Lecture 21

Therefore,

$$A^k = \begin{pmatrix} \cos(2k\theta) & -\sin(2k\theta) \\ \sin(2k\theta) & \cos(2k\theta) \end{pmatrix}. \tag{122}$$

Applying A^k to $|\psi\rangle$ the basis $\{|\psi_0\rangle, |\psi_1\rangle\}$gives

$$\begin{pmatrix} \cos(2k\theta) & -\sin(2k\theta) \\ \sin(2k\theta) & \cos(2k\theta) \end{pmatrix} \begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix} = \begin{pmatrix} \cos(2k\theta)\cos(\theta) - \sin(2k\theta)\sin(\theta) \\ \sin(2k\theta)\cos(\theta) + \cos(2k\theta)\sin(\theta) \end{pmatrix} = \begin{pmatrix} \cos((2k+1)\theta) \\ \sin((2k+1)\theta) \end{pmatrix}. \tag{123}$$

Therefore, back in the original basis,

$$(GU_f)^k |\psi\rangle = (-1)^k(\cos((2k+1)\theta)|\psi_0\rangle + \sin((2k+1)\theta)|\psi_1\rangle). \tag{124}$$

This is the key *amplitude amplification* formula.

The probability of measuring $|x^*\rangle$ (the marked element) is

$$\begin{aligned} |\langle x^*|(GU_f)^k|\psi\rangle\rangle|^2 &= |\langle \psi_1|(GU_f)^k|\psi\rangle\rangle|^2 \\ &= \sin^2((2k+1)\theta). \end{aligned}$$

Now we choose k optimally, that is $(2k+1)\theta = \pi/2$, so set $k := \lceil \pi/(4\theta) - 1/2 \rceil$ but $\theta = \arcsin(\sqrt{1/N}) \geq \sqrt{1/N}$, so $k \leq \lceil (\pi/4)\sqrt{N} \rceil$. If $k = \pi/(4\theta) - 1/2$, the probability of measuring $|x^*\rangle$ is 1, with the extra ceiling, can check that the probability is at least $1 - 1/N \approx 1$ for N large. Comment: see Lecture 3 here for details

The number of queries used is about $(\pi/4)\sqrt{N}$. □

Remark 7. The algorithm can be extended to work when the number of marked elements is unknown, using techniques like fixed-point amplitude amplification: see [Yoder, Low, and Chuang].

Grover's algorithm is optimal in the query model We follow the BBBV97 argument. Comment: give some intuition

For $t \in \{1, \dots, T\}$, let

$$|\psi_i\rangle = \sum_{x,b,w} \alpha^t_{x,b,w} |x, b, w\rangle \tag{125}$$

denote the state of the algorithm just after U_i when run on $f\colon \{0,1\}^n \to \{0,1\}$ such that $f(x) = 0$ for all $x \in \{0,1\}^n$.

For $x \in \{0,1\}^n$ and $t \in \{1, \dots, T\}$, let

$$w^t_x := \sum_{b,w} |\alpha^t_{x,b,z}|^2. \tag{126}$$

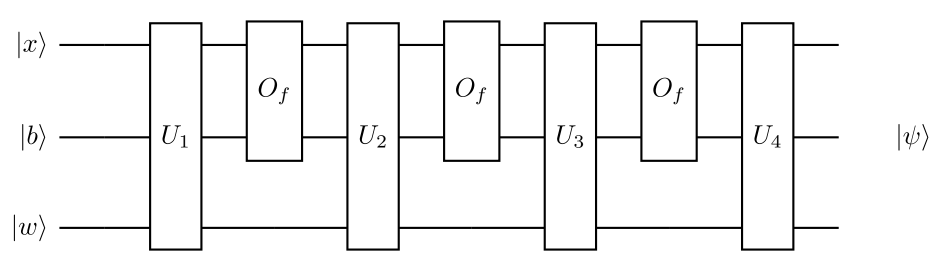
For $x \in \{0,1\}^n$, define the query weight (or magnitude) on x as

$$w_x := \sum_{t=1}^T w^t_x = \sum_{i=1}^T \sum_{b,z} |\alpha_{x,b,z}|^2; \tag{127}$$

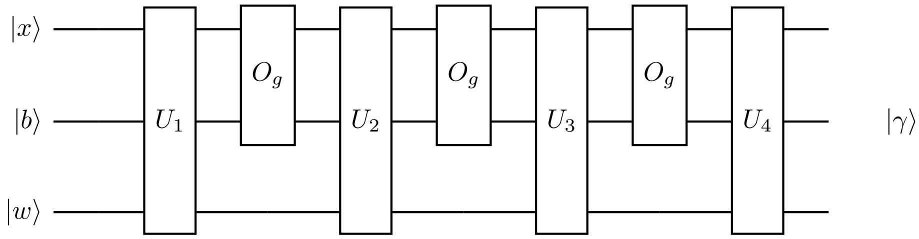
Observe that

$$\sum_x w_x = T. \tag{128}$$

So there must exists x^* such that $w_{x^*} \leq T/N$.
Let $g\colon \{0,1\}^n \to \{0,1\}$ be the function such that $g(x^*) = 1$ and $g(x) = 0$ for all $x \neq x^*$.
Example when $T = 3$. (The number T counts the number of queries to f.)
Let the output of this circuit be $|\psi\rangle$.



Let the output of this circuit be $|\gamma\rangle$.



Note that the circuit producing $|\psi\rangle$ and $|\gamma\rangle$ have the *same* U_i's and only differ in $O_f \leftrightarrow O_g$. This models the fact that the algorithm can only access f or g through queries.

Claim 1. $\| \, |\psi\rangle - |\gamma\rangle \, \| \leq 2 \sum_{t=1}^{T} \sqrt{w_{x^*}^t}$

Proof. Proof uses the hybrid argument. $\square$