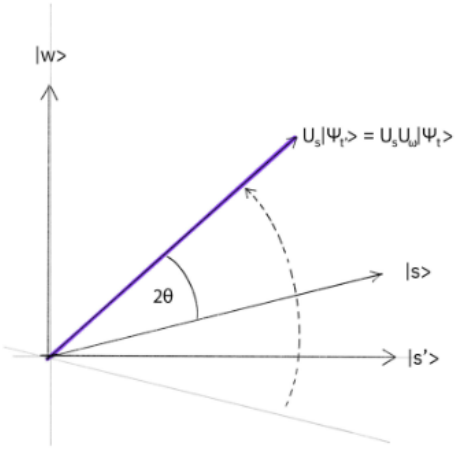
左图对应于由垂直向量 |w⟩ 和 |s'⟩ 跨越的二维平面，它允许将初始状态表示为 |s⟩=sinθ|w⟩+cosθ|s'⟩ 其中 $\theta = arcsin\langle s|w\rangle = arcsin\frac{1}{\sqrt{N}}$。 右图是状态|s⟩ 幅度的条形图 。

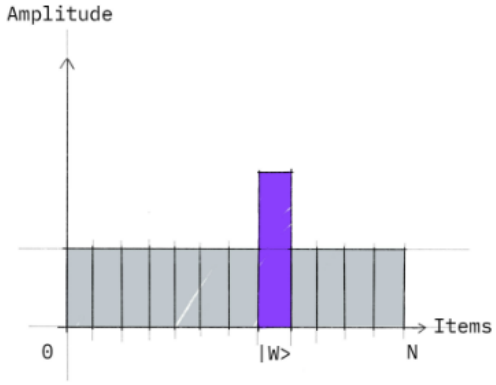
第 2 步：我们将预言机映射 U_f 作用于状态 |s⟩。



在几何上，这对应于**状态 |s⟩ 关于 |s'⟩ 的映射。** 这种变换意味着|w⟩状态前面的幅度变为负值，这反过来意味着平均幅度（由虚线表示）已经降低。

第 3 步：我们现在**对状态 |s⟩ 应用额外的映射** (Us)：Us = 2|s⟩⟨s|-1。 该转换将状态映射到 UsUf|s⟩ 并完成转换。



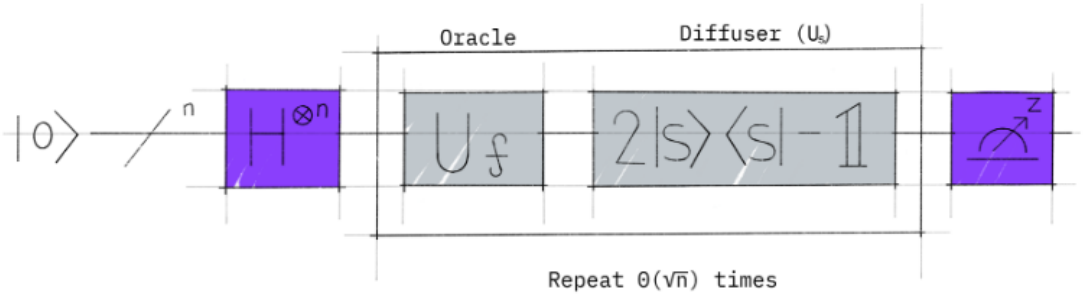


两个映射总是对应一个旋转。 **变换 UsUf 使初始状态 |s⟩ 更靠近获胜者 |w⟩。** 幅值条形图中反射 Us 的作用可以理解为对平均幅值的映射。 由于第一次映射降低了平均幅度，因此这种变换将 **|w⟩ 的负幅度提高到其原始值的大约三倍，同时降低其他幅度。** 然后我们**转到第 2 步以重复该应用程序。** 此过程将**重复多次，以归零获胜者。**

在 t 步之后，我们将处于状态 $|\psi_t\rangle$ 其中：$|\psi_t\rangle = (U_s U_f)^t |s\rangle$。

我们需要应用旋转多少次？ 事实证明，大约 **√N 次旋转就足够了。** 当查看状态 |ψ⟩ 的幅度时，这一点变得清晰。 我们可以看到**|w⟩的幅度随着应用程序的数量 $tN^{-1/2}$线性增长。** 但是，由于我们处理的是**幅度而不是概率**，因此向量空间的维度以平方根的形式输入。 因此，在此过程中被**放大的是幅度，而不仅仅是概率。**

在有多个解 M 的情况下，可以证明大约 √(N/M) 次旋转就足够了。



2. 示例：2 个量子位

让我们先看一下格罗弗算法 N=4 的情况，它是用 2 个量子比特实现的。 在这种特殊情况下，只需旋转一次即可将初始状态 |s⟩ 旋转到获胜者 |w⟩[3]：

1. 根据上面的介绍，在 N=4 的情况下，我们有

$$\theta = \arcsin\frac{1}{2} = \frac{\pi}{6}.$$

经过 t 步，我们有

$$(U_s U_\omega)^t |s\rangle = \sin\theta_t |\omega\rangle + \cos\theta_t |s'\rangle,$$

其中：

$$\theta_t = (2t+1)\theta.$$

为了获得 |ω⟩，我们需要 θt=π/2，将 θ=π/6 插入上面的结果为 t=1。 这意味着在 t=1 旋转之后，搜索到的元素被找到。

现在，我们将通过一个使用特定预言机的示例来进行说明。

Oracle for |ω⟩=|11⟩

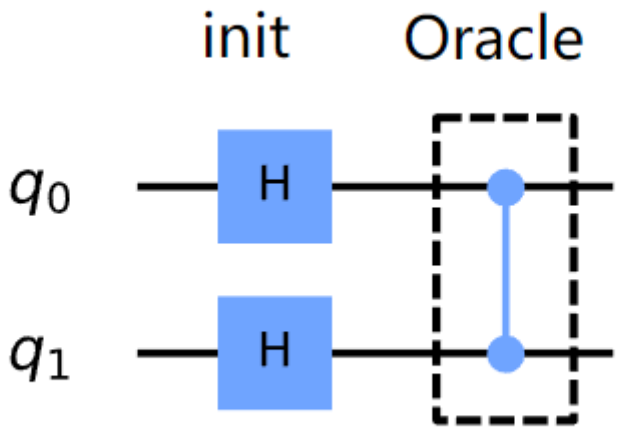
我们来看|w⟩=|11⟩的情况。 在这种情况下，预言机 Uω 的行为如下：

$$U_\omega|s\rangle = U_\omega\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle).$$

或者是：

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

您可以将其识别为受控 Z 门。因此，对于这个例子，我们的预言机只是受控 Z 门：



Reflection Us

为了完成电路，我们需要实现**附加映射 Us=2|s⟩⟨s|-1。** 由于这是关于 |s⟩ 的反映，我们希望**为与 |s⟩ 正交的每个状态添加一个负相位。**

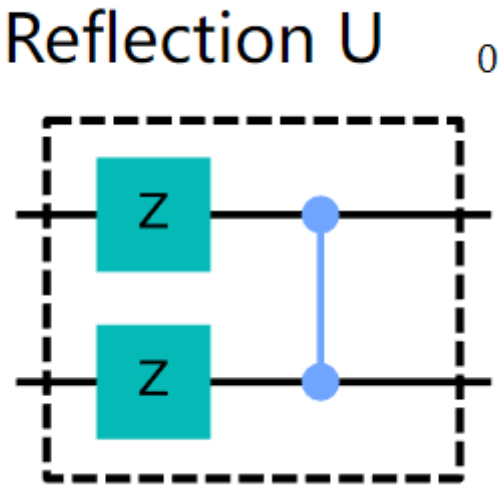
我们可以做到这一点的一种方法是使用转换状态的操作**|s⟩→|0⟩**，我们已经知道是应用于每个量子比特的 Hadamard 门：

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

然后我们应用一个电路，将负相位添加到与 |0⟩ 正交的状态：

$$U_0 \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle)$$

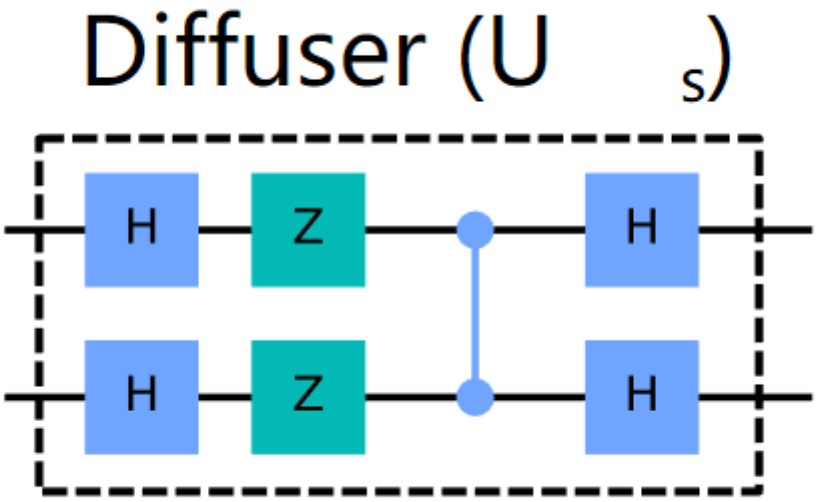
即除了 |00⟩ 之外，每个状态的符号都被翻转。 可以很容易地验证，实现 U0 的一种方法是以下电路：



最后，我们执行转换状态的操作 |0⟩→|s⟩（再次是 H 门）：

$$H^{\otimes n}U_0H^{\otimes n} = U_s$$

完整的电路 Us 我们看起来像这样：



Full Circuit for |w⟩=|11⟩

由于在 N=4 的特殊情况下只需要旋转一次，我们可以结合上述组件来构建用于情况 |w⟩=|11⟩ 的 Grover 算法的完整电路：