Lecture 16.

We have seen that in order to break the RSA cryptosystem, one needs to factorize a number $n = pq$ with $p, q \gg 0$ distinct prime numbers. No classical algorithm, which can factor any n-bit integer in time $O(n^k)$ for a fixed k is known (polynomial-time algorithm). The largest number factored was RSA-250, a 829-bit number with 250 decimal digits. That was in 2020. Our next goal is to discuss an algorithm, which is quantum. It runs in $O(n^2 \log(n) \log(\log(n)))$ quantum gates (is polynomial) and was invented by Peter Shor in 1994. The algorithm relies on quantum Fourier transform, which we will discuss now.

Discrete Fourier Transform (DFT).

Def-n. The <u>discrete Fourier transform</u> for a finite group G is a linear operator from the space of functions on that group to itself.

We will restrict our discussion to abelian (commutative) groups. Let's start with cyclic groups, i.e. $G = (\mathbb{Z}_N, +)$.

$$F_N := DFT_{\mathbb{Z}_N} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & \omega^{N-1} & \cdots & \cdots & \omega^{2N-2} \end{pmatrix}$$

, where $\omega = e^{2\pi i/N}$ is the primitive Nth root of 1.

The discrete Fourier transform is the operator given in the basis of δ-functions: $\{\delta_0, \dots, \delta_{N-1} \in \mathbb{C}[\mathbb{Z}_N]\}$ with $\delta_i(k) := \delta_{ik} = \begin{cases} 1, & i=k \\ 0, & i \neq k \end{cases}$ by the matrix F_N.

Let's show that F_N is a unitary operator (so it can be applied to qubits). It will be helpful to take a look at the 'continuous analogue' of the story.

Let $S^1 = \{\lambda \in \mathbb{C}^* \mid |\lambda| = 1\}$ be the unit circle and $C(S^1)$ the set of continuous maps $S^1 \to S^1$. Recall that we can parameterize the unit circle with a single variable $t \in [0, 2\pi)$ via $(x,y) = (\cos(t), \sin(t))$. Define the Hermitian inner product on $C(S^1)$ via $\langle f, g \rangle := \frac{1}{2\pi} \int_0^{2\pi} \overline{f(t)} g(t)\, dt$.

Lemma. The set of f-ns $\{f_n(t) = e^{int}\}_{n \in \mathbb{Z}_{\geq 0}}$ consists of orthonormal f-ns in $C(S^1)$.

Proof. Notice that $\overline{e^{int}} = e^{-int}$ (as t is a real number), hence $\langle f_n, f_m \rangle = \frac{1}{2\pi} \int_0^{2\pi} \overline{e^{int}} \cdot e^{imt}\, dt = \begin{cases} \frac{1}{2\pi} \int_0^{2\pi} dt = 1, & n = m. \\ \frac{1}{2\pi} \int_0^{2\pi} e^{i(n-m)t} dt = \frac{e^{i(n-m)t}}{2\pi i(n-m)} \Big|_0^{2\pi} = 0 \end{cases}$

In order to show that F_N is unitary, one needs to verify that the column vectors are orthonormal (of unit norm and orthogonal to each other). Notice that the k^{th} column is essentially 'discrete analogue' of the function $\frac{e^{ikt}}{\sqrt{N}} = \frac{f_k(t)}{\sqrt{N}}$.

Indeed, the jk-entry of F_N is $\frac{1}{\sqrt{N}}\omega^{kj} = \left(e^{\frac{2\pi i}{N}\cdot jk}\right)/\sqrt{N} = \frac{f_k(j)}{\sqrt{N}}$.

The other substitution that we need is $\int_0^{2\pi} \rightsquigarrow \sum_{s=0}^{N-1}$. We check that $\langle F_N^{\text{column}(k)}, F_N^{\text{column}(j)} \rangle = \frac{1}{N}\sum_{s=0}^{N-1} \overline{\omega^{ks}}\cdot \omega^{js} =$

$$= \frac{1}{N}\sum_{s=0}^{N-1} \omega^{(j-k)s} = \begin{cases} \frac{1}{N}(\underbrace{1+\dots+1}_{N}) = 1, & j=k. \\ \frac{1}{N}\sum_{s=0}^{N-1} t^s = \frac{1}{N}\cdot\frac{1-t^N}{1-t} = 0. \end{cases}$$

$(t = \omega^{j-k}$ and $t^N = e^{\frac{2\pi i\cdot(j-k)\cdot N}{N}} = e^{2\pi i(j-k)} = 1)$

<u>Rmk.</u> F_N is symmetric $(\omega^{js} = \omega^{sj})$, hence, $F_N^t = F_N$ and $F_N^{-1} = F_N^{\dagger} = \overline{F_N}$.

<u>Example.</u> Let $N=4$, i.e. $G = \mathbb{Z}/4\mathbb{Z}$. Then $F_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & -1 \end{pmatrix}$

$(\omega = e^{2\pi i/4} = i)$

In case $N=2$ with $\omega = e^{2\pi i/2} = -1$, we get $F_2 = H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

<u>Fact.</u> Any finite abelian group G is isomorphic to a product of cyclic groups: $G \simeq \mathbb{Z}_{N_1}\times\mathbb{Z}_{N_2}\times\dots\times\mathbb{Z}_{N_k}$ with $N_i \in \mathbb{Z}_{>1}$ (not necessarily distinct). We define the discrete Fourier transform for G via the tensor product

$$DFT_G := F_{N_1}\otimes F_{N_2}\otimes\dots\otimes F_{N_k}.$$

<u>Exercise.</u> The groups $\mathbb{Z}_6$ and $\mathbb{Z}_2\times\mathbb{Z}_3$ are isomorphic. Compare $DFT_{\mathbb{Z}_2\times\mathbb{Z}_3} = F_2\otimes F_3$ with F_6.

Back to the factorization problem: $n=pq$, so we assume that n is not even and $p\neq q$.

Let's pick an arbitrary number $x\in\mathbb{Z}_n$ and compute $\gcd(x,n)$ using Euclid's algorithm. If $\gcd(x,n)\neq 1$, then we have found a divisor of n (p or q), so we assume $\gcd(x,n)=1$ and $x\in\mathbb{Z}_n^\times$ (the multiplicative group). Let r be the order of x in $\mathbb{Z}_n^\times$ (smallest positive integer with $x^r\equiv 1 \pmod n$)). Moreover, let's assume $r=2k$ is even (this will happen with probability $3/4$) giving

$$x^r\equiv 1 \pmod N \iff x^{2k}-1\equiv 0 \pmod N \iff (x^k-1)(x^k+1)\equiv 0 \pmod N$$
$$\iff (x^k-1)(x^k+1)=kN \text{ for some } k>0.$$

Notice that $x^k-1\not\equiv 0 \pmod N$, as otherwise k would be the order of x. It is not hard to show that with probability greater or equal to $\frac{1}{2}$ r is even and $(x^{r/2}+1)\not\equiv 0 \pmod N$ implying
$$1<\gcd(x^k-1,N)<N \text{ and } 1<\gcd(x^k+1,N)<N$$
and allowing us to find factors of N once r is found.

<u>Rmk.</u> Let $f:\mathbb{N}\to\mathbb{Z}_n$ be a function with the property that $f(a)=f(b) \iff a\equiv b \pmod r$, i.e. f is a periodic function with period r. We have reduced the factorization problem to period-finding problem for the function $f_x:\mathbb{N}\to\mathbb{Z}_N$ with $f_x(a)=x^a$.

Shor's algorithm.

Q: How can we find the period?

Slogan: Hadamard - Oracle - DFT.

Recall that Simon's algorithm could be summarized as

Hadamard - Oracle - Hadamard,

so the main difference is in the last part.

Let's work out the details.

① The starting (initial) state vector is $|0^\ell\rangle|0^\ell\rangle$ with ℓ being a number with $N^2 < 2^\ell < 2N^2$. After applying the Hadamard operator to first ℓ qubits followed by the oracle, we end up with the state

$$\frac{1}{\sqrt{q}}\sum_{i=0}^{q-1} |i\rangle|f(i)\rangle \quad (\text{here } q := 2^\ell).$$

② Next we measure the second register. The result is $\frac{1}{\sqrt{m}}\sum_{i=0}^{m-1} |ir+k\rangle$ for some k with $f(|k\rangle)$ being equal to the result of the measurement (k is the smallest number with this value of f) and $m = \lfloor q/r \rfloor$ or $\lceil q/r \rceil$ (easy to find which one in concrete examples).

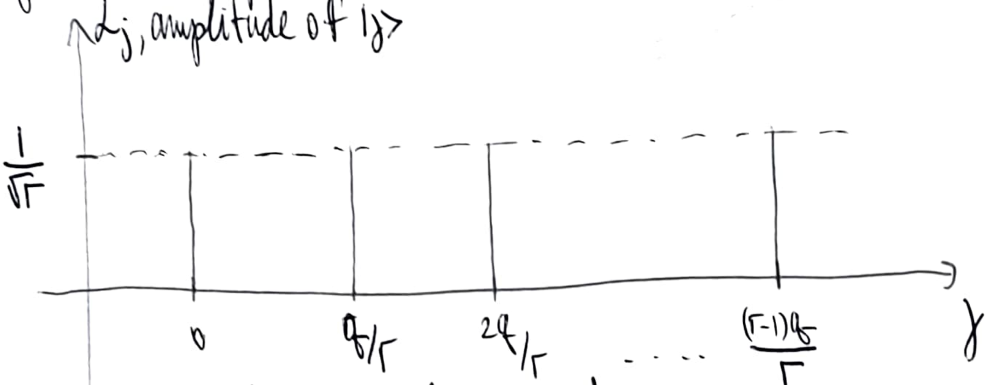
③ Apply the DFT:

$$F_q\left(\frac{1}{\sqrt{m}}\sum_{i=0}^{m-1}|ir+k\rangle\right) = \frac{1}{\sqrt{m}}\sum_{i=0}^{m-1}\frac{1}{\sqrt{q}}\sum_{j=0}^{q-1}\omega^{(k+ir)j}|j\rangle =$$

$$= \frac{1}{\sqrt{mq}}\sum_{j=0}^{q-1}\omega^{kj}\left(\sum_{i=0}^{m-1}\omega^{irj}\right)|j\rangle \quad (\star)$$

Notice that $\sum_{i=0}^{m-1}\omega^{irj} = \begin{cases} m, & rj \equiv 0 \pmod{q} \\ \frac{1-\omega^{rjm}}{1-\omega^{rj}}, & \text{otherwise.}\end{cases}$

Let's take a closer look at state vector ☆. For simplicity we will first analyze the case when r divides q. This is unlikely to happen but will give the right intuition regarding what is going on. If r divides q, then $\lfloor q/r \rfloor = \lceil q/r \rceil$, so $m = q/r$ and $\omega^{rjm} = e^{\frac{2\pi i}{q}\cdot r \cdot j \cdot \frac{q}{r}} = e^{2\pi i j} = 1$ implying all amplitudes $\frac{1-\omega^{rjm}}{1-\omega^{rj}}$ with $rj \not\equiv 0 \pmod{q}$ vanish, while the amplitudes of $|j\rangle = |s \cdot \frac{q}{r}\rangle$ are equal to $\frac{m}{\sqrt{mq}} = \sqrt{\frac{m}{q}} = \frac{1}{\sqrt{r}}$ (there are r such values of j so $r \cdot \left(\frac{1}{\sqrt{r}}\right)^2 = 1$, the sum of the squares of probabilities is 1).



(4) Measuring the first register gives some number $\frac{sq}{r} =: \ell$. This can be rewritten as $\frac{s}{r} = \frac{\ell}{q}$, where we know ℓ and q, but not s and r.

If s and r happen to be coprime then $r = \frac{q}{\gcd(\ell, q)}$. The expected number of random choices of $0 < s < r+1$ to hit s with $\gcd(s, r) = 1$ is $O(\log(\log(r)))$. After obtaining $\tilde{r} = \frac{q}{\gcd(\ell, q)}$ (we don't know if $\gcd(s,r) = 1$ ☆☆), one checks whether $x^{r} \equiv 1 \pmod{n}$. If so, the period is $r = \tilde{r}$.

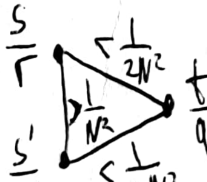
As $q=2^l$, it is unlikely that r divides q, so the amplitudes $\frac{1}{\sqrt{mq}}\frac{1-\omega^{rjm}}{1-\omega^{rj}}$ will not vanish. Let's estimate the absolute value of such an amplitude. We will use that $|1-e^{i\theta}|=2|\sin(\theta/2)|$ (see HW exercise).

$$\left|\text{Amplitude of } |j\rangle\right| = \frac{1}{\sqrt{mq}}\cdot\frac{|1-\omega^{rjm}|}{|1-\omega^{rj}|} = \frac{1}{\sqrt{mq}}\cdot\frac{\left|\sin\left(\frac{\pi rjm}{q}\right)\right|}{\left|\sin\left(\frac{\pi rj}{q}\right)\right|}$$
$(rj \equiv 0 \pmod q)$

Notice that for $m \gg 0$ the numerator oscillates much faster than denominator. The abs. value of amplitude is large when the denominator is close to 0, i.e. $\frac{\pi rj}{q} \approx \pi k$, $k\in\mathbb{Z} \Leftrightarrow j \approx k\cdot\frac{q}{r}$, $k\in\mathbb{Z}$.
One can deduce that the outcome of Shor's algorithm will likely (with high probability) be a number t with

$$\left|\frac{t}{q}-\frac{s}{r}\right| < \frac{1}{2q} \quad (\star)$$

<u>Key observation.</u> Two fractions s/r and s'/r' with denominators $\le N$ are at least $\frac{1}{N^2}$ apart. As $q>N^2$, $\frac{1}{2q}<\frac{1}{2N^2}$ giving that $\frac{s}{r}$ satisfying $(\star)$ is unique.



$r, r' \le N$

Triangle inequality is violated:
$$\left(<\frac{1}{2N^2}\right)+\left(<\frac{1}{2N^2}\right) < \frac{2}{2N^2} = \frac{1}{N^2}$$
(sum of two sides of a triangle cannot be less than the remaining side).

<u>Q:</u> How can we find $\frac{s}{r}$?

<u>Continued fractions:</u> given a number $p/q \in \mathbb{Q}$ write it as $\frac{p}{q} = a_0 + \cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots}}}$

$a_i \in \mathbb{Z}_{\ge 0}$.

Let $\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}$, then $\left|\frac{p}{q} - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$.

find continued fraction for

<u>Example.</u> Let's (approximate) the number $\frac{5}{13}$.

$$\frac{5}{13} = 0 + \frac{1}{\frac{13}{5}} = 0 + \frac{1}{2+\frac{3}{5}} = 0 + \cfrac{1}{2+\cfrac{1}{5/3}} = 0 + \cfrac{1}{2+\cfrac{1}{1+\frac{2}{3}}} =$$

$$= 0 + \cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{2}}}}.$$

$a_0 = 0$, $a_1 = 2$, $a_2 = 1$, $a_3 = 1$, $a_4 = 2$.

We get approximations:

$$\frac{p_0}{q_0} = 0, \quad \frac{p_1}{q_1} = \frac{1}{2}, \quad \frac{p_2}{q_2} = \frac{1}{2+\frac{1}{1}} = \frac{1}{3}, \quad \frac{p_3}{q_3} = \cfrac{1}{2+\cfrac{1}{1+1}} = \frac{2}{5}.$$

In general p_n and q_n can be computed recursively via

$p_0 = a_0$, $p_1 = a_1 a_0 + 1$, $p_n = a_n p_{n-1} + p_{n-2}$

$q_0 = 1$, $q_1 = a_1$, $q_n = a_n q_{n-1} + q_{n-2}$.