QFT_n — Q. Fourier Transform on n qubits.

Recall: For $k \geq 2$:

$\omega := e^{2\pi i/k}$

$DFT_k e_j = \frac{1}{\sqrt{k}} \sum_{\ell=0}^{k-1} \omega^{j\ell} e_\ell$

QFT_n is "essentially" DFT_{2^n} unitary on n-qubit Hilbert space

For $x \in \{0,1\}^n$, interpret x as an integer in $\mathbb{Z}_{2^n}$ $(0 \leq x < 2^n)$ via the usual binary rep.

$$QFT_n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_{2^n}} \omega^{xy} |y\rangle$$

$\omega := e^{2\pi i/2^n}$

Notation: Let $e_n(x) := e^{2\pi i x/2^n}$

- $e_n(0) = 1$
- $e_n(x+y) = e_n(x) e_n(y)$
- $e_n(-x) = e_n(x)^{-1}$
- $e_n(x) = e_n(x \bmod 2^n)$
- [because $e_n(2^n) = e^{2\pi i} = 1$]
- $e_n(x) = e_{n+r}(2^r x)$ $[r \geq -n]$

So

$$QFT_n |x\rangle = \frac{1}{2^{n/2}} \sum_y e_n(xy) |y\rangle$$

$$= \frac{1}{2^{n/2}} (|0\rangle + e_1(x)|1\rangle) \otimes (|0\rangle + e_2(x)|1\rangle) \otimes \cdots \otimes (|0\rangle + e_n(x)|1\rangle) \otimes \cdots \otimes (|0\rangle + e_n(x)|1\rangle)$$

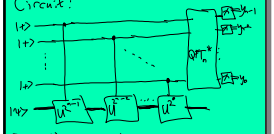
App: Phase Estimation

Given unitary U and an eigenvector $|\psi\rangle$ of U with eigenvalue $e^{i\theta}$ $(\theta \in \mathbb{R}$ unknown)

Task is to find θ (or a good approximation thereof) as a classical value.

Assume that (CU^{2^k}) can be implemented as a gate.

Circuit:



Run the circuit:

$$|+\rangle^{\otimes n} \otimes |\psi\rangle = \frac{1}{2^{n/2}} (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle) \otimes |\psi\rangle$$

$$= \frac{1}{2^{n/2}} \left(\bigotimes_{k=1}^{n} (|0\rangle + |1\rangle) \right) \otimes |\psi\rangle$$

Contribution from the k'th control:

$$\cdots \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes |\psi\rangle$$

$$= \cdots \otimes |0\rangle \otimes \cdots \otimes |\psi\rangle + \cdots \otimes |1\rangle \otimes \cdots \otimes |\psi\rangle$$

$$\xrightarrow{CU^{2^k}} \cdots \otimes |0\rangle \otimes \cdots \otimes |\psi\rangle + e^{i\theta 2^k} (\cdots \otimes |1\rangle \otimes \cdots \otimes |\psi\rangle)$$

$$= \cdots \otimes (|0\rangle + e^{i\theta 2^k} |1\rangle) \otimes \cdots \otimes |\psi\rangle$$

After all the controls:

$$\bigotimes_{k=1}^{n} (|0\rangle + e^{i\theta 2^k} |1\rangle) \otimes |\psi\rangle$$

$$= \bigotimes_{k=1}^{n} (|0\rangle + e_k(2^k f) |1\rangle) \otimes |\psi\rangle$$

where $f := \theta/2\pi$

$\theta \in [0, 2\pi)$

$\therefore f \in [0, 1)$

$$\bigotimes_{k=1}^{n} (|0\rangle + e_k(2^k f) |1\rangle)$$

$$= QFT_n |2^n f\rangle$$

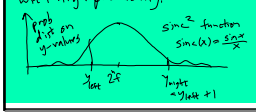
(assuming $2^n f$ is an integer (in $\mathbb{Z}_{2^n}$))

$$\xrightarrow{QFT_n^\dagger} |2^n f\rangle$$

measure: get $y_{n-1} \cdots y_0 = 2^n f$

multiply both sides by $\frac{2\pi}{2^n}$ to get θ.

If $2^n f$ is not an integer, then we get θ within roughly n bits of accuracy with high probability.



Shor's Algo for integer factorization (set-up)

Let N be an integer (composite). Find $x, y \in \mathbb{Z}_N$ such that $\underbrace{x^2 \equiv y^2 \pmod N}_{x^2 \equiv_N y^2}$ but $x \not\equiv_N \pm y$.

Suppose x, y as above.

Then $N \mid x^2 - y^2 = (x+y)(x-y)$ (divides)

but $N \nmid x+y$ (because $x \not\equiv_N -y$)

and $N \nmid x-y$ (because $x \not\equiv_N y$)

$N = p_1^{e_1} \cdots p_k^{e_k}$ prime factorization

$p_1^{e_1} \cdots p_k^{e_k} \mid (x+y)(x-y)$

$(x+y)(x-y) = N\ell$ $(\ell \in \mathbb{Z})$

$= p_1^{e_1} \cdots p_k^{e_k} \ell$

Neither $x+y$ nor $x-y$ includes all of $p_1^{e_1} \cdots p_k^{e_k}$

so $x+y$, $x-y$ both include nontrivial factors of N.

Compute $\gcd(N, x+y)$ (or $\gcd(N, x-y)$) both are nontrivial factors of N.

Repeat the process to get a complete factorization of N.

Order-finding: Given N,

Let $\mathbb{Z}_N^* := \{x \in \mathbb{Z}_N : \gcd(N, x) = 1\}$

Fact: For all $x \in \mathbb{Z}_N^*$ there exists a unique smallest positive $r \in \mathbb{Z}$ such that $x^r \equiv_N 1$

Ex: $N = 13$

$x = 2$

x	x^2	x^3	x^4	x^5
2	4	8	16	6

x^6	x^7	x^8	$x^9 \equiv_N 3$	x^{10}
12	11	9	5	10

x^{11}	x^{12}
7	1

$\text{ord}(x) = 12$

Shor's quantum algorithm finds $\text{ord}(x)$ with high probability

Claim: Given a way to find $\text{ord}(z)$ for any $z \in \mathbb{Z}_N^*$, this can be used to find x, y as above ($x^2 \equiv_N y^2$, $x \not\equiv_N \pm y$). [with high probability].