Lecture 16: Shor's alg.

Goal: exp. gap between classical & quantum comp.

oracle problems: $f: X \to Y$ (finite Y)

- a classical oracle for f: $x \in X \longrightarrow y = f(x) \in Y$
- a quantum oracle for f:

$$|\psi_{inp}\rangle = \sum_{x \in X} \psi_x |x, 0\rangle \longrightarrow |\psi_{out}\rangle = \sum_{x \in X} \psi_x |x, f(x)\rangle$$

Goal: learn property of f with min. queries

ex.: (1) Find $x \in X$ s.t. $f(x) = 1$.

(2) Suppose $f: \mathbb{F} \to \mathbb{F}$ is a deg. d poly. Find f.

oracle alg.: uses f as a black box (oracle)

often f is an efficiently computable func.

e.g. $f_p(x) = (x^2 \bmod p)$

Recall: f is computable by circuit with s classical gates
$\Rightarrow$ one quantum query takes s c-swap gates.

Today's problem: period finding

abstractly: Let $(G, +)$ be an abelian group ($x+y = y+x$)
let $H < G$ a subgroup, where $|G/H|$ finite.

Def: $f: G \to S$ is H-periodic if

$$\forall x, y \in G: \quad f(x) = f(y) \iff x - y \in H$$

in particular: $\forall x \in G, \pi \in H: \quad f(x + \pi) = f(x)$

Goal: find π given oracle for f.

examples:

(1) $f: \mathbb{Z}_2^n \to S$ (arbitrary) has period $\pi \in \mathbb{Z}_2^n$ $\quad (H = \{0, \pi\})$

if $\forall x \in \mathbb{Z}_2^n : f(x \oplus \pi) = f(x)$

Thm (Simon '94): can find $\pi \in \mathbb{Z}_2^n$ using one quantum query and $o(n)$ quantum gates

$(n=1$: Deutsch$)$

(2) $f: \mathbb{Z} \to S$ has period $\pi \in \mathbb{Z}$ $\quad (H = \{0, \pm\pi, \pm 2\pi, \ldots\})$

if $\forall x \in \mathbb{Z}: f(x+\pi) = f(x)$. $\quad (f(x)=f(y) \Leftrightarrow \pi \mid x-y)$

Thm (Shor '94): can find $\pi \in \mathbb{Z}^{>0}$ using one quantum query and $o(\log|\pi|)$ quantum gates

(3) $f: \mathbb{Z}^n \to S$ has period $H = \mathrm{span}(\pi_1, \pi_2, \ldots, \pi_n)$

Thm (Shor '94): can find $\pi_1, \ldots, \pi_n \in \mathbb{Z}^n$

using $o(n)$ quantum queries and $O\left(\sum_{i=1}^{n} \log|\pi_i|\right)$ Q. gates.

Applications

(1) Factoring integers $N = p \cdot q \in \mathbb{Z}$ (e.g., 1000 digits)

best known classical alg: $\approx O\left(e^{\sqrt[3]{\log N}}\right)$ ← exp. gap (maybe)

Quantum: $O(\log^3 N)$ Q. gates!!

How? choose random $g \in \{1, \dots, N-1\}$

define: $F: \mathbb{Z} \to \mathbb{Z}/N$ $(G = \mathbb{Z}/N)$

$$\boxed{x \to (g^x \bmod N)}$$ [$O(\log^3 N)$ gates to compute]

periodic: $1, g, g^2, g^3, \dots, g^{\pi-1}, g^{\pi} = 1, g^{\pi+1} = g, \dots, g^{2\pi-1}, g^{2\pi} = 1, \dots \pmod N$

$\forall x \in \mathbb{Z}: \quad F(x) = F(x + \pi)$

Euler's thm: - F has period π dividing $\varphi(N) = (p-1)(q-1)$
- often smallest $\pi = \frac{1}{2}\varphi(N)$.

easy fact: given $\varphi(N)$, can factor N.

Shor's alg. finds π in time $O(\log^3 N)$!

(2) Dlog: Let $G = \{1, g, g^2, \dots, g^{q-1}\}$ be a finite cyclic group

Dlog: given $(g, h = g^\alpha)$ find $1 \le \alpha < q \in \mathbb{Z}$.

best general classical alg: $O(\sqrt{q})$ ← exp. gap

Quantum: $O(\log q)$ group operations. ←

How? define $f: \mathbb{Z}^2 \to G$

$$(x,y) \to g^x \cdot h^y \in G$$

periods: $\{(0,q), (q,0), (\alpha,-1)\}$ ← and linear combinations.

Shor's alg. finds all periods in $o(\log q)$ group ops.

$\Rightarrow$ finds α.

Finding smallest period $\pi \in \mathbb{Z}^{>0}$ of $f: \mathbb{Z} \to S$

- set $n = \lceil 2\log_2 \pi \rceil$ so that $\pi^2 < 2^{2n}$

- compute:

$$|0^n, 0 \in S\rangle \xrightarrow{H^{\otimes n}} \sum_{j=0}^{2^n-1} |j, 0\rangle$$

time consuming step for factoring & dlog

query/compute f $\longrightarrow$ $\sum_{j=0}^{2^n-1} |j, f(j)\rangle$

measure 2nd cell to get some $z = f(k) \in S$ $\longrightarrow$ $\sum_{\substack{j=0 \\ j \equiv k \pmod{\pi}}}^{2^n-1} |j, z\rangle = \psi_\pi$

ex: $\pi = 5$, $2^n = 128$. Suppose $z = f(2) \in S$

Then $\psi_\pi = \frac{1}{\sqrt{26}}\left(|2\rangle + |7\rangle + |12\rangle + |17\rangle + |22\rangle + \dots + |127\rangle\right)|z\rangle =$

$$= \frac{1}{\sqrt{26}}\left(\sum_{j=0}^{25} |j\cdot\pi + 2\rangle\right)|z\rangle \qquad \leftarrow 2^n \text{ dim.}$$

Next: <u>Quantum Fourier Transform</u> (QFT_n) on ψ_π.

Let $w := e^{2\pi i/2^n}$ ← 2^n th root of unity.

QFT_n: For $0 \le j \le 2^n - 1$ maps $|j\rangle \to \frac{1}{2^{n/2}} \cdot \sum_{r=0}^{2^n-1} w^{r\cdot j} \cdot |r\rangle$

$QFT_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$, $\quad w = -1$

$QFT_2 = \frac{1}{2}\left(\begin{array}{c|c|c|c} 1 & 1 & 1 & 1 \\ \hline 1 & i & -1 & -i \\ \hline 1 & -1 & 1 & -1 \\ \hline 1 & -i & -1 & i \end{array}\right)$, $\quad w = i$ $\qquad$ (j=0, j=1, j=2, j=3) , …

QFT_n: <u>$2^n \times 2^n$ matrix</u>, powers of $w = e^{(2\pi i/2^n)}$.

<u>Fact:</u> QFT_n can be computed using $o(n^2)$ gates!

n H-gates, and $\binom{n}{2}$ <u>R_w-gates</u> $\qquad$ (FFT)

need Kitaev approx.

Now: apply QFT_n to first cell of ψ_π.

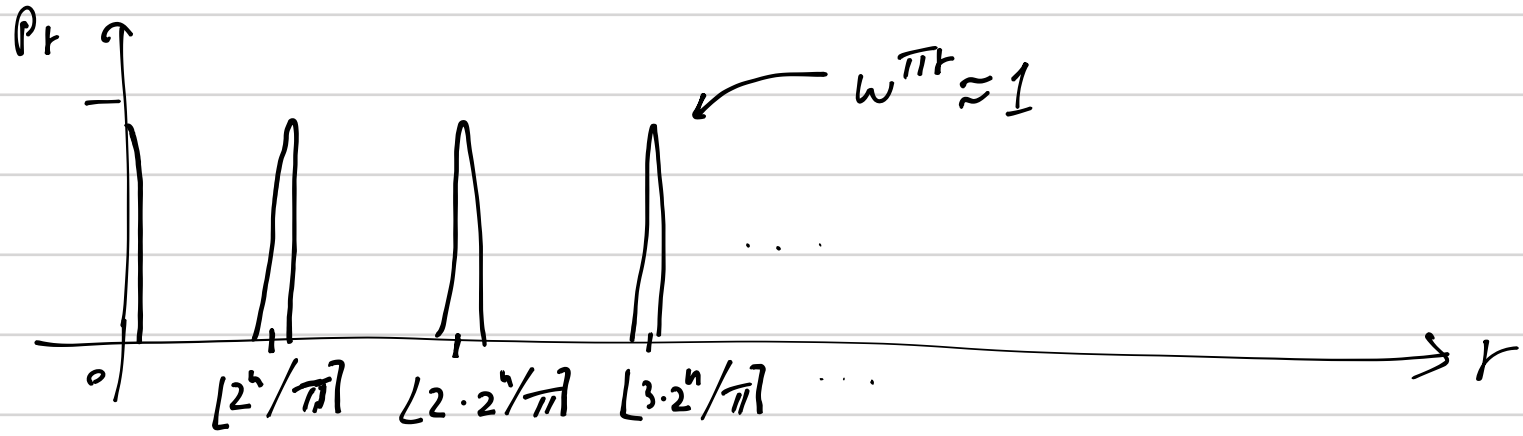
$f(k) = z$

$$QFT_n \cdot \psi_n = \sum_{r=0}^{2^n-1} \left[\sum_{j=0}^{\lfloor 2^n/\pi \rfloor} \omega^{r\cdot(\pi\cdot j + k)} \right] |r\rangle |z\rangle$$

k fixed

measure first cell:

$$\text{Prob}(r) \propto \left| \sum_{j=0}^{\lfloor 2^n/\pi \rfloor} (\omega^{\pi r})^j \right|^2$$



So: $r = \lfloor c \cdot \frac{2^n}{\pi} \rceil = c \cdot \frac{2^n}{\pi} + \delta$ for $c \in \mathbb{Z}$, $|\delta| \le \frac{1}{2}$

$$\Rightarrow \left| \frac{r}{2^n} - \frac{c}{\pi} \right| \le \frac{\frac{1}{2}}{2^n} \le \frac{1}{2\pi^2}$$

$\frac{r}{2^n}$: known; $\frac{c}{\pi}$: unknown

$\pi^2 \le 2^n$

$\Rightarrow$ Can find $\frac{c}{\pi}$ using cont. frac. alg.

$\Rightarrow$ gives π when $\gcd(c, \pi) = 1$.

Run Time: (1) compute $f(j)$ $\leftarrow$ $O(\log^3 N)$

For factoring (2) do DFT $\leftarrow$ $O(\log^2 N)$

open problem: hidden shift

Let $f, g : \mathbb{Z} \to S$ s.t. $g(x) = f(x+\Delta)$, $\forall x \in \mathbb{Z}$

Goal: Find $\Delta \in \mathbb{Z}$ (hidden shift)

Classically: $o(\Delta)$

Best known quantum (Kuperberg): $e^{\sqrt{\log|\Delta|}}$

Can we do better? poly($|\Delta|$)? open.

Shor's alg: (cont.)

Recap: $f: \mathbb{Z} \to S$ is π-periodic ($\pi \in \mathbb{Z}$) if

$$\forall x, y \in \mathbb{Z}: \quad f(x) = f(y) \iff \pi \mid x - y$$

Shor's alg: Find period π using one quantum query to f and $O(\log^2 \pi)$ quantum gates.

Apps: Factoring ints. Dlog in any finite cyclic group ($f: \mathbb{Z}^2 \to S$) in Quantum poly. time.

Alg: set $n = \lceil 2 \log_2 \pi \rceil$ so that $\pi^2 < 2^n$.

$$|0^n\rangle |0 \in S\rangle \xrightarrow{H^{\otimes n}} \sum_{j=0}^{2^n-1} |j\rangle |0\rangle \xrightarrow[f]{\text{query}} \sum_{j=0}^{2^n-1} |j\rangle |f(j)\rangle$$

measure right cell to get $z = f(k) \in S$

$$\xrightarrow{} \sum_{\substack{j=0 \\ j \equiv k \pmod{\pi}}}^{2^n-1} |j\rangle |z\rangle = \sum_{q=0}^{\lfloor 2^n/\pi \rfloor} |\underbrace{\pi \cdot q + k}_{j}\rangle |z\rangle$$

$f(k) = z$

$$\xrightarrow[\text{gates}]{QFT_n} \sum_{r=0}^{2^n-1} \left[\sum_{q=0}^{\lfloor 2^n/\pi \rfloor} \omega^{r \cdot (\pi \cdot q + k)} \right] |r\rangle |z\rangle$$

$O(\log^2 n)$ gates H, R_ω

z fixed

$\omega = e^{2\pi i / 2^n}$

$\longrightarrow$ measure left cell. $\longrightarrow$ $\pi \in \mathbb{Z}$

to get r.

For r $0 \le r \le 2^n - 1$:

$$\text{Prob}(r) \propto \left| \sum_{q=0}^{\lfloor 2^n/\pi \rfloor} (\omega^{\pi r})^q \right|^2$$