北京邮电大学

第6讲 量子搜索和量子计数算法

高　飞
网络空间安全学院

提纲

- Grover 算法
  - 量子搜索
  - 幅度放大
  - 量子计数（量子幅度估计）

1. L. K. Grover, Quantum Mechanics Helps in Searching for a Needle in a Haystack, Phys. Rev. Lett. 79, 325 (1997).
2. G. Brassard, P. Høyer, M. Mosca, and A. Tapp, *Quantum Amplitude Amplification and Estimation*, Contemporary Mathematics Series, Millenium Vol. 305 (AMS, New York, 2002).

问题描述

- 问题：如何在一个大小为N的无结构数据集中寻找满足特定条件的一个目标元素（假设其中目标元素个数为M）？
- 经典方法复杂度：$\mathcal{O}\left(\frac{N}{M}\right)$，量子搜索复杂度：$\mathcal{O}(\sqrt{\frac{N}{M}})$

前提假设：存在有效算法求下述映射，即易判断一个元素是否目标

- 有效算法：如果一个算法的输入规模为 n 比特，而实现该算法需要的基本门的个数为 $\mathcal{O}(\mathrm{poly}\ n)$，称该算法是问题的一个有效算法[1]

定义：从数据集元素地址 x（n比特，$n=\log N$）到$\{0,1\}$上的映射

$$f(x):\{0,1\}^n \longrightarrow \{0,1\}$$

若地址 x 上的数据 d_x 是一个目标元素，有$f(x)=1$; 否则, $f(x)=0$

注：不论搜索空间是什么（比如可以是不连续的数值集合），只要有一个“地址到元素”的映射，就可以实现 $f(x)$

[1] Andrew M. Childs, Lecture Notes on Quantum Algorithms, 2017.

问题描述

- 问题：如何在一个大小为N的无结构数据集中寻找满足特定条件的一个目标元素（假设其中目标元素个数为M）？
- 经典方法复杂度：$\mathcal{O}\left(\frac{N}{M}\right)$，量子搜索复杂度：$\mathcal{O}(\sqrt{\frac{N}{M}})$

地址 x	数据d_x	是否解？
000	d_0	0
001	d_1	0
010	d_2	0
011	d_3	0
100	d_4	1
101	d_5	
110	d_6	
111	d_7	

经典：逐条判断，遇到解后输出相应地址

$$f(x):\{0,1\}^n \longrightarrow \{0,1\}$$

量子：？

问题描述

- 问题：如何在一个大小为N的无结构数据集中寻找满足特定条件的一个目标元素（假设其中目标元素个数为M）？
- 经典方法复杂度：$\mathcal{O}\left(\frac{N}{M}\right)$，量子搜索复杂度：$\mathcal{O}(\sqrt{\frac{N}{M}})$

地址 x	数据d_x	是否解？
000	d_0	0
001	d_1	0
010	d_2	0
011	d_3	0
100	d_4	1
101	d_5	0
110	d_6	0
111	d_7	0

经典：逐条判断，遇到解后输出相应地址

$$f(x):\{0,1\}^n \longrightarrow \{0,1\}$$

量子：并行判断

问题：如何标记解地址 $\xleftarrow{\text{须标记解}}$ 问题：如何测出解地址

$$\sum_{x=0}^{N-1}\frac{|x\rangle}{\sqrt{N}} \longrightarrow \frac{\sum_{f(x)=0}|x\rangle - \sum_{f(x)=1}|x\rangle}{\sqrt{N}}$$

标记解： Oracle

- Oracle：用来区分一个数据是否为目标值的黑盒
  - 经典：根据地址 x 采样出一个数据 d_x，请求Oracle计算 $f(x)$，即请Oracle协助判断 d_x 是否为目标
  - 量子：可实现“并行”查询

经典: $x \in \{0,1\}^n$ → $f(x)$: $\{0,1\}^n \longrightarrow \{0,1\}$ → $f(x) \in \{0,1\}$

仅输出1个结果

量子: $\sum_{x=0}^{N-1} \frac{|x\rangle}{\sqrt{N}}$ → *Oracle O*: $|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$ → $\frac{\sum_{f(x)=0}|x\rangle - \sum_{f(x)=1}|x\rangle}{\sqrt{N}}$

输出所有结果的叠加

标记解：Oracle

- Oracle：用来区分一个数据是否为目标值的黑盒
  - 经典：根据地址 x 采样出一个数据 d_x，请求Oracle计算 $f(x)$，即请Oracle协助判断 d_x 是否为目标
  - 量子：可实现“并行”查询

- 实现Oracle的大体思路
  - 在Grover算法之前，已经有文献讨论Oracle的存在性和复杂度 [1]

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle \quad \xrightarrow{?} \quad |x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$$

实现函数调用的一般形式（可逆）

希望：制备所有地址的叠加态，通过调用Oracle把目标和非目标项以相位区分开，借此把目标“标记”出来，然后再想法把目标概率幅放大

[1] C. H. Bennett, SIAM J. Comput. 18, 766–776, 1989

标记解：Oracle

- Oracle：用来区分一个数据是否为目标值的黑盒
  - 经典：根据地址 x 采样出一个数据 d_x，请求Oracle计算 $f(x)$，即请Oracle协助判断 d_x 是否为目标
  - 量子：可实现“并行”查询
- 实现Oracle的大体思路
  - 在Grover算法之前，已经有文献讨论Oracle的存在性和复杂度 [1]

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

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

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

[1] C. H. Bennett, SIAM J. Comput. 18, 766–776, 1989

北京邮电大学 Beijing University of Posts and Telecommunications

Oracle构造细节

- 目的: 标记地址叠加态中的目标地址，即让目标地址系数取反：

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

QRAM实现，复杂度为$\mathcal{O}(\log N)$ [1]

穷举密钥时不需要QRAM

$$|x\rangle|0\rangle|0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \xrightarrow{step1:LOAD} |x\rangle|d_x\rangle|0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \xrightarrow{step2:f} |x\rangle|d_x\rangle|f(x)\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

$$\xrightarrow{step\ 3} \begin{cases} -|x\rangle|d_x\rangle|f(x)\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}, if\ f(x)=1 \\ |x\rangle|d_x\rangle|f(x)\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}, if\ f(x)=0 \end{cases} \xrightarrow{step\ 4} (-1)^{f(x)}|x\rangle|0\rangle|0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

C-NOT门， $\mathcal{O}(1)$

Step1&2的逆操作

如果在经典计算机上可以有效实现$x \to f(x)$，那么可以在量子计算机上有效实现$|x,y\rangle \to |x, y\oplus f(x)\rangle$。[2] 其复杂度为$\mathcal{O}(\text{poly} \log N)$

即，当可以有效判断是否解时，Oracle的一次调用复杂度一般为$\mathcal{O}(\text{poly} \log N)$

[1] V. Giovannetti, et al, Phys. Rev. Lett. 100, 160501; [2] A. M. Childs, Lecture Notes on Quantum Algorithms, 2017

问题描述

- 问题：如何在一个大小为N的无结构数据集中寻找满足特定条件的一个目标元素（假设其中目标元素个数为M）？
- 经典方法复杂度：$\mathcal{O}\left(\frac{N}{M}\right)$，量子搜索复杂度：$\mathcal{O}(\sqrt{\frac{N}{M}})$

地址 x	数据d_x	是否解？
000	d_0	0
001	d_1	0
010	d_2	0
011	d_3	0
100	d_4	1
101	d_5	0
110	d_6	0
111	d_7	0

经典：逐条判断，遇到解后输出相应地址

$$f(x):\{0,1\}^n \longrightarrow \{0,1\}$$

量子：并行判断

问题：如何标记解地址 $\xleftarrow{\text{须标记解}}$ 问题：如何测出解地址

$$\sum_{x=0}^{N-1}\frac{|x\rangle}{\sqrt{N}} \longrightarrow \frac{\sum_{f(x)=0}|x\rangle-\sum_{f(x)=1}|x\rangle}{\sqrt{N}}$$

测出解：Grover算法

(1) 制备 $|0\rangle^{\otimes n}$

(2) 执行 $H^{\otimes n}$，得

$$|\psi\rangle = \sum_{x=0}^{N-1} \frac{|x\rangle}{\sqrt{N}} = \sqrt{\frac{N-M}{N}} \frac{\sum_{f(x)=0} |x\rangle}{\sqrt{N-M}} + \sqrt{\frac{M}{N}} \frac{\sum_{f(x)=1} |x\rangle}{\sqrt{M}}$$

$$= \cos(\theta)|\psi_0\rangle + \sin(\theta)|\psi_1\rangle$$

- 生成所有地址的均匀叠加态
- 把目标元和非目标元分开写，$|\psi_1\rangle$表示目标元地址的叠加，$|\psi_0\rangle$表示非目标元地址的叠加
- 算法的目标是让$|\psi_1\rangle$的概率幅变大，最后通过测量得到其中一个目标元

测出解：Grover算法

(1) 制备 $|0\rangle^{\otimes n}$

(2) 执行 $H^{\otimes n}$，得

$$|\psi\rangle = \sum_{x=0}^{N-1} \frac{|x\rangle}{\sqrt{N}} = \sqrt{\frac{N-M}{N}} \frac{\sum_{f(x)=0} |x\rangle}{\sqrt{N-M}} + \sqrt{\frac{M}{N}} \frac{\sum_{f(x)=1} |x\rangle}{\sqrt{M}}$$

$$= \cos(\theta)|\psi_0\rangle + \sin(\theta)|\psi_1\rangle$$

(3) 执行 Oracle O，得 $\cos(\theta)|\psi_0\rangle - \sin(\theta)|\psi_1\rangle$

- 通过访问Oracle，将目标元标记出来（相位取反）

测出解：Grover算法

(1) 制备 $|0\rangle^{\otimes n}$

(2) 执行 $H^{\otimes n}$，得

$$|\psi\rangle = \sum_{x=0}^{N-1} \frac{|x\rangle}{\sqrt{N}} = \sqrt{\frac{N-M}{N}} \frac{\sum_{f(x)=0} |x\rangle}{\sqrt{N-M}} + \sqrt{\frac{M}{N}} \frac{\sum_{f(x)=1} |x\rangle}{\sqrt{M}}$$

$$= \cos(\theta)|\psi_0\rangle + \sin(\theta)|\psi_1\rangle$$

(3) 执行 Oracle O，得 $\cos(\theta)|\psi_0\rangle - \sin(\theta)|\psi_1\rangle$

(4) 执行酉操作 $2|\psi\rangle\langle\psi| - I$，得 $\cos(3\theta)|\psi_0\rangle + \sin(3\theta)|\psi_1\rangle$

n量子比特

- $2|\psi\rangle\langle\psi| - I = H^{\otimes n}(2\underline{|0\rangle\langle}0| - I)H^{\otimes n}$，因此是酉的（易证$2|0\rangle\langle 0| - I$为酉）
- 其中$2|0\rangle\langle 0| - I$能通过$C^n(U)$门实现，复杂度为$O(\log N)$ [1]
- 看几何解释更容易理解为何θ变为3θ，且符号变化

[1] M. A. Nielsen & I. L. Chuang, Quantum Computation and Quantum Information

- 把(3)-(4)的操作设为G：做一次角度增加 2θ

$$G := (2|\psi\rangle\langle\psi| - I)O = (2|\psi\rangle\langle\psi| - I)(2|\psi_0\rangle\langle\psi_0| - I)$$

$$G^k|\psi\rangle = \cos((2k+1)\,\theta)|\psi_0\rangle + \sin((2k+1)\theta)|\psi_1\rangle$$

- 选取合适的k，使得$\sin((2k+1)\theta)$接近于1（前提：知道解的个数），也即$(2k+1)\theta \approx \pi/2$

(3) 执行 Oracle O，得 $\cos(\theta)|\psi_0\rangle - \sin(\theta)|\psi_1\rangle$

(4) 执行酉操作 $2|\psi\rangle\langle\psi| - I$，得 $\cos(3\theta)|\psi_0\rangle + \sin(3\theta)|\psi_1\rangle$

(5) 重复执行(3)-(4) $k = \left\lfloor \frac{\pi}{4\theta} \right\rfloor \approx \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor$次，得到接近于$|\psi_1\rangle$的态

当 θ 的取值比较小时, $\theta \approx \sin(\theta)$

测出解：Grover算法

(1) 制备 $|0\rangle^{\otimes n}$

(2) 执行 $H^{\otimes n}$，得

$$|\psi\rangle = \sum_{x=0}^{N-1} \frac{|x\rangle}{\sqrt{N}} = \sqrt{\frac{N-M}{N}} \frac{\sum_{f(x)=0} |x\rangle}{\sqrt{N-M}} + \sqrt{\frac{M}{N}} \frac{\sum_{f(x)=1} |x\rangle}{\sqrt{M}}$$

$$= \cos(\theta)|\psi_0\rangle + \sin(\theta)|\psi_1\rangle$$

(3) 执行 Oracle O，得 $\cos(\theta)|\psi_0\rangle - \sin(\theta)|\psi_1\rangle$

(4) 执行酉操作 $2|\psi\rangle\langle\psi| - I$，得 $\cos(3\theta)|\psi_0\rangle + \sin(3\theta)|\psi_1\rangle$

(5) 重复执行(3)-(4) $k = \left\lfloor \frac{\pi}{4\theta} \right\rfloor \approx \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor$次，得到接近于$|\psi_1\rangle$的态

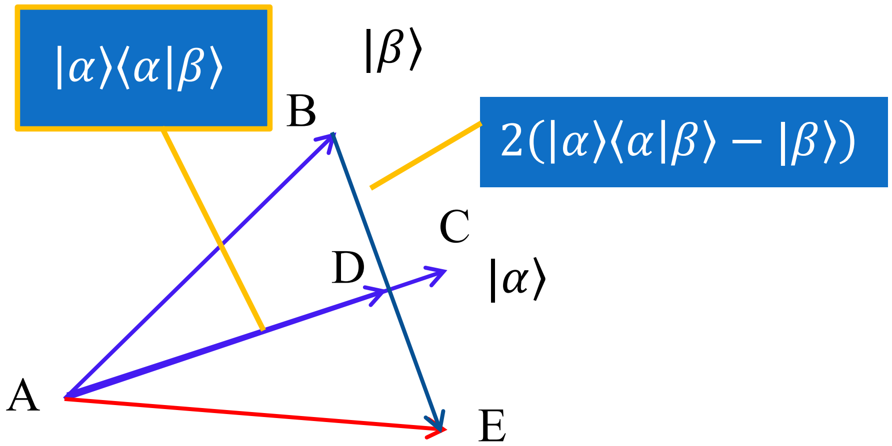
(6) 测量，并验证结果，算法以接近1的概率得到其中一个目标元

算法复杂度以(3)中Oracle调用（每次调用的复杂度a * 调用次数b）为主。不知具体问题时无法给出a，故算法复杂度常以b来衡量，即$\mathcal{O}(\sqrt{N/M})$

- 经典算法也要做oracle调用（每次调用的复杂度类似），看调用次数足以表明量子算法优势
- 如前所述，当可以有效判断是否解时，Oracle的一次调用复杂度并不大，一般为$\mathcal{O}(\text{poly}\log N)$

几何解释

先看如何求一个向量$|\beta\rangle$关于另一个向量$|\alpha\rangle$的对称向量

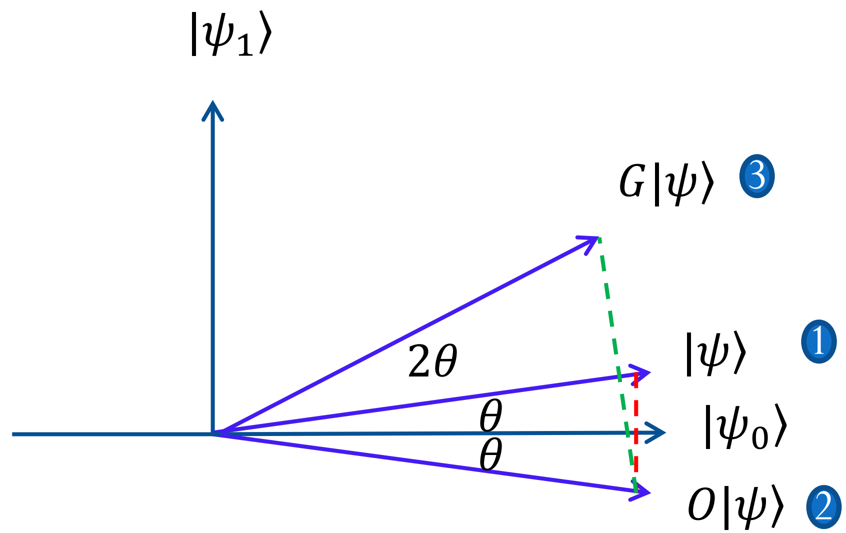


$2(|\alpha\rangle\langle\alpha|\beta\rangle - |\beta\rangle) + |\beta\rangle$

$= \underline{(2|\alpha\rangle\langle\alpha| - I)}|\beta\rangle$

关于 $|\alpha\rangle$ 取对称的操作

再看 $G = (2|\psi\rangle\langle\psi| - I)\underbrace{(2|\psi_0\rangle\langle\psi_0| - I)}_{\text{Oracle}}$



1. $|\psi\rangle = \cos(\theta)\,|\psi_0\rangle + \sin(\theta)\,|\psi_1\rangle$
2. $O = (2|\psi_0\rangle\langle\psi_0| - I)$：关于 $|\psi_0\rangle$ 取对称
3. $2|\psi\rangle\langle\psi| - I$：关于 $|\psi\rangle$ 取对称

$G|\psi\rangle = \cos(3\theta)|\psi_0\rangle + \sin(3\theta)|\psi_1\rangle$

思考：是否存在更高效的翻转操作?

注：从几何图像可见，$2|\psi_0\rangle\langle\psi_0| - I$在$|\psi_0\rangle$、$|\psi_1\rangle$及其叠加态上的作用等价于 $I - 2|\psi_1\rangle\langle\psi_1|$（尽管两者不等）。因此$G$也可写成$G = -(I - 2|\psi\rangle\langle\psi|)(I - 2|\psi_1\rangle\langle\psi_1|)$

M=1的例子

Algorithm: Quantum search

Inputs: (1) a black box oracle O which performs the transformation $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$, where $f(x) = 0$ for all $0 \leq x < 2^n$ except x_0, for which $f(x_0) = 1$; (2) $n+1$ qubits in the state $|0\rangle$.

Outputs: x_0.

Runtime: $O(\sqrt{2^n})$ operations. Succeeds with probability $O(1)$.

Procedure:

1. $|0\rangle^{\otimes n}|0\rangle$ — initial state

2. $\rightarrow \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$ — apply $H^{\otimes n}$ to the first n qubits, and HX to the last qubit

3. $\rightarrow \left[(2|\psi\rangle\langle\psi|-I)O\right]^R \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$ — apply the Grover iteration $R \approx \lceil \pi\sqrt{2^n}/4 \rceil$ times.

   $\approx |x_0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$

4. $\rightarrow x_0$ — measure the first n qubits

总结

目标	输入	输出	成功率	复杂度
从包含N个元素的无序数据库中，找到M个目标元素中的一个（的地址）	$\lvert 0\rangle^{\otimes n+1}$ ($n=\log N$)	$\approx \lvert\psi_1\rangle$	$\mathcal{O}(1)$	$\mathcal{O}(\sqrt{N/M})$ 二次加速

➢ 前提条件

- ❑ 有一个可有效判断是否目标元的Oracle（有效判断解+QRAM）
- ❑ 要知道解的个数，如果不知道
  - 可以先做量子计数，再做搜索
  - 更优地，用改进算法[1]，不知道θ也可搜，且复杂度级别相同

[1] M. Boyer, G. Brassard, P. Høyer, A. Tapp. Tight bounds on quantum searching.

提纲

- Grover 算法
  - 量子搜索
  - 幅度放大
  - 量子计数（量子幅度估计）

幅度放大

- 问题: 在Grover算法中如果初态$|\psi\rangle = \sum_{x=0}^{N-1} \frac{|x\rangle}{\sqrt{N}}$被替换为任意一个态$|\psi\rangle = U|0\rangle = \cos(\theta)|\psi_0\rangle + \sin(\theta)|\psi_1\rangle$, 如何进行量子搜索?

这里某个叠加项x的概率幅可能为0，也可能比其它概率幅大，不均匀

幅度放大

- 问题: 在Grover算法中如果初态$|\psi\rangle = \sum_{x=0}^{N-1} \frac{|x\rangle}{\sqrt{N}}$被替换为任意一个态$|\psi\rangle = U|0\rangle = \cos(\theta)|\psi_0\rangle + \sin(\theta)|\psi_1\rangle$, 如何进行量子搜索?
- 解决： 还是迭代，只是$|\psi\rangle$变了，将标准的G迭代

$$G = (2|\psi\rangle\langle\psi| - I)\,(2|\psi_0\rangle\langle\psi_0| - I)$$

稍作调整

$$G = R_\psi R_{\psi_0} = (2|\psi\rangle\langle\psi| - I)\,(2|\psi_0\rangle\langle\psi_0| - I)$$
$$= U(2|0\rangle\langle 0| - I)U^\dagger R_{\psi_0} = UR_0U^\dagger R_{\psi_0}$$

$R_\alpha = 2|\alpha\rangle\langle\alpha| - I$

- 复杂度：同样为执行$k = \left\lceil \frac{\pi}{4\theta} \right\rceil$次迭代

- 很多问题中，要用该算法作为中间算法对需要的态进行幅度放大
- 但是，必须有制备该初态的U门和$U^\dagger$门，并能标记是解的叠加项（可有效判断是否是解），才能做G操作，进而放大解的幅度（如未知态不行）

提纲

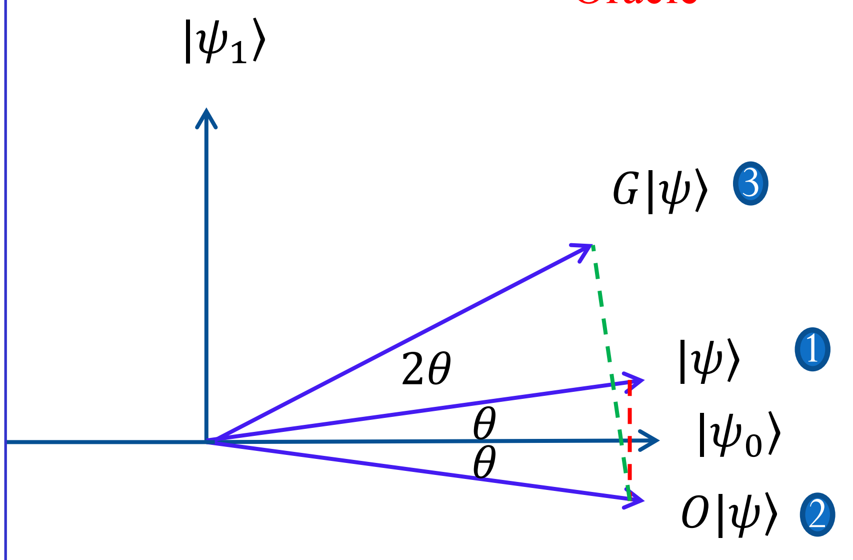
- Grover 算法
  - ❑量子搜索
  - ❑幅度放大
  - ❑量子计数（量子幅度估计）

量子计数

- 计数: 对一个搜索问题，如何确定其解的个数
- 在Grover搜索中有 $\sqrt{M/N} = \sin(\theta)$，因此问题可以转化为求$\theta$
- 在$\{|\psi_0\rangle, |\psi_1\rangle\}$基的表象下，迭代算子$G$可以写成以下形式

$$G = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix} \quad 即 \begin{cases} G|\psi_0\rangle = \cos(2\theta)|\psi_0\rangle + \sin(2\theta)|\psi_1\rangle \\ G|\psi_1\rangle = -\sin(2\theta)|\psi_0\rangle + \cos(2\theta)\,|\psi_1\rangle \end{cases}$$

$$G = (2|\psi\rangle\langle\psi| - I)\underbrace{(2|\psi_0\rangle\langle\psi_0| - I)}_{\text{Oracle}}$$



量子计数

- 计数: 对一个搜索问题，如何确定其解的个数
- 在Grover搜索中有 $\sqrt{M/N} = \sin(\theta)$，因此问题可以转化为求$\theta$
- 在$\{|\psi_0\rangle, |\psi_1\rangle\}$基的表象下，迭代算子$G$可以写成以下形式

$$G = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix} \quad \text{即} \begin{cases} G|\psi_0\rangle = \cos(2\theta)|\psi_0\rangle + \sin(2\theta)|\psi_1\rangle \\ G|\psi_1\rangle = -\sin(2\theta)|\psi_0\rangle + \cos(2\theta)\,|\psi_1\rangle \end{cases}$$

- 矩阵G的特征值和其对应的特征向量分别为

$$\lambda_\pm = e^{\pm 2i\theta}, \quad |\psi_\pm\rangle = \frac{|\psi_0\rangle \mp i|\psi_1\rangle}{\sqrt{2}}$$

- 而初态$|\psi\rangle$正好是两个本征态的叠加（注：两分项概率幅不同）

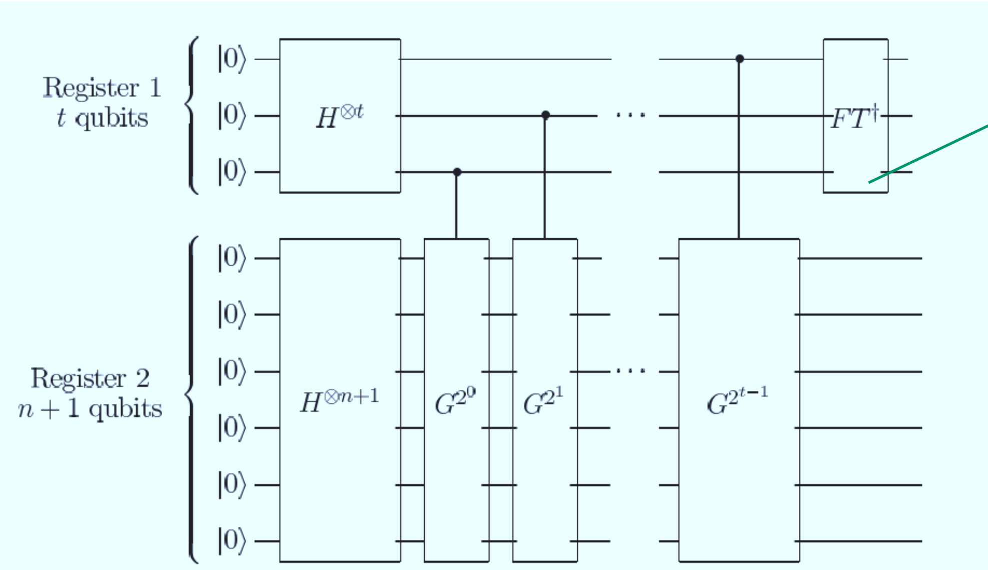
$$|\psi\rangle = \cos(\theta)|\psi_0\rangle + \sin(\theta)|\psi_1\rangle = \frac{e^{i\theta}|\psi_+\rangle + e^{-i\theta}|\psi_-\rangle}{\sqrt{2}}$$

$$|0\rangle|\psi\rangle \xrightarrow{\text{相位估计}: \mathrm{U}\to\mathrm{G},\ \sum_u c_u|u\rangle \to \frac{e^{i\theta}|\psi_+\rangle + e^{-i\theta}|\psi_-\rangle}{\sqrt{2}}} \frac{e^{i\theta}|2\tilde{\theta}\rangle|\psi_+\rangle + e^{-i\theta}|2\pi - 2\tilde{\theta}\rangle|\psi_-\rangle}{\sqrt{2}}$$

测量，可得到 $2\tilde{\theta}$ 或 $2\pi - 2\tilde{\theta}$，因此可得$\sqrt{\frac{M}{N}} = \sin(\theta) = \sin(\pi - \theta)$

从U容易实现控制U（见HHL）

复杂度



类似于相位估计复杂度：$\mathcal{O}(\frac{1}{\Delta\theta}(2+\frac{1}{2\eta})T_G)$

其中$\Delta\theta$表示θ的误差，$1-\eta$是成功概率的下界（这里可取常数），T_G为执行一次G需要的时间。

利用上述算法，可以得到$\mathrm{M}=\mathrm{N}\cdot\sin^2\theta$的一个估计。假设估计的误差为ΔM，则

$$\left|\frac{\Delta\mathrm{M}}{N}\right| = |\sin^2(\theta+\Delta\theta)-\sin^2\theta| = |\sin(\theta+\Delta\theta)+\sin(\theta)||\sin(\theta+\Delta\theta)-\sin(\theta)|$$

$$\leq |\,2\sin(\theta)+\ \Delta\theta|\cdot|\Delta\theta| = 2\sqrt{M/N}|\Delta\theta|+\Delta\theta^2$$

泰勒展开

因此 $|\Delta\mathrm{M}| \leq (2\sqrt{MN}|\Delta\theta|+N\Delta\theta^2)$

令$|\Delta\mathrm{M}|\leq\epsilon$。此时可取$\Delta\theta$为$\mathcal{O}(\epsilon/\sqrt{MN})$，因此算法复杂度为$\mathcal{O}(\frac{\sqrt{MN}}{\epsilon})$。

总结

目标	输入	输出	误差	复杂度
对于搜索问题，给定一个可以识别N个元素里面M个目标元素的量子oracle O，求出M的值	$\|0\rangle$	$(e^{i\theta}\|2\tilde{\theta}\rangle\|\psi_+\rangle + e^{-i\theta}\|2\pi-2\tilde{\theta}\rangle\|\psi_-\rangle)/\sqrt{2}$	ϵ	$\mathcal{O}(\frac{\sqrt{NM}}{\epsilon})$（成功概率取常数）二次加速

- 经典算法：如果想要以至少3/4的概率得到精度为$\mathcal{O}(c\sqrt{M})$ 的 M 的估计（c为常数），至少需要进行 $\Omega(N)$ 次Oracle调用
- 量子算法：复杂度为 $\mathcal{O}(\frac{\sqrt{MN}}{\epsilon}\left(2+\frac{1}{2\eta}\right))$ （为方便比较加上了成功概率项），其中若精度ϵ的取值和经典情形相同，为 $\mathcal{O}(c\sqrt{M})$，同时成功概率 $1-\eta=\frac{3}{4}$ 时，需要的Oracle调用次数为 $\mathcal{O}(\sqrt{N})$

思考：初态不是均匀叠加态时，能否做计数？此时G算子的矩阵形式、特征值和特征向量，初态在G特征向量下的展开形式，相位估计的末态分别有何不同？

Email: gaof@bupt.edu.cn
Tel: 86 -10 -62283192
Web: www.bupt.edu.cn

谢 谢！