Discrete Fourier Transform (DFT)

$f: \{0,1,\dots,N-1\} \to \mathbb{C}$ → N complex numbers $(f_0,\dots,f_{N-1})$

$$\boxed{\tilde{f}_m = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} f_n \, e^{\frac{2\pi i}{N} nm}}$$ DFT

reverse form ←
$$\boxed{f_n = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} \tilde{f}_m \, e^{-\frac{2\pi i}{N} nm}}$$ reverse DFT

Let $U_{mn} = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N} nm}$ } U is $N \times N$ matrix

$\tilde{f}_m = \sum_n U_{mn} f_n$ $\tilde{f} = Uf$ (in matrix notation)

$f_n = \sum_m U^*_{mn} \tilde{f}_m = \sum_m (U^\dagger)_{nm} \tilde{f}_m \to f = U^\dagger \tilde{f}$

$f = U^\dagger \tilde{f} = \underline{U^\dagger U} f \to U^\dagger U = 1 \to U$ is unitary

Parseval's Rule:

$$\left.\sum_n |\tilde{f}_n|^2 = \sum_n |f_n|^2 \right\} \quad \|\tilde{f}\| = \|f\|$$

norm-preserving property

☆ Quantum Fourier Transform

Let $|0\rangle, |1\rangle, \dots, |N-1\rangle$ be an orthonormal basis (for an N-dimensional Hilbert space)

Define

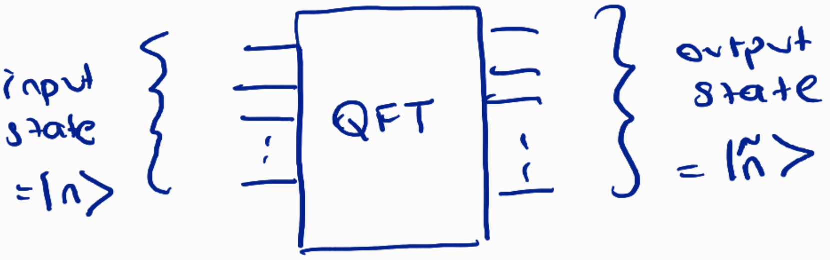
$$\boxed{|\tilde{m}\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{\frac{2\pi i}{N} nm} |n\rangle}$$ QFT

$\Rightarrow |\tilde{0}\rangle, |\tilde{1}\rangle, \dots, |\widetilde{N-1}\rangle$ is also an orthonormal basis

$\langle n|n'\rangle = \delta_{nn'} \quad \Rightarrow \quad \langle \tilde{m}|\tilde{m}'\rangle = \delta_{mm'}$

$$|n\rangle = \frac{1}{\sqrt{N}} \sum_{m=0}^{\infty} e^{-\frac{2\pi i}{N} nm} |m\rangle$$ Inverse

★ As part of Quantum Circuit



For $N=2$, Hadamard gate is a QFT.

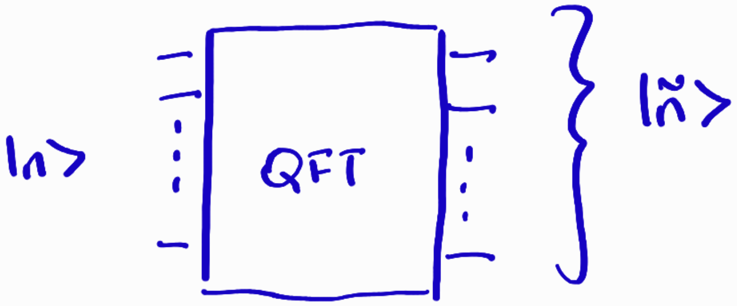
$$e^{-\frac{2\pi i}{N} nm} = e^{-\pi i nm} = (-)^{nm} = \pm 1$$

$$U = H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$|0\rangle \; — \boxed{H} \longrightarrow |\tilde{0}\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|1\rangle \; — \boxed{H} \longrightarrow |\tilde{1}\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

★ If $N = 2^n$ (dimension of Hilbert space of n qubits) then QFT can be realized quickly with $n \log n$ elementary steps.



$$(QFT)\,|n\rangle = |\tilde{n}\rangle = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} e^{\frac{2\pi i}{N} nm} |m\rangle$$

Period Finding Problem:

$$f(x) : X \longrightarrow \mathbb{N}$$

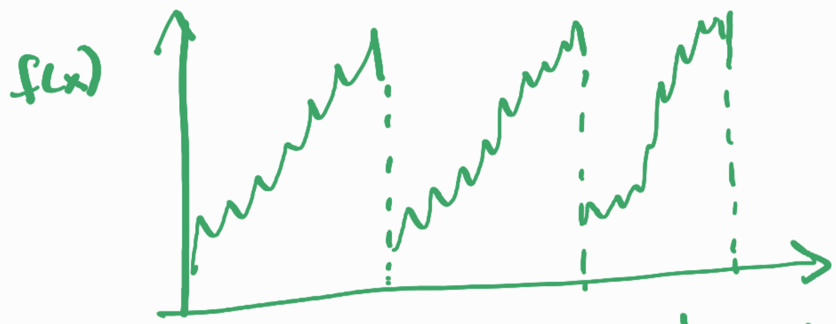
$$\{0, 1, \cdots, N-1\}$$

$f(x)$ is a periodic function. There is an integer T such that $f(x+T) = f(x)$

$x+T$ should be interpreted as modulo N.

There is a chip that computes $f(x)$.

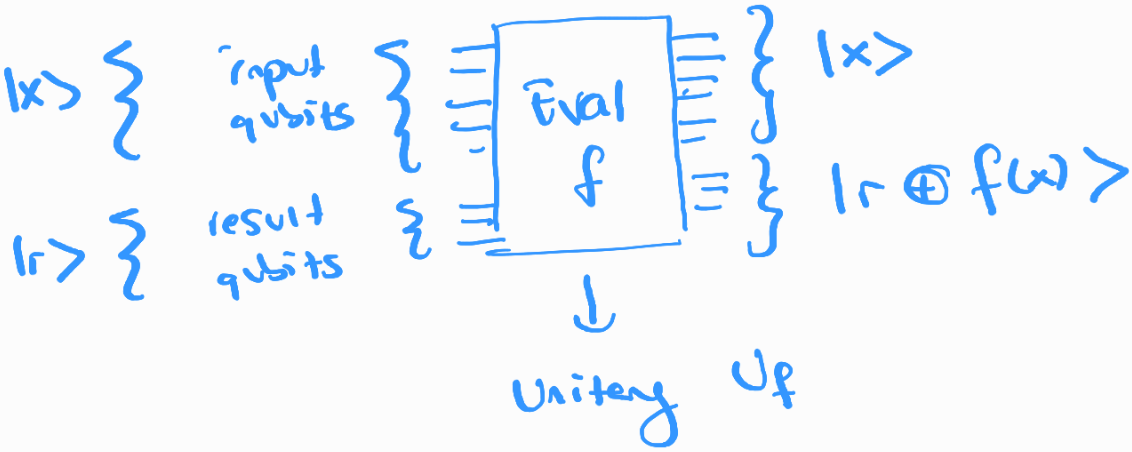
Find the period T by doing minimum possible number of use of the chip.



$$f(x) = f(x') \Leftrightarrow x - x' = (\text{integer})\,T$$

classical algorithm is long.

☆ Quantum Algorithm for Period Finding



$$U_f\,|x\rangle_I \otimes |r\rangle_R = |x\rangle_I \otimes |r \oplus f(x)\rangle_R$$

Step 1 • Prepare input qubits I in the superposition state

$$|\phi\rangle_{in} = \frac{1}{\sqrt{N}}\left(|0\rangle + |1\rangle + \cdots + |N-1\rangle\right)$$

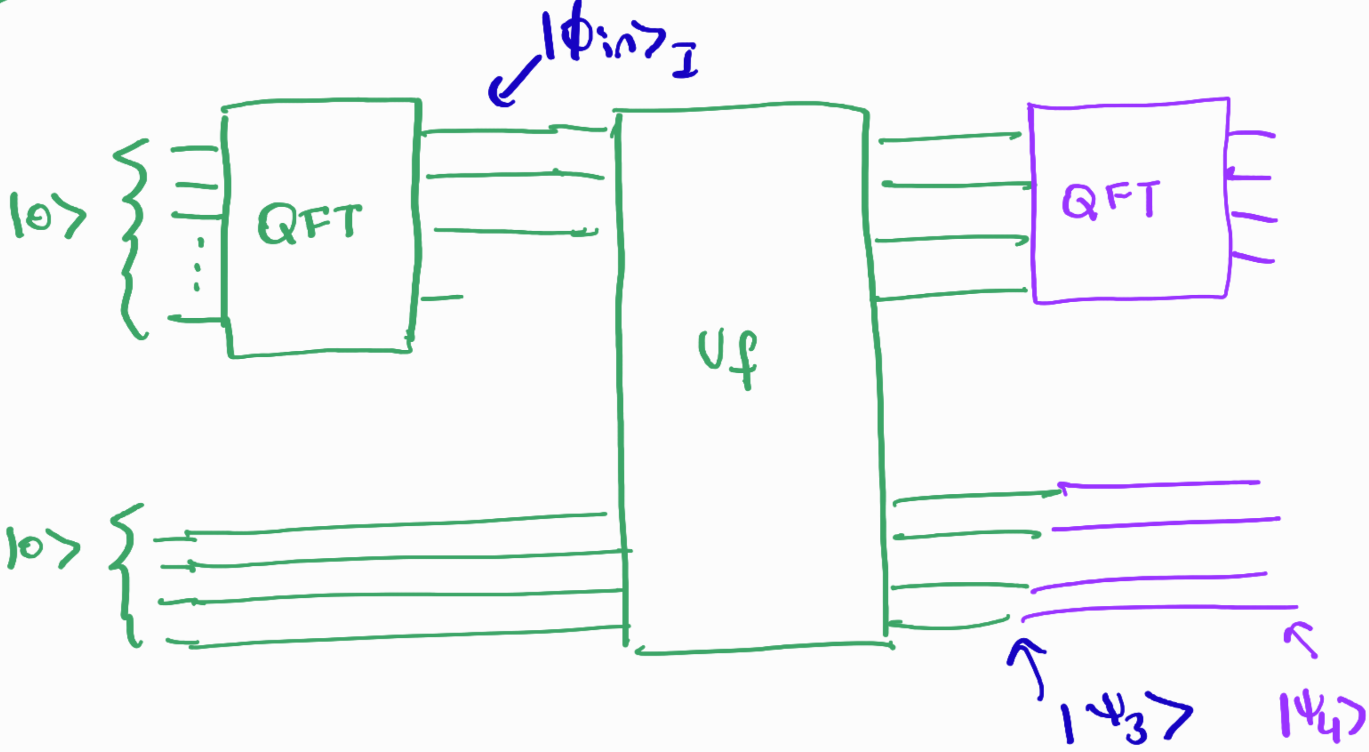
$$|\phi\rangle_{in} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle = (QFT)\,|0\rangle$$

or

$$= \left(H^{\otimes n}\right)|0\rangle \quad (\text{if } N = 2^n)$$

• Prepare R in $|0\rangle$ state

Step 2 Evaluate f(x) (once)



$$|\psi_3\rangle = U_f\,|\Phi_{in}\rangle_J \otimes |0\rangle_R$$

$$= U_f\,\frac{1}{\sqrt{N}}\sum_x |x\rangle_I \otimes |0\rangle_R = \frac{1}{\sqrt{N}}\sum_x |x\rangle_J \otimes |f(x)\rangle_R$$

Step 3 Apply QFT to Input Qubits I

$$|\psi_4\rangle = \frac{1}{\sqrt{N}}\sum_x (QFT)\,|x\rangle \otimes \underbrace{|f(x)\rangle_R}_{f(x)=f_\alpha}$$

$$= \frac{1}{N}\sum_{xy} e^{\frac{2\pi i}{N}xy}\,|y\rangle \otimes |f(x)\rangle_R$$

f(x) takes T different values (assumption)

$$f_0, f_1, \ldots, f_{T-1}, \underbrace{f_0}_{f(T)}, f_1, \ldots$$

$$|\psi_3\rangle = \frac{1}{\sqrt{N}} \sum_{\alpha} \left(|x_\alpha\rangle + |x_{\alpha+T}\rangle + |x_{\alpha+2T}\rangle + \dots \right) \otimes |f_\alpha\rangle_R$$

$$|\psi_4\rangle = \frac{1}{N} \sum_{\alpha} \left(\sum_{xy} e^{\frac{2\pi i}{N} xy} |y\rangle \right) \otimes |f_\alpha\rangle_R$$

$\boxed{x = x_\alpha + kT}$ where $k = 0, 1, 2, \dots, \frac{N}{T} - 1$

$$|\psi_4\rangle = \frac{1}{N} \sum_{\alpha} \left(\sum_{y} \sum_{k} e^{\frac{2\pi i}{N} (x_\alpha + kT) y} |y\rangle_I \right) \otimes |f_\alpha\rangle_R$$

$$\left(\sum_{y} e^{\frac{2\pi i}{N} x_\alpha y} |y\rangle \right) \left(\sum_{k}^{\frac{N}{T}-1} e^{\frac{2\pi i}{N} Tyk} \right)$$

if $\left(e^{\frac{2\pi i}{N} Ty} \neq 1 \right)$ then this term is zero.

if y is an integer multiple of N/T.

if $\left(e^{\frac{2\pi i}{N} Ty} = 1 \right)$ then this term gives $\frac{N}{T}$

$$|\psi_4\rangle = \frac{1}{\cancel{N}} \frac{\cancel{N}}{T} \sum_{\alpha} \left(\sum_{q} e^{\frac{2\pi i}{N} x_\alpha y} |y\rangle \right) \otimes |f_\alpha\rangle_R$$

$$\left(y = \frac{N}{T} q\right)$$

$$|\psi_4\rangle = \frac{1}{T} \sum_{\alpha, q} \left| y = \frac{N}{T} q \right\rangle \otimes |f_\alpha\rangle_R$$

Step 4 Now measure I and R seperately.

→ you get random $|f_\alpha\rangle$ useless info

You get y = an integer multiple of N/T

Step 5 Repeat this procedure m times.

You got values $\underbrace{y_1, y_2, \ldots, y_m}$ from I measurements

find the greatest common divisor (gcd) of these numbers.

$\frac{N}{T}$ divides all those numbers

$$\frac{N}{T} \,\Big|\, \gcd(y_1, \ldots, y_m)$$

repeat

→ We can then find $\frac{N}{T}$

→ We can compute $T = \frac{N^{\to\text{known}}}{(N/T)} = \frac{N}{\gcd(y_1, \ldots, y_m)}$