QWORLD

QUANTUM FOURIER TRANSFORM

Jibran Rashid

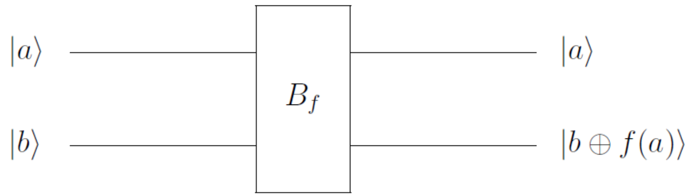
QSilver

Quantum Summer School 2021

August 4

Engineers, Physicists, Mathematicians and Computer Scientists ALL use Fourier Transforms

Classical Gates Via Unitaries



$$B_f : |a\rangle|b\rangle \longrightarrow |a\rangle|b \oplus f(a)\rangle$$

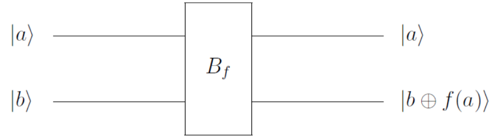
$$f : \{0,1\}^n \longrightarrow \{0,1\}^m$$

Can now accept superpositions as input!

x_1	x_2	$\text{AND}(x_1, x_2)$
0	0	0
0	1	0
1	0	0
1	1	1

Phase Kickback

Set $|b\rangle = |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$



$f : \{0,1\}^n \longrightarrow \{0,1\}$

Consider $B_f|a\rangle|-\rangle$

$$= B_f|a\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = \frac{1}{\sqrt{2}}\left(B_f|a\rangle|0\rangle - B_f|a\rangle|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(|a\rangle|0 \oplus f(0)\rangle - |a\rangle|1 \oplus f(a)\rangle\right)$$

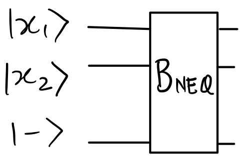
$$\left.\begin{array}{l} \text{if } f(a) = 0 \longrightarrow |0\rangle - |1\rangle \\ \phantom{\text{if }} f(a) = 1 \longrightarrow |1\rangle - |0\rangle \end{array}\right\} (-1)^{f(a)}\left(|0\rangle - |1\rangle\right)$$

$$= (-1)^{f(a)}|a\rangle \left(\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right)$$

$$B_f : |a\rangle|-\rangle \longrightarrow (-1)^{f(a)}|a\rangle|-\rangle$$

An Example

Consider $NEQ(x_1, x_2)$



x_1	x_2	$NEQ(x_1, x_2)$
0	0	0
0	1	1
1	0	1
1	1	0

$$B_{NEQ} : |x_1 x_2\rangle|-\rangle \longrightarrow (-1)^{f(x_1,x_2)}|x_1 x_2\rangle|-\rangle$$

$$B_{NEQ}|00\rangle = |00\rangle$$

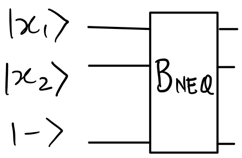
$$B_{NEQ}|01\rangle = -|01\rangle$$

$$B_{NEQ}|10\rangle = -|10\rangle$$

$$B_{NEQ}|11\rangle = |11\rangle$$

An Example

Consider $NEQ(x_1, x_2)$



x_1	x_2	$NEQ(x_1, x_2)$
0	0	0
0	1	1
1	0	1
1	1	0

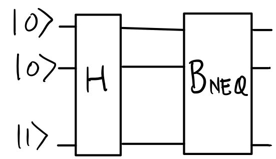
$$B_{NEQ} : |x_1 x_2\rangle|-\rangle \longrightarrow (-1)^{f(x_1,x_2)}|x_1 x_2\rangle|-\rangle$$

$$B_{NEQ}|00\rangle = |00\rangle$$

$$B_{NEQ}|01\rangle = -|01\rangle$$

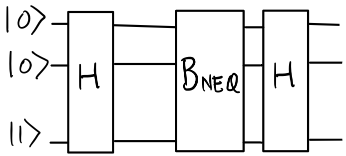
$$B_{NEQ}|10\rangle = -|10\rangle$$

$$B_{NEQ}|11\rangle = |11\rangle$$



$$\frac{1}{2}\left(|00\rangle - |01\rangle - |10\rangle + |11\rangle\right)$$

An Example



x_1	x_2	$NEQ(x_1, x_2)$
0	0	0
0	1	1
1	0	1
1	1	0

$$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$$

What if we apply Hadamard again

$$\frac{1}{2}(|++\rangle - |+-\rangle - |-+\rangle + |--\rangle) = |11\rangle$$

What is the amplitude of $|11\rangle \longrightarrow \frac{1}{2}\left(\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\left(-\frac{1}{\sqrt{2}}\right) - \left(-\frac{1}{\sqrt{2}}\right)\left(\frac{1}{\sqrt{2}}\right) + \left(-\frac{1}{\sqrt{2}}\right)\left(-\frac{1}{\sqrt{2}}\right)\right)$

$$= 1$$

An Example

$$H^{\otimes 3}\underbrace{|110\rangle}_{x} = |{-}{-}{+}\rangle = \frac{1}{\sqrt{8}}\big(|0\rangle - |1\rangle\big)\big(|0\rangle - |1\rangle\big)\big(|0\rangle + |1\rangle\big)$$

$$= \frac{1}{\sqrt{8}} \sum_{s\in\{0,1\}^3} \; ? \quad |s\rangle$$

What is the sign in front of $|s\rangle$?

$$|s\rangle = \begin{array}{c} 000 \\ 001 \\ 010 \\ \vdots \\ 111 \end{array}$$

An Example

$$H^{\otimes 3}\,|\underbrace{110}_{x}\rangle = |{-}{-}{+}\rangle = \frac{1}{\sqrt{8}}\underbrace{(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)}$$

$$= \frac{1}{\sqrt{8}}\sum_{s\in\{0,1\}^3} \; ? \; |s\rangle$$

What is the sign in front of $|s\rangle$?

Sign contribution from expansion

$(x = 110)$

$\|s\rangle =$	
000	$+++ = +$
001	$+++ = +$
010	$+-+ = -$
$\vdots$	
111	$--+ = +$

An Example

$$H^{\otimes 3} \underbrace{|110\rangle}_{x} = |{-}{-}{+}\rangle = \frac{1}{\sqrt{8}} \underbrace{(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)}$$

$$= \frac{1}{\sqrt{8}} \sum_{s \in \{0,1\}^3} \; ? \quad |s\rangle$$

What is the sign in front of $|s\rangle$?

In general if $s_i = 0$ sign is always $+$

if $s_i = 1$, sign is $\begin{cases} - & \text{if } x_i = 1 \\ + & \text{if } x_i = 0 \end{cases}$

$|s\rangle =$

000	$+++ = +$
001	$+++ = +$
010	$+-+ = -$
⋮	⋮
111	$--+ = +$

An Example

$$H^{\otimes 3}\,|\underbrace{110}_{x}\rangle = |--+\rangle = \frac{1}{\sqrt{8}}\underbrace{(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)}$$

$$= \frac{1}{\sqrt{8}}\sum_{s\in\{0,1\}^3} \; ? \; |s\rangle$$

So, sign in front of $|s\rangle$ is given by

$$\prod_{i:s_i=1}(-1)^{x_i} = (-1)^{\sum_{i:s_i=1} x_i \pmod 2}$$

$$= (-1)^{XOR_s(x)} = -1^{s\cdot x}$$

In general if $s_i = 0$ sign is always $+$

if $s_i = 1$, sign is $\begin{cases} - & \text{if } x_i = 1 \\ + & \text{if } x_i = 0 \end{cases}$

$XOR_s(x) \longrightarrow$ XOR of bits x_i where $s_i = 1$

An Example

So, $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}} \sum_{s\in\{0,1\}^n} (-1)^{XOR_s(x)} |s\rangle$ $\quad N = 2^n$

Note: $XOR_s(x) = \sum_{i:s_i=1} x_i \bmod 2 = \sum_{i=1}^{n} s_i x_i \bmod 2$

$= XOR_x(s)$

So we also have

$$H^{\otimes n}|s\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} (-1)^{XOR_s(x)} |x\rangle$$

$$\Rightarrow \quad H^{\otimes n}\left(\frac{1}{\sqrt{N}} \sum_{x} (-1)^{XOR_s(x)} |x\rangle\right) = |s\rangle$$

An Example

So, $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}} \sum_{s \in \{0,1\}^n} (-1)^{XOR_s(x)} |s\rangle$

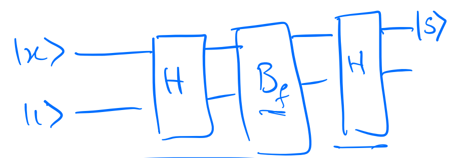
Note: $XOR_s(x) = \sum_{i: s_i = 1} x_i \mod 2 = \sum_{i=1}^{n} s_i x_i \mod 2$

$= XOR_x(s)$

So we also have

$H^{\otimes n}|s\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} (-1)^{XOR_s(x)} |x\rangle$

$\Rightarrow \quad H^{\otimes n}\left(\frac{1}{\sqrt{N}} \sum_x \underbrace{(-1)^{XOR_s(x)}}_{\text{Finding pattern}} |x\rangle\right) = \underline{|s\rangle}$



$\boxed{\underline{f}(x) = s \cdot x}$

$XOR_s(x)$

$NEQ(x_1, x_2) = XOR_s(x_1, x_2)$

for $s = 11$

$n = 5$

$s = \underline{1}\,\underline{1}\,0\,0\,\underline{1}$

$f(x) =$

Finding Patterns

① Make superposition of all inputs

$$H^{\otimes n} |0^n\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Finding Patterns

① Make superposition of all inputs

$$H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle$$

② Get answers in the amplitude

$$B_f \text{ gives } \frac{1}{\sqrt{N}}\sum_{x}(-1)^{f(x)}|x\rangle$$

Call $F(x) = (-1)^{f(x)}$

$F: \{0,1\}^n \longrightarrow \{\pm 1\}$

$0 \longrightarrow 1$

$1 \longrightarrow -1$

Loading up data in the vector

$$\frac{1}{\sqrt{N}}\begin{bmatrix} F(00\ldots0) \\ F(00\ldots1) \\ \vdots \\ F(11\ldots1) \end{bmatrix}$$

Finding Patterns

① Make superposition of all inputs

$$H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle$$

② Get answers in the amplitude

B_f gives $\frac{1}{\sqrt{N}}\sum_x (-1)^{f(x)}|x\rangle$

Call $F(x) = (-1)^{f(x)}$

$F: \{0,1\}^n \longrightarrow \{\pm 1\}$

$0 \longrightarrow 1$

$1 \longrightarrow -1$

③ Create interference

$H^{\otimes n}$ again

$$H^{\otimes n}\left(\frac{1}{\sqrt{N}}\sum_x F(x)|x\rangle\right)$$

$$= \frac{1}{\sqrt{N}}\sum_x F(x)\, H^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}}\sum_s \, ? \; |s\rangle$$

Loading up data in the vector

$$\frac{1}{\sqrt{N}}\begin{bmatrix} F(00..0) \\ F(00...1) \\ \vdots \\ F(11...1) \end{bmatrix}$$

Finding Patterns

① Make superposition of all inputs ② Get answers in the amplitude

③ Create interference

The Boolean Fourier Transform

$H^{\otimes n}$ does the job for us

if the pattern we are looking for is of an XOR function

Finding Patterns

① Make superposition of all inputs ② Get answers in the amplitude

③ Create interference

The Boolean Fourier Transform

$H^{\otimes n}$ does the job for us

if the pattern we are looking for is of an XOR function

Data vector of length N $\longrightarrow$ Fourier Transform $\longrightarrow$ s^{th} entry of length N vector identifies "strength" of s^{th} pattern in the data

(Can be <u>any</u> orthonormal basis for $\mathbb{C}^N$)

$\{|\chi_0\rangle, |\chi_1\rangle, \dots, |\chi_{N-1}\rangle\}$

(think of them as N pattern vectors)

Classically we have a physical vector of size N

Qtm we benefit by having $N = 2^n$

Finding Patterns

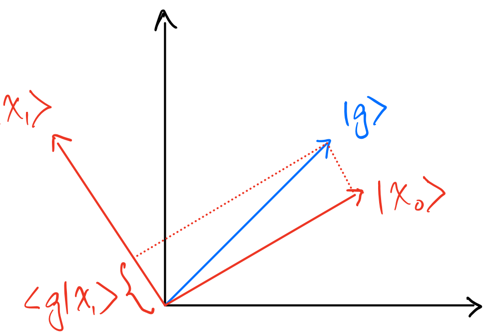
Def: For any $g: \{0,1\}^n \to \mathbb{C}$, $|g\rangle$ denotes $\frac{1}{\sqrt{N}} \sum_x g(x)|x\rangle$

$|g\rangle$ is a qtm state iff

$$\frac{1}{N} \sum_x |g(x)|^2 = 1$$

"Strength of pattern" in $|g\rangle$ given by coefficients of $|g\rangle$ when represented in $|\chi_s\rangle$ basis.

"Strength of $|\chi_s\rangle$": $\langle \chi_s | g\rangle$



Boolean Fourier Transform

Decompose $g : \{0,1\}^n \longrightarrow \mathbb{C}$ into basis of XOR functions

$$\chi_s : \{0,1\}^n \longrightarrow \{\pm 1\}$$

$$x \longmapsto (-1)^{XOR_s(x)}, \quad s \in \{0,1\}^n \qquad (-1)^{s \cdot x}$$

Build χ for $n=1$, $N=2$

$$XOR_s(x) = \sum_{s_i=1} x_i \bmod 2$$

$$\begin{array}{cc} & \chi_{s=0} \qquad\qquad \chi_{s=1} \\ |x\rangle \begin{cases} |0\rangle \\ |1\rangle \end{cases} & \frac{1}{\sqrt{2}}\begin{pmatrix} +1 \\ +1 \end{pmatrix}, \ \frac{1}{\sqrt{2}}\begin{pmatrix} +1 \\ -1 \end{pmatrix} \end{array}$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Boolean Fourier Transform

Decompose $g:\{0,1\}^n \longrightarrow \mathbb{C}$ into basis of XOR functions

$$\chi_s : \{0,1\}^n \longrightarrow \{\pm 1\}$$
$$x \longmapsto (-1)^{XOR_s(x)} \quad , s \in \{0,1\}^n \qquad (-1)^{s.x}$$

Build χ for $n=1$, $N=2$

$$XOR_s(x) = \sum_{s_i=1} x_i \bmod 2$$

$$\begin{array}{c|cc} & \chi_{s=0} & \chi_{s=1} \\ |x\rangle \left\{ \begin{array}{c} |0\rangle \\ |1\rangle \end{array} \right. & \frac{1}{\sqrt{2}}\begin{pmatrix} +1 \\ +1 \end{pmatrix} & \frac{1}{\sqrt{2}}\begin{pmatrix} +1 \\ -1 \end{pmatrix} \end{array}$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Similarly, for $n=2$

$$\begin{array}{c|c} {}_{|x\rangle}\backslash^{|s\rangle} & \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \end{array}$$

Finding Patterns

Property of XOR pattern functions $\chi_s(x) = (-1)^{s \cdot x}$

$$\chi_s(x+y) = \chi_s(x)\,\chi_s(y)$$

$$(-1)^{s\cdot(x+y)} = (-1)^{s\cdot x + s\cdot y} = (-1)^{s\cdot x}(-1)^{s\cdot y} = \chi_s(x)\,\chi_s(y)$$

$\chi_s : \mathbb{Z}_N \longrightarrow \mathbb{C}$ $\qquad \mathbb{Z}_N = \{0, 1, \ldots, N-1\}$

i) $\chi_s(x+0) = \chi_s(x) \cdot \chi_s(0)$

$\quad \chi_s(x) = \chi_s(x) \cdot \chi_s(0) \implies \underline{\chi_s(0) = 1 \ \forall s}$

ii) $\chi_s(\underbrace{x + x + x \ldots x}_{N \text{ times}}) = \chi_s(x) \cdot \chi_s(x) \cdots \chi_s(x) = \chi_s(x)^N$

$\quad \chi_s(\underline{Nx \bmod N}) = \chi_s(0) = \boxed{\chi_s(x)^N = 1} \longrightarrow$ N roots of unity

$$\chi_s(x) = e^{\frac{2\pi i}{N} s x}, \quad s, x \in \{0, 1, \ldots, N-1\}$$

Finding Patterns

Fourier Transform over $\mathbb{Z}_N$ (integers mod N)

Decomposes $g: \mathbb{Z}_N \longrightarrow \mathbb{C}$ into

$\chi_0, \chi_1, \ldots, \chi_{N-1}$, where

$\chi_s(x) = \omega_N^{sx}$ → product (mod N)

s → int, x → mod N

ω_N → primitive N^{th} root of unity

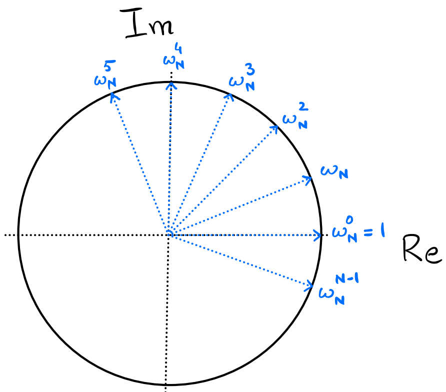
$e^{2\pi i/N}$

$s, x \in \{0, 1, \ldots, N-1\}$

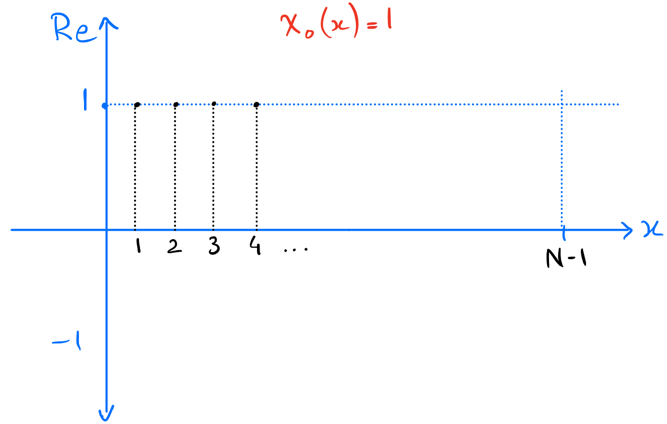
Possible to generalize to other groups G, beyond $\mathbb{F}_2^n$, $\mathbb{Z}_N$.

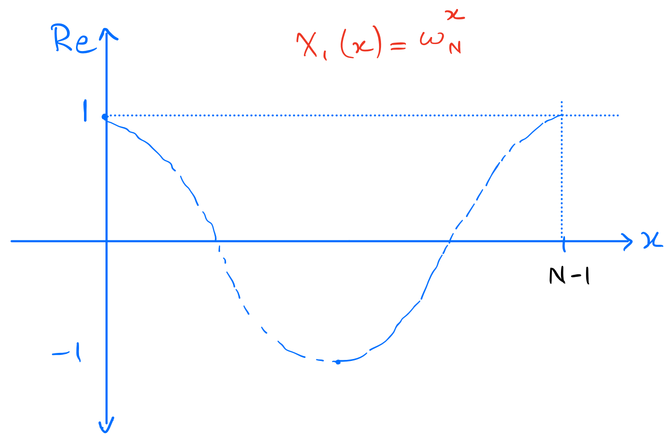
Finding Patterns

$n = 4, \quad N = 16$

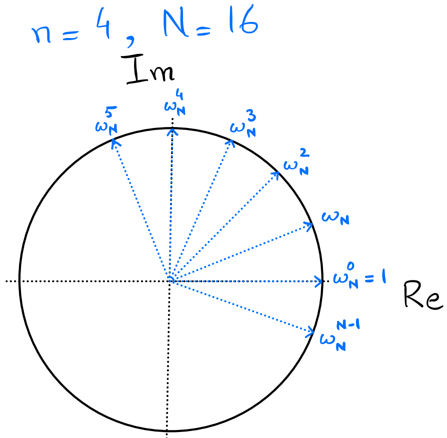


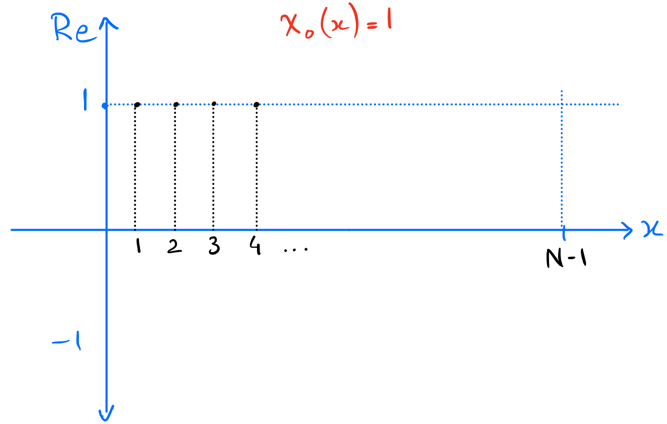
$$\omega_N = e^{2\pi i/N}$$
$$= \cos \frac{2\pi}{N} + i \sin \frac{2\pi}{N}$$

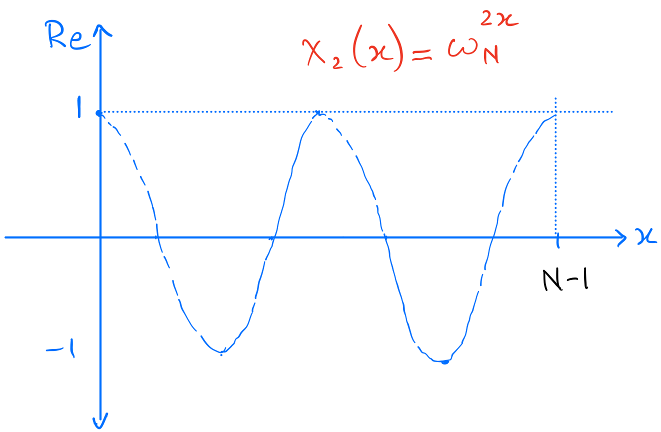


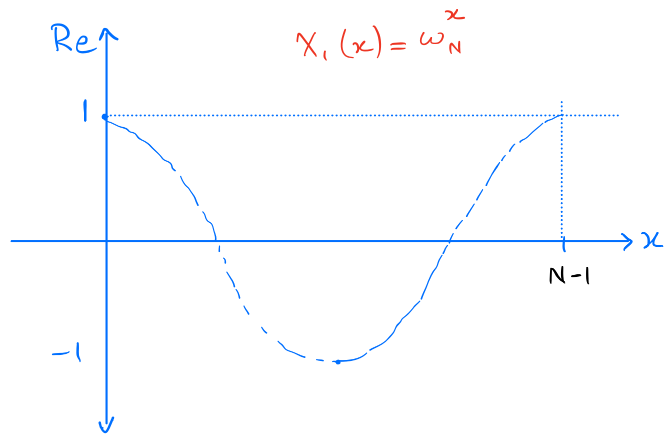


Finding Patterns









The Quantum Fourier Transform

Facts

1. $\chi_0(x) = 1 \quad \forall x$

2. $\chi_s(x)^* = \left(\omega_N^{sx}\right)^*$
$= \omega_N^{-sx}$

3. $\chi_s(x) = \omega_N^{sx}$
$= \chi_x(s)$

4. $|\chi_0\rangle, |\chi_1\rangle, \ldots, |\chi_{N-1}\rangle$ are orthonormal

5. Can you determine a nice matrix representation for $(\mathrm{QFT}_N)^2$?

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{N-1} \\ 1 & w^2 & w^4 & \cdots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \cdots & w^{(N-1)^2} \end{pmatrix}$$

$$\mathrm{QFT}_N\,|j\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi i jk/N}\,|k\rangle$$

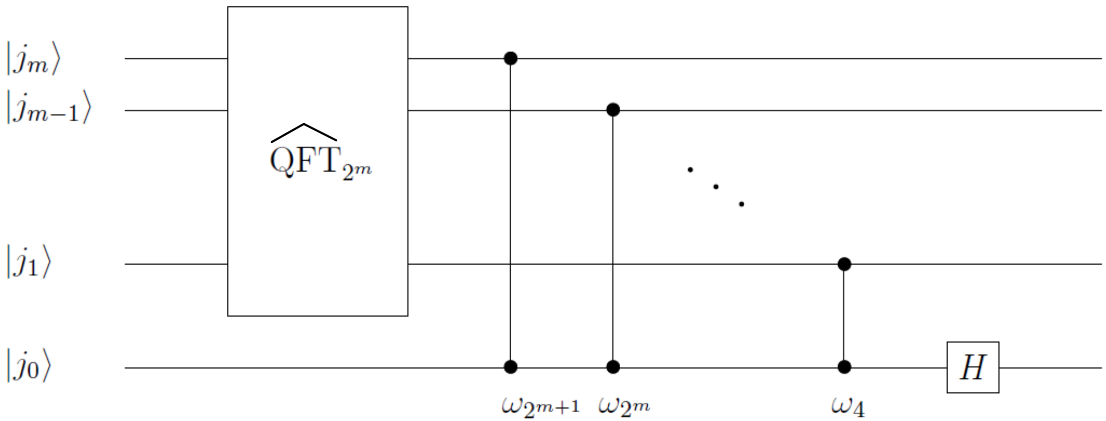
QFT Exampe Matrices

$$F_2 = H = \frac{1}{\sqrt{2}}\begin{bmatrix} \omega^0 & \omega^0 \\ \omega^0 & \omega^1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \omega = e^{2\pi i/2}$$

$$F_4 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^0 & \omega^2 \\ 1 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}, \quad \omega = e^{2\pi i/4}$$

$$F_8 = \frac{1}{2\sqrt{2}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}, \quad \omega = e^{2\pi i/8}$$

QFT Circuit



Note output qubits are in reverse order

Above circuit has $O(m^2)$ gates

Reference http://www.cs.cmu.edu/~odonnell/quantum18/ (Lectures 11 to 14)