Quantum searching and NP

Unstructured search for a unique item in $N = 2^n$ items.

Given: oracle for f : n-bits → 1-bit

Promise: there is exactly one x_0 with $f(x_0) = 1$

Problem: find x_0 (with constant probability)

Quantum oracle $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$ as usual.

Classically: $O(N)$ queries necessary and sufficient—
query k times: prob(see x_0) $= k/N$ so $k = O(N)$ for const prob.

Quantumly: can do with $O(\sqrt{N})$ queries (plus $O(\log N)$ processing o'head per query)

Also — no quantum procs can do it with fewer than $O(\sqrt{N})$ queries.

So get (only) a quadratic speed-up.

Remark 1

Structured vs. unstructured search

Given linear ordering of $N = 2^n$ items (e.g. alphabetical phonebook) can find any desired item with

Classically: $1 \log N = n$ queries necessary & sufficient

Can show

Quantumly:

$$\frac{1}{\pi} n + O(1) \leq \#\text{queries} \leq 0.53n$$

- constant factor improvement but still impossible classically!

"What kind of structure is good for quantum vs classical computing?"

Remark 2.

"Physical" vs "Mathematical" search

Search computer file/phonebook vs search for constraint satisfaction etc.

Physical database $N = 2^n$ items, laid out as N physical systems

e.g. lookup table of values of unique-sat f: n-bits → 1-bit

- need $O(N)$ physical resources to represent it.
- need $O(N)$ elementary gates just to examine items at $O(N)$ distance ("typical" query)

– so swamps $\sqrt{N}$ reduction in number of queries!

– pointing to good item gives x_0 in unary! (distance from end) & then unary → binary conversion needs expon(n) time!

Remark 2 (cont.)

Mathematical search

Have abstract space of $N = 2^n$ possibilities (no a priori physical existence!) e.g. satisfiability or constraint satisfaction problems

- can easily construct representation of any candidate x as $O(n)$-bit string (binary representation)
- can easily test if it is good e.g. have formula/oracle for f or list of constraint formulae to check.
- now requires only $O(n)$ effort to access any item or set up uniform superposition query etc

– So N vs $\sqrt{N}$ query complexity is significant.

Preliminaries on projections & reflections for n-qubit states

In Grover's quantum searching algorithm all states will have <u>real</u> components and have nice visualisation in real Euclidean geometry.

For any n-qubit ket vector $|\alpha\rangle$ (column)

Bra vector $\langle\alpha| = |\alpha\rangle^\dagger$ is dual (row)

$P_\alpha = |\alpha\rangle\langle\alpha|$ is operator of "projection parallel to $|\alpha\rangle$"

$P_\alpha|\beta\rangle = (|\alpha\rangle\langle\alpha|)|\beta\rangle = |\alpha\rangle\langle\alpha|\beta\rangle$

Any $|\beta\rangle = x|\alpha\rangle + |\alpha^\perp\rangle$ uniquely with $|\alpha^\perp\rangle \perp |\alpha\rangle$

and then $P_\alpha|\beta\rangle = x|\alpha\rangle$ $x = \langle\alpha|\beta\rangle$.

$I_\alpha = I - 2|\alpha\rangle\langle\alpha|$ is "reflection in hyperplane $\perp$ to $|\alpha\rangle$"

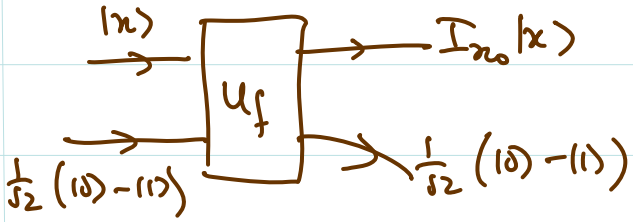
$I_\alpha|\beta\rangle = |\beta\rangle - 2|\alpha\rangle\langle\alpha|\beta\rangle$

$= -x|\alpha\rangle + |\alpha^\perp\rangle$

Grover's algorithm

Instead of U_f we'll use I_{x_0} on n-qubits

$$I_{x_0}|x\rangle = \begin{cases} |x\rangle & x \neq x_0 \\ -|x\rangle & x = x_0 \end{cases}$$



$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad H_n = H \otimes \cdots \otimes H \text{ on } n \text{ qubits}$$

Introduce Grover iteration operator

$$Q = -H_n I_0 H_n I_{x_0}$$

$I_0 \equiv I_{|0\ldots0\rangle}$ inverts sign of $|0\ldots0\rangle$ component.

Starting state

$$|\psi_0\rangle = H_n|0\ldots0\rangle = \frac{1}{\sqrt{N}} \sum_{\text{all } x} |x\rangle$$

Iteration:

$$|\psi_{n+1}\rangle = Q|\psi_n\rangle \qquad n = 1, 2, \ldots$$

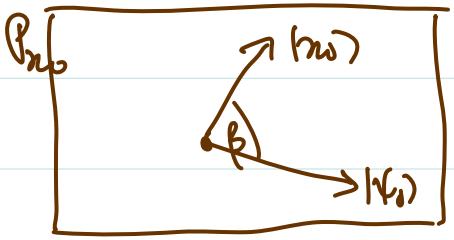
all real numbers.

Will prove:

Let P_{x_0} be plane spanned by (initially unknown) $|x_0\rangle$ & $|\psi_0\rangle$

(a) In P_{x_0} Q is rotation through 2α where $\sin\alpha = \frac{1}{\sqrt{N}}$

(b) In $2^n - 2$ dim orthogonal complement $P_{x_0}^{\perp}$, $Q = -I$



$\langle x_0|\psi_0\rangle = \frac{1}{\sqrt{N}}$ for all x_0.

$\beta = \arccos\frac{1}{\sqrt{N}}$ $\left(\approx \frac{\pi}{2} \text{ large } N\right)$

Hence: apply Q to $|\psi_0\rangle$ $\frac{\beta}{2\alpha}$ times i.e. $\frac{\arccos\frac{1}{\sqrt{N}}}{2\arcsin\frac{1}{\sqrt{N}}}$ times

and measure, to see x_0 with high probability.

Large N: $\beta \approx \frac{\pi}{2}$ $\alpha \approx \sin\alpha = \frac{1}{\sqrt{N}}$ so need $\frac{\pi}{4}\sqrt{N}$ iterations

Each use of Q needs <u>one</u> use of I_{x_0} & hence U_f.

plus $O(\log N)$ extra steps (H_n & I_0).

Proof that algorithm works

Fact 1: for any n-qubit U & state $|\psi\rangle$

$$U I_{|\psi\rangle} U^\dagger = U(I - 2|\psi\rangle\langle\psi|)U^\dagger = I_{U|\psi\rangle}.$$

Also $H^\dagger = H$ so

$$Q = -H_n I_0 H_n I_{x_0} = -I_{H_n|0\ldots0\rangle} I_{x_0} = -I_{|\psi_0\rangle} I_{|x_0\rangle}$$

for any $|v\rangle$ in P_{x_0}:

$$|v\rangle = a|x_0\rangle + b|\psi_0\rangle$$

$I_{|\psi_0\rangle}$ (resp. I_{x_0}) adds scalar mult of $|\psi_0\rangle$ (resp. $|x_0\rangle$)

so $Q|v\rangle \in P_{x_0}$ too.

i.e. $Q : P_{x_0} \to P_{x_0}$ linear, unitary

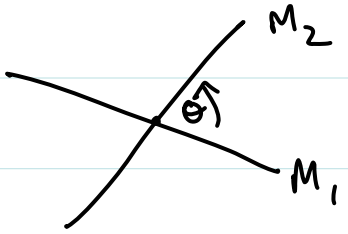
What is it?

Restricted to (real) plane P_{π_0}

$I_{|\pi_0\rangle}$ is reflection in line perp. to $|\pi_0\rangle$

$I_{|\psi_0\rangle}$ is reflection in line perp. to $|\psi_0\rangle$

Fact 2. In real 2-dim geometry



M_1, M_2 mirror lines

Reflection in M_1 followed by M_2

= rotation thru twice angle θ between M_1 & M_2

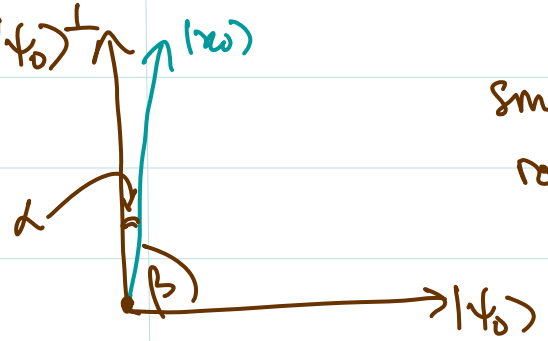
Hence $Q = -$ [rot^n thru twice angle between $|\pi_0\rangle$ & $|\psi_0\rangle$]

$\nwarrow 2\beta = 2\arccos\frac{1}{\sqrt{2}} \approx \pi$ (large!)

Fact 3. If I_v is reflection in mirror M perp. to v
then $-I_v$ is reflection in $M^\perp$, perp to M i.e. ||el to v.

[Any $|u\rangle = a|v\rangle + b|v^\perp\rangle$ for $|v\rangle, |v^\perp\rangle$ chosen orthonormal.
I_v reverses sign of a & $I_{v^\perp}$ reverses sign of $b \equiv -I_v$ action.]

Hence Q = rot^n thru 2α
where α = angle betwn
$|x_0\rangle$ & $|\psi_0\rangle^\perp$ in P_{x_0}
So $\sin\alpha = \cos\beta = \frac{1}{\sqrt{n}}$



small incremental rotation 2α

If $|A\rangle \perp P_{x_0}$ i.e. $\langle x_0|A\rangle = \langle\psi_0|A\rangle = 0$

then $I_{x_0}|A\rangle = (I - 2|x_0\rangle\langle x_0|)|A\rangle = |A\rangle$

$I_{|\psi_0\rangle}|A\rangle = \quad \ldots \quad = A$

So $Q|A\rangle = -I_{|\psi_0\rangle} I_{x_0}|A\rangle = -A$

i.e. $Q = -I$ in $P_{x_0}^\perp$.

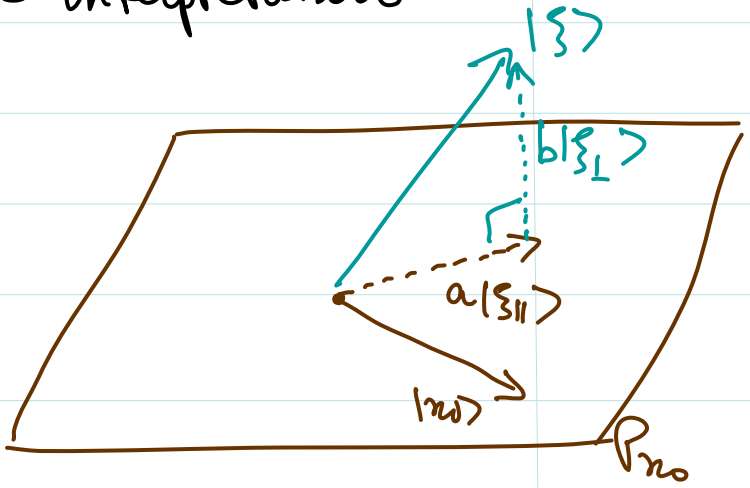
Can significantly generalise Grover's algorithm!

- start state $|\psi_0\rangle \rightsquigarrow$ any $|\xi\rangle$.
- $I_{x_0} \rightsquigarrow I_G$ multiple good solutions (even if number is unknown)
- $H_n \rightsquigarrow$ general U.

Example 1 $\quad |\psi_0\rangle \rightsquigarrow |\xi\rangle$

$Q = -H_n I_0 H_n I_{x_0}$ as before

Geometric interpretation



$|\xi\rangle = a|\xi_{||}\rangle + b|\xi_\perp\rangle$

$|\xi_{||}\rangle$: rotates around to x_0

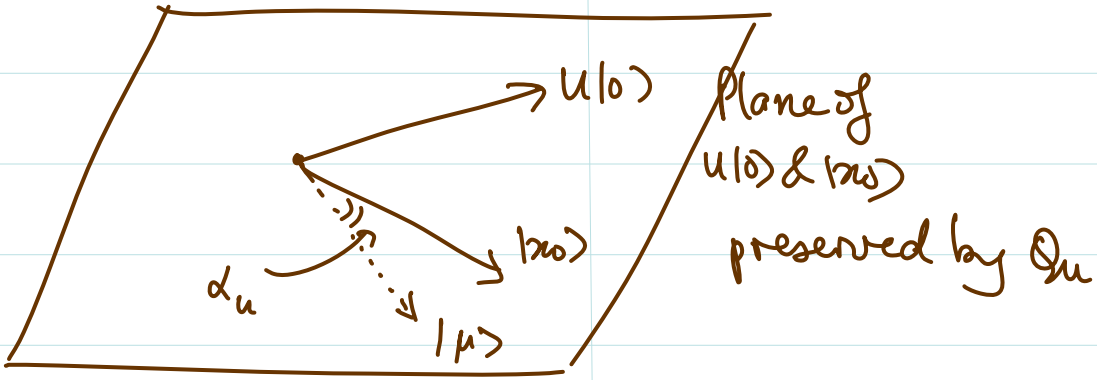
$|\xi_\perp\rangle$: just flips with $\pm$ signs

Hence prob(seeing x_0 at end) $= |a|^2$

Example 2. Replace H_n by arbitrary U

$Q_U = -U I_0 U^\dagger I_{x_0}$ starting state $|\psi_U\rangle = U|0\ldots0\rangle$

As before, facts $\Rightarrow$ $Q_U = -I_{U|0\rangle} I_{x_0} = I_{|\mu\rangle} I_{x_0}$ $\begin{cases} |\mu\rangle \perp |x_0\rangle \text{ in plane} \\ \text{of } U|0\ldots0\rangle \text{ \& } |x_0\rangle \end{cases}$



In Plane: Q_U = rot^n thru $2\alpha_U$: $\sin\alpha_U = |\langle x_0|U|0\rangle| = |u_{0,x_0}|$

Now # iterations to finish near $|x_0\rangle$ depends on U & x_0

If N large, U random $|\langle x_0|U|0\rangle| \ll 1$ (random states almost orthogonal)

So need $K = \pi/2 \,/\, |u_{0,x_0}| = O\left(\frac{1}{|u_{0,x_0}|}\right)$ iterations.

If just make $U|0\ldots0\rangle$ & measure, see x_0 only with prob $|u_{0,x_0}|^2$ ← So $O(K^2)$ tries.

Amplitude Amplification

Had $x = x_0$ "good" Start with equal superposition $\frac{1}{\sqrt{N}} \sum_{\text{all } x} |x\rangle$

$x \neq x_0$ "bad"

Q enhances amplitude of 'good' at expense of 'bad'.

More generally

$|0\rangle, |1\rangle, \ldots, |N-1\rangle$ set of orthonormal states

$G = \{x_1, x_2, \ldots x_k\}$ "good" labels (rest are "bad")

Assume can compute indicator function

$f_G : \{0, 1, \ldots, N-1\} \longrightarrow \{0, 1\}$

$f_G(\text{good}) = 1 \quad f_G(\text{bad}) = 0$

$\mathcal{G}$ = good subspace $\quad \mathcal{G}^{\perp}$ = bad subspace

As before, from f_G construct operator

$$I_G|x\rangle = \begin{cases} -|x\rangle & x \text{ good} \quad K \text{ values} \\ |x\rangle & x \text{ bad} \quad N-K \text{ values} \end{cases}$$

Let A (for "algorithm") be any unitary operator

Consider

$$Q = -A I_0 A^+ I_G$$

iterated on starting state

$$A|0\rangle = a|\text{good}\rangle + b|\text{bad}\rangle \qquad |a|^2 + |b|^2 = 1$$

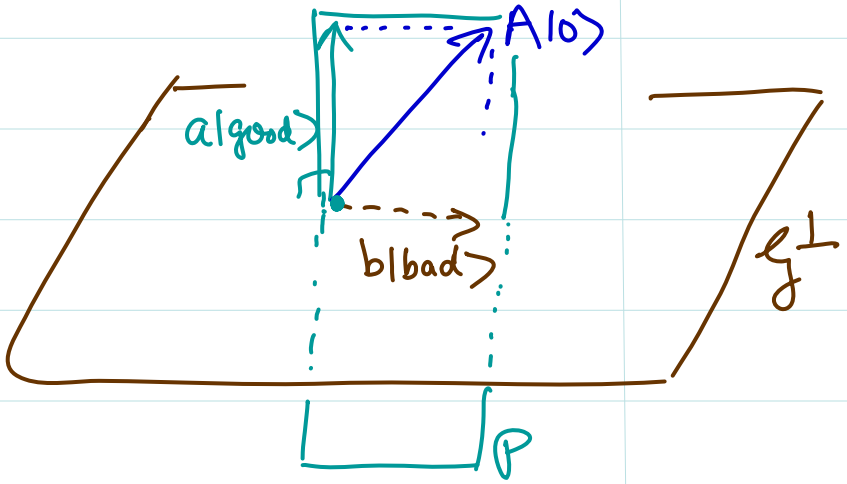
I_G: "reflection" in mirror subspace of dim $N-K$

inverting K orthogonal directions

— still have geometric interp. of above process.

AA theorem: Let P be plane spanned by $A|0\rangle$ and its good projection $|good\rangle$.

Then in P, action of Q is rotation in P by angle 2α where $\sin\alpha = |a| =$ length of initial good component.



but in P $^{\perp}$
Q is not just $-I$ now
(as it was before)

As before $Q = -I_{A|0\rangle} I_\xi$

i.e. $\xi \cap P$ = line of $|good\rangle$

Now I_ξ inverts good components of any state

But in P there is only one good direction $|good\rangle$

So in P $\quad I_Q = I_{|good\rangle}$

$\quad Q = -I_{A|0\rangle} I_{|good\rangle}$

and theorem follows exactly as before.

Thus after $O\left(\frac{1}{|a|}\right)$ iterations of Q $A|0\rangle$ will be rotated to be (very near to) its good projection $|good\rangle$ and can measure a good label with (almost) certainty

So also, final prob dist of good labels same as in initial state for these labels.

Interpretation

A = Quantum algorithm (sequence of quantum gates) starting on standard state $|0\rangle$

G = set of desired computational outcomes

Indicator function: check if answer x is good or not.

eg. A = factoring algorithm on input N

G = set of factors of N

Generally algorithm does not work with certainty

$|a|^2$ = prob of being successful in one run ← for quantum algorithms often known a priori

Thus $O\left(\frac{1}{|a|^2}\right)$ repetitions needed to be successful with const. probability.

But

Run algorithm once to get $A|0\rangle$ & don't measure it!

* Apply Q $O\left(\frac{1}{|a|}\right)$ times $\Rightarrow$ get good result with high prob.

↖ actually $\frac{\arccos|a|}{2\arcsin|a|}$ times

Each iteration of Q needs A once, A^{-1} once.

A^{-1}: inverse gates of A in reverse order

(similar computational demands)

i.e. time required to get good answer with high prob.

is reduced by square root factor for general quantum algorithms.

Also: preparation of exotic states - -

Corollary

Satisfiability with unknown number of solutions.

Boolean f: n-bits $\to$ 1-bit

r (unknown) x's $x_1, x_2, \ldots, x_r$ with $f(x) = 1$

$$I_f: \quad I_f|x\rangle = \begin{cases} |x\rangle & \text{if } f(x)=0 \text{ ie. } x \neq x_1, \ldots, x_r \\ -|x\rangle & \text{if } f(x)=1 \text{ ie. } x = x_1, \ldots, x_r \end{cases}$$

Use $Q_f = -H_n I_0 H_n I_f = -I_{|\psi_0\rangle} I_f$

start state $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{\text{all } x} |x\rangle$

Write $|\psi_f\rangle = \frac{1}{\sqrt{r}} \sum_{i=1}^{r} |x_i\rangle$ good projection of $|\psi_0\rangle$ re-normalised.

We'll suppose $r << N$

eg. if $r = O(N)$ can decide SAT easily with high prob by just random $f(x)$ tries.

AA theorem gives:

Let P_f be plane of $|\psi_0\rangle$ & $|\psi_f\rangle$. Then Q_f preserves this plane and its action is rotation thru 2α for

$$\sin\alpha = \langle\psi_0|\psi_f\rangle = \sqrt{\frac{r}{N}} \quad \text{so } \alpha \approx \sqrt{\frac{r}{N}}$$

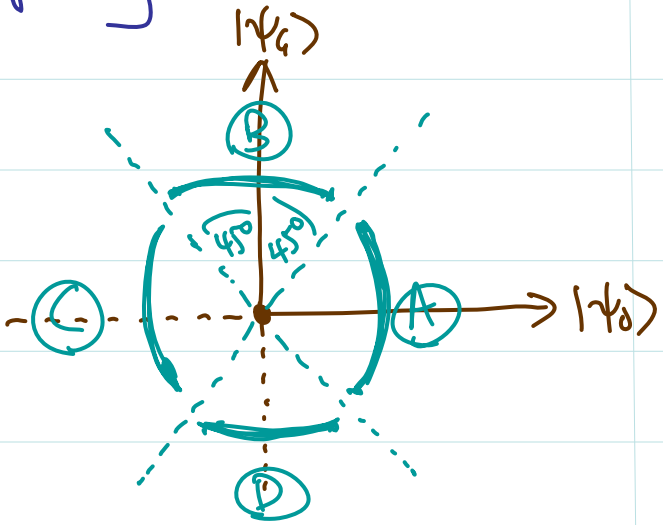
So need $\dfrac{\arccos\sqrt{\frac{r}{N}}}{2\arcsin\sqrt{\frac{r}{N}}} \approx \dfrac{\pi}{4}\sqrt{\dfrac{N}{r}}$ iterations

But r unknown, so when do we stop iterating?

Solution! — Choose $0 < K < \frac{\pi}{4}\sqrt{N}$ uniformly @ random and do K iterations. Each iteration is small angle $2\alpha \approx 2\sqrt{\frac{r}{N}}$

So $0 <$ total angle $< \sqrt{r}\,\pi/2 = \sqrt{r}$ quadrants.

is uniformly random in this range (in small discrete steps of 2α)



$|\psi_0\rangle$ almost $\perp$ to $|\psi_f\rangle$

look @ "45°-rotated" quadrants

(A) (B) (C) (D)

Final state is in quadrants (B) & (D) with prob $\frac{1}{2}$

Then have $|\langle\psi_f|\psi_{final}\rangle|^2 \geq \cos^2 45° = \frac{1}{2}$

So see a good solution overall with prob at least $\frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}$.

So repeat M=const times and will see a satisfying x with prob $\left(1 - \frac{1}{4^M}\right) \geq 1 -$ "any ϵ" if one exists.