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 start

Today

- Discrete Fourier Transform
- Quantum Fourier Tranform

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.

Vector or Function?

How can I write the function $f\colon [N] \to C$ as a vector?

A) $\mathrm{f} = \sum_{x=0\ to\ N-1} f(x)|x\rangle_n$

B) $\mathrm{f} = (f(x), 0, \dots, 0)$

C) $\mathrm{f} = (f(x), f(x), \dots, f(x))$.

D) $\mathrm{f} = \sum_{x=0\ to\ 2^N-1} f(x)|x\rangle_n$

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

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

Roots of unity

What are the primitive 2nd roots of unity?

A) $0{,}1$

B) $-1, e^{\pi i}$

C) $\mathrm{e}^{\pi i}, e^{2\pi i}$

D) $\mathrm{e}^{\pi i}, e^{2\pi i}, e^{3\pi i}$

Hadamard

What is the action of the n-fold Hadamard on the basis vector x?

A) $H^{\otimes n}|x\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_y |y\rangle_n$

B) $H^{\otimes n}|x\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_y e^{\pi i x\cdot y}|y\rangle_n$

C) $H^{\otimes n}|x\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_y (-1)|y\rangle_n$

D) $H^{\otimes n}|x\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_y e^{2\pi i x\cdot y}|y\rangle_n$

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 $\frac{1}{\sqrt{m}}\left(\sum_k |x_0 + kr\rangle\right)$

- Exercise in class