Last time

Rotate, compute, rotate

- Given "data" $F: \{0,1\}^n \to \{0,1\}$ and "pattern vectors" $|\chi_s\rangle, s \in \{0,1\}^n$
- Step 1: Load the data

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

- Step 2: Apply the Fourier transform w.r.t. $|\chi_s\rangle$, (χ-basis to standard basis)

$$\sum_s \langle \chi_s \mid f \rangle |s\rangle$$

- Step 3: Measure in the standard basis. Readout is $|s\rangle$ with probability $|\langle \chi_s \mid f \rangle|^2$

Two quantum algorithms so far

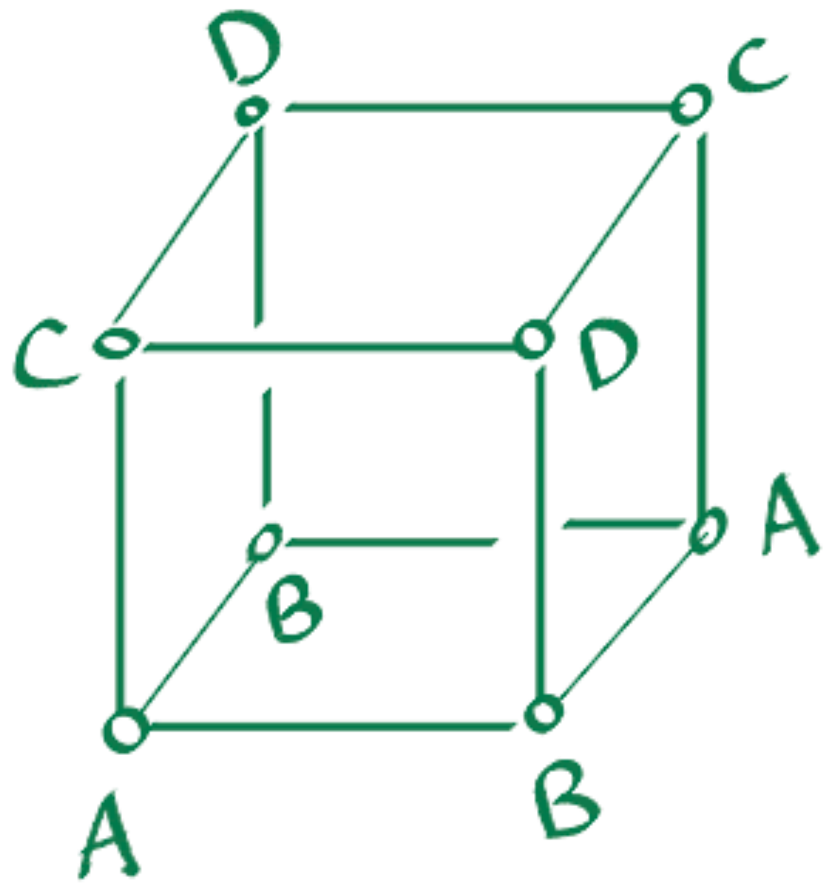
- Bernstein–Vazirani
  - Mystery Boolean function $F(x) = \text{XOR}_s(x) = x \cdot s \bmod 2$
  - Use quantum circuit Q_F implementing F once to find secret s
- Deutsch–Jozsa
  - F is constantly zero or balanced

Simon's algorithm

- Key difference
  - Need more than 1 application of Q_F
  - F will be a Boolean function with multiple output bits
  - $F\colon \{0,1\}^n \to \{0,1\}^m$
- Think of F as a labeling of $\{0,1\}^n$; each label encoded by some m-bit string

- Example

X	F(x)
000	A
001	B
010	C
011	D
100	B
101	A
110	D
111	C



A = 00
B = 01
C = 10
D = 11

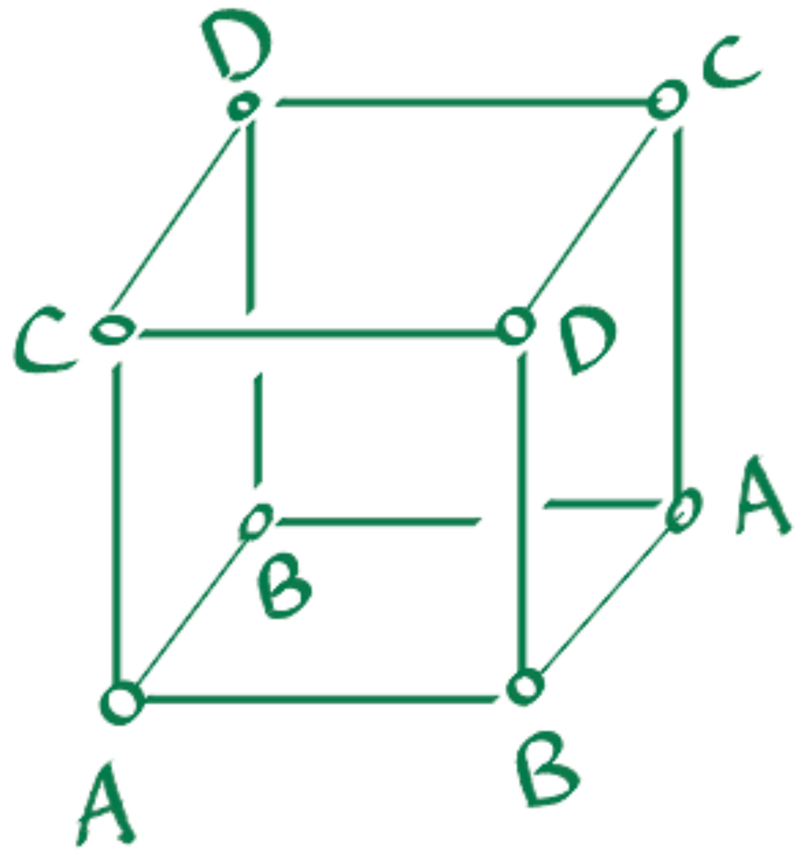
Periodic labeling

- Special promise on F: it is L-periodic for $L \in \{0,1\}^n$ and $L \neq 0\ldots0$ if $F(x+L) = F(x)$ for every x, where $x + L$ is bitwise addition mod 2

- In other words, F gives same label to all $x, x + L$ pairs

- Example: $L =$?

x	F(x)
000	A
001	B
010	C
011	D
100	B
101	A
110	D
111	C



A = 00
B = 01
C = 10
D = 11

Simon's problem

- Given L-periodic F for some secret $L \in \{0,1\}^n$
- Also promised that F gives different labels to different pairs $x, x + L$
- In other words, $F(x) = F(y)$ if and only if $x = y$ or $x + L = y$
- As a consequence F uses exactly 2^{n-1} different labels
- Given "black-box access" to Q_F implementing F, determine L
- Classical solution?
    - Need at least $\sqrt{N} = \sqrt{2^n}$ classical applications of F. Why?

Quantumly, can do it with at most $4n$ applications of Q_F

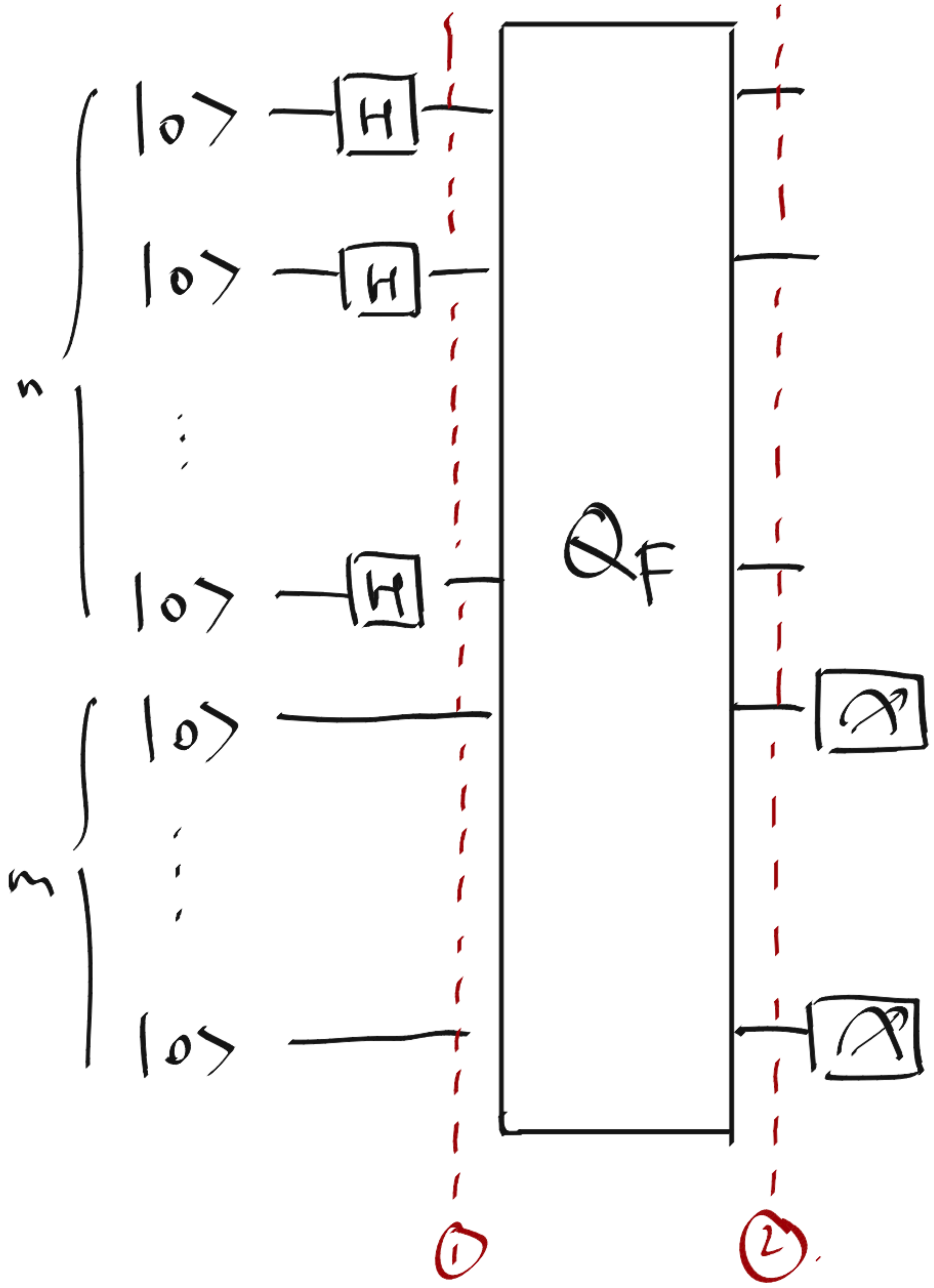
Probability of failure is small

Need $50n$ applications so that probability of failure $\leq 10^{-6}$

$4n$ **vs** $\sqrt{2^n}$**, exponential improvement**

Loading data

- Joint state at (1)?
- Joint state at (2)?
- New idea: measure the answer qubits!
- State collapses to …?
- Discard the answer qubits
- End of “data loading”



Rotate, compute, rotate

- Apply the Boolean Fourier transform

$$H^{\otimes n}\left(\frac{1}{\sqrt{2}}|x^*\rangle + |x^* + L\rangle\right)$$

- What's the resulting state?
- Now measure, …

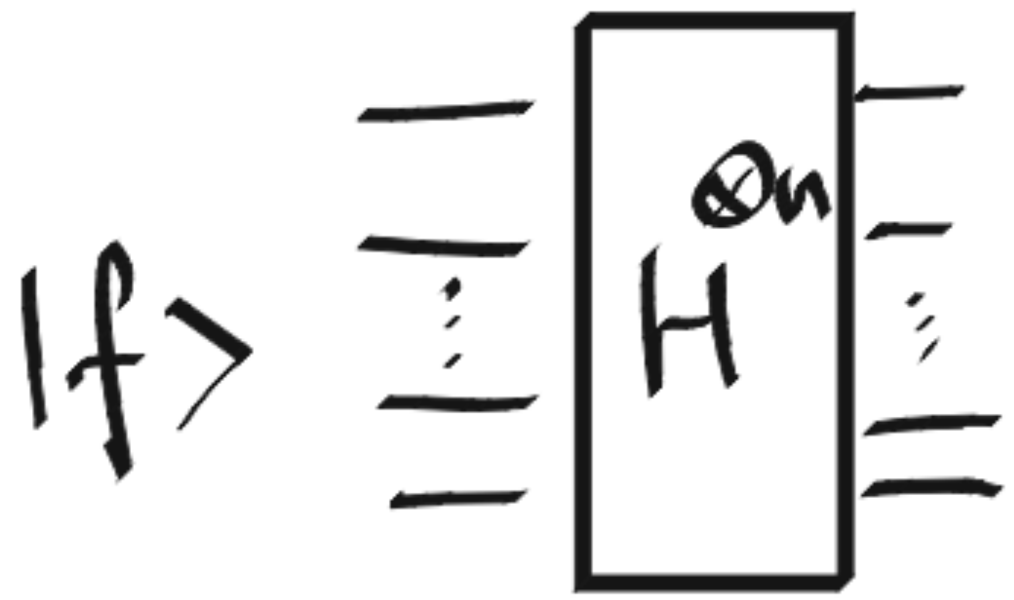
- Now repeat the above process.
- Each repetition uses $2n$ H gates, 1 Q_F and $m + n$ measurements
- Get a random equation $s \cdot L = 0$ from all 2^{n-1} possible s
- Repeat $n - 1$ times. Obtain $s_i \cdot L = 0$ for $i = 1, \ldots, 4n$
- Solve for L using classical Gaussian elimination
- What's the probability that L cannot be determined?

Fourier transform for $\mathbb{F}_2^n$

- Pattern vectors $|\chi_s\rangle$, where $\chi_s(x) = (-1)^{s \cdot x}$ and $s \cdot x$ is dot product in $\mathbb{F}_2^n$
- Key feature: $\chi_s(x+y) = \chi_s(x)\chi_s(y)$
- Decompose $f\colon \{0,1\}^n \to \{\pm 1\}$ into strengths of χ_s:

$$|f\rangle = \sum_s \langle \chi_s \mid f \rangle |\chi_s\rangle$$

- Quantum circuit



Fourier transform for $\mathbb{Z}/N\mathbb{Z}$

- $\mathbb{Z}/N\mathbb{Z}$ integers modulo N

- Pattern vectors $\chi_0, \ldots, \chi_{N-1} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ defined by

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

- Quantum circuit uses about n^2 1-qubit & 2-qubit gates when $N = 2^n$

- Remark: Can compute the strengths $\langle \chi_s \mid f \rangle$ to high accuracy with $O(n \log n)$ gates. Also works when N is not a power of 2.

- Again associate $f\colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ to vector

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} f(x)|x\rangle$$

- $|f\rangle$ is a quantum state if and only if …?

- Want N pattern vectors $\chi_0, \ldots, \chi_{N-1}$ such that $|\chi_0\rangle, \ldots, |\chi_{N-1}\rangle$ are orthonormal basis vectors

- Want the same key feature for $\chi_s\colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$

  - Need $\chi_s(x) = \chi_s(x+0) = \chi_s(x)\chi_s(0)$, and so $\chi_s(0) = 1$ (otherwise $\chi_s = 0$)

  - Need $\chi_s(x) = \chi_s(1)^x$

  - Need $1 = \chi_s(0) = \chi_s(N) = \chi_s(1)^N$, and so $\chi_s(1)$ is N-th root of unity

- 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.