CSCE 785 | Shor's Algo

10/24/2023

$a \in \mathbb{Z}_n$, a is invertible mod n if $\exists b \in \mathbb{Z}_n$,

$ab \equiv 1 \pmod{n}$ $\quad [ab = 1 \text{ in } \mathbb{Z}_n]$

Fact: a is invertible iff $\gcd(a,n) = 1$ (a and n are coprime).

Define $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a,n) = 1\}$.

$\mathbb{Z}_n^*$ is closed under mult in $\mathbb{Z}_n$.

Def: Given $a \in \mathbb{Z}_n^*$, define order of a ($\text{ord}(a)$) as the least $r > 0$ such that $a^r = 1$ in $\mathbb{Z}_n$

$1 = a^0, a^1, a^2, \ldots, a^r = 1, a^{r+1} = a, a^{r+2} = a^2, \ldots$ in $\mathbb{Z}_n$

☆ Factoring reduces to orderfinding.

Example: $n = 14$. $\mathbb{Z}_{14} = \{0, \ldots, 13\}$

$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$ $\qquad a = 3$

$\text{ord}(3) = 6$

$\text{ord}(9) = 3$

$1, 3, \underset{3^2}{9}, \underset{3^3}{13}, \underset{3^4}{11}, \underset{3^5}{5}, \underset{3^6}{1}$

$1, 9, 11, 1$

Given a "black box" subroutine that finds $\mathrm{ord}(a)$ for any $a \in \mathbb{Z}_n^*$ where n is odd and has ≥ 2 distinct prime factors. Here is a probabilistic algo to find a nontrivial factor of n efficiently:

Given n in binary as input:

1. If n is even, then output 2 and quit.
2. If $n = a^b$ for some $a, b \geq 2$, then output a and quit.
   [Estimate $\sqrt[b]{n}$ by binary search for $2 \leq b \leq \log_2 n$]
3. Choose a random $x \in \mathbb{Z}$ such that $2 \leq x \leq n-1$. If $\gcd(n,x) > 1$, then output $\gcd(n,x)$ and quit. [can compute gcd's quickly by Euclid's algorithm]
4. Now: $x \in \mathbb{Z}_n^*$. Use the black box to return $r := \mathrm{ord}(x)$ in $\mathbb{Z}_n$.
5. If r is odd, then go back to step 3.
6. r is even. Compute $y := x^{r/2}$ in $\mathbb{Z}_n$.
   binary exponentiation
7. If $y \equiv -1 \pmod{n}$ (i.e., $y = n-1$), then go to step 3.

8. Compute gcd$(n, y-1)$ // $y \not\equiv -1 \pmod n$
and return the result. Success!

Proof that Step 8 succeeds.

[all arith in $\mathbb{Z}_n$] $y := x^{r/2}$, so $y^2 = x^{\overset{\text{ord}(x)}{\overset{\shortparallel}{r}}} = 1$ (in $\mathbb{Z}_n$)

I.e., n divides $y^2 - 1 = (y+1)(y-1)$
but $y \not\equiv -1$ so n does not divide $y+1$
and $y \not\equiv 1$ either, $[y = x^{r/2} \not\equiv 1]$
b/c x has order r
so n does not divide $y-1$

Summary n divides $(y+1)(y-1)$
but does not divide either factor.

Let $n = q_1 q_2 \cdots q_k$ prime factorization of n,
~~Some of the~~ $(y+1)(y-1)$ includes all of the q_i as factors, but neither $y+1$ nor $y-1$ includes all the q_i as factors
$\therefore$ $y-1$ includes a nontrivial factor of n as a factor. ▨

Not proven: succeed with high probability.

Shor's algo provides the black box above. (4)

~~Agenda~~ Agenda — Define Quantum Fourier Transform (QFT)

- Shor's Algo using QFT
- Implementing QFT as a circuit.

<u>Def</u>: The Discrete Fourier Transform

$$\mathrm{DFT}_m : \mathbb{C}^m \longrightarrow \mathbb{C}^m \quad \text{unitary, linear}$$

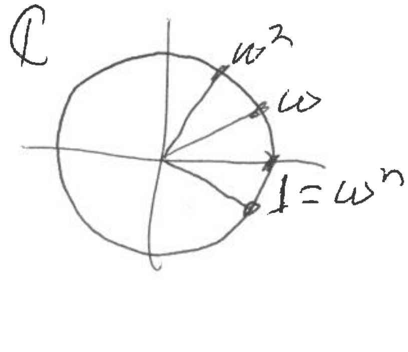
Given ~~$|x\rangle \in \mathbb{C}^m$~~ $x = (x_0, \dots, x_{m-1}) \in \mathbb{C}^m$

$$\cancel{\mathrm{DFT}_m |x\rangle := \frac{1}{\sqrt{m}} \sum_{y \in \mathbb{Z}_m} \exp(2i\pi xy)|y\rangle}$$

$\mathrm{DFT}_m(x) = y = (y_0, \dots, y_{m-1}) \in \mathbb{C}^m$ such that

$$y_j = \frac{1}{\sqrt{m}} \sum_{\substack{k=0 \\ [k \in \mathbb{Z}_m]}}^{m-1} \underbrace{\exp(2\overset{\sqrt{-1}}{i}\pi jk/m)}_{\omega^{jk}} x_k$$

Let $\omega := \exp(2i\pi/m)$ $\quad [\omega^n = 1 = e^{2i\pi}]$



$$\mathrm{DFT}_m = \frac{1}{\sqrt{m}} \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ \\ \\ m-1 \end{array} \begin{array}{c} \begin{array}{cccccc} & 1 & 2 & & & m-1 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & \cdots & & 1 \\ 1 & \omega & \omega^2 & & & \omega^{m-1} \\ 1 & \omega^2 & \omega^4 & \cdots & & \vdots \\ \vdots & & & \omega^{jk} & & \vdots \\ 1 & \underset{\omega^*}{\omega^{m-1}} & & \cdots & & \end{bmatrix} \end{array}$$

DFT_m is unitary.

$$\cancel{\left[(DFT_m)^*(DFT_m)\right]_{jj} = \frac{1}{\sqrt{m}}\sum_{k\in\mathbb{Z}_m}\omega^{jk}}$$ (Next time)