Breaking RSA encryption-Shor's Algorithm

PHYS/CSCI 3090

Prof. Alexandra Kolla

Alexandra.Kolla@Colorado.edu
ECES 122

Prof. Graeme Smith

Graeme.Smith@Colorado.edu
JILA S326

https://home.cs.colorado.edu/~alko5368/indexCSCI3090.html

Come see us!

- Alexandra Kolla/ Graeme Smith: Friday 3:00-4:00 pm, JILA X317.
- Ariel Shlosberg: Tu/Th 2:00-4:00pm, DUANG2B90 (physics help room)
- Steven Kordonowy: Th 11am-12pm, ECAE 124.
- Matteo Wilczak: Wednesday, 1-2pm, DUANG2B90 (physics help room)

Last Class

- Period finding, DFT, QFT

Today

- Finish Period finding

The problem

- One is told that f is periodic under ordinary addition, $f(y) = f(x)$, if $y = kr + x$, for any integer k.
- i.e x and y differ by an integral multiple or period r.
- The problem is to find the period r.

DFT

- Let $\omega = e^{2\pi i/N}$ a primitive N-th root of unity
- $f = \big(f(0), f(1), \dots, f(N-1)\big)$ a function
- The Discrete Fourier Transform of f is defined as

$$\mathrm{F} = \big(F(0), F(1), \dots, F(N-1)\big)$$

- Where $F(k) = \sum_n \omega^{kn} f(n)$

QFT

- Say we have n qubits. (So 2^n possible basis vectors).
- $\omega = e^{\frac{2\pi i}{2^n}}$
- $U_{FT}|x\rangle_n = \frac{1}{2^{\frac{n}{2}}}\sum_y \omega^{xy}|y\rangle_n$

QFT

- $f = \big(f(0), f(1), \ldots, f(N-1)\big), \mathrm{N} = 2^{\mathrm{n}}$
- $f = \sum_x f(x)|x\rangle_n$
- $U_{FT}(\sum_x f(x)|x\rangle_n) = \sum_y F(y)|y\rangle_n$
- $F(y) = \frac{1}{2^{\frac{n}{2}}} \sum_x \omega^{xy} f(x)$
- So $U_{FT}(\sum_x f(x)|x\rangle_n) = \frac{1}{2^{\frac{n}{2}}} \sum_y \sum_x \omega^{xy} f(x)\,|y\rangle_n$

QFT in matrix form

$$\begin{pmatrix} F(0) \\ F(1) \\ \dots \\ F(N-1) \end{pmatrix} =$$

$$\frac{1}{\sqrt{M}} \begin{bmatrix} 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{M-2} & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \dots & \dots & \omega^{2(M-1)} \\ 1 & \omega^j & \omega^{2j} & \dots & \dots & \omega^{(M-1)j} \\ & & & & \dots & \\ 1 & \omega^{M-1} & \omega^{2(M-1)} & \dots & & \omega^{(M-1)(M-1)} \end{bmatrix} \begin{pmatrix} f(0) \\ f(1) \\ \dots \\ f(N-1) \end{pmatrix}$$

QFT in matrix form

- Suggests an N^2 algorithm. Classical FFT is performed in O(NlogN) steps
- Quantum FT exponentially faster, $O(\log^2 N)$!
- Wait, how can an algorithm run in time less than the size of input??

Smaller than input size?

We know that no algorithm can run in time less than linear in the input size n, sinc
it at least has to read the input in $\Omega(n)$ time.
How can the QFT run in time log N?

A)Quantum computers achieve exponential speedup

B)QFT does not need to read the whole input like binary search

C) Input size is actually logN

D)Some serious magic happening

QFT in matrix form

- Suggests an N^2 algorithm. Classical FFT is performed in

O(NlogN) steps

- Quantum FT exponentially faster, $O(\log^2 N)$!
- Wait, how can an algorithm run in time less than the size of input??
- Classical FFT always outputs the whole Fourier transorm. While Quantum FT is more like Sampling. Measure F(k) with some probability.

The Algorithm

- 1) Prepare: $(H^{\otimes n} \otimes \mathrm{I})\ |0\rangle_n \ \ |0\rangle_{n_0} =$
$\frac{1}{2^{n/2}} \sum_{0<x\leq 2^n} |x\rangle_n\ |0\rangle_n$

- 2) Single application of oracle (can be done efficiently for our f):

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

- 3)Measure output register: If I get some value of f, say f(x_0), then input register is $\frac{1}{\sqrt{m}}(\sum_k |x_0 + kr\rangle)$

The Algorithm

- 4) Apply QFT to $\frac{1}{\sqrt{m}}\left(\sum_k |x_0 + kr\rangle\right)$

How many multiples of r?

Assume that r divides N.
The superposition $(\sum_k |x_0 + kr\rangle)$ consists of how many different multiples of r?

A) N

B) N/r

C) r

D) It depends on x_0

The Algorithm

- Assume, for now, that r divides N.
- The superposition $\left(\sum_k |x_0 + kr\rangle\right)$ consists of N/r different multiples of r.
- So my state after collapse is

$$\frac{1}{\sqrt{\frac{N}{r}}}\left(\sum_{k=0\ to \frac{N}{r}} |x_0 + kr\rangle\right)$$

The Algorithm

- Theorem:

Suppose the input to QFT is periodic with period r, for some r that divides N. Then the output will be a multiple of N/k, and it is equally likely to be any of the r multiples of N/r.

- Now we repeat the experiment a few times and take GCD of all the indices returned, we get N/r (and thus r) w.h.p.

The Algorithm

- 4) Apply QFT to $\frac{1}{\sqrt{\frac{N}{r}}}\sum_j |x_0 + jr\rangle$. First assume $x_0 = 0$.
- Claim (ex. in class):

If $|a\rangle = \frac{1}{\sqrt{\frac{N}{r}}}\left(\sum_j |jr\rangle\right)$ then

$$U_{FT}(|a\rangle) = |\beta\rangle = \frac{1}{\sqrt{r}}\left(\sum_{j=0 \ to \ r-1} \left|\frac{jN}{r}\right\rangle\right)$$

Sums of roots of unity.

What is the sum $1+\omega^{jr}+\omega^{2jr}+\omega^{3jr}+\cdots+\omega^{(\frac{N}{r}-1)jr}$, where $\omega = e^{2\pi i/N}$

A) N/r-1

B) 0

C) 1

D) It depends on jr mod (N)