Shor Algorithm

Periods

$f: \mathbb{Z} \to G$ is periodic if $\exists r \in \mathbb{Z}$ s.t.

$f(x+r) = f(x) \quad \forall x \in \mathbb{Z}$

---

ex: $f(x) = g^x \bmod m$.

$\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}^\times$

further nice property:

if $f(x) = f(y)$, then $r \mid y - x$.

---

period of f is $\log_g(1)$

$f(x) = x \; P$

Quantum Computations

let $2^{n_0} > \#G$ output

$n = 2n_0$ input

so $2^n > (\#G)^2$

get state $|0\rangle_n |0\rangle_{n_0}$

apply $H^{\otimes n} \otimes 1$

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x_n\rangle |0\rangle_{n_0}$$

apply U_f

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_{n_0}$$

take a measurement of the output register.

$$|\psi\rangle_n |f_0\rangle_{n_0} = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n |f_0\rangle_{n_0}$$

x_0 is smallest int s.t. $f(x_0) = f_0$

m is # of inputs that give f_0.

$$m = \left\lfloor \frac{2^n}{r} \right\rfloor \text{ or } m = \left\lfloor 2^n/r \right\rfloor + 1.$$

$\{x \mid f(x) = f_0\}$

If cloning

measure twice, get $x_0 + k_1 r$, $x_0 + k_2 r$

difference is $(k_2 - k_1) r$

three times also get $(k_3 - k_1) r$

and gcd would probably be r.

$$|\psi\rangle_n = \frac{1}{\sqrt{m}} \sum_{K=0}^{m-1} |x_0 + Kr\rangle_n$$

$$U_{FT}|\psi\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \left(\frac{1}{\sqrt{m}} \sum_{K=0}^{m-1} e^{2\pi i (x_0 + Kr) y / 2^n} |y\rangle_n \right)$$

$$= \frac{1}{\sqrt{2^n m}} \sum_{y=0}^{2^n-1} \sum_{K=0}^{m-1} \exp\left(2\pi i x_0 y / 2^n + 2\pi i K r y / 2^n\right) |y\rangle_n$$

$$= \frac{1}{\sqrt{2^n m}} \sum_{y=0}^{2^n-1} \exp(2\pi i x_0 y / 2^n) \left(\sum_{K=0}^{m-1} \exp(2\pi i K r y / 2^n) \right) |y\rangle_n$$

Measure.

$$p(y) = \left| \frac{1}{\sqrt{2^n m}} \exp(2\pi i x_0 y / 2^n) \left(\sum_{K=0}^{m-1} \exp(2\pi i K r y / 2^n) \right) \right|^2$$

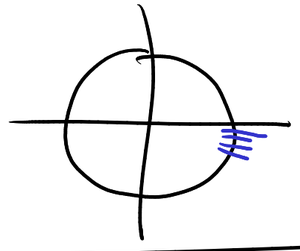
$$= \frac{1}{2^n m} \cdot 1 \left| \sum_{K=0}^{m-1} \exp(2\pi i K r y / 2^n) \right|^2$$

$\exp(x) = e^x$

$e^{a+b} = e^a e^b$

$e^{ix} = \cos(x) + i \sin(x)$

$|e^{ix}| = \cos^2(x) + \sin^2(x) = 1.$



$\exp\left(K \cdot \frac{ry}{2^n} \cdot 2\pi i\right)$

$p(y)$ is biggest when $\frac{yr}{2^n}$ is close to 1.

Lemma!
prob that $|y - j2^n/r| < 1/2$ is $\geq .4$.

Then!

$$\left| \frac{y}{2^n} - \frac{\hat{j}}{r} \right| < \frac{1}{2^{n+1}}$$

Know $y, 2^n$

so I have precise estimate of j/r.

$$\frac{\hat{j}}{r} \in \left(\frac{y}{2^n} - \frac{1}{2^{n+1}}, \frac{y}{2^n} + \frac{1}{2^{n+1}} \right)$$

Since $r < 2^{n_0} = \sqrt{2^n}$

there is at most one rational w/denom $< 2^{n_0}$ in this interval.

Know j_0/r_0 in lowest terms.

$> 50\%$ chance that $r_0 = r$

use classical computer to check $f(r_0)$

if $\uparrow$ done

else, check $f(2r_0), f(3r_0), f(4r_0)$, —

likely this works.

else

start over.

Pf of lemma

$\cos(-x) = \cos(x)$

$\sin(-x) = -\sin(x)$

Let $y_j = j2^n/r + \delta_j$ for $|\delta_j| \le 1/2$

$$\exp(2\pi i k r y_j/2^n) = \exp(2\pi i k j + 2\pi i k r \delta_j/2^n)$$

$$\sum_{k=0}^{m-1} \exp(2\pi i k r y_j/2^n) = \sum_{k=0}^{m-1} \left(\exp(2\pi i r \delta_j/2^n)\right)^k = \frac{1-\exp(2\pi i r \delta_j/2^n)^m}{1-\exp(2\pi i r \delta_j/2^n)}$$

$$\left|1-\exp(2\pi i r \delta_j/2^n)\right|^2 = 2 - \exp(2\pi i r \delta_j/2^n) - \exp(-2\pi i r \delta_j/2^n)$$

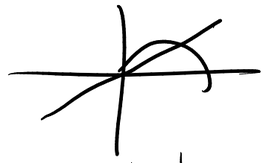
$$= 2 - \left(\cos(2\pi r \delta_j/2^n) + i\sin(2\pi r \delta_j/2^n)\right) - \left(\cos(-2\pi r \delta_j/2^n) + i\sin(-2\pi r \delta_j/2^n)\right)$$

$$= 2 - 2\cos(2\pi r \delta_j/2^n)$$

$$= 4\sin^2(\pi r \delta_j/2^n)$$

$$\left|1-\exp(2\pi i r \delta_j/2^n)^m\right|^2 = 4\sin^2(\pi m r \delta_j/2^n)$$

$$p(y_j) = \frac{1}{2^n m} \frac{\sin^2(\pi \delta_j m r/2^n)}{\sin^2(\pi \delta_j r/2^n)}$$



$|\sin(x)| \geq \left|\frac{2x}{\pi}\right|$

$\sin(x) \approx x$ for small x.

since $m \approx \frac{2^n}{r}$

$$p(y_j) \approx \frac{r}{(2^n)^2} \frac{\sin^2(\pi \delta_j)}{\sin^2(\pi \delta_j r/2^n)} \approx \frac{r}{(2^n)^2} \frac{\sin^2(\pi \delta_j)}{(\pi \delta_j)^2 (r/2^n)^2} = \frac{1}{r} \cdot \frac{\sin^2(\pi \delta_j)}{(\pi \delta_j)^2}$$

$$\geq \frac{1}{r} \cdot \frac{\left(\frac{2\pi \delta_j}{\pi}\right)^2}{(\pi \delta_j)^2} = \frac{4}{\pi^2 r}.$$

But, there are r such y_j

so $p(|y - j2^n/r| \leq 1/2) \geq r \cdot \frac{4}{\pi^2 r} = \frac{4}{\pi^2} \approx .4053\ldots$