Grover's alg.

Problem: given oracle $f: X \to \{0,1\}$, $N = |X|$
find $x \in X$ s.t. $f(x) = 1$.

Suppose $K > 0$ solutions:
- classically: $O(N/K)$ queries to f. (optimal)
- Grover's alg: $O(\sqrt{N/K})$ quantum queries to f (optimal)

when $K=1$: $O(\sqrt{N})$ vs. $O(N)$ classically.

Applications:

(1) cipher $E: \mathcal{K} \times \mathcal{M} \to \mathcal{C}$

Given $m \in \mathcal{M}$ and $c = E(k,m)$, find $k \in \mathcal{K}$.

Classically: $O(|\mathcal{K}|)$ $\Rightarrow$ $\mathcal{K} = \{0,1\}^{128}$ (128-bit security)

Quantum: define $f(x) = \begin{cases} 1 & \text{if } c = E(x,m) \\ 0 & \text{otherwise} \end{cases}$

Grover: find k using $O(|\mathcal{K}|^{1/2})$ evals. of E.

$\Rightarrow$ need to double key size $\mathcal{K} = \{0,1\}^{256}$ (128-bit security)

In reality: error correction wipes out advantage.

(2) <u>collision finding</u>: random $H: X \to Y$ $\quad Y = \{0,1\}^n$

collision: $x_0 \neq x_1 \in X$ s.t. $H(x_0) = H(x_1)$

<u>classically</u>: $O(2^{n/2})$ evals. of H (birthday paradox)

<u>Quantum</u>: $O(2^{n/3})$ evals. of H (optimal)

1: choose random $T = \{x_1, \dots, x_{2^{n/3}}\} \subseteq X$
compute $y_i \leftarrow H(x_i)$ $\quad i = 1, \dots, 2^{n/3}$.
$\Big\}\ 2^{n/3}$ queries

2: define $F(x) = \begin{cases} 1 & \text{if } [x \notin T \text{ and } H(x) \in H(T)] \\ 0 & \text{otherwise} \end{cases}$

choose random $S = \{\tilde{x}_1, \dots, \tilde{x}_{2^{2n/3}}\} \subseteq X$

$\Rightarrow E[\#(i,j) : x_i = \tilde{x}_j] = \frac{|S| \times |T|}{2^n} = \frac{2^{2n/3} \times 2^{n/3}}{2^n} = \underline{1}$

$\Rightarrow$ Grover finds j s.t. $F(\tilde{x}_j) = 1$
using $\sqrt{2^{2n/3}} = 2^{n/3}$ quant. queries to H.

<u>Total</u>: $2^{n/3}$ classical queries + $2^{n/3}$ quantum queries

<u>Run time</u>: $2^{n/3}$ with <u>$2^{n/3}$ qbits for F.</u>

<u>Bad news</u>: with $2^{n/3}$ processors, can <u>classically</u> find collision in time $2^{n/3}$. $\quad (2^{2n/3}$ queries to $H)$

<u>Open</u>: is there a $2^{n/3}$ query collision finder using $O(1)$ qbits ??

The algorithm: $f: X \to \{0,1\}$ $\qquad X = \{0,1\}^n,\ |X| = 2^n = N.$

Quantum query: $\sum_{x,b} \psi_{x,b} |x,b\rangle \to \sum_{x,b} \psi_{x,b} |x, b \oplus f(x)\rangle$

implies: $\boxed{\sum_{x \in X} \psi_x |x\rangle \to \sum_{x \in X} (-1)^{f(x)} \psi_x |x\rangle}$ $\quad (*)$

(phase kickback)

How: $\left(\sum_{x \in X} \psi_x |x\rangle\right)\left(|0\rangle - |1\rangle\right) \to$

$$\left(\sum_{x \in X} \psi_x |x\rangle\right)\left(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle\right) = \left(\sum_{x \in X} (-1)^{f(x)} \psi_x \cdot |x\rangle\right)\left(|0\rangle - |1\rangle\right)$$

- Quantum query: $\quad \mathcal{O} \in \mathbb{C}^{2^n \times 2^n}$ $\quad$ (implements $(*)$)
- Let $\psi_0 = \frac{1}{\sqrt{N}} \sum_{x \in X} |x\rangle$. Define: $R := 2\left(|\psi_0\rangle\langle\psi_0|\right) - I \in \mathbb{C}^{2^n \times 2^n}$

Fact: R can be implemented using $\approx 3n$ gates

Proof: $$R = H^{\otimes n} \cdot \big(\underbrace{2(|0\rangle\langle 0|) - I}_{\begin{pmatrix} 1 & & 0 \\ & -1 & \\ 0 & & -1 \end{pmatrix}}\big) \cdot H^{\otimes n}$$

Grover's alg:

(1) start in state ψ_0 $\quad \left(= H^{\otimes n} \cdot |0\rangle\right) \in \mathbb{C}^{(2^n)}$

(2) For $i = 1, \ldots, \left\lfloor \frac{\pi}{4} \sqrt{N/K} \right\rfloor$ do: $\psi_i \leftarrow R \cdot \mathcal{O} \cdot \psi_{i-1}$

(3) measure $\psi_{\sqrt{N/K}}$ to get $x \in X$

Thm: $\Pr[F(x)=1] > \frac{1}{2}$

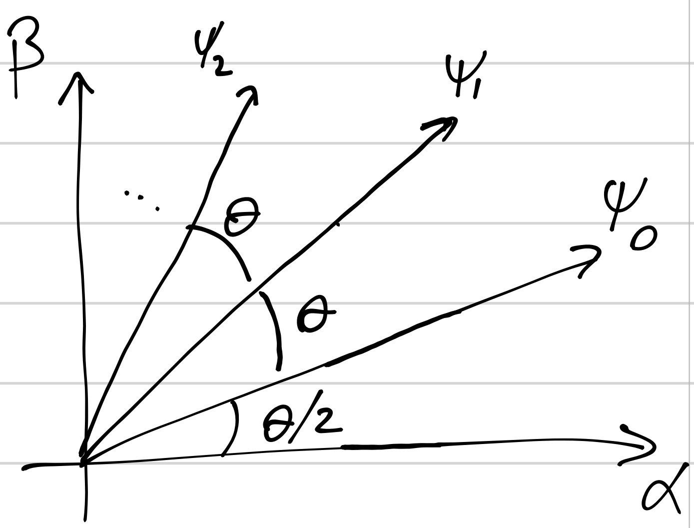
Proof idea:

Let $\alpha := \frac{1}{\sqrt{N-K}} \sum_{\substack{x\in X\\ F(x)=0}} |x\rangle$, $\beta := \frac{1}{\sqrt{K}} \sum_{\substack{x \in X \\ F(x)=1}} |x\rangle$, $\alpha \perp \beta$.

Then $\psi_0 \in \text{span}(\alpha, \beta)$ ($K = \#$ solutions)

Fact: $R \cdot D$ is a rotation of span(α,β) by θ degrees where

$$\boxed{\sin\theta = \frac{2\sqrt{(N-K)K}}{N}}$$



$K \ll N \Rightarrow \sin(\theta)$ small $\Rightarrow \theta \approx \sin\theta \approx 2\sqrt{\frac{K}{N}}$

$\Rightarrow$ after $\frac{\pi}{4}\sqrt{\frac{N}{K}}$ iterations: $\Theta \approx \frac{\pi}{2}$

$\Rightarrow$ measuring will give elem. of β w/prob. $> \frac{1}{2}$.

- Need to stop after $\frac{\pi}{4}\sqrt{\frac{N}{K}}$ iterations to not over shoot.

Notes: (1) amplitude amplification:

prob. $\varepsilon = \frac{K}{N} \xrightarrow{\text{amplify}}$ prob. ≈ 1, work $= \sqrt{\frac{1}{\varepsilon}}$

(2) bad news: impractical due to error correction overhead.