HW return
NAND-help

**Ph 452** Lecture 15

## IQI Quick Review

- Geometric Grover
- Factoring → order-finding

## Order finding:

Input: $N \in \mathbb{N}$ with $N \geq 2$, $a \in \{2, \dots, N-1\}$, $\gcd(a,N)=1$

Output: $\min\{r \mid a^r \equiv 1 \bmod N\}$

$=$ period of $f(i) = x^i \bmod N$

exponential in # digits of N

Best-known classical alg: $O(2^n)$, $n = \lceil \log_2(N-1) \rceil$

## As a query problem:

$g: X \to Y$, $X \subseteq \Sigma^N$

$N \in \mathbb{N}$, $n = \lceil \log_2 N \rceil$ $\Sigma = \mathbb{Z}_N$ $Y = \mathbb{Z}_N$

$(N < 2^n)$

$i \equiv j \bmod r$

for factoring, know that $N \neq 2^n$!

$X = \{ x_0 \dots x_{N-1} \in \Sigma^N \mid x_i = x_j \text{ iff } i = \{j, j \pm r, j \pm 2r, \dots\} \}$

$\iff i \equiv j \bmod r$

$g(x) = r$

$X = \{ x_0 \dots x_{N-1} \in \Sigma^N \mid x_i = a^i \bmod N \}$

Example: $a = 3$, $N = 10$ $n = 4$, $2^n = 16$

| $i$: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | $N-1$ | | | |
| $x_i$: | 1 | 3 | 9 | 7 | 1 | 3 | 9 | 7 | 1 | 3 | 9 | 7 | ... |

$(r=4)$

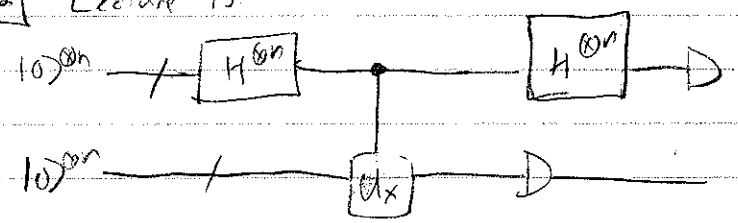
cf. Simon's Problem: $n \in \mathbb{N}$, $N = 2^n$, $\Sigma = \mathbb{B}^n$, $Y = \mathbb{B}$

$X = \{ x_0 \dots x_{N-1} \in \Sigma^N \mid x_i = x_j \text{ iff } i = j \oplus s \}$

~~$i_k \equiv j_k \bmod s_k$~~

$g(x) = \begin{cases} 0 & s = 0^n \\ 1 & s \neq 0^n \end{cases}$

Ph 452 Lecture 15



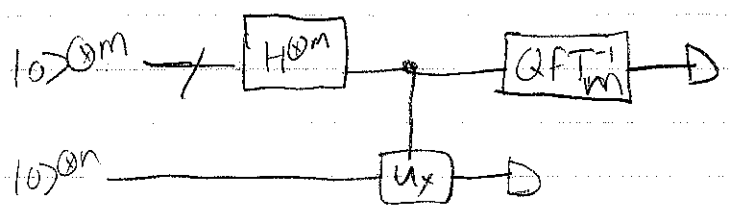

Yields $i$ : $s \cdot i = 0$

$n+1$ calls : determines $s$ w/prob $> 1/4$

$4(n+1)$ calls: determines $s$ w/prob $> 2/3$

$\rightarrow Q_2(F) = O(n)$

Order-finding alg: (Shor)




$N^2 \leq \overset{M}{\overset{\shortparallel}{2^m}} \leq N^4$

$N \leq 2^n$, $n := \lceil \log_2 N \rceil$

$(2n \leq m \leq 4n)$

$U_x |i\rangle|j\rangle = \begin{cases} |i\rangle|j \oplus x_i\rangle & i \in N \\ |i\rangle|j\rangle & i > N \end{cases}$

Case 1: $r \mid M$

(w/prob $> \frac{4}{\pi^2}$)

will explain alg later

yields $i$ : $\frac{i}{M} = \frac{k}{r}$ for some $k$ (roughly) uniformly over $\{0, \ldots, r-1\}$

$\rightarrow$ Continued fraction algorithm (CFA) finds $\frac{k}{r}$ in lowest terms ($O(m^3) = O(n^3)$ steps)

will expand upon later

1 call: $\text{prob}[\gcd(k,r) = 1] > \frac{1}{2 \log M} \Rightarrow r$ found

$O(n)$ calls: $r$ found w/prob $\geq 2/3$

Each call: can be implemented in $O(n^2)$ steps (modular exponentiation)

$\rightarrow O(n^3)$ steps

$\boxed{\text{Ph 452}}$ Lecture 15

<u>Case 2:</u> $r \nmid M$ (more likely)

yields i: $\left|\frac{i}{M} - \frac{k}{r}\right| \le \frac{1}{2M}$ for some uniform $0 \le k \le r$

Thm 3.1 in NC. Proved in App. 4 $\longrightarrow$ <u>Theorem:</u> Given $\varphi \in (0,1)$ and $N \geq 2$, there is at most one fraction $\frac{k}{r}$ with $0 \le k, r \le N$, $r \ne 0$, $\gcd(k,r)=1$ satisfying

$$\left|\varphi - \frac{k}{r}\right| \le \frac{1}{2N^2}$$

Moreover, given $\varphi$, $N$, the CFA will find $k, r$ in $O(n^3)$ steps

1 call: finds $r$ w/ prob$[\gcd(k,r)=1] > 2^{-1}/5M$

$O(n)$ calls: " " " $\geq 2/3$

Each call: $O(n^2)$ steps

$\Rightarrow O(n^3)$ steps!

$\Rightarrow$ $\boxed{O(n^3) \text{ steps overall!}}$

$\boxed{\text{Ph 432}}$ Lecture 15

<u>Discrete Fourier Transform</u> : Useful in signal processing, e.g.

$$DFT(\vec{x} \in \mathbb{C}^N) = \tilde{\vec{x}},$$

$$\boxed{\tilde{x}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \underbrace{e^{-2\pi i j k/N}}_{=\omega^{-jk}} x_j} \qquad \omega := e^{2\pi i/N}$$

$$= F_{jk}$$

$$DFT^{-1}(\tilde{\vec{x}}) : \quad x_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{jk} x_j$$

$$DFT^{-1}([0,1,0]^T) = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ \omega \\ \omega^2 \end{bmatrix}$$

$\rightarrow \mathcal{O}(N^2)$ multiplications, additions

<u>Fast Fourier Transform</u>: $\mathcal{O}(N \log N)$ operations

multiplication

$j = j_{n-1} j_{n-2} \cdots j_0$ $\qquad \frac{jk}{2^n} = j_{n-1}(.k_0) + j_{n-2}(.k_1 k_0) + \cdots + j_0(.k_{n-1} \cdots k_0)$ } $n$ sums!

$k = k_{n-1} k_{n-2} \cdots k_0$ $\qquad$ Must do $n$ sums $\forall$ $N$ values of $j$ $\rightarrow \mathcal{O}(N \log N)$

<u>Quantum Fourier transform</u>: $\mathcal{O}((\log N)^2)$ operations

Let $N = 2^n$ here (recall $QFT^{-1}$ on $M = 2^m$ in order-find)

$$\boxed{QFT : |j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi i j k/N} |k\rangle} \qquad \text{DFT on amplitudes!}$$

cf $U_{WH} : |j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (-1)^{jk} |k\rangle$

$$= \frac{1}{\sqrt{N}} \left(|0\rangle + (-1)^{j_{n-1}}|1\rangle\right)\left(|0\rangle + (-1)^{j_{n-2}}|1\rangle\right) \cdots \left(|0\rangle + (-1)^{j_0}|1\rangle\right)$$

$$j = j_0 j_1 \cdots j_{n-1} = j_{n-1} 2^{n-1} + j_{n-2} 2^{n-2} + \cdots + j_0 2^0$$
$$\equiv \sum_{\ell=0}^{n-1} j_\ell 2^\ell$$

# Ph 452 Lecture 15

## Product representation:

N&C eqs 5.5–5.10

$$\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{2^n}}|k\rangle = \frac{1}{\sqrt{N}}\sum_{k_0=0}^{1}\cdots\sum_{k_{n-1}=0}^{1} e^{2\pi i j \sum_{\ell=0}^{n-1} k_\ell 2^{\ell-n}}|k_{n-1}\cdots k_0\rangle$$

Note: my convention of $j = j_{n-1}\cdots j_0$ differs from N&C's convention of $j = j_1\cdots j_n$

Mine is better because it better matches how we write decimal numbers.

$$= \frac{1}{\sqrt{N}}\sum\cdots\sum \bigotimes_{\ell=0}^{n-1} e^{2\pi i j k_\ell 2^{\ell-n}}|k_\ell\rangle$$

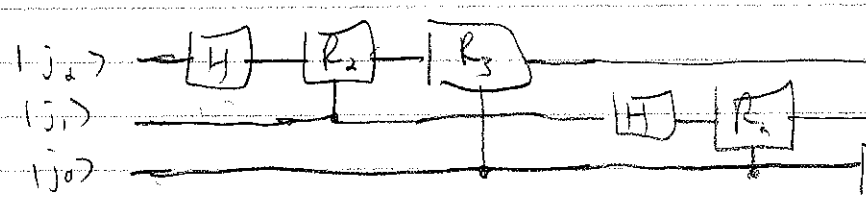
$$= \frac{1}{\sqrt{N}}\bigotimes_{\ell=0}^{n-1}\left[\sum_{k_\ell=0}^{1} e^{2\pi i j k_\ell 2^{\ell-n}}|k_\ell\rangle\right]$$

$$= \frac{1}{\sqrt{N}}\bigotimes_{\ell=0}^{n-1}\left[|0\rangle + e^{2\pi i j\, 2^{-n+1}}|1\rangle\right]$$ ignore multiples of $2\pi$

$$= \frac{1}{\sqrt{N}}\left(|0\rangle + e^{2\pi i\, 0.j_0}|1\rangle\right)\left(|0\rangle + e^{2\pi i\, 0.j_1 j_0}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i\, 0.j_{n-1}\cdots j_0}|1\rangle\right)$$

## Quantum circuit for QFT:

Let $R_d := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2^d}\end{pmatrix}$, $|j\rangle := |j_2 j_1 j_0\rangle$




$|\tilde{j}_2\rangle = (|0\rangle + e^{2\pi i (0.j_2 j_1 j_0)}|1\rangle)$

$|\tilde{j}_1\rangle = (|0\rangle + e^{2\pi i (0.j_1 j_0)}|1\rangle)$

$|\tilde{j}_0\rangle = (|0\rangle + e^{2\pi i (0.j_0)}|1\rangle)$

Output qubits must be reversed to give QFT.

$$H|j_i\rangle = (|0\rangle + e^{2\pi i (0.j_i)}|1\rangle)$$

Generally: $n$ H gates (1/qubit)
$\binom{n}{2}$ $R_d$ gates (1/qubit pair)
$n/2$ SWAP gates (to reverse output)
$\Big\}$ $\mathcal{O}(n^2)$ gates