

How to nest search algorithms

Brassard-Høyer-Mosca-Tapp '00

Setting: $g: \{0, \dots, N-1\} \rightarrow \{0, 1\}$

($g(x) = 1$ means " x is an answer" we are looking for)

A : unitary gate on $\mathbb{C}^N$ s.t. a measurement of $A|0\rangle$ in the basis $(|x\rangle)_{0 \leq x < N}$ gives some $|x\rangle$ s.t. $g(x) = 1$ with probability $p \ll 1$.

Thm Put $Q = AU_0A^\dagger U_g$ with

U_g : phase query for g , $U_g|x\rangle = \begin{cases} -|0\rangle & x=0 \\ |x\rangle & x \neq 0 \end{cases}$

Then, with $k \sim \frac{\pi}{4\sqrt{p}}$, a meas. of $Q^k A|0\rangle$

gives some $|x\rangle$ s.t. $g(x) = 1$ with prob. $\sim 1-p$

Rem. Grover's algorithm: $A = H^{\otimes n}$ with $N = 2^n$

$$H^{\otimes n}|0 \dots 0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

$\Rightarrow$ measurement will give any $|x\rangle$ with prob. $\frac{1}{N}$
 if there are k solutions to $g(x^*) = 1$, $p = \frac{k}{N}$.

$H^{\otimes n} U_0 H^{\otimes n} = D$ diffusion op.

Proof: key points

1. $AU_0A^\dagger$ and U_g are selfadjoint unitary ops ($T = T^\dagger = T^{-1}$ so $T^2 = I_N$, etc.)

$\Rightarrow$ behave like reflections

$$2. |\psi\rangle = A|0\rangle = \alpha |\psi''\rangle + \beta |\psi'\rangle$$

$$|\psi'\rangle = \sum_{x: g(x)=0} \beta_x |x\rangle, \quad |\psi''\rangle = \sum_{x: g(x)=1} \alpha_x |x\rangle$$

$\Rightarrow AU_0A^\dagger$ and U_g preserve the span of $|\psi'\rangle, |\psi''\rangle$

3. $|\alpha|^2 = p$ from assumption about p

$\Rightarrow Q$ behaves like a rot. of angle $2\sqrt{p}$.

To see Point 2, claim about $A U_0 A^\dagger = V$

$$V|\psi\rangle = -|\psi\rangle, \quad V|\varphi\rangle = |\varphi\rangle \quad \text{if} \quad \langle\psi|\varphi\rangle = 0$$

span of $|\psi'\rangle$ and $|\psi''\rangle = \text{span of } |\psi\rangle \text{ and}$

$$|\varphi\rangle = -\beta^* |\psi''\rangle + \alpha^* |\psi'\rangle$$

Rem. we can also use different $(A_i)_{0 \leq i < k}$ at each step as long as $A_i|0\rangle \sim A_j|0\rangle$
 $\varepsilon \sim \sqrt{p}$

How to turn this into nesting:

Suppose we want to determine if $f: \{0,1\}^{2n_0} \rightarrow \{0,1\}^{2n_0}$ is one-to-one (element distinctness)

$$g: \{0,1\}^{2n_0} \times \{0,1\}^{2n_0} \rightarrow \{0,1\}$$

$$g(z, w) = 1 \quad \text{iff} \quad z \neq w \text{ and } f(z) = f(w)$$

At the i -th step:

- choose $y^i \in \{0,1\}^{n_0}$ randomly
- then compute $f(y^i, x)$ for all $x \in \{0,1\}^{n_0}$
- A_i : the unitary gate $\sum_x |y^i x\rangle \langle y^i x| \otimes G_{i,x} + \sum_{y \neq y^i} \text{"Id"}$
 $G_{i,x}$: Grover's algo. searching w s.t.
 $f(w) = f(y^i, x)$

$$\text{i.e. } G_{i,x} = (DU_{h_{i,x}})^{k_i} H^{\otimes 2n_0}, \quad h_{i,x}(w) = 1 \quad \text{iff} \quad f(w) = f(y^i, x)$$

$$k_i \text{ randomly chosen } 0 \sim \frac{\pi 2^{n_0}}{4}$$

Then $A_i|0 \dots 0\rangle$ finds $g(y^i, x, w) = 1$ with prob.

$$p \sim \frac{1}{2^{n_0}} \quad (\text{see yesterday's note}) \quad \text{at least.}$$

$A_i|0 \dots 0\rangle \sim A_j|0 \dots 0\rangle$ because $\{y^i x, y^j x : x \in \{0,1\}^{n_0}\}$ is small, A_i & A_j agree outside this

Quick diversion to complexity theory

We have various "problems" in math / comp. sci, such as

- decide prime factors of a given integer N
- decide if two graphs $\Gamma = (\underbrace{V}_{\text{vertex set}}, \underbrace{E \subset V \times V}_{\text{edge set}})$ and Γ' are isomorphic
- given a graph Γ , weight func. $f: E \rightarrow \mathbb{R}_+$, find a cycle C in Γ minimizing $\sum_{e \in C} f(e)$ (travelling salesman problem)
- given a program P , decide if it will terminate or not (halting problem)

Some are not to have any algorithm to decide:
 halting problem, etc.
 are proven

Others have algorithms, but

- class P: polynom time algorithm to find an answer
- class NP: $\exists$ algorithm to find an answer
verification of candidate for answer can be done in polynom. time
- class NEXP: $\exists$ algo. to find an answer in an exponential time

Classical computer can simulate quantum computers

$\Rightarrow$ NEXP contains

- class BQP: $\exists$ quantum algo. in polynomial steps, with uniform bound on error prob.

