# QFT Summary

$m = 2^n$, $n$ = # of qubits  $m \times m$

Classical discrete fourier transform: $O(m^2)$ via matrix multiplication

$O(m \log m)$ Fast Fourier transform.

Quantum computer: $O(\log^2(m))$ standard gates.

What does it do?

On a periodic superposition of $n$ qubits of period $r$

$$\frac{1}{\sqrt{m/r}} \sum_{k=0}^{m/r} |\ell + kr\rangle \quad \left\{ \begin{array}{l} |x\rangle \text{ included} \\ \iff x \equiv \ell \pmod r \end{array} \right.$$

the result is a state w/ magnitude of coeff of $|x\rangle$ peaks sharply @ $\frac{m}{r}\mathbb{Z} = \{0, \frac{m}{r}, 2\frac{m}{r}, 3\frac{m}{r}, \dots\}$


## Quantum Big Picture

(computational basis)

① qubits/registers: states are $\mathbb{C}$-linear combinations of classical states $|00\cdots0\rangle, |00\cdots1\rangle, \dots$

② measurement w.r.t. basis: prob. of obtaining a classical state is $|\text{coeff}|^2$. collapses state!

③ entanglement: w.r.t. basis whether it is a product of individual states (a sort of independence vibe)

④ gates: unitary transformations

⑤ parallelism: can compute $|x\rangle|0\rangle \longmapsto |x\rangle|f(x)\rangle$ $f$ = classical fn.

⑥ Q.F.T.: takes a periodic superposition (period $r$, $m$ states, $m = 2^n$) to a superposition supported near $\frac{m}{r}\mathbb{Z}$.

## Factoring N

Recall: If we can find $x \in \mathbb{Z}/N\mathbb{Z}$ s.t. $x^2 \equiv 1$, $x \not\equiv \pm 1 \ (N)$ then $\gcd(x \pm 1, N)$ is a non-trivial factor.

## Example

$N = 15$, $\varphi(15) = 8$

| | $\alpha^0$ | $\alpha^1$ | $\alpha^2$ | $\alpha^3$ | $\alpha^4$ | $\alpha^5$ | $\alpha^6$ ⋯ |
|---|---|---|---|---|---|---|---|
| $\alpha = 2$ | 1 | 2 | 4 | 8 | 1 | 2 | 4 |
| $\alpha = 13$ | 1 | 13 | 4 | 7 | 1 | 13 | 4 |
| $\alpha = 11$ | 1 | 11 | 1 | 11 | 1 | | |

fail

□ = interesting square root

**Idea:** Reduce factoring to period finding

① Take a random $\alpha$

② Find the multiplicative order of $\alpha$ ($\alpha^r \equiv 1 \bmod N$) ★ HARD

③ Hope $r$ is even. $\approx 1/2$ prob.

④ Hope $\alpha^{r/2} \not\equiv \pm 1$ $\approx 1/2$ prob.

⑤ $\gcd(\alpha^{r/2} \pm 1, N)$ a non-triv. factor

If we know order of 2 is 4, try $\gcd(\alpha^2+1, N) = \gcd(5,15) = 5$.

## Shor's Algorithm to factor N (eg. break RSA)

classical ① Take random $\alpha$ mod $N$, $\alpha \neq 0$ (could check $\gcd(\alpha, N)$)

quantum ② + ctd. frac. (classical) Find the mult. order $r$ of $\alpha$ mod $N$.
i.e. period of $x \mapsto \alpha^x \bmod N$
$f(x) = \alpha^x \bmod N$.

classical ③ check if $r$ is even, and $\alpha^{r/2} \not\equiv \pm 1 \pmod N$. } expect prob $\geq \frac{1}{4}$.
↳ if not, try new $\alpha$ (Step ①)
↳ if so, continue

classical ④ $\gcd(\alpha^{r/2} - 1, N)$ is a factor.

---

## Period Finding on a Quantum Computer

Given: $f: \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ s.t. $\boxed{f(x) = f(y) \iff x \equiv y \ (r)}$

Goal: find $r$.

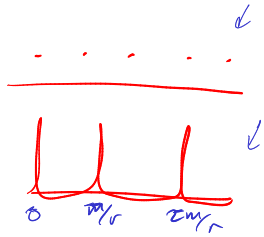
Initialize 2 registers of qubits to $|\vec{0}\rangle|\vec{0}\rangle$ { 1st register has $m_0$ qubits; 2nd $n_0$ qubits

$m = 2^{m_0}$ $n = 2^{n_0}$

$$|\vec{0}\rangle|\vec{0}\rangle \xrightarrow[\text{on 1st reg.}]{QFT_m^{-1}} \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} |\vec{x}\rangle|\vec{0}\rangle$$

$$\xrightarrow[\text{on 1st} \to \text{2nd}]{U_f} \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} |\vec{x}\rangle|f(\vec{x})\rangle$$

$$\xrightarrow[\text{2nd}]{\text{measure}} \frac{1}{\sqrt{m/r}} \sum_{k=0}^{\lceil m/r \rceil - 1} |l + kr\rangle|f(l)\rangle$$




$$\xrightarrow{QFT_m} \frac{1}{\sqrt{m}} \frac{1}{\sqrt{m/r}} \sum_{y=0}^{m-1} \sum_{k=0}^{m/r - 1} \omega^{(l+kr)y} |y\rangle|f(l)\rangle$$

$$\xrightarrow[\text{in 1st reg}]{\text{measure}} \text{get } |y\rangle|f(l)\rangle \text{ for a single } y \text{ near } \frac{m}{r}\mathbb{Z}.$$

Classically: determine $r$ from $m$, $y$. $y \approx t\frac{m}{r}$, $t \in \mathbb{Z}$.