Last time

Sign-implementation

- The Boolean function $F: \{0,1\}^n \to \{0,1\}$ is *sign-implemented* by $Q_F^{\pm}$ if it maps $|x\rangle|00\ldots0\rangle$ to $(-1)^{F(x)}|x\rangle|0\ldots0\rangle$ for every $x \in \{0,1\}^n$

- Denote $f: \{0,1\}^n \to \{\pm 1\}$ by $f(x) = (-1)^{F(x)}$

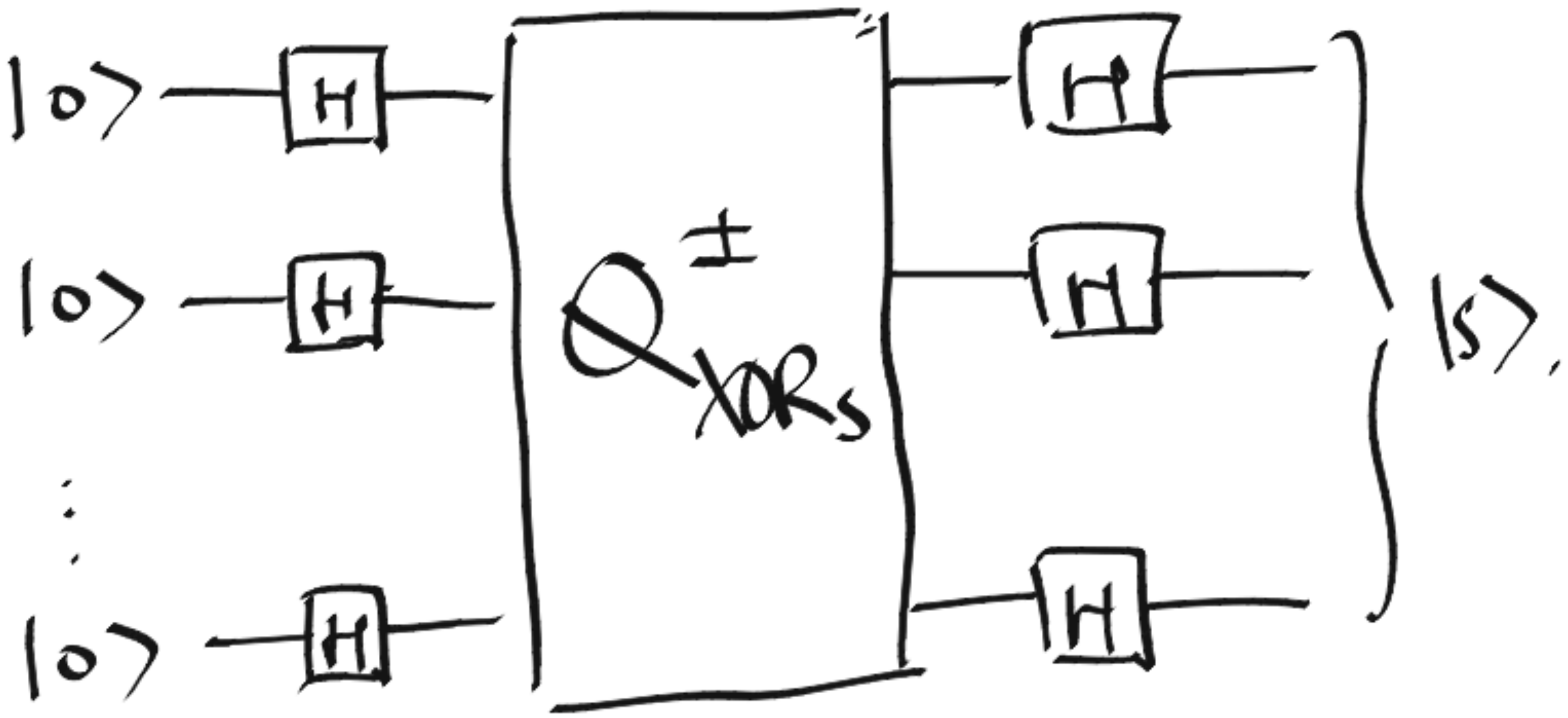
- "Rotate": Initialize n qubits $|0\rangle$'s. Put them through $H^{\otimes n}$. Obtain

$$|+\rangle \otimes \ldots \otimes |+\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle, \text{ where } N = 2^n$$

- Definition: Uniform superposition.

Rotate, compute, rotate

- Compute: Plug uniform superposition into $Q_F^{\pm}$ and obtain …
- Rotate: Apply Boolean Fourier Transform $H^{\otimes n}$ again, and obtain …
- What is $H^{\otimes n}|x\rangle$ for $x \in \{0,1\}^n$?
- Example
    - $x = 00\ldots0$
    - $x = 011$
- $H^{\otimes n}|x\rangle = \dfrac{1}{\sqrt{N}} \sum_{s\in\{0,1\}^n} \pm |s\rangle$. What is the sign on $|s\rangle$?



What is the sign on $|s\rangle$?

- In general, the sign on $|s\rangle$ is a product of n signs
  - If $s_i = 0$, the i-th sign is always $+$
  - If $s_i = 1$, the i-th sign is $(-1)^{x_i}$
  - Upshot: the i-th sign is $(-1)^{s_i x_i}$
  - Overall, the sign is $(-1)^{\sum_i x_i s_i} = (-1)^{x \cdot s}$
- Theorem: For every $x \in \{0,1\}^n$,

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

- Theorem: For every $x \in \{0,1\}^n$,

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

- Corollary

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

- Application: Someone hands you a sign-implementation of XOR_s, defined by $\text{XOR}_s(x) = x \cdot s \bmod 2$ without telling you s. Only need to feed in 1 input to learn s with 100% accuracy!

Comparison

Classical inputs only

- $x \mapsto \mathsf{XOR}_s(x) = x \cdot s \bmod 2$
- How many applications of XOR_s are needed?

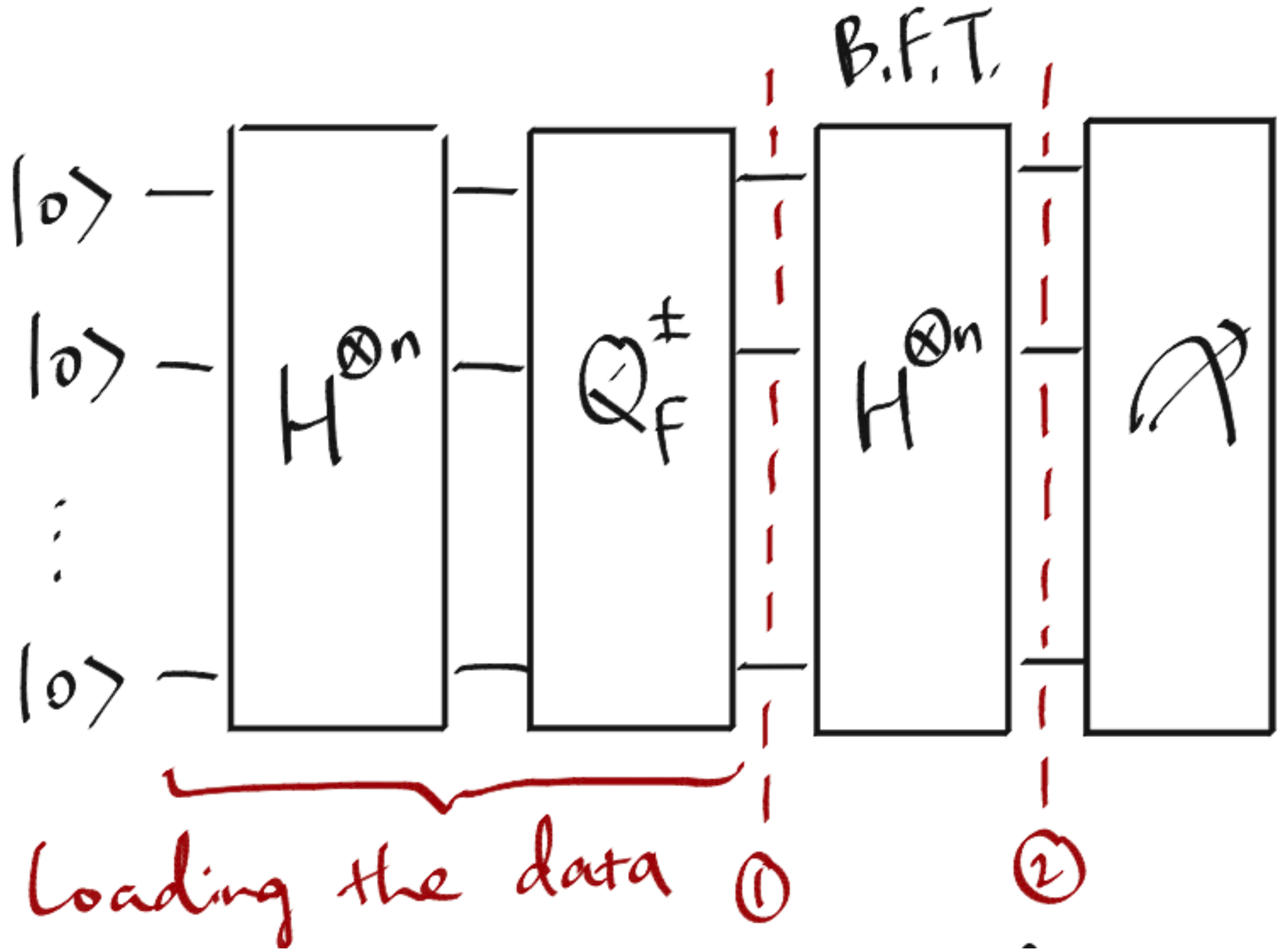
The general framework

to find patterns in implicitly-represented data

- Data vector $|g\rangle \in \mathbb{C}^N$ of length N
- Apply Fourier transform with "pattern vectors" $|\chi_0\rangle, \ldots, |\chi_{N-1}\rangle$
- Obtain another vector of length N, where s-th entry is "strength of $|\chi_s\rangle$ pattern in the data vector".
- Quantum:
  - $N = 2^n$ (say $n = 1000$)
  - Vectors implicitly represented by n-qubit state

- Pattern vectors $|\chi_0\rangle, \ldots, |\chi_{N-1}\rangle$ can be any orthonormal basis of $\mathbb{C}^N$
- "Strength of patterns $|\chi_0\rangle, \ldots, |\chi_{N-1}\rangle$ in $|g\rangle$" is just the coefficients when $|g\rangle$ is represented in $|\chi_0\rangle, \ldots, |\chi_{N-1}\rangle$ basis, that is, $\langle \chi_s \mid g\rangle$.
- Let $U \in \mathbb{C}^{N\times N}$ be the matrix with columns $|\chi_0\rangle, \ldots, |\chi_{N-1}\rangle$
    - U is unitary
    - U maps the standard basis to the χ-basis
    - U^{-1} or $U^\dagger$ maps the χ-basis to the standard basis
    - $U^\dagger$ maps $|g\rangle$ to …
- Want:
    - Interesting / useful" pattern vectors
    - Associated change of basis U easy to implement by quantum gates

XOR pattern revisited



- $F: \{0,1\}^n \to \{0,1\}$
- The state at (1) is

$$\underbrace{\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ \vdots \\ 1 \end{bmatrix}}_{F} \to \underbrace{\begin{bmatrix} +1 \\ -1 \\ -1 \\ +1 \\ \vdots \end{bmatrix}}_{f} \to \underbrace{\frac{1}{\sqrt{N}} \begin{bmatrix} +1 \\ -1 \\ -1 \\ +1 \\ \vdots \end{bmatrix}}_{|f\rangle}$$

F ↑ length 2^n (truth table)

$|f\rangle$. unit vector of length N.

- What are the pattern vectors $|\chi_s\rangle$?
    - $\chi_s: \{0,1\}^n \to \{\pm 1\}$ defined by $\chi_s(x) = (-1)^{s \cdot x}$
    - $H^{\otimes n}|s\rangle = |\chi_s\rangle$

- $H^{\otimes n}$ maps the standard basis to the χ-basis
- $H^{\otimes n}$ maps the χ-basis to the standard basis (why?)
- At (1), the just state can be written as

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

- At (2)

$$H^{\otimes n}|f\rangle = \sum_s \langle \chi_s \mid f\rangle |s\rangle$$

- Interpretation of the “strength” $\langle \chi_s \mid f \rangle$
    - Note $\chi_s, f\colon \{0,1\}^n \to \{\pm 1\}$
    - $\langle \chi_s \mid f \rangle = \ldots$
- Another application [Deutsch–Jozsa ’92]
    - Given Q_F implementing $F\colon \{0,1\}^n \to \{0,1\}$
    - Promised: either $F(x) = 0$ for all x or F is “balanced”
    - Find a way to decide which?