Lecture 20

Grover's search algorithm. Grover's algorithm solves the problem of *unstructured search*. Suppose we have a function $f\colon \{0,1\}^n \to \{0,1\}$, and we are promised that either:

1. $f(x) = 0$ for all $x \in \{0,1\}^n$, or
2. there exists a unique $x^* \in \{0,1\}^n$ such that $f(x^*) = 1$ and $f(x) = 0$ for all $x \neq x^*$.

The goal is to determine which case holds, and if there is a marked element x^*, to find it. Comment: Think of f as evaluating a SAT formula.

Classically, you would need to query roughly 2^n values in the worst case. Grover's algorithm can solve this problem using $O(\sqrt{2^n})$ queries, giving a quadratic speedup.

Fact 10. In the classical query model, distinguishing these two cases requires $\Omega(2^n)$ queries in the worst case, since you might need to check nearly all 2^n possible inputs before finding x^* (or confirming no such x^* exists).

Recall from Lecture 13 that the quantum phase oracle for $f\colon \{0,1\}^n \to \{0,1\}$ is given by

$$U_f \left|x\right\rangle \left|b\right\rangle = (-1)^{b\cdot f(x)} \left|x\right\rangle \left|b\right\rangle, \tag{112}$$

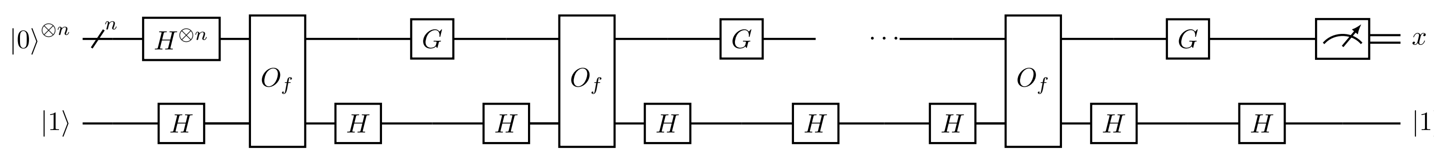
where $x \in \{0,1\}^n, b \in \{0,1\}$. The phase kickback trick shows that $U_f = (\mathbb{1}_{2^n} \otimes H) O_f (\mathbb{1}_{2^n} \otimes H)$.

Proposition 9 (Grover's algorithm)**.** *Given query access to $f\colon \{0,1\}^n \to \{0,1\}$ where either $f(x) = 0$ for all x, or there exists a unique $x^* \in \{0,1\}^n$ with $f(x^*) = 1$, Grover's algorithm can distinguish these cases and find x^* (if it exists) using*

$$O(\sqrt{2^n}) = O(2^{n/2}) \tag{113}$$

queries to f.

The quantum circuit for Grover's algorithm is:



where the pair (U_f, G) is repeated $k \approx \frac{\pi}{4}\sqrt{2^n}$ times. The intermediate H gates on the ancilla could be deleted as they satisfy $H^2 = \mathbb{1}$ – drawing them makes it clear where the U_fs come from.

Proof. Let $N := 2^n$. Let $\left|\psi\right\rangle$ denote the N-dimensional quantum state

$$\left|\psi\right\rangle := H^{\otimes n} \left|0^n\right\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} \left|x\right\rangle. \tag{114}$$

Let $G \in \mathbb{C}^{N\times N}$ denote the *Grover diffusion operator*:

$$G := \mathbb{1}_N - 2|\psi\rangle\langle\psi|. \tag{115}$$

Comment: may discuss decomposing this operator into elementary quantum gates if there's time, else just Google or see, e.g., the first answer to this StackExchange post.

Let $V_f \in \mathbb{C}^{N\times N}$ denote the operation U_f implements on the first register when the ancilla qubit register is set to $\left|1\right\rangle$, i.e.,

$$V_f\colon \left|x\right\rangle \mapsto (-1)^{f(x)} \left|x\right\rangle \tag{116}$$

Then, the pair (U_f, G) forming each block implements the "Grover iteration" unitary GV_f on the first register. So suffices to analyze $(GV_f)^k \left|\psi\right\rangle$.

We analyze two cases:

1. **Case: $f(x) = 0$ for all $x \in \{0,1\}^n$.** In this case, $V_f \left|x\right\rangle = \left|x\right\rangle$ for all x, so $(GV_f)^k = G^k$. Since $G\left|\psi\right\rangle = -\left|\psi\right\rangle$, we have $G^k \left|\psi\right\rangle = (-1)^k \left|\psi\right\rangle$. Therefore, measuring $(GV_f)^k \left|\psi\right\rangle$ gives a uniformly random $x \in \{0,1\}^n$, and we can verify that $f(x) = 0$, confirming this case.

2. **Case: there exists unique $x^* \in \{0,1\}^n$ with $f(x^*) = 1$.** Define the following quantum states:

$$|\psi_0\rangle := \frac{1}{\sqrt{N-1}} \sum_{x|f(x)=0} |x\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x^*} |x\rangle \,, \tag{117}$$

$$|\psi_1\rangle := |x^*\rangle \,. \tag{118}$$

These are normalized states: $|\psi_0\rangle$ corresponds to the unmarked elements, and $|\psi_1\rangle$ is the unique marked element. Note that $\langle\psi_0|\psi_1\rangle = 0$ (orthogonal).

The initial state $|\psi\rangle$ can be written as

$$|\psi\rangle = \sqrt{\frac{N-1}{N}} |\psi_0\rangle + \sqrt{\frac{1}{N}} |\psi_1\rangle = \cos(\theta) |\psi_0\rangle + \sin(\theta) |\psi_1\rangle \,, \tag{119}$$

where $\theta := \arcsin(\sqrt{1/N}) \in (0, \pi/2]$.

Analysis of Grover iteration GV_f:

We compute how GV_f acts on $|\psi_0\rangle$ and $|\psi_1\rangle$:

$$\begin{aligned}
GV_f |\psi_0\rangle &= G |\psi_0\rangle \quad (\text{since } V_f |\psi_0\rangle = |\psi_0\rangle) \\
&= |\psi_0\rangle - 2 |\psi\rangle \langle\psi|\psi_0\rangle \\
&= |\psi_0\rangle - 2\cos(\theta) |\psi\rangle \\
&= |\psi_0\rangle - 2\cos(\theta)(\cos(\theta) |\psi_0\rangle + \sin(\theta) |\psi_1\rangle) \\
&= (1 - 2\cos^2(\theta)) |\psi_0\rangle - 2\cos(\theta)\sin(\theta) |\psi_1\rangle \\
&= -\cos(2\theta) |\psi_0\rangle - \sin(2\theta) |\psi_1\rangle \,.
\end{aligned}$$

Similarly,

$$\begin{aligned}
GV_f |\psi_1\rangle &= -G |\psi_1\rangle \quad (\text{since } U_f |\psi_1\rangle = -|\psi_1\rangle) \\
&= -|\psi_1\rangle + 2 |\psi\rangle \langle\psi|\psi_1\rangle \\
&= -|\psi_1\rangle + 2\sin(\theta) |\psi\rangle \\
&= 2\sin(\theta)(\cos(\theta) |\psi_0\rangle + \sin(\theta) |\psi_1\rangle) - |\psi_1\rangle \\
&= 2\sin(\theta)\cos(\theta) |\psi_0\rangle + (2\sin^2(\theta) - 1) |\psi_1\rangle \\
&= \sin(2\theta) |\psi_0\rangle - \cos(2\theta) |\psi_1\rangle \,.
\end{aligned}$$

Therefore, GV_f always maps the 2-dimensional subspace $\mathrm{span}(|\psi_0\rangle, |\psi_1\rangle)$ to itself. We can reduce the analysis to linear algebra in $\mathbb{C}^2$ by working in the basis $\{|\psi_0\rangle, |\psi_1\rangle\}$.

In this basis, $|\psi\rangle$ is represented as

$$\begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix}, \tag{120}$$

and $-GV_f$ is represented as the matrix

$$A := \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix}. \tag{121}$$

This is the rotation matrix by angle 2θ anticlockwise!

Comment: Note that $G = \mathbb{1}_N - 2|\psi\rangle\langle\psi|$ is a reflection about the hyperplane perpendicular to $|\psi\rangle$, while $V_f = \mathbb{1}_N - 2|\psi_1\rangle\langle\psi_1|$ (check!) is a reflection about the hyperplane perpendicular to $|\psi_1\rangle$, so the above calculations also proves the mathematical fact that a product of two reflections is a rotation.