

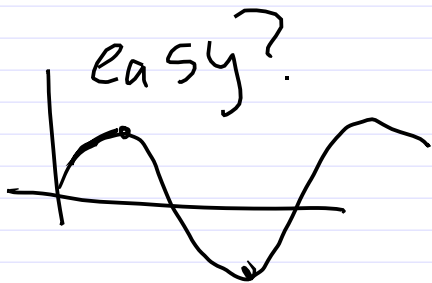
Period Finding (real setting)

Consider $f(x) = b^x \bmod N$

"discrete exponential"

Suppose $f(x+r) = f(x)$

has period r , $b^r \bmod N = 1$



try m times $\binom{m}{2} = \frac{m(m-1)}{2}$ pairs

f is an n -bit function

so x has 2^n values

$$\binom{m}{2} \sim m^2 \sim 2^n$$

$$m \sim 2^{n/2}$$

$$\text{QC } f(x) = b^x \text{ mod } N \quad f(x) = f(x+r)$$

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

$$U_f H^{\otimes n} |0\rangle_n |0\rangle_{n_0} = \frac{1}{2^{n/2}} \sum_{0 \leq x < 2^n} |x\rangle_n |f(x)\rangle_{n_0}$$

measure output qubits $f(x_0)$, input will be

$$\begin{aligned} |\Psi\rangle_n &= \frac{1}{\sqrt{m}} \left(|x_0\rangle + |x_0+r\rangle + |x_0+2r\rangle + \dots \right) \\ &= \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0+kr\rangle |f(x_0)\rangle \end{aligned}$$

Challenge:

get rid of x_0 to learn about r .

Solution: $H^{\otimes n} \rightarrow U_{FT}$

$$U_{FT} |x\rangle_n = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{2\pi i xy / 2^n} |y\rangle_n$$

Ordinary F.T. $\underline{f(x)} = \int_{\omega} e^{i\omega x} \tilde{f}_{\omega}$

$$\tilde{f}_{\omega} = \int_{x'} e^{-i\omega x'} f(x')$$

$$\int_x e^{i(\omega - \omega') x'} = \delta(\omega - \omega')$$

verify that $U_{FT}^{\dagger} = U_{FT}^{-1}$:

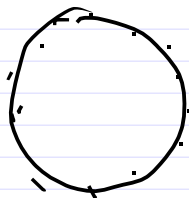
$$\langle x' | U_{FT}^\dagger U_{FT} | x \rangle$$

$$\langle x' | x \rangle = \delta_{x'x}$$

$$= \frac{1}{2^n} \sum_{y, y'} \langle y' | e^{-2\pi i x' y / 2^n} e^{2\pi i x y / 2^n} | y \rangle$$

$$= \frac{1}{2^n} \sum_{0 \leq y < 2^n} e^{2\pi i y (x - x') / 2^n}$$

$$= \delta_{x, x'}$$



[sum of phases around unit circle in \mathbb{C} , or see next page, which uses

$$S(r) = 1 + r + r^2 + \dots + r^{n-1}$$

$$rS(r) = S(r) + r^n - 1$$

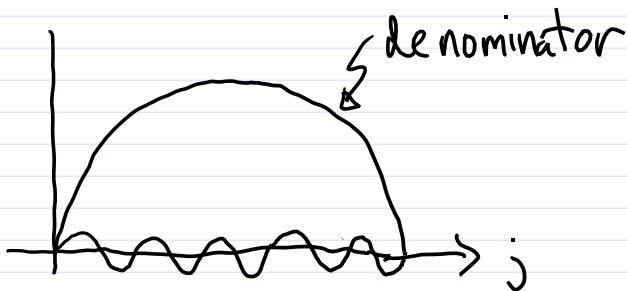
$$(1-r)S(r) = 1 - r^n \quad \& \quad S(r) = \frac{1-r^n}{1-r}$$

$$\frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i j k / N} = \delta_{j0}$$

Let $w = e^{2\pi i / N}$

$$\frac{1}{N} \sum_{k=0}^{N-1} w^{jk} = \frac{1}{N} \frac{1 - w^{Nj}}{1 - w^j} = \frac{1}{N} \frac{w^{Nj/2}}{w^{j/2}} \frac{w^{Nj/2} - w^{-Nj/2}}{w^{j/2} - w^{-j/2}}$$

$$\star = \frac{1}{N} w^{(N-1)j/2} \frac{\sin \pi j}{\sin \pi j / N}$$



Numerator: N half periods

vanishes for $j \neq 0$

$$j \rightarrow 0 \rightarrow \frac{1}{N} \frac{\pi}{\pi/N} = 1$$

$$= \delta_{j0}$$

$$\left(\star \text{ recall } \sin(x) = \frac{e^{ix} - e^{-ix}}{2i} \right)$$

Effect on amplitudes

$$\text{UFT} \left(\sum_{0 \leq x < 2^n} \gamma(x) |x\rangle \right) = \sum_{0 \leq x < 2^n} \tilde{\gamma}(x) |x\rangle$$

$$\tilde{\gamma}(x) = \frac{1}{2^{n/2}} \sum_{0 \leq y < 2^n} e^{2\pi i xy / 2^n} \gamma(y)$$

(usual active vs. passive)

$\gamma(x)$ are 2^n complex numbers

$\tilde{\gamma}(x)$ " " "

Ordinary FT $\sim (2^n)^2$

FFT $\sim n(2^n)$

Q.C. $O(n^2)$

$\left(\begin{array}{l} N \ln N \\ N = 2^n \end{array} \right)$

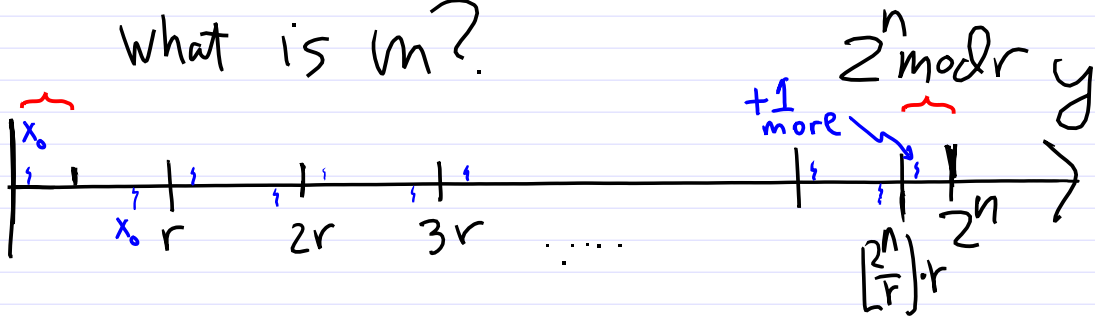
$$U_f |x\rangle_n |0\rangle_{n_0} = |x\rangle_n |f(x)\rangle_{n_0}$$

$$U_f \frac{1}{2^{n/2}} \sum_{0 \leq x < 2^n} |x\rangle_n |0\rangle_{n_0} = U_f \underbrace{H^{\otimes n}}_{|+\rangle^{\otimes n}} |0\rangle |0\rangle_{n_0}$$

$$= \frac{1}{2^{n/2}} \sum_x |x\rangle_n |f(x)\rangle_{n_0} \quad \text{measure output}$$

$$\rightarrow \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n |f(x_0)\rangle_{n_0}$$

What is m ?



$$m = \lfloor \frac{2^n}{r} \rfloor \quad \text{if } x_0 > 2^n \bmod r$$

$$m = \lfloor \frac{2^n}{r} \rfloor + 1 \quad \text{if } x_0 < 2^n \bmod r$$

$$|\psi\rangle_n = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle |f(x_0)\rangle$$

$$U_{FT} |\psi\rangle_n = \frac{1}{2^{n/2}} \sum_y \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} e^{2\pi i (x_0 + kr)y/2^n} |y\rangle$$

$$= \sum_{0 < y \leq 2^n} e^{2\pi i x_0 y/2^n} \frac{1}{\sqrt{2^n m}} \left(\sum_{k=0}^{m-1} e^{2\pi i k r y/2^n} \right) |y\rangle$$

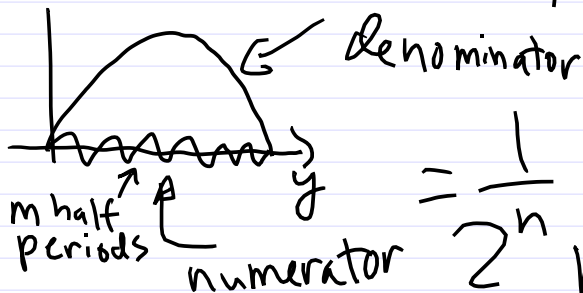
(just a phase)

now measure y , x_0 disappears:

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

Peaked at $y \approx 2^n / r j$

$$p(y) = \frac{1}{2^n m} \left| \frac{1 - e^{2\pi i m r y / 2^n}}{1 - e^{2\pi i r y / 2^n}} \right|^2$$



$$= \frac{1}{2^n m} \frac{\sin^2 \pi m r y / 2^n}{\sin^2 \pi r y / 2^n}$$

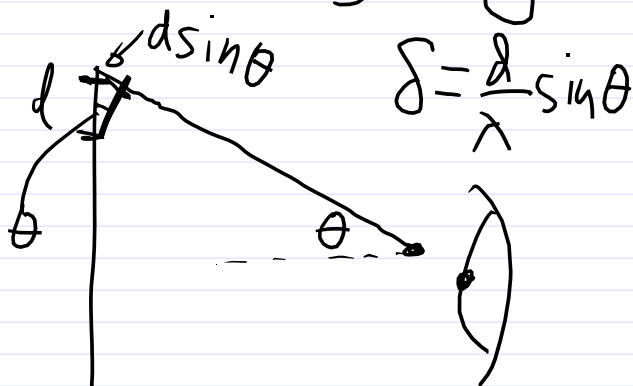
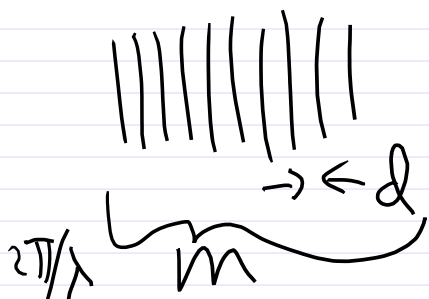
Now only appreciable

near \rightarrow

$$y = j \cdot 2^n / r$$

needs classical work to extract r from (nearest integer to) $j \cdot 2^n / r$

Recall diffraction grating



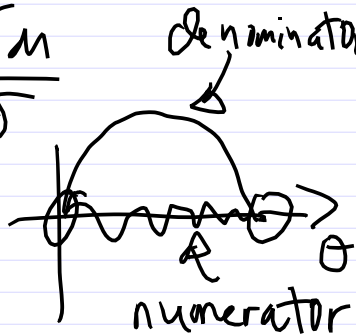
e^{ikx} - phase

$$\sum_{k=0}^{m-1} e^{2\pi i \delta k} = \frac{1 - e^{2\pi i \delta m}}{1 - e^{2\pi i \delta}}$$

$$= \frac{e^{i\pi \delta m}}{e^{i\pi \delta}} \frac{\sin \pi \delta m}{\sin \pi \delta}$$

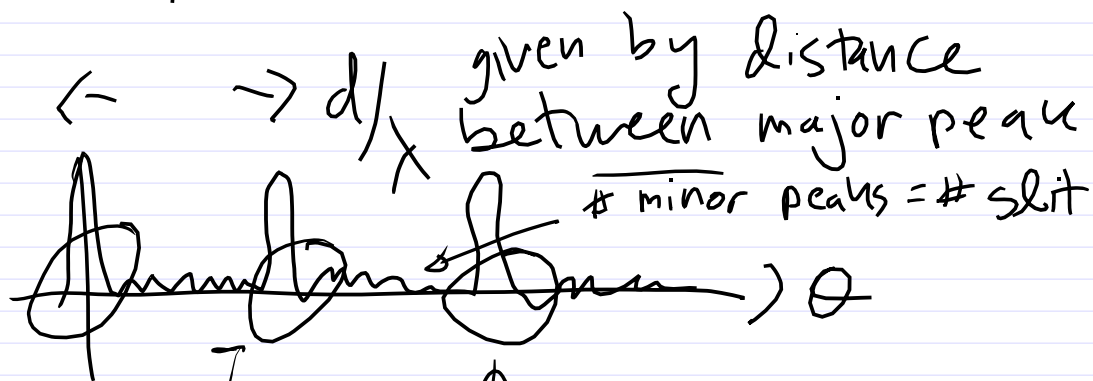
denominator

$$| | |^2 = \frac{\sin^2 \pi \delta m}{\sin^2 \pi \delta}$$



$$\text{Intensity}(\theta) = \left| \right|^2 = \frac{\sin^2 \pi \delta m}{\sin^2 \pi \delta}$$

$$\delta = d/\lambda \sin \theta$$



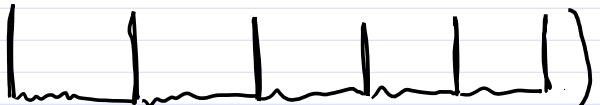
$$d/\lambda \sim r/2^n$$

$$j d/\lambda$$

$$y x j \frac{2^n}{r}$$

Technical Statement (for next time:
if $y/2^n$ is an estimate for j/r
that differs from it by less
than $1/2r^2$, then j/r will appear
as one of the "partial sums"
in the continued-fraction expansion
of $y/2^n$. (Both concepts to

be covered,
but recall $|j/r - j'/r'| = \frac{|r'j - jr'|}{rr'} \geq \frac{1}{rr'}$)

But this is the technical reason
why the input bits are doubled,
giving so many periods m . (In the
diffraction grating analog, taking
large #slits m gives sharper focus
on the peaks )