QWORLD

QUANTUM FOURIER TRANSFORM

Jibran Rashid

QSilver

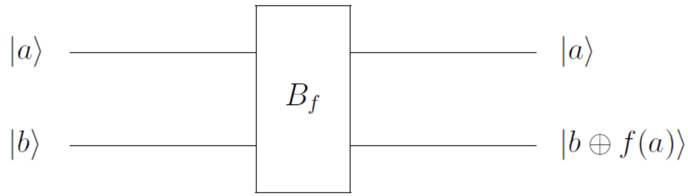
Global Quantum Programming Workshop

May 19, 2021

An engineer, a physicist and a mathematician…

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

Classical Gates Via Unitaries



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

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

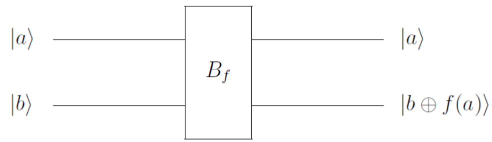
Can now accept superpositions as input!

Phase Kickback

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

Recall

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



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

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

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

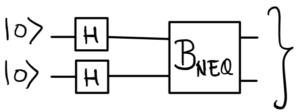
$$\text{if} \quad \left.\begin{array}{l} f(a)=0 \longrightarrow |0\rangle - |1\rangle \\ f(a)=1 \longrightarrow |1\rangle - |0\rangle \end{array}\right\} (-1)^{f(a)}\left(|0\rangle - |1\rangle\right)$$

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

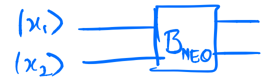
$$B_f : |a\rangle|-\rangle \longrightarrow \underline{(-1)^{f(a)}|a\rangle}\underbrace{|-\rangle}_{\text{don't need to worry about it}}$$

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



$$\underline{|00\rangle} \longrightarrow \underline{B_{NEQ}|00\rangle}$$

$$(-1)^{\overline{BNEQ(00)}}|00\rangle$$

$$|00\rangle$$

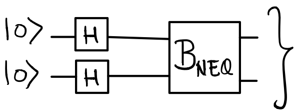
$$|01\rangle \longrightarrow -|01\rangle$$

$$|10\rangle \longrightarrow -|10\rangle$$

$$|11\rangle \longrightarrow |11\rangle$$

An Example

Consider $NEQ(x_1, x_2)$



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

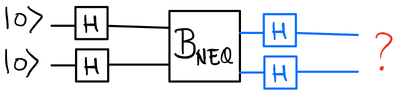
What if we apply $H^{\otimes 2}$ again

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

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



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

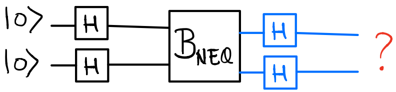
What if we apply $H^{\otimes 2}$ again

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

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



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

What if we apply $H^{\otimes 2}$ again

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

Amplitude on $|11\rangle$ is $\frac{1}{2}\left(\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\left(-\frac{1}{\sqrt{2}}\right) - \left(-\frac{1}{\sqrt{2}}\right)\frac{1}{\sqrt{2}} + -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right) = 1$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = \frac{1}{2}\left(\cdots \quad \cdots \quad |11\rangle\right)$$

Finding Patterns

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

③ Create interference

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

② B_f gives $\frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle$

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

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

$0 \rightarrow 1$

$1 \rightarrow -1$

③ $H^{\otimes n}$ again

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

$$= \frac{1}{\sqrt{N}} \sum_x F(x) H^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}} \sum_s \underbrace{?}_{\text{Fourier coefficients}} |s\rangle$$

Loading up data in the vector

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

An Example

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

$$= \frac{1}{\sqrt{8}} \sum_{s \in \{0,1\}^3} \underset{\to (-1)^{s \cdot x}}{\underline{?}} \; |s\rangle$$

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

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

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

So, sign on $|s\rangle$ is

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

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

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

An Example

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

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

$= XOR_x(s)$

So we also have

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

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

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: $XOR_s(x) = \sum_{i:s_i=1} x_i \mod 2 = \sum_{i=1}^{n} s_i x_i \mod 2$ $\longrightarrow$ this is symmetric

$= XOR_x(s)$

So we also have

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

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

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

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

Finding Pattern

$NEQ(x_1,x_2) = XOR_s(x_1,x_2)$ for $s = 11$

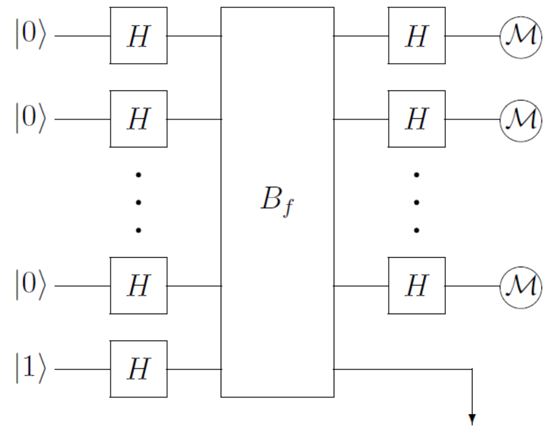
Bernstein-Vazirani Problem

Suppose a function $f : \{0,1\}^n \to \{0,1\}$ is given as a black-box in the usual way, i.e., as a unitary transformation B_f that acts as follows for all $x \in \{0,1\}^n$ and $y \in \{0,1\}$:

$$B_f : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle .$$

This time you are promised that there exists some string $s \in \{0,1\}^n$ such that $f(x) = s \cdot x$ for all $x \in \{0,1\}^n$, where

$$s \cdot x = \sum_{i=1}^{n} s_i x_i \pmod 2.$$



$$\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$= \left(\frac{1}{\sqrt{2^n}} \sum_x (-1)^{s \cdot x} |x\rangle \right) |-\rangle$$

$$\xrightarrow{H^{\otimes n} \otimes \mathbb{1}} |s\rangle |-\rangle$$

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 ⟶ Fourier Transform ⟶ s^{th} entry of length N vector identifies "strength" of s^{th} pattern in the data

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

$\{ |x_0\rangle, |x_1\rangle, \ldots, |x_{N-1}\rangle \}$

(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

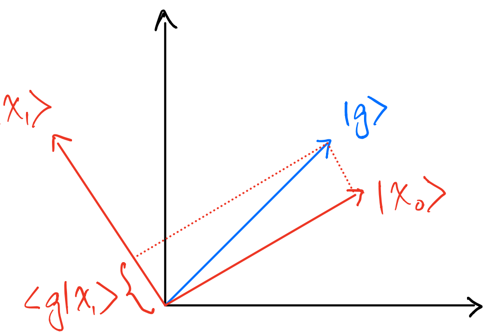
Def: For any $g: \{0,1\}^n \in \mathbb{C}$, $|g\rangle$ denotes $\frac{1}{\sqrt{N}} \sum_x g(x)|x\rangle$

$|g\rangle$ 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

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

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

Build χ for $n=1$, $N=2$

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

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

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

Similarly, $H^{\otimes 2}$

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

Finding Patterns

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

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

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

$$\chi_s : \mathbb{Z}_N \longrightarrow \mathbb{C}$$

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

$\chi_s(x) = \chi_s(x)\cdot\chi_s(0) \Longrightarrow \boxed{\chi_s(0) = 1}\ \forall s$, $\chi_s(x) = 0$ X

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

$\chi_s(Nx \bmod N) = \chi_s(0) = \chi_s(x)^N = 1 \longrightarrow$ N roots of unity

So, $\chi_s(x) = e^{\frac{2\pi i}{N} s x}$

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

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)

ints mod N

→ ω_N → primitive N^{th} root of unity

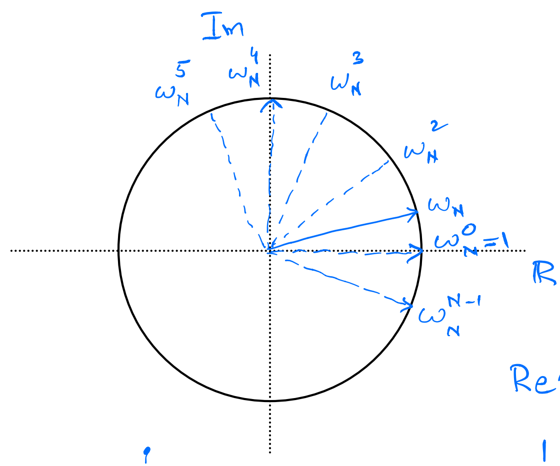
$e^{2\pi i/N}$

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

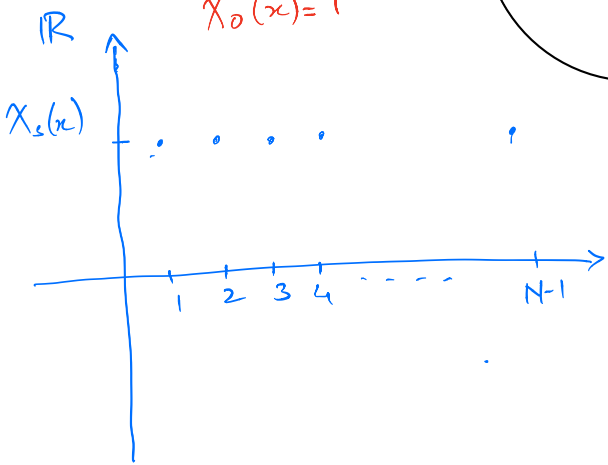
Finding Patterns

$N = 16$

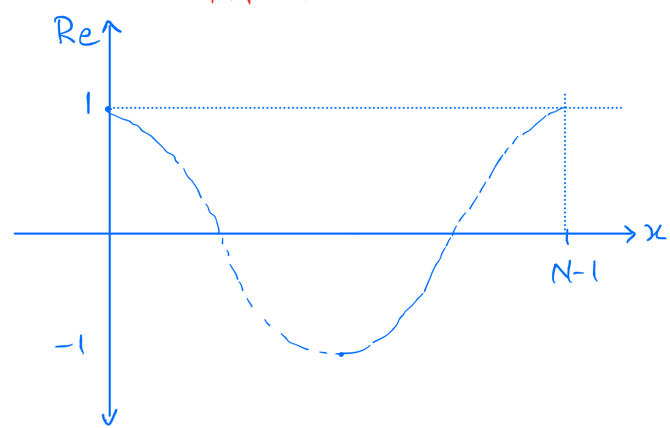
$$\omega_N = e^{\frac{2\pi i}{N}} = \cos\frac{2\pi}{N} + i\sin\frac{2\pi}{N}$$



$\chi_0(x) = 1$



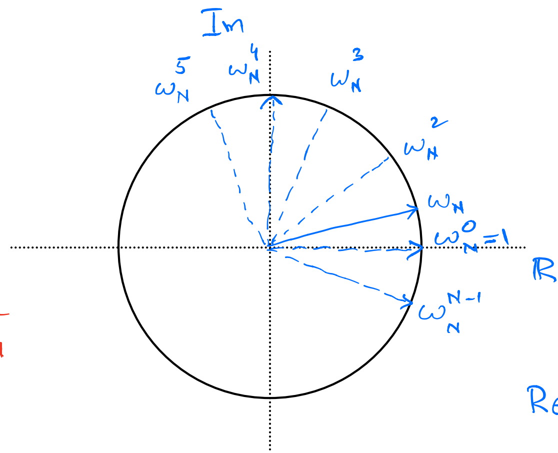
$\chi_1(x) = \omega_N^x$



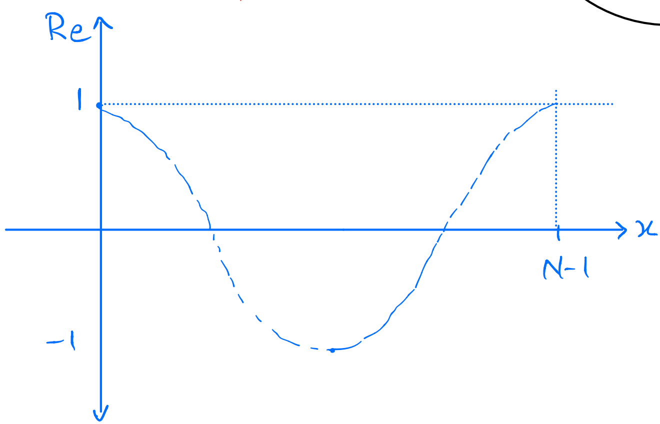
Finding Patterns

$N = 16$

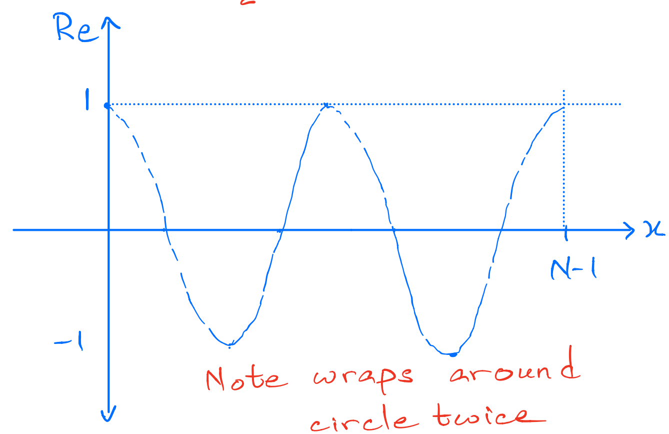
$$\omega_N = e^{\frac{2\pi i}{N}}$$
$$= \cos\frac{2\pi}{N} + i\sin\frac{2\pi}{N}$$



$\chi_1(x) = \omega_N^{x}$



$\chi_2(x) = \omega_N^{2x}$



Note wraps around circle twice

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

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

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

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

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

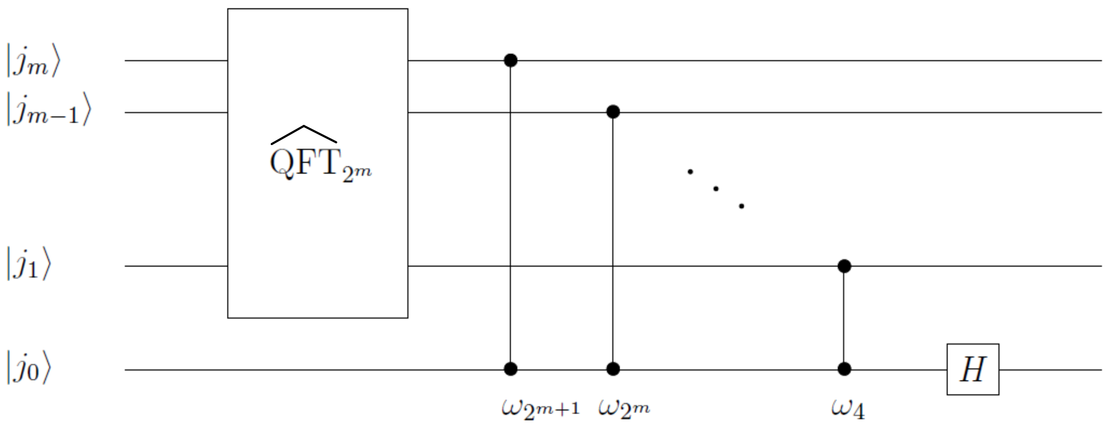
QFT Exampe Matrices

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

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

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

QFT Circuit



Note output qubits are in reverse order

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