Is there a better algorithm?

Possibly. Observe that our algorithm was agnostic to the structure of φ. It just relied on the property that we can efficiently check if $\varphi(x) = 0$ or 1.

This is called "unconstrained search". We produced a q. alg for unconstrained search which in turn yields an algorithm for any special case of search such as finding the sol. to NP-complete problems (which have significantly more structure).

Today, we prove that no q. alg. can solve unconstrained search better than Grover's.

Def. (Unconstrained search) Let $N = 2^n$.

Let $f : [N] \to \{0,1\}$. A query algorithm for f is one consisting of standard q. comp. axioms + access to the unitary

$$O_f : |x, b\rangle \mapsto (-1)^{b \cdot f(x)} |x, b\rangle \quad \text{for } x \in [N],\ b \in \{0,1\}.$$

O_f = "the oracle". A query algorithm for unconstrained search is one that outputs an x s.t. $f(x) = 1$ w.h.p.

Thm Any query alg for unconstrained search requires $\Omega(\sqrt{N})$ queries.

We will prove the decision version is hard.

Def. (Decision)

$f: [N] \to \{0, 1\}$ s.t.

① either $f \equiv 0$ or

② $f(z') = 1$ for exactly 1 value of z'.

For an alg., let A^f be the random variable as the output (classical).

If it solves the problem,

① If $f \equiv 0$, then $\Pr[A^f = 1] \leq 1/3$

② If $f(z') = 1$ for exactly 1 value, then

$$\Pr[A^f = 1] \geq 2/3.$$

Case ①: $O_f : |x\rangle|b\rangle \longmapsto (-1)^{b \cdot 0} |x, b\rangle = |x, b\rangle$

so $O_f = \mathbb{1}$

Case ②: $O_f : |x\rangle|b\rangle \longmapsto (-1)^{b \cdot \mathbb{1}\{x = z'\}} |x, b\rangle$

so $O_f = \mathbb{1} - 2|z', 1\rangle\langle z', 1|.$

Let's define $z = (z', 1)$.

so Case ① is $O = \mathbb{1}$ or case ②, $O = P_z = \mathbb{1} - 2|z\rangle\langle z|.$

Revised setup: O is either $\mathbb{1}$ or P_z for some z. Any q. alg that decides which of the two cases requires $\Omega(\sqrt{N})$ queries to O.

Thm Any q. alg that decides this requires $\frac{1}{6}\sqrt{N}$ oracle queries.

Intuition

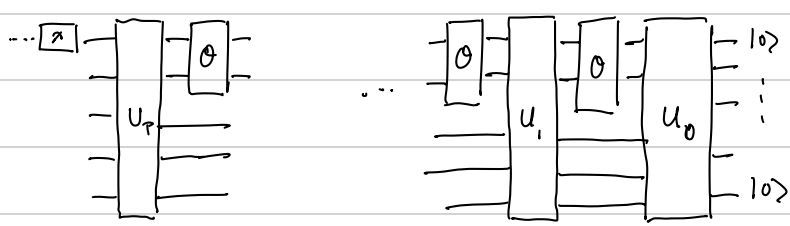
For a random vec $|\phi\rangle \in \mathbb{C}^N$, $\mathbb{1}|\phi\rangle \approx P_z|\phi\rangle$.

$$|\phi\rangle = \sum \alpha_x |x\rangle \quad \text{then} \quad P_z|\phi\rangle = \sum_{x \neq z} \alpha_x |x\rangle - \alpha_z |z\rangle$$

A random vector has only $1/\sqrt{N}$ mass α_z. So, the applications of P_z and $\mathbb{1}$ are roughly the same and can be interchanged at only a negligible cost.

Pf of thm

Drawing of generic T query alg. $U_0, \ldots, U_T$ are any unitaries.



Assume the algorithm correctly decides the decision version of the problem:

For any $z \in [N]$, let

$$|\Psi_z\rangle = U_T \; P_z \; U_{T-1} \; P_z \; \cdots \; P_z \; U_1 \; P_z \; U_0 \; |0 \ldots 0\rangle$$

and let

$$|\Psi_{\mathbb{1}}\rangle = U_T \; \mathbb{1} \; U_{T-1} \; \mathbb{1} \; \cdots \; \mathbb{1} \; U_1 \; \mathbb{1} \; U_0 \; |0 \ldots 0\rangle$$

Now, $\| |\Psi_z\rangle - |\Psi_{\mathbb{1}}\rangle \| \geq 1/3$ b.c. the first qubit of $|\Psi_z\rangle$ measures to 1 w pr $\geq 2/3$ and first qubit of $|\Psi_{\mathbb{1}}\rangle$ w pr $\leq 1/3$ and so they can be distinguished w pr $\geq 1/3$.

$$|h_T\rangle = U_T \; \mathbb{1} \; U_{T-1} \; \mathbb{1} \; \cdots \; \mathbb{1} \; U_1 \; \mathbb{1} \; U_0 \; |0 \ldots 0\rangle$$

$$|h_{T-1}\rangle = U_T \; P_z \; U_{T-1} \; \mathbb{1} \; \cdots \; \mathbb{1} \; U_1 \; \mathbb{1} \; U_0 \; |0 \ldots 0\rangle$$

$$|h_{T-1}\rangle = U_T \; P_z \; U_{T-1} \; P_z \; \cdots \; \mathbb{1} \; U_1 \; \mathbb{1} \; U_0 \; |0 \ldots 0\rangle$$

$$|h_0\rangle = U_T \; P_z \; U_{T-1} \; P_z \; \cdots \; P_z \; U_1 \; P_z \; U_0 \; |0 \ldots 0\rangle$$

$|h_T\rangle = |\psi_{11}\rangle$ and $|h_0\rangle = |\psi_z\rangle$.

$$\| |\psi_{11}\rangle - |\psi_z\rangle \| = \| |h_T\rangle - |h_0\rangle \|$$

$$\leq \sum_{j=1}^{T} \| |h_j\rangle - |h_{j-1}\rangle \|.$$

$$\| |h_T\rangle - |h_{T-1}\rangle \| = \| U_T (\mathbb{1} - P_z) U_{T-1} \cdots U_0 |0 \ldots 0\rangle \|$$

$$= \| U_T (2|z\rangle\langle z|) U_{T-1} \cdots U_0 |0 \ldots 0\rangle \|$$

$$= 2 \| \langle z | U_{T-1} \cdots U_0 |0 \ldots 0\rangle \|$$

This has a physical interpretation. If $|\varphi_j\rangle = U_j \cdots U_0 |0 \ldots 0\rangle$.

Then let

$$P_{x,j} = \Pr\{ |\varphi_j\rangle \text{ measures to } x \}$$

$$= \| \langle x | U_j \cdots U_0 |0 \ldots 0\rangle \|^2.$$

So, $\| |h_T\rangle - |h_{T-1}\rangle \| = 2\sqrt{P_{z,T-1}}$.

Similarly, show $\| |h_{T-1}\rangle - |h_{T-2}\rangle \| = 2\sqrt{p_{z,T-2}}$

and $\| |h_j\rangle - |h_{j-1}\rangle \| = 2\sqrt{p_{z,j}}$.

Then, $\frac{1}{3} \leq 2 \sum_{j=0}^{T-1} \sqrt{p_{z,j}}$.

This is true for any $z \in [N]$ such that $\mathbb{1}$ & P_z are distinguished.
But, we can distinguish $\mathbb{1}$ & all $\{P_z\}$. So,

$$\frac{1}{6} N \leq \sum_{z \in [N]} \sum_{j=0}^{T-1} \sqrt{p_{z,j}}$$

$$= \sum_{j=0}^{T} \left(N \cdot \underbrace{\sum_{z \in [N]} p_{z,j}}_{\leq 1} \right)^{1/2}$$

$$\leq \sum_{j=0}^{T} \sqrt{N}$$

$$= T\sqrt{N}.$$

$$\Rightarrow T \geq \frac{1}{6}\sqrt{N}.$$