10/5/10 QIC 710 Lecture 7 Quantum Fourier transform

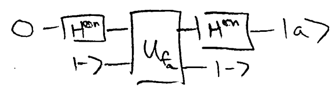
Announcements: Laura Mancinska TA W 1-2pm MC5136A , Dave Bacon

Last lectures:

Deutsch-Josza, Bernstein-Vazirani, Simon

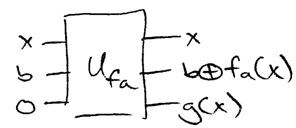
- quantum parallelism: key in quantum algorithm design
  provided U_f leaves no garbage, can apply f to multiple inputs in superposition, and later interfere those paths to extract an answer

eg. in B-V



$f_a(x) = x \cdot a \mod 2$

what if U_{f_a} left garbage?



by principle of deferred measurement, might as well measure the garbage $\Rightarrow$ paths no longer interfere

-need to erase extra information

- Hadamard transform to detect linear structure in $\mathbb{Z}_2^n$

$$\sum_x (-1)^{x \cdot a} |x\rangle \overset{H^{\otimes n}}{\longleftrightarrow} |a\rangle$$

$$|a\rangle + |b\rangle \overset{H^{\otimes n}}{\longleftrightarrow} \sum_{x:\, x\cdot a = x \cdot b} (-1)^{x \cdot a} |x\rangle$$

ie. $x \cdot (a+b) = 0$

$$U_{+y} H^{\otimes n} |a\rangle = (-1)^{y \cdot a} H^{\otimes n} |a\rangle \quad \text{eigenvectors } \forall a, \forall y$$

Today: Fourier transform & Quantum Fourier transform, QFT mod 2^n.

Fourier transform.

$F_N : \mathbb{C}^N \to \mathbb{C}^N$

$F_N(x) = y$, $y_k = \sum_{j=0}^{N-1} e^{\frac{2\pi i}{N} jk} x_j / \sqrt{N}$

$$\text{ie.} \quad F_N(x) = \begin{array}{c c} & j \\ k & \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \\ 1 & \omega^3 & \omega^6 & \cdots & \\ 1 & & \omega_N^{jk} & & \\ 1 & & & & \end{pmatrix} \end{array} \begin{pmatrix} x_0 \\ \vdots \\ \vdots \\ x_{N-1} \end{pmatrix}$$

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

Observe: This matrix is unitary!

$$\langle i | F_N^\dagger F_N | j \rangle = \sum_k \langle i | F_N^\dagger | k \rangle \langle k | F_N | j \rangle / N$$
$$= \sum_k \omega_N^{-ik} \cdot \omega_N^{kj} / N = \sum_k \omega_N^{k(j-i)} / N$$
$$= \begin{cases} 1 & \text{if } i = j \\ 1 + \omega^{j-i} + \omega^{2(j-i)} + \cdots + \omega^{(N-1)(j-i)} = 0, & \text{o.w.} \end{cases}$$

Classically: FFT $O(N \log N)$

Quantumly: $O((\log N)^2)$ exact

$O(\log N \log \frac{1}{\varepsilon})$ for precision ε.

- note the difference:

classically, the input & output are lists of complex numbers

quantumly, they are the amplitudes of a quantum state

$$\sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{QFT} \sum_{k=0}^{N-1} y_k |k\rangle$$

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{kj} |k\rangle$$

$N = 2^n$: $|j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega_{2^n}^{kj} |k\rangle$

$$\propto \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \omega_{2^n}^{j(2^{n-1}k_1 + 2^{n-2}k_2 + \cdots + 2^0 k_n)} |k_1 k_2 \cdots k_n\rangle$$

$$= \sum_{k_1 \cdots k_n} \omega_2^{jk_1} \omega_4^{jk_2} \cdots \omega_N^{jk_n} |k_1 \cdots k_n\rangle$$

$$= \bigotimes_{\ell=1}^{n} \left(\sum_{k_\ell=0}^{1} \omega_{2^\ell}^{jk_\ell} |k_\ell\rangle \right) = \bigotimes_{\ell=1}^{n} \left(|0\rangle + \omega_{2^\ell}^{j} |1\rangle \right)$$

$\omega_{2^\ell}^{j} = e^{2\pi i \cdot \frac{j}{2^\ell}}$

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n$$
$$2^{-\ell} j = j_1 2^{n-1-\ell} + j_2 2^{n-2-\ell} + \cdots + j_n 2^{-\ell}$$
$$2\pi 2^{-\ell} j = 2\pi (j_{n-\ell+1} 2^{-1} + j_{n-\ell+2} 2^{-2} + \cdots + j_n 2^{-\ell}) \mod 2\pi$$
$$= 2\pi \cdot (0.j_{n-\ell+1} \cdots j_n)$$ since integer multiples of 2π drop

Properties of the Fourier transform:

1. $F_N|0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ F.T. picks out symmetries

2. for $T_a = \sum_x |x+a\rangle\langle x|$ shifts only change the phases

$$|\psi\rangle = \sum_x \alpha_x |x\rangle$$
$$T_a|\psi\rangle = \sum_x \alpha_x |x+a\rangle = \sum_x \alpha_{x-a}|x\rangle$$
$$\langle y|F_N T_a|\psi\rangle = \frac{1}{\sqrt{N}}\sum_x \alpha_x \omega^{y(x+a)} = \omega^{ay}\langle y|F_N|\psi\rangle$$

phase shifts $\to$ translations $P_a = \sum_x \omega^{ax}|x\rangle\langle x|$
$$\langle y|F_N P_a|\psi\rangle = \frac{1}{\sqrt{N}}\sum_x \alpha_x \omega^{(y+a)x} = \langle y+a|F_N|\psi\rangle$$
$\Rightarrow$ $T_{-a}F_N = F_N P_a$

3. Letting $|f\rangle = \sum_x f(x)|x\rangle$
$$F_N|\cos(\tfrac{2\pi}{n}k)\rangle \propto |k\rangle + |-k\rangle$$
$$F_N|\text{Gaussian}(\sigma)\rangle \approx |\text{Gaussian}(\sim\tfrac{1}{\sigma})\rangle$$

4. If $N = l\cdot m$, periodic pulses $\to$ periodic pulses (with inverse period)
$$\frac{1}{\sqrt{l}} F_N \sum_{j=0}^{l-1}|m\cdot j\rangle = \frac{1}{\sqrt{m}}\sum_{j=0}^{m-1}|l\cdot j\rangle$$

why? $\langle k|\frac{1}{\sqrt{l}}F_N\sum_j|mj\rangle = \frac{1}{\sqrt{lN}}\sum_j \omega^{kmj} = \ldots$

5. convolution

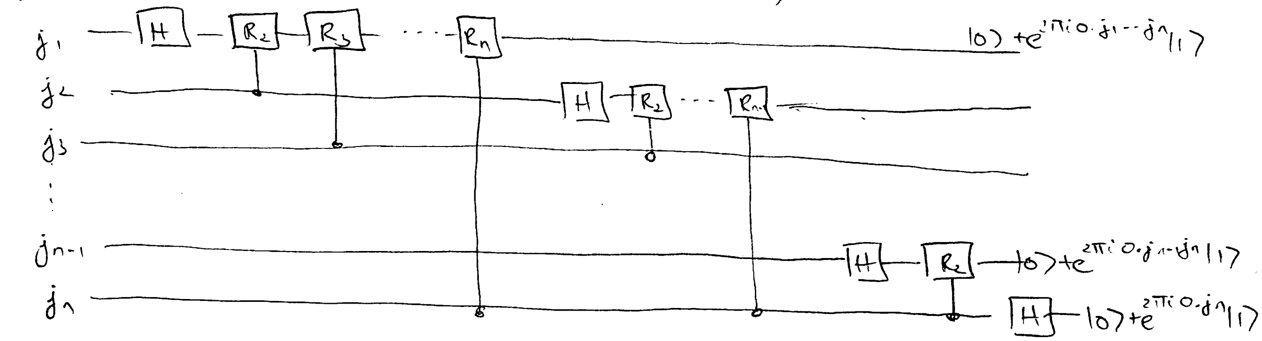
Let $(f*g)(x) = \sum_y f(y)g(x-y)$
$$\langle z|F_N|f*g\rangle = \frac{1}{\sqrt{N}}\sum_{xy}\omega^{xz}f(y)g(x-y)$$
$$= \frac{1}{\sqrt{N}}\sum_y \omega^{yz}f(y)\sum_x \omega^{(x-y)z}g(x-y)$$
$$= \frac{1}{\sqrt{N}}\Big(\sum_y \omega^{yz}f(y)\Big)\Big(\sum_x \omega^{xz}g(x)\Big) = \sqrt{N}\langle z|F_N|f\rangle\langle z|F_N|g\rangle$$

convolution $\leftrightarrow$ multiplication

(computationally much cheaper than naive convolution)
$\Theta(n\log n)$ $\Theta(n^2)$

- less useful quantumly than classically

$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$



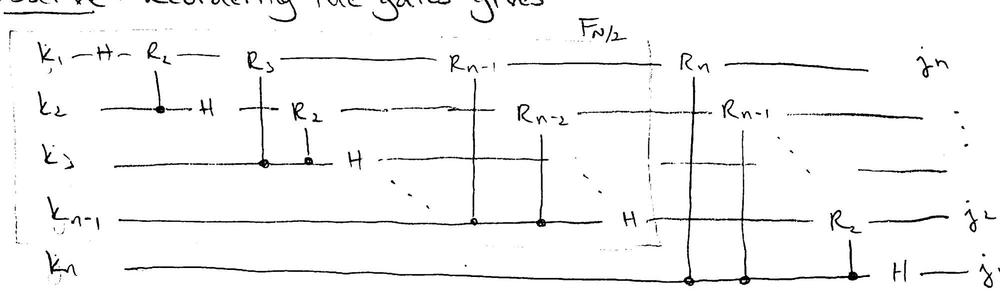
outputs in reverse order

$|j_n\rangle = |0\rangle \mapsto |0\rangle + |1\rangle$

$|1\rangle \mapsto |0\rangle - |1\rangle$

controlled rotation takes ~5 gates $\Rightarrow O(n^2)$ gates $= O((\log N)^2)$

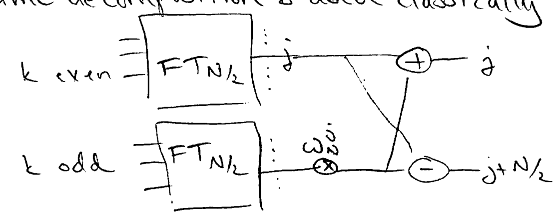
Observe: Reordering the gates gives



Reordering rows & columns of F_N matrix gives

$$\begin{array}{c|cc} & \text{even } 2k & \text{odd } 2k+1 \\ \hline j = j_1 \ldots j_{n-1} & \omega^{j \cdot 2k} & \omega^{j(2k+1)} \\ j + \frac{N}{2} & \omega^{(j+\frac{N}{2})2k} & \omega^{(j+\frac{N}{2})(2k+1)} \end{array} = \begin{array}{c|cc} & k_n = 0 & k_n = 1, j_1 \ldots \\ \hline j_n = 0 & \omega_{N/2}^{jk} & \omega_N^{j}\,\omega_{N/2}^{jk} \\ j_n = 1 & \omega_{N/2}^{jk} & -\omega_N^{j}\,\omega_{N/2}^{jk} \end{array}$$

The same decomposition is used classically in the FFT (fast Fourier transformation):



$T(N) = 2T(\frac{N}{2}) + O(N)$
$= O(N \log N)$.

FFT: $O(N \log N)$ quantumly $T(N) = T(N/2) + O(\log N) = O(\log^2 N)$

Quantum: $\log N$ qubits $\sum_j \alpha_j |j\rangle \mapsto \sum_j \hat{\alpha}_j |j\rangle$ $O(\log^{O(1)} N)$

disadvantage: $\hat{\alpha}_j$s inaccessible, but can measure j w/prob. $|\hat{\alpha}_j|^2$ "Fourier sampling"