Quantum Fourier Transform (QFT) and its circuit implementation

Define QFT: a basis change.

$$|x\rangle \longrightarrow U^F |x\rangle$$

$$= \sum_y U^F_{xy} |y\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_y \omega^{xy} |y\rangle$$

$$\omega = e^{i\frac{2\pi}{N}}, \quad \omega^N = 1$$

here $|x\rangle$, $|y\rangle$ are n-bit quantum states,

$N = 2^n$

As an operator / gate:

$$\hat{U}^F = \frac{1}{\sqrt{N}} \sum_x \sum_y \omega^{xy} |y\rangle\langle x|$$

it is unitary

Note: previous in the Walsh trans, we have $(-1)^{x \cdot y}$, here ω^{xy}.

Example: single qubit, $n=1$, $N=2$, $\omega = -1$

$$\frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{xy} |y\rangle$$

$$|x=0\rangle \longrightarrow \frac{1}{\sqrt{2}} [|0\rangle + |1\rangle] = |+\rangle$$

$$|x=1\rangle \longrightarrow \frac{1}{\sqrt{2}} [|0\rangle - |1\rangle] = |-\rangle$$

$\therefore U^F$ is just $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Another example: $n=4$, $N=16$

($n=2$ will be left as home work)

Let $x = x_3 x_2 x_1 x_0$ in binary form, $x_i = 0, 1$

$y = y_3 y_2 y_1 y_0$

Consider $\frac{1}{\sqrt{16}} \sum_{y=0}^{15} w^{xy} |y\rangle$

$$= \frac{1}{4} \sum_{y_i=0,1} w^{x\left(\sum_{j=0}^{3} y_j 2^j\right)} |y_3 y_2 y_1 y_0\rangle$$

↓ sum in exponent

product $(w^{x y_3 8})(w^{x y_2 4})(w^{x y_1 2}) \cdot (w^{x y_0})$

$$= \bigotimes_i \left(w^{x y_i 2^i} |y_i\rangle \frac{1}{\sqrt{2}}\right)$$

It's a tensor product of 4 terms!

explicitly

$$= \left(\frac{|0\rangle + w^{8x}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + w^{4x}|1\rangle}{\sqrt{2}}\right)$$

$$\otimes \left(\frac{|0\rangle + w^{2x}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + w^{x}|1\rangle}{\sqrt{2}}\right)$$

$$= |\gamma_3\rangle \otimes |\gamma_2\rangle \otimes |\gamma_1\rangle \otimes \gamma_0$$

Now let's look at $|\gamma_i\rangle$, this will also tell us how to implement the QFT using quantum circuits.

① $w^{8x} = w^{(8x_3 + 4x_2 + 2x_1 + x_0)8}$

note $w^{16} = 1$, so $w^{64x_3} = 1$ etc

only x_0 survives

$= w^{8x_0}$ $\qquad w^8 = -1$

$= (-1)^{x_0}$

i.e. $|0\rangle \xrightarrow{x_0} |+\rangle$

$|1\rangle \longrightarrow |-\rangle$

$$|\gamma_3\rangle = \frac{|0\rangle + (-1)^{x_0}|1\rangle}{\sqrt{2}}$$

$$= H|x_0\rangle$$

note it only involves x_0.

② $w^{4x} = w^{(8x_3 + 4x_2 + 2x_1 + x_0)4}$

$= w^{8x_1 + 4x_0}$

$= (-1)^{x_1} \cdot (w^4)^{x_0}$ only depends on x_0, x_1

$\therefore |\gamma_2\rangle = P_{\frac{\pi}{4}} H |x_1\rangle$

where P_ϕ is the Controlled phase gate

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix},$$ with x_0 the controll b.t

i.e. $x_0 = 0$, nothing happens

$x_0 = 1$, $w^4 = e^{i\frac{\pi}{4}}$,

Similarly,

③ $w^{2x} = w^{8x_2 + 4x_1 + 2x_0}$

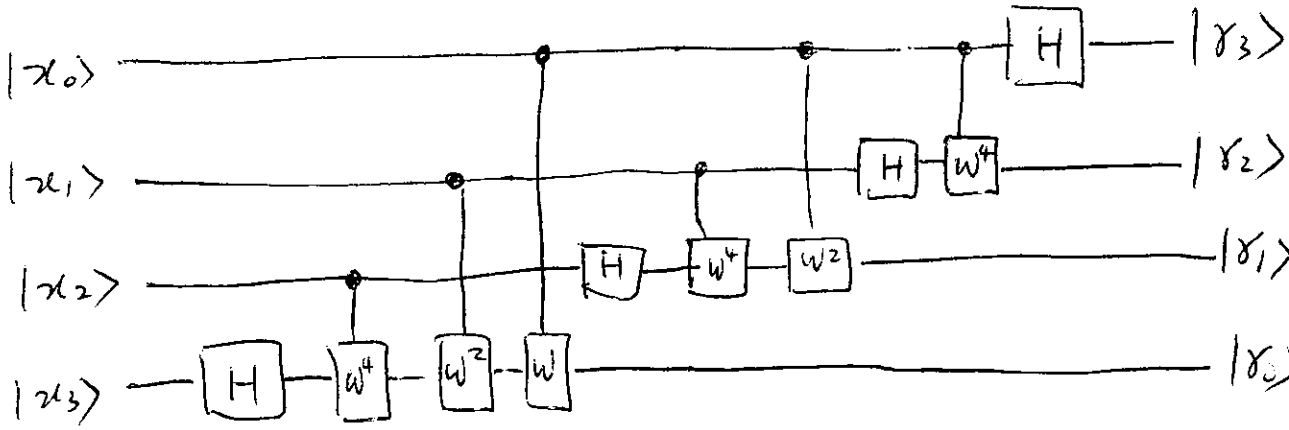
$= (-1)^{x_2} (w^4)^{x_1} (w^2)^{x_0}$

Again controlled phase gate $w^2 = e^{i\frac{\pi}{8}}$

④ $w^x = w^{8x_3 + 4x_2 + 2x_1 + x_0}$

$= (-1)^{x_3} (w^4)^{x_2} (w^2)^{x_1} (w)^{x_0}$

The quantum circuit for this



obviously, this circuit is recursive, and can be easily generalized to arbitrary n.

Note: in the output, the higher bits appear on top, we can rearrange

$|y_3\rangle$ $\quad\quad$ $|y_0\rangle$

$|y_2\rangle \longrightarrow |y_1\rangle$

$|y_1\rangle$ $\quad\quad$ $|y_2\rangle$

$|y_0\rangle$ $\quad\quad$ $|y_3\rangle$

by a series of SWAP gates.

Application of QFT: Period Finding

- Simon's problem: period finding over domain Z_2^n
- We'll focus on $Z_N = \{0, 1, 2, \cdots N-1\}$
- This forms the basis for Shor's algorithm of factorization (next lecture)

Period Finding Problem: $x \in Z_N$

A function $f(x)$ is periodic, i.e.

$\exists r$, such that $f(x) = f(x+r)$, for $\forall x \in Z_N$

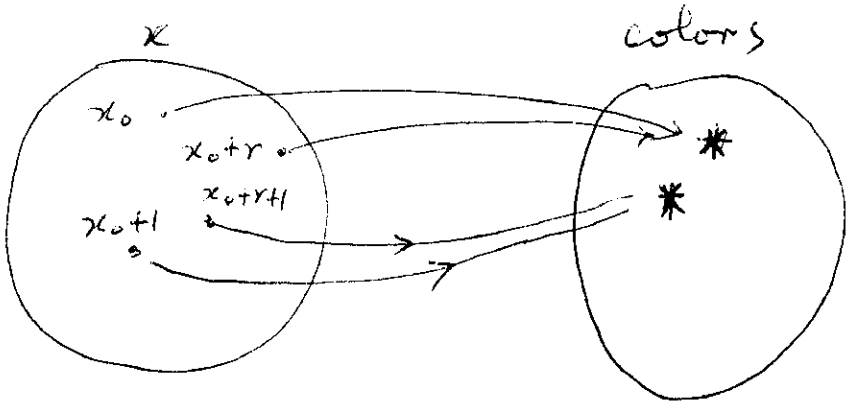
Find r.

Assume $f(x) \neq f(y)$, if x and y do not differ by multiples of r.
i.e. if $f(x) = f(y)$, $x = y + kr$, $k \in Z$.

To visualize the scenario, let the distinct function values to "colors", to form a set

$$\{C\} = \{R, G, B, \cdots\}$$

$$= \{f(x_0), f(x_0+1), f(x_0+2), \cdots f(x_0+r-1)\}$$

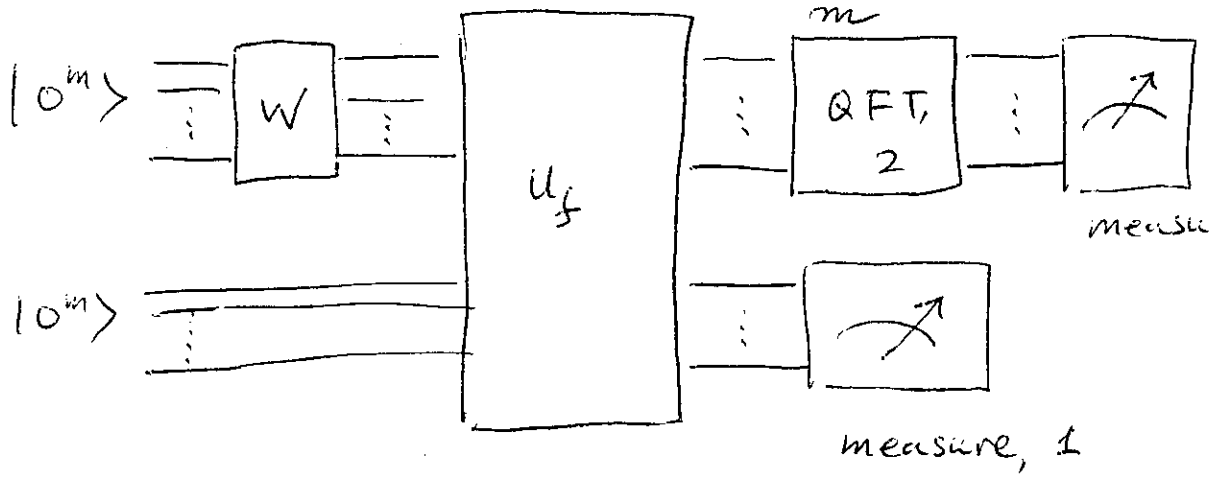


Note this problem can be solved efficiently on classical computers

The quantum algorithm:

Let $N = 2^m$

$|0^m\rangle = |0\rangle \otimes |0\rangle \cdots \otimes |0\rangle$ (m times)



① create superposition

$$|0^m\rangle \xrightarrow{W} \frac{1}{\sqrt{N}} \sum_{x \in Z_n} |x\rangle$$

and the bottom $|0^m\rangle$ are ancilla state

② Send the state into quantum oracle (function f)

$$\frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes |0^m\rangle \xrightarrow{U_f} \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes |f(x)\rangle$$

$0^m \oplus f(x)$

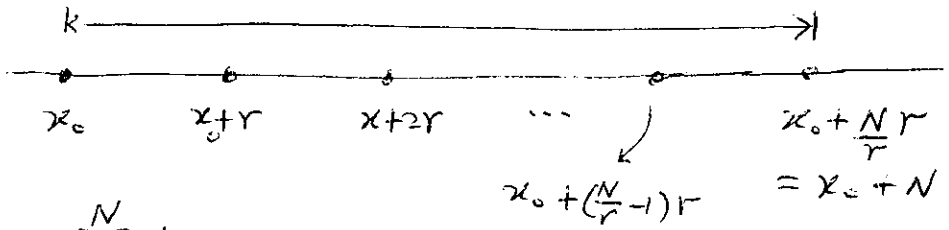
③ Measure the bottom m-bits, the result will be some random value of $f(x)$, i.e. Color,

Suppose we get C,

and let x_0 be the smallest value of x such that $f(x_0) = C$.

After the measurement, the state "collapses" to a superposition of all pre-image of c:

$$\left.\begin{aligned} f(x_0) &= c \\ f(x_0+r) &= c \\ &\vdots \\ f\left(x_0+\left(\tfrac{N}{r}-1\right)r\right) &= c \end{aligned}\right\} \quad \frac{N}{r} \text{ possibilities see below.}$$



$$\therefore \underbrace{\frac{1}{\sqrt{\frac{N}{r}}} \sum_{t=0}^{\frac{N}{r}-1} |x_0+tr\rangle}_{|\psi\rangle} \otimes |f(x_0)\rangle$$

$|f(x_0)\rangle = |c\rangle$, neglect this from now on, focus on the top m-bits, $|\psi\rangle$.

(4) Apply QFT to $|\psi\rangle$, we get

$$U^F |\psi\rangle$$

$$= \frac{1}{\sqrt{\frac{N}{r}}} \frac{1}{\sqrt{N}} \sum_y \sum_t \omega^{(x_0+tr)y} |y\rangle$$

recall $\omega = e^{i\frac{2\pi}{N}}$

(5) Measure the top m-bits, we'll get some value y. Now we show that the only possible values are multiples of $\frac{N}{r}$, i.e.

$$y = k \cdot \frac{N}{r}, \quad k \in \mathbb{Z}.$$

★ Suppose $y = k \cdot \frac{N}{r}$, simplify the sum

$$\omega^{x_0 y} \sum_t \omega^{t r y} |y\rangle$$

$$= \text{''} \sum_t \omega^{t k N} |y\rangle$$

Constructive interference ↓ $(\omega^N)^{tk} = (1)^{tk} = 1$

$$= \omega^{x_0 y} \cdot |y\rangle \cdot \frac{N}{r}$$

$$\therefore U^F |y\rangle = \sqrt{\frac{r}{N}} \frac{1}{\sqrt{N}} \sum_k \omega^{x_0 k \frac{N}{r}} |y = k\tfrac{N}{r}\rangle$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega^{x_0 k \frac{N}{r}} |y = k\tfrac{N}{r}\rangle$$

↑ phase factor

i.e. the probability of finding $y = k\frac{N}{r}$ is

$$\frac{1}{r}$$

i.e. with equal probability.

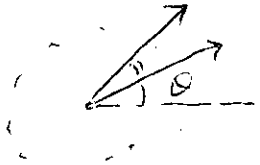
★ Suppose $y \neq kN/r$, then

$$\sum_t \omega^{t r y} = \sum_t e^{i\theta t} = 0$$

Assume $\frac{N}{r} \in \mathbb{Z}$.

$e^{i\frac{2\pi}{N} r y \cdot t}$

geometrically



vector sum to zero

algebraically,

$$\sum_{t=0}^{N/r-1} (\omega^{ry})^t$$

$$= \frac{1 - (\omega^{ry})^{N/r}}{1 - \omega^{ry}}$$

$$= \frac{1 - (\omega^N)^y}{''} = \frac{0}{''} = 0$$

∴ the measurement yields $y = k\frac{N}{r}$, for some random choice of $k = 0, 1, \cdots, r-1$.

(6) Repeat the whole procedure, for sufficient # of times; Compute the greatest common divisor (gcd) of $k\frac{N}{r}$, we get $\frac{N}{r}$. (neglect $k = 0$)

(7) From $\frac{N}{r}$, Since we know N, we can figure out r, the period.

Example: the simple case of $r = 2$,

Suppose $f(x) = x \bmod 2$,

$N = 8$, then

$$\{f(x)\} = \{f(0), f(1), \cdots f(7)\}$$
$$= \{0, 1, 0, 1, 0, 1, 0, 1\}$$

Input $\frac{1}{\sqrt{8}} \sum_x |x\rangle \otimes |0^8\rangle$

After U_f: $\frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle \otimes |x \bmod 2\rangle$

$\swarrow |f(x)\rangle$

measure 1: collapse to $|0\rangle$ or $|1\rangle$,

Suppose it's $|1\rangle$:

$$|4\rangle = \frac{1}{\sqrt{4}}(|1\rangle + |3\rangle + |5\rangle + |7\rangle)$$

After QFT:

$$\frac{1}{\sqrt{4}}\frac{1}{\sqrt{8}} \sum_{x=1,3,5,7} \sum_{y} \omega^{xy} |y\rangle \qquad \omega^4 = e^{i\pi} = -1$$

non zero only for $y = 0, 4$

$$= \frac{1}{4\sqrt{2}} [\, 4 \cdot 1 \cdot |0\rangle + 4(-1)|4\rangle \,]$$

$$= \frac{1}{\sqrt{2}} [\, |0\rangle - |4\rangle \,]$$

What about the case $|f(x)\rangle = |1\rangle$?

$$|4\rangle = \frac{1}{2}[\, |0\rangle + |2\rangle + |4\rangle + |6\rangle \,]$$

after QFT

$$\frac{1}{2} \cdot \frac{1}{\sqrt{8}} \sum_{x=0,2,4,6} \sum_{y} \omega^{xy} |y\rangle$$

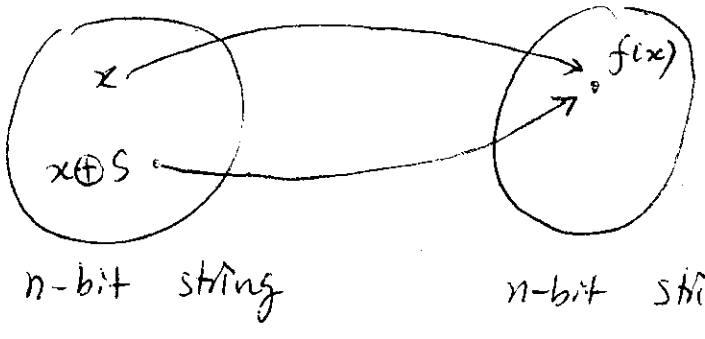
Again $y = 0, 4$

$$= \frac{1}{\sqrt{2}} [\, |0\rangle + |4\rangle \,]$$

in both cases, equal probability finding $|0\rangle$ and $|4\rangle = \frac{1}{2}$.

After a few measurement, we'll get $|4\rangle$, and deduce $\frac{N}{r} = 4$; since $N = 8$, $r = 2$.

Comments: **Simon's problem** is very similar



$f(x) = f(x \oplus S)$

Find secret string S.