11/11/10 Grover's Search quantum algorithm

Search problem

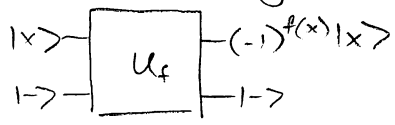
Let $f: \{0,1\}^n \to \{0,1\}$.

Find an x so $f(x)=1$, if there is one.

Classical algorithm: Try the different x, one at a time $\Rightarrow \Theta(2^n)$ calls.

Quantum algorithm:

Assume, for simplicity, that $f(x)=1$ has a unique solution, $f(a)=1$.



General abstract quantum algorithm design paradigm:

Let R_1, R_2 be reflections (i.e., $R_1^2 = R_2^2 = \mathbb{1}$).

Apply $R_1 R_2 R_1 R_2 R_1 R_2 \cdots$ alternating reflections

(more later)

In this case, V_f is a reflection, $V_f^2 = \mathbb{1}$, $V_f = \mathbb{1} - 2|a\rangle\langle a|$.

Since, so far as we know, all inputs are equally likely, we should use something symmetrical. As the symmetrical state is $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$, a natural choice is to reflect about the 1D subspace spanned by $|\psi\rangle$, i.e., let

$$W = 2|\psi\rangle\langle\psi| - \mathbb{1}.$$

Algorithm.

Start in state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$

Apply V

Apply W

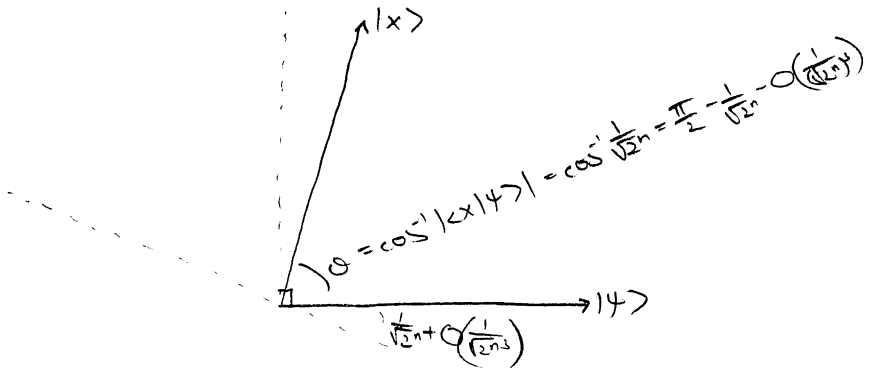
Apply V

Apply W

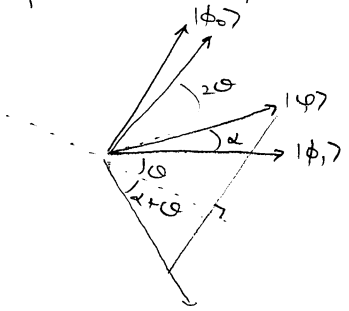
$\vdots$

Analysis:

Consider the subspace spanned by $|x\rangle$ and $|\psi\rangle$



The operators V and W both fix this subspace. Therefore the quantum computer state will always lie in this subspace



→ the product $(2|\phi_1\rangle\langle\phi_1| - \mathbb{1})(\mathbb{1} - 2|\phi_0\rangle\langle\phi_0|)$ implements a rotation by angle 2θ

⇒ state rotates by $2\theta \approx \frac{2}{\sqrt{2^n}}$ in every iteration

After $\sim \frac{\pi/2}{2/\sqrt{2^n}} = O(\sqrt{2^n})$ iterations, the state lies close to $|x\rangle$. Measuring in the computational basis will give x with constant probability.

Implementing the algorithm:

As we have done before

the "diffusion operator" $W = 2|\psi\rangle\langle\psi| - \mathbb{1} = 2\begin{pmatrix} \frac{1}{N} & \cdots & \frac{1}{N} \\ \vdots & & \vdots \\ \frac{1}{N} & \cdots & \frac{1}{N} \end{pmatrix} - \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

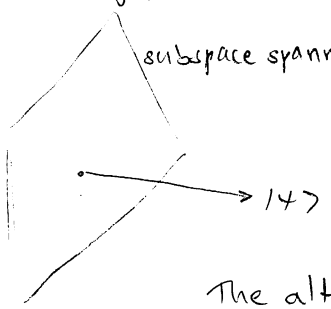
$= H^{\otimes n}\left(2|0^n\rangle\langle 0^n| - \mathbb{1}\right)H^{\otimes n}$

can be implemented with $O(n)$ gates, and is independent of f

⇒ Overall complexity is $O(\sqrt{2^n})$ calls to f and $O(\sqrt{2^n}\, n)$ total operations.

— a square-root speedup!

More generally, if there are M solutions $a_1, \ldots, a_M$, then $V_f = \mathbb{1} - 2\sum_{j=1}^{M} |a_j\rangle\langle a_j|$.



The alternating reflections, by symmetry, will keep the state in the two-dimensional subspace spanned by

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \quad \text{and} \quad |\phi\rangle = \frac{1}{\sqrt{M}} \sum_{j=1}^{M} |a_j\rangle$$

Since $\langle\psi|\phi\rangle = \frac{M}{\sqrt{NM}} = \sqrt{\frac{M}{N}}$ with $N = 2^n$, the number of steps required is only $O\left(\sqrt{\frac{N}{M}}\right)$. (Classically N/M steps are needed.)

If M is unknown, then guess

$$\tilde{M} = N, \quad \tilde{M} = N/2, \quad \tilde{M} = N/4, \ldots, \quad \tilde{M} = 1$$

going down until a solution is found.

Applications of Grover's search algorithm

1. Solve NP-complete problems?

   Let f be the evaluation of a 3SAT formula, so $f(x) = 1$ means x is a satisfying assignment

   $\sqrt{2^n}$ instead of 2^n steps

   (still exponential time)

2. Unsorted database search

   let x index the items in a database, $f(x)$ a predicate on that database entry

   note: database needs to be stored in memory that can be accessed coherently (ie. in superposition) at unit cost

3. Many other algorithms use Search as a subroutine, e.g., Minimum, Approx. Counting, Collision, Matrix Mult. Verification
   $n^{1/2} \to n^{1/3}$ $\quad$ $n^2 \to n^{1.75}$

Lower bounds:

SAT: $f(x_1, \ldots, x_n) = c_1 \wedge c_2 \wedge \cdots \wedge c_m$

Is there a satisfying assignment?

$SAT \leq_R$ Unique-SAT [Valiant, V. Vazirani]

a poly(n)-time algorithm would give P = NP

a poly(n)-time quantum algorithm would give BQP ⊇ NP.

Theorem: Let f be a black-box-accessible function either $f \equiv 0$ or $\exists!\, a$ such that $f(a) = 1$.

Then any quantum search algorithm must make $\Omega(\sqrt{N}) = \Omega(2^{n/2})$ queries.

(no black-box exponential speedup is possible for SAT)

Proof: Suppose A solves search in T steps.

Calibration: Run A on $f \equiv 0$

$|\phi_t\rangle$ = state after t queries $= \sum_x |x\rangle \otimes |\alpha_{tx}\rangle = U_t |\phi_{t-1}\rangle$

(first register: query register; second register: workspace)

$\||\phi_t\rangle\| = 1 \Rightarrow \forall t, \sum_x \||\alpha_{tx}\rangle\|^2 = 1$

Since $\sum_{t=0}^{T-1} \sum_x \||\alpha_{tx}\rangle\|^2 = T = \sum_x \sum_t \||\alpha_{tx}\rangle\|^2$

there is some z with $\sum_t \||\alpha_{tz}\rangle\|^2 \leq \frac{T}{N}$. Fix z.

Hybrid argument: Now run A on g with $g(z) = 1$, $g(x) = 0\ \forall x \neq z$.

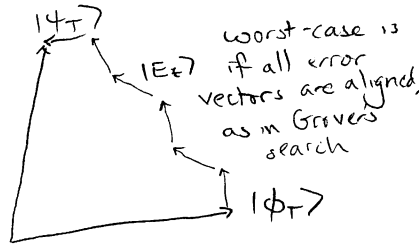
$|\psi_t\rangle$ = state after t queries $= U_t (\mathbb{1} - 2|z\rangle\langle z|) |\psi_{t-1}\rangle$

$|\psi_0\rangle = |\phi_0\rangle$

$|\psi_1\rangle = U_1 (\mathbb{1} - 2|z\rangle\langle z|) |\psi_0\rangle$

$= U_1 |\phi_0\rangle - 2|z\rangle|\alpha_{0z}\rangle$

$= |\phi_1\rangle + |E_0\rangle$



$|\psi_2\rangle = U_2 (\mathbb{1} - 2|z\rangle\langle z|) |\psi_1\rangle$

$= U_2 |\phi_1\rangle - 2|z\rangle|\alpha_{1z}\rangle + U_2 (\mathbb{1} - 2|z\rangle\langle z|) |E_0\rangle$

$\vdots$

$|\psi_T\rangle = |\phi_T\rangle + |\tilde{E}_0\rangle + |\tilde{E}_1\rangle + \cdots + |\tilde{E}_{T-1}\rangle$

$\Rightarrow \||\psi_T\rangle - |\phi_T\rangle\| \leq \sum_{t=0}^{T-1} \||E_T\rangle\| = 2 \sum_t \||\alpha_{tz}\rangle\|$

$\leq 2\sqrt{T} \left(\sum_t \||\alpha_{tz}\rangle\|^2 \right)^{1/2}$ by Cauchy-Schwarz

$\leq 2\sqrt{T} \sqrt{\frac{T}{N}}$

$= \frac{2T}{\sqrt{N}} \Rightarrow T = \Omega(\sqrt{N})$ □