Last time

- Definition: For $s \in \mathbb{Z}/N\mathbb{Z}$, define $\chi_s : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ by

$$\chi_s(x) = \omega^{sx}, \text{ where } \omega \text{ is the } N\text{-th root of unity}$$

- Example: $\chi_0(x), \chi_1(x), \chi_2(x)$
- Properties:
  - $\chi_0(x) = 1$
  - $\chi_s(x)^* = \chi_{-s}(x)$
  - $\chi_s(x) = \chi_x(s)$

- Theorem: $|\chi_0\rangle, |\chi_1\rangle, \ldots, |\chi_{N-1}\rangle$ form an orthonormal basis.
- Corollary: the matrix $\begin{bmatrix} |\chi_0\rangle & |\chi_1\rangle & \ldots & |\chi_{N-1}\rangle \end{bmatrix}$ is unitary.
- The above matrix transforms the standard basis to the χ-basis.
- Its inverse is called the discrete Fourier transform DFT$_N$
- Example: N = 4, DFT$_N^{-1} = \ldots$, DFT$_N = \ldots$
- Therefore, DFT$_N|x\rangle = \ldots$, which maps the χ-basis to the standard basis
- Given $|f\rangle \in \mathbb{C}^N$, what is DFT$_N|f\rangle$ and what is $\langle \chi_s \mid f\rangle$?
- Implementing DFT$_N$ with $N = 2^n$ with $n(n+1)/2$ gates

Implementation of DFT$_N$

- Say $n = 4$ and $N = 16$
- For $0 \leq x < 16$, DFT$_{16}|x\rangle = \ldots$
- Implementation using 1+2+3+4 gates…

Simon's algorithm over $\mathbb{Z}/N\mathbb{Z}$

- Given black-box access to quantum circuit Q_F implementing
- $F: \mathbb{Z}/N\mathbb{Z} \to \{0,1\}^m$
- Think of F as a labeling of $\mathbb{Z}/N\mathbb{Z}$
- Promised F is L-periodic: $\forall x, F(x) = F(x+L) = F(x+2L) = \ldots$ and otherwise labels are distinct, that is, $F(x) = F(y)$ if and only if $y - x$ is multiple of L.
- Task: find L

e.g.

	0	1	2	3	4	5	6		N-1
F	A	B	C	D	A	B	C	...	D

$L = 4.$ $A = 00$, $B = 01$, $C = 10$, $D = 11$.

- Observe: L divides N. Assuming $N = 2^n$, $L \in \{1, 2, 2^2, \ldots, 2^{n-1}\}$
- Classically…
- Remark: no need to assume $N = 2^n$ except when implementing DFT_N

Quantum Fourier sampling

- Load F to quantum state
- Discrete Fourier transform
- Load: what's the joint state?
- Measure answer qubits, the joint state collapses to?
- Now apply DFT_N, the final state is …
- What is $\langle \chi_s \mid g \rangle$?