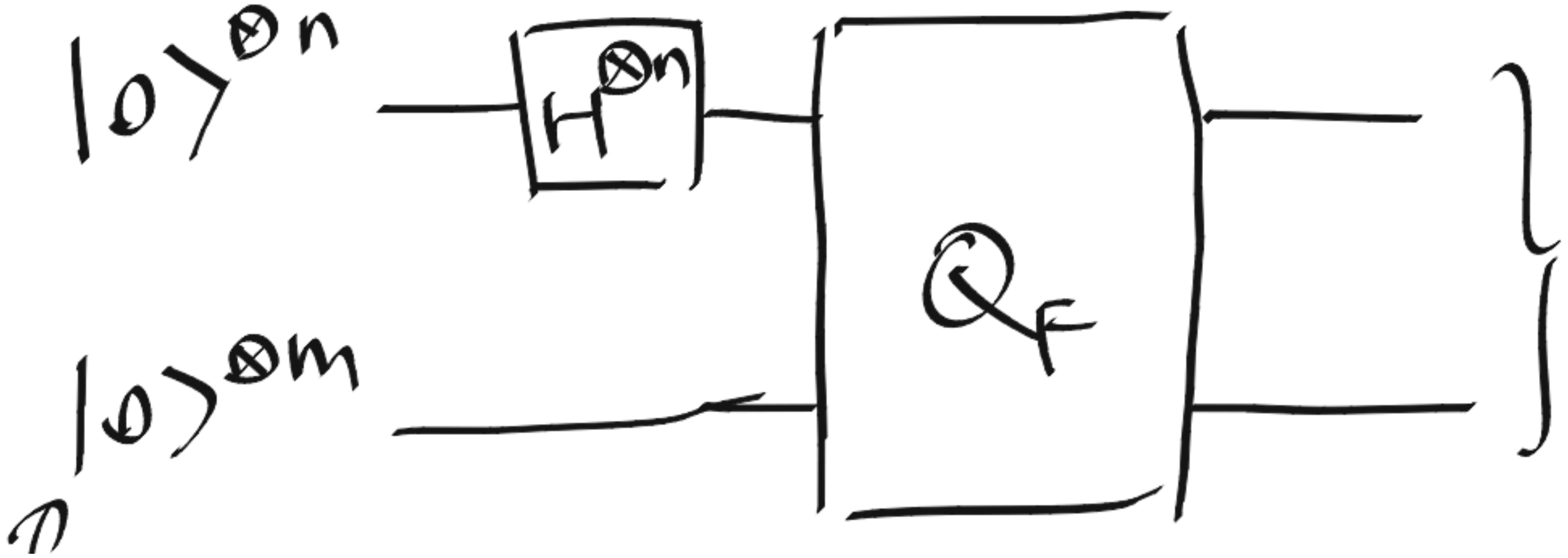
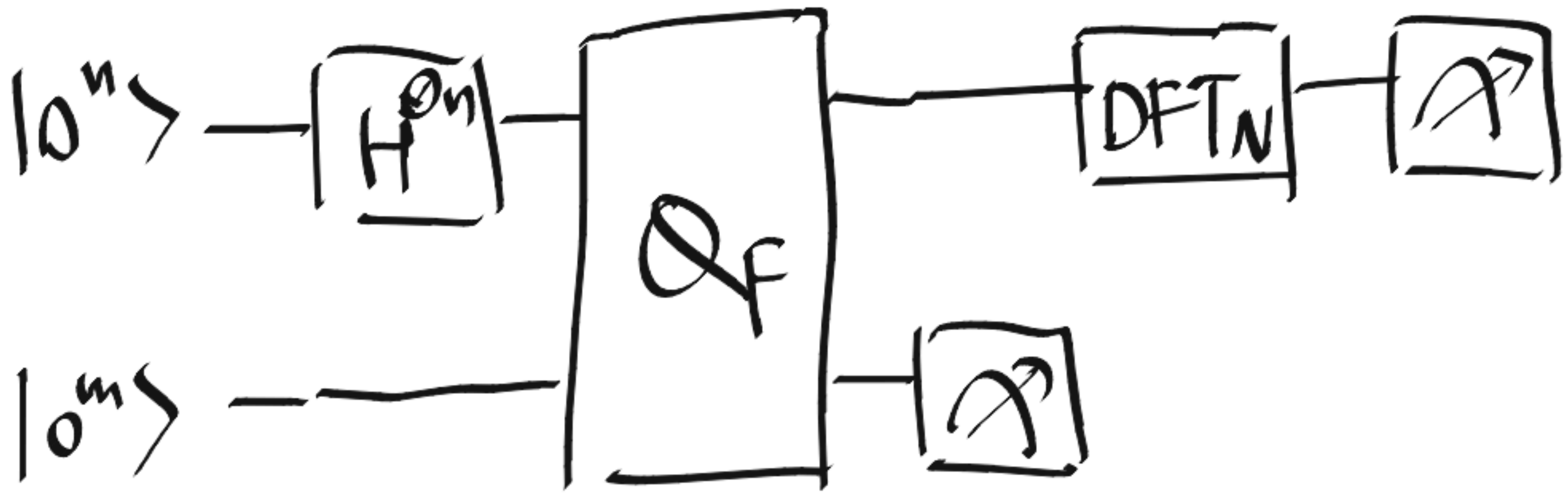
Quantum Fourier sampling

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

Summary



- L-periodic $F: \mathbb{Z}/N\mathbb{Z} \to \{0,1\}^m$
- Load F: n Hadamard gates, 1 Q_F
- DFT_N: at most n^2 gates
- Measurement: gives uniform random $s \in \{0, M, 2M, 3M, \ldots\}$, where $M = N/L$
- Claim: repeat twice, get $k_1 M, k_2 M$ for some random $0 \leq k_1, k_2 < L$
- There is a good chance of learning M, hence $L = N/M$
- Claim: For k_1, k_2 randomly sampled from $\{0,1,\ldots,L-1\}$, the probability they are co-prime is about $6/\pi^2$

What if L does not divide N?

No wrap around towards end

Example: ABCABCABCABCABCA

- Observation: each label used $\lfloor M \rfloor$ or $\lceil M \rceil$ times
- Claim: For each value $0,[M],[2M],[3M],\ldots,[(L-1)M]$, readout is that value w.p. at least $0.4/L$

Approximate period finding

- Given $F\colon \{0,1,2,\ldots,N-1\} \to \{0,1\}^m$ which is L-periodic (without warp around) and $N = 2^n$
- Then with about n^2 gates and one application of Q_F, we get a clue about L:

$s = [k \cdot M]$, where $k \in \{0,1,\ldots,L-1\}$ randomly chosen; else "junk"

- Question: how to use the clue s to find L?

- Additional assumption: L has m bits, and N has $10m$ bits
- Note: L is way smaller than N, and N/L might not be integer
- The clue s is about $k \cdot N/L$, and so s/N is about k/L
- Fact: Classical algorithm can efficiently figure out fraction k/L in lowest terms
- Example: Let $N = 2^{20}$ and $s = 740171$, and L has less than 5 bits.
- Idea: “continued fraction”
- Hope $k \in \{0,1,\ldots,L-1\}$ is a prime (which happens with probability $1/m$ by the prime number theorem)

Period-finding to number factoring

- Question: How does this period-finding ability help use factor numbers?
- Input: B big integer, m bits (e.g., $m = 1024$)
- Goal 1: factorize B. Hardest case: $B = PQ$ (interesting for breaking RSA)
- Goal 2: Find nontrivial R such that $R^2 = 1 \pmod{B}$
  (nontrivial means $R \neq \pm 1 \pmod{B}$)
- Question 1: How does R help factor B? Example: $B = 91$ and $R = 27$
- Question 2: How to find R?

How to find R?

- Input: B big integer, m bits (e.g., $m = 1024$)
- Pick $A \in \{1,\ldots,B-1\}$ and we may assume that $\gcd(A,B) = 1$.
- Let L be the order of A in $(\mathbb{Z}/B\mathbb{Z})^*$, which is the smallest positive L such that $A^L = 1 \pmod{B}$
- Example: $B = 91$ and $A = 3$
- Pick $N = 2^{10m}$. Now the sequence $A^0 \bmod B, A^1 \bmod B, A^2 \bmod B, \ldots, A^{N-1} \bmod B$ is L -periodic. We can efficiently implement the function $F\colon \{0,1,2,\ldots,N-1\} \to \{0,1\}^m$ with roughly m^3 quantum gates, and then use period-finding to get L
- Hope L is even and $A^{L/2} \neq \pm 1 \pmod{B}$, which happens with probability $\geq 1/4$
- Take $R = A^{L/2} \bmod B$