Last time

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

 $\chi_{S}(x) = \omega^{SX}$, where ω is the N-th root of unity

- Example: $\chi_0(x), \chi_1(x), \chi_2(x)$
- Properties:
 - $\chi_0(x) = 1$
 - $\bullet \ \chi_{\scriptscriptstyle S}(x)^* = \chi_{-\scriptscriptstyle S}(x)$
 - $\bullet \ \chi_{S}(x) = \chi_{X}(S)$

- Theorem: $|\chi_0\rangle, |\chi_1\rangle, \dots, |\chi_{N-1}\rangle$ form an orthonormal basis.
- Corollary: the matrix $[|\chi_0\rangle \ |\chi_1\rangle \ \dots \ |\chi_{N-1}\rangle]$ 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, $DFT_N^{-1} = ...$, $DFT_N = ...$
- Therefore, $\mathrm{DFT}_N|x\rangle=...$, which maps the χ -basis to the standard basis
- Given $|f\rangle \in \mathbb{C}^N$, what is $\mathrm{DFT}_N|f\rangle$ 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 $0 \le x < 16$, DFT₁₆ $|x\rangle = ...$
- Implementation using 1+2+3+4 gates...

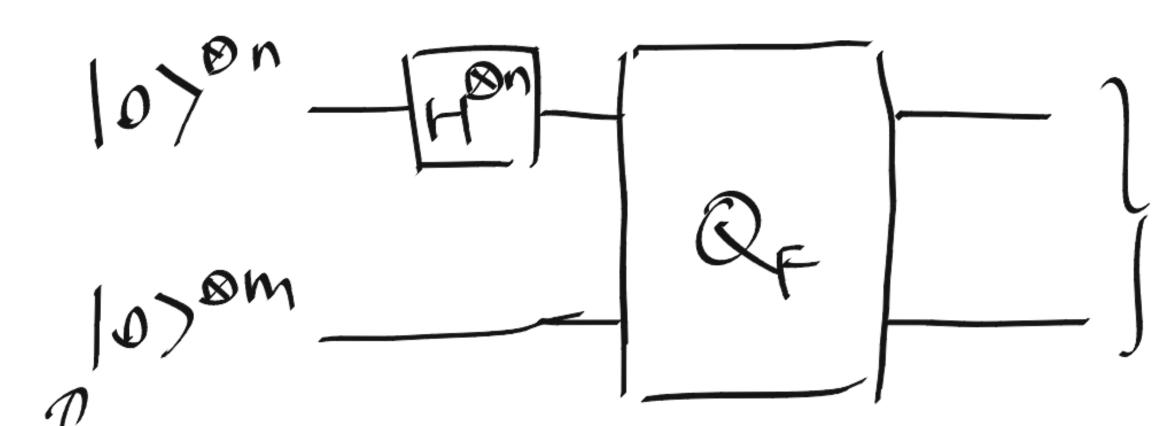
Simon's algorithm over $\mathbb{Z}/N\mathbb{Z}$

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

- 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 $\langle \chi_s \mid g \rangle$?