量子软件前沿作业

韦璐｜PB1600702

黑箱（black box）或者谕示机（oracle）是量子算法里面很重要的装置。有时候，为了完成一定的计算任务，我们先假设有某种黑箱可以完成某种计算任务，我们并不关心黑箱内部的构成，而只是把它当作一个整体来使用，我们知道它在一定的input下面有特定的output。黑箱的引入，可以帮助我们去研究和分析我们所关心的计算问题的核心部分。

在Deutsch-Jozsa算法中，我们要判断一个给定函数是常函数函数还是平衡函数，对于一个输入的函数，我们的输出结果应该是针对常函数还是平衡函数的判断结果。给定一个函数，黑箱是在实现函数$f(x)$时所引入的。也即是说，算法的input data(即函数$f(x)$)通过黑箱引入到量子线路里面。

在Grover搜索算法中，黑箱的作用是类似的。本来我们有一个大的数据集，其中有一个标记子集，我们的目标是搜索得到这些标记子集中的元素。这个问题也可以转换为一个boolean函数，也就是说标记子集的特征函数，如果元素在标记子集中，其输出值为1，否则为0。这时候，给定问题的信息就在函数$f(x)$里面了。黑箱的引入同样也是实现$f(x)$, 黑箱将$f(x)$的信息引入到量子线路中。

I. Deutsch-Jozsa算法

Deutsch-Jozsa算法目标

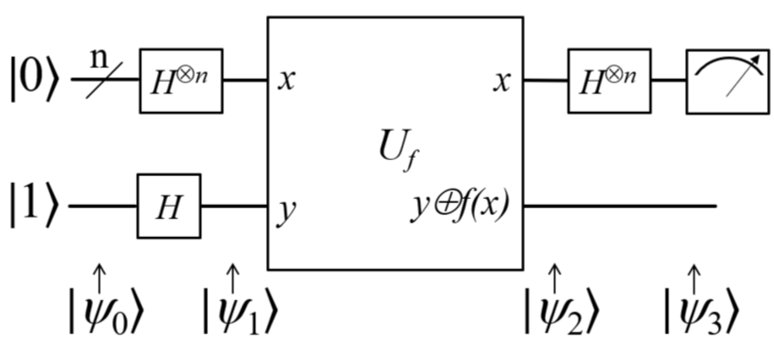
Deutsch-Jozsa算法考虑的是一个这样的问题：我们有一个黑箱（black box or oracle），它能够实现一个特殊类型n-比特Boolean函数$f:\{0,1\}^n \to \{0,1\}$，这个函数的输出结果有以下两种可能：

- $f(x)$是个常函数，也就是说，对所有的输入值，他给出一样的结果，要么0，要么1；
- $f(x)$是个平衡（balanced）函数，对于2^n个输入值，它给出一半的0，一半的1.

我们的目标是：判断$f(x)$是常函数函数平衡函数。

Deutsch-Jozsa算法步骤

Deutsch-Jozsa算法的量子线路图如下： 其中黑箱（oracle）就是U_f部分。H代表Hadamard门，最右端



的工作线路我们通过测量来读取结果。

其具体操作步骤如下：

- 初态制备为，工作线路$|0\rangle^{\otimes n}$，辅助线路制备为$|1\rangle$。我们有如下的初态

$$|\psi_0\rangle = |\text{working}_0\rangle \otimes |\text{ancilla}_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle. \tag{1}$$

- 接着分别对工作线路和辅助线路进行Hadamard门操作，

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

  我们会得到如下的量子态

$$|\psi_1\rangle = |\text{working}_1\rangle \otimes |\text{ancilla}_1\rangle = \frac{1}{2^{(n+1)/2}}(\sum_{x=0}^{2^n-1}|x\rangle) \otimes (|0\rangle - |1\rangle). \tag{2}$$

- 执行黑箱（oracle）操作U_f。其具体操作如下

$$\begin{aligned}
&\text{Oracle}: \quad |\text{ working }_1\rangle \otimes \mid \text{ancilla }_1\rangle \\
&\to \tfrac{1}{2^{(n+1)/2}}\left(\textstyle\sum_{x=0}^{2^n-1}|x\rangle\right)(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) \\
&= \tfrac{1}{2^{(n+1)/2}}\left(\textstyle\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right)(|0\rangle - |1\rangle) = |\psi_2\rangle
\end{aligned} \tag{3}$$

  这里所有的比特加法都是模2的。我们发现，如果$f(x)$取0时，他会使得辅助比特保持不变，如果$f(x)$取1时，他会使得辅助比特整体有一个-1。

- 丢弃辅助比特，对工作线路进行Hadamard门操作，这时候注意到，工作线路的量子态为

$$\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle \tag{4}$$

  注意到

$$H^{\otimes n}|x\rangle = \sum_{x=1}^{2^n-1}(-1)^{x\cdot y}|y\rangle \tag{5}$$

  于是我们有

$$\begin{aligned}
H^{\otimes n}\left(\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right) &= \sum_{x=0}^{2^n-1}(-1)^{f(x)}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle \\
&= \sum_{x,y=0}^{2^n-1}(-1)^{f(x)+x\cdot y}|y\rangle.
\end{aligned} \tag{6}$$

- 测量并且读取结果。我们选取$y=0$ (即$|y\rangle = |0\rangle^{\otimes n}$) 作为测量基进行测量，这时候，我们有

$$Pr(y=0) = \left|\sum_{x=0}^{2^n-1}(-1)^{f(x)}\right|^2 = \begin{cases} 1 & f(x) \text{ 为常数} \\ 0 & f(x) \text{ 为平衡} \end{cases} \tag{7}$$

我们知道经典算法的验证次数为$O(2^n)$，而Deutsch-Jozsa算法需要的操作步数为$O(n)$, Deutsch-Jozsa算法对这个问题提供了指数加速。

II. Grover搜索算法

Grover搜索算法的目标

假设我们有一个$N=2^n$元素的数据集S，我们将数据标记为$x=0,1,\cdots,2^{n-1}$，我们想在其中找到M个目标数据$T\subset S$ (也就是T的元素个数为$|T|=M$)，自然地$1\le M\le N$。这个问题很自然地可以被表述为一个Boolean函数

$$f(x) = \begin{cases} 1, x \in T \\ 0, x \notin T \end{cases} \tag{8}$$

Grover搜索算法的具体步骤

Oracle—和Deutsch-Jozsa算法类似，Grover搜索算法要用到黑箱(oracle)。具体来说，对于Gover搜索的目标函数$f(x)$，我们引入一个辅助线路，以及一个黑箱操作

$$\text{oracle:} \quad |x\rangle \otimes |a\rangle \to |x\rangle \otimes |f(x) \oplus a\rangle. \tag{9}$$

如果我们将辅助线路量子态制备为

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{10}$$

于是我们会有黑箱操作

$$\text{oracle } U_f: \quad |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \to (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{11}$$

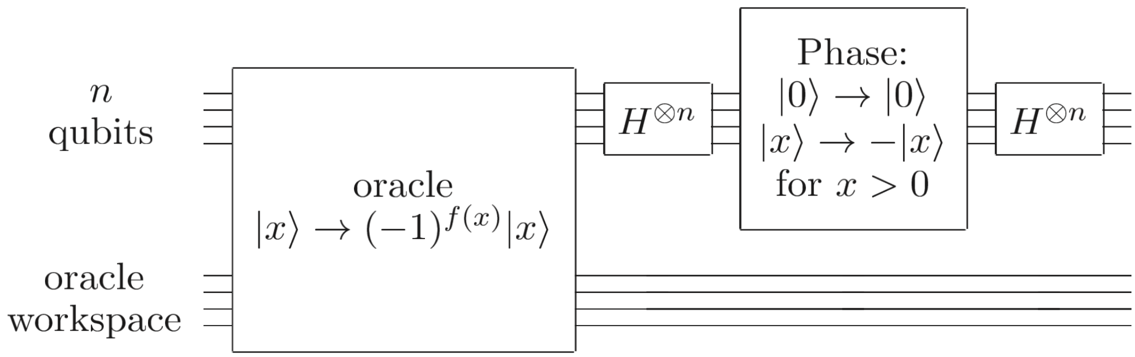
如果我们丢掉辅助线路，我们会发现，我们有黑箱操作

$$\text{oracle}: \quad |x\rangle \to (-1)^{f(x)}|x\rangle. \tag{12}$$

oracle的效果是将问题的信息引入到量子线路中去。

Grover迭代线路—Grover算法中最核心的步骤是Grover迭代。所以我们先看Grover迭代的具体操作及其几何解释。

Grover迭代的的量子线路图如下



其操作是一步一步的执行，有四步，第一步是执行黑箱操作，第二部Hadamard门，第三部是phase变化，保持0的phase不变，别的phase均反转，最后一步是Hadamard门操作。我们主要来看一下它的几何意义。

注意到后面三步的效果可以等效为

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I \tag{13}$$

其中$|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$是等权叠加态。结合第一步的oracle操作，我们知道Grover迭代算子为

$$G = (2|\psi\rangle\langle\psi| - I)U_f. \tag{14}$$

给定的数据集为S, 其元素个数为$N = |S|$，我们将S中的元素用比特串标记$x \in S$，x是n-比特串。而目标数据集为$T \subset S$，其元素个数为$M = |T|$。我们定义如下的量子态

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}}\sum_{x\in S-T}|x\rangle, \quad |\beta\rangle = \frac{1}{\sqrt{M}}\sum_{x\in T}|x\rangle. \tag{15}$$

等权叠加态$|\psi\rangle = \frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^{\otimes n}$可以被写成

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle. \tag{16}$$

首先oracle操作相当于对所有T里面的元素做phase反转，也即是说

$$|\beta\rangle \to -|\beta\rangle. \tag{17}$$

这意味着，它是在$|\alpha\rangle$和$|\beta\rangle$张成的平面内沿着$|\alpha\rangle$做镜像翻转。

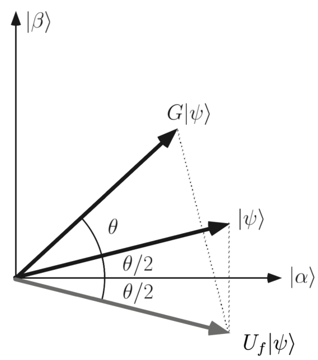
其次$2|\psi\rangle\langle\psi| - I$也是在$|\alpha\rangle$和$|\beta\rangle$张成的平面内沿着$|\psi\rangle$做一个镜像翻转。这很容易理解, 考虑在$|\alpha\rangle$和$|\beta\rangle$张成的平面内与$|\psi\rangle$垂直的量子态$|\psi^{\perp}\rangle$。对于任何处于$|\alpha\rangle$和$|\beta\rangle$张成的平面内的量子态，我们有

$$|\Phi\rangle = a|\psi\rangle + b|\psi^{\perp}\rangle. \tag{18}$$

将$2|\psi\rangle\langle\psi| - I$作用上去我们有

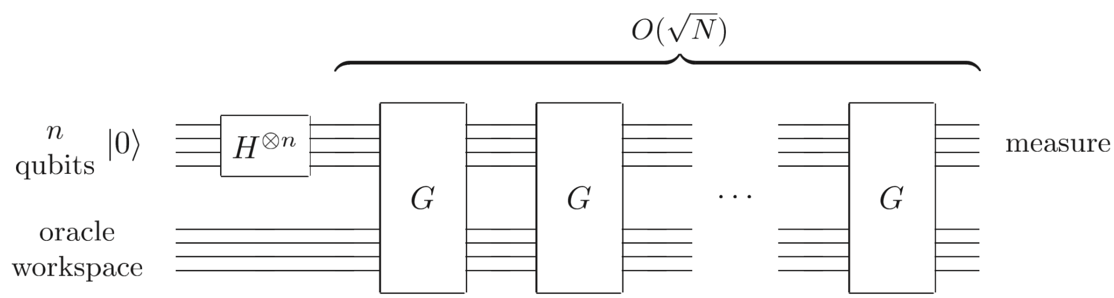
$$(2|\psi\rangle\langle\psi| - I)|\Phi\rangle = a|\psi\rangle - b|\psi^{\perp}\rangle. \tag{19}$$

如果我们定义角度$\cos\theta/2 = \sqrt{(N-N)/N}$, 于是一个Grover迭代的效果就相当于是将初态$|\psi\rangle$先沿着$|\alpha\rangle$镜像翻转，将得到态再沿着$|\psi\rangle$做镜像翻转。其效果下图:



我们的目标是$|\beta\rangle$。通过多次旋转，我们会逐渐接近$|\beta\rangle$。这里我们仍然要强调oracle将目标数据集或者等价地说，讲目标函数的信息引入到了量子线路中。

那具体的Grover算法的操作过程就是多次进行Grover迭代，如下图所示



经典的搜算算法的复杂性是$O(N)$，而Grover搜索算法的复杂性是$O(\sqrt{N})$，可以看到它实现了开方加速。可以看到黑箱是将计算问题的信息引入到算法里面。我们并没有去关系黑箱的具体构造，而只是把它当作一个整体来使用。