Quantum Circuits

Based on John Watrous's notes and also

Scott Aaronson: www.scottaaronson.com/democritus/

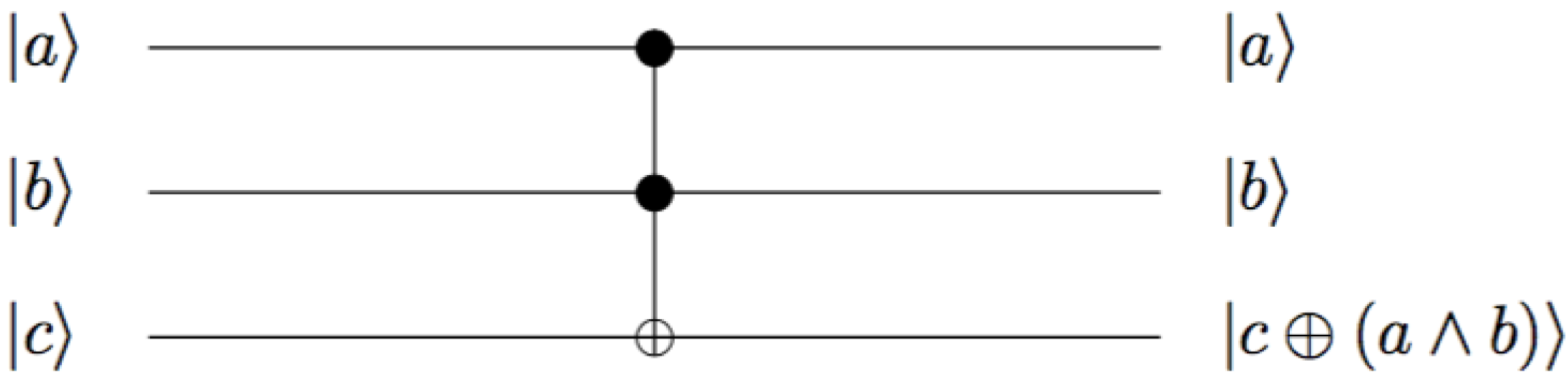
John Preskill: www.theory.caltech.edu/people/preskill/ph229

Outline

Simulating classical circuits with quantum circuits

- The complexity class Reversible-P
  - Universal gate set for reversible circuits
  - P = Reversible-P
- The complexity class QBP
  - Universal gate set for quantum circuits
  - BPP ⊆ QBP ⊆ PSPACE

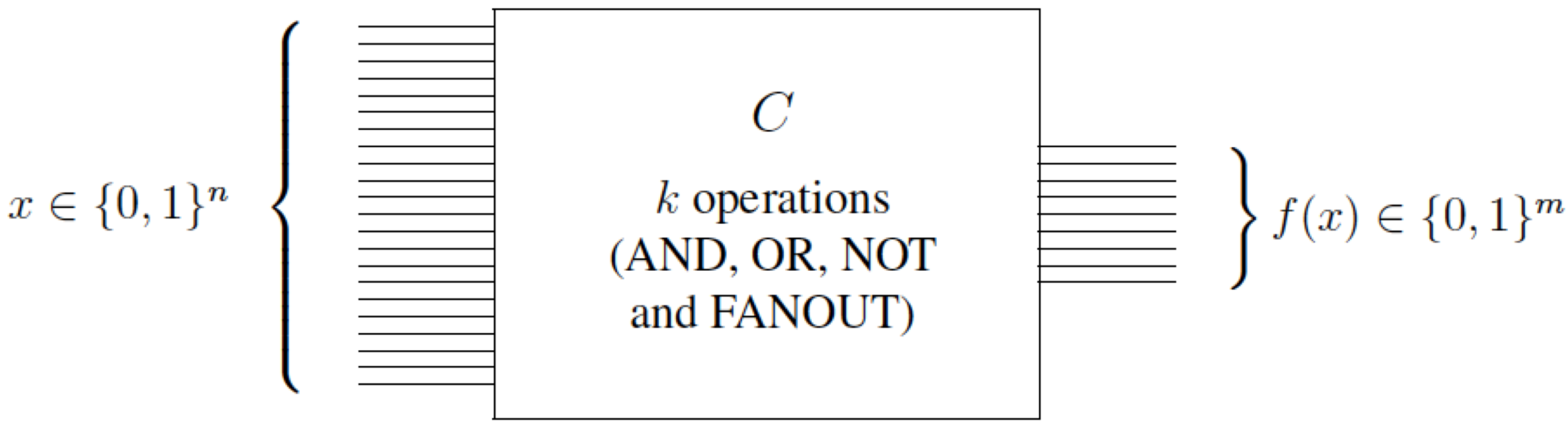
Review: Toffoli gates



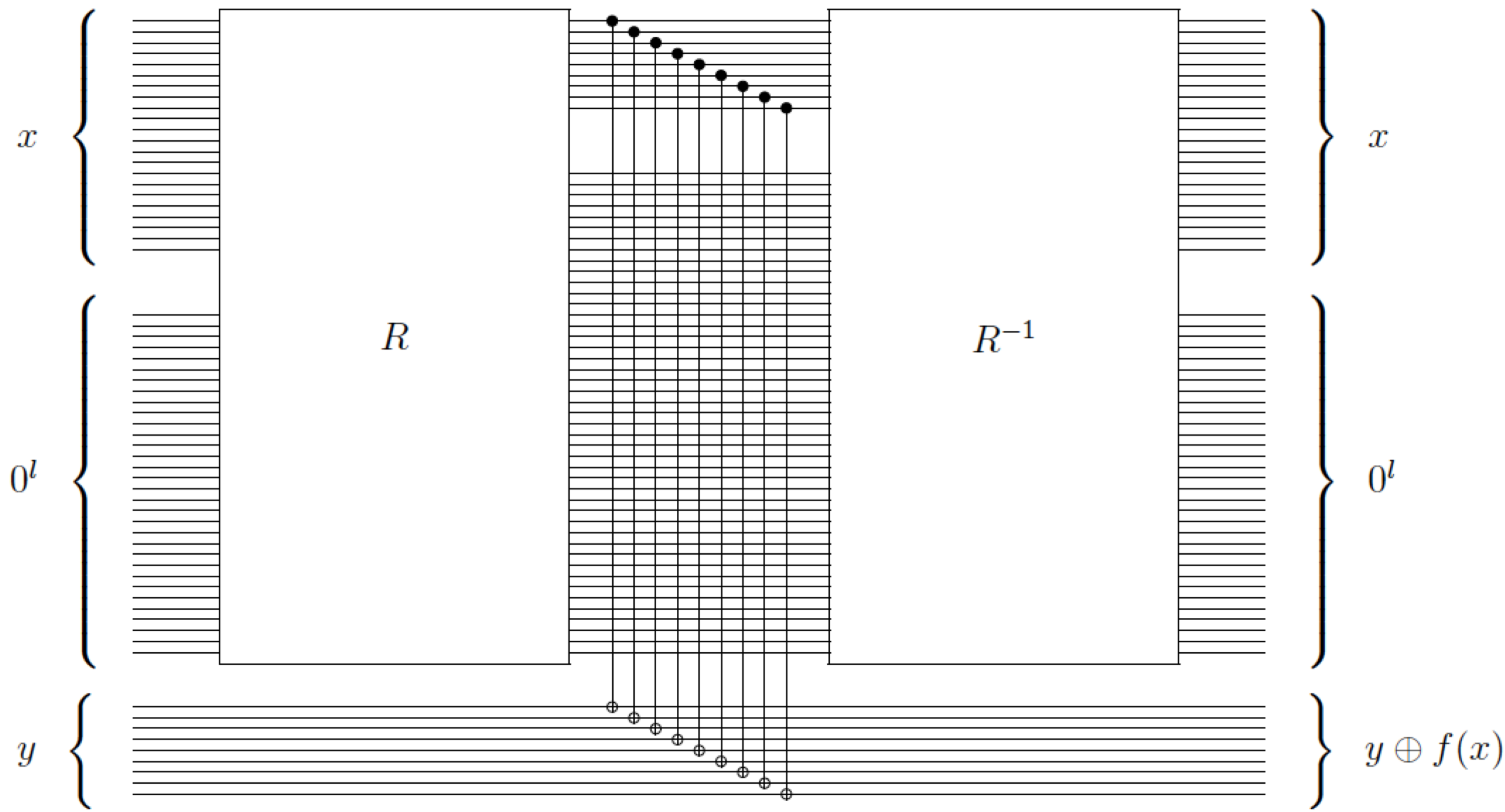
$|c \oplus (a \wedge b)\rangle$

- If a =1 and b= 1, NOT c
- Otherwise c

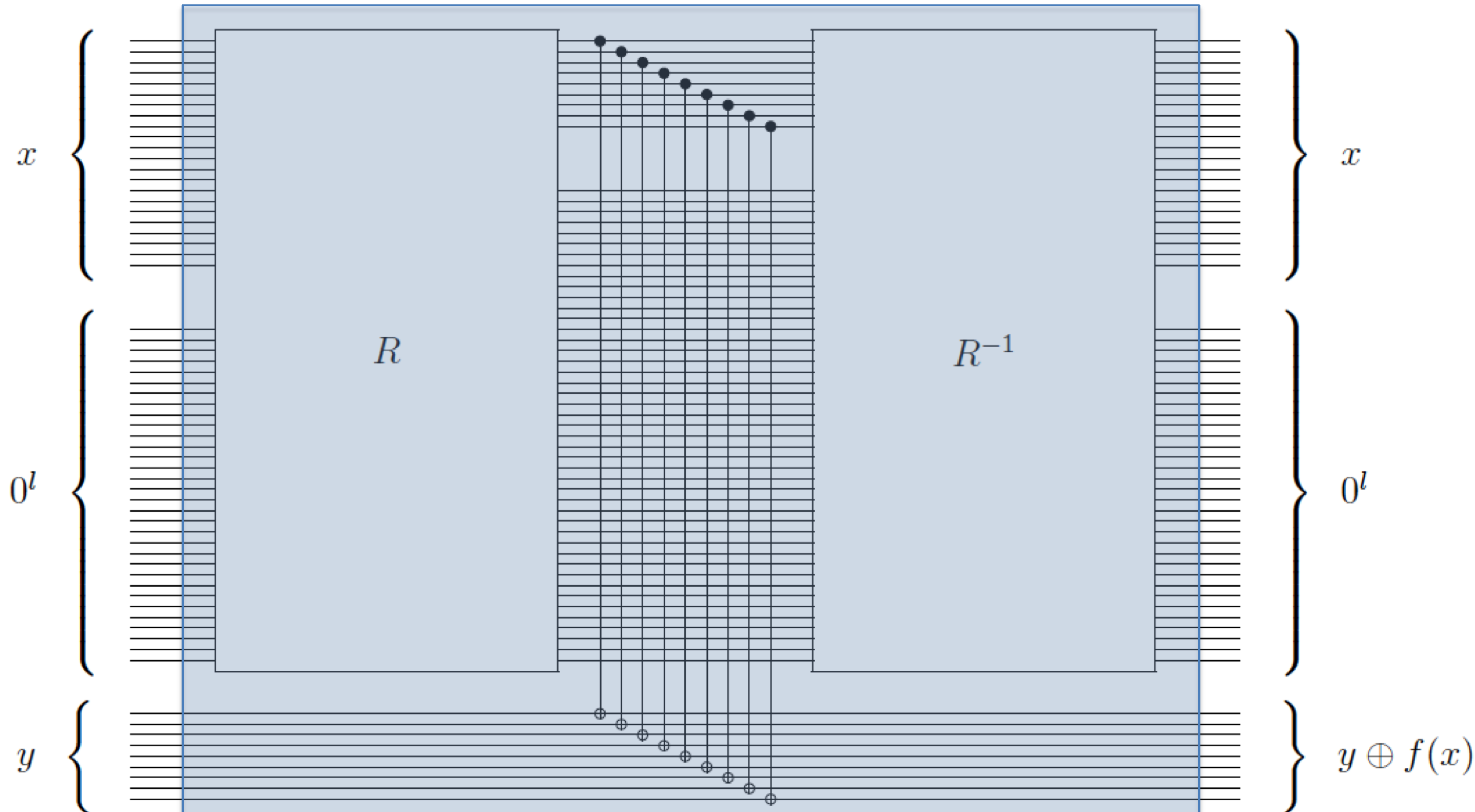
Classical Circuits → Reversible Circuits



Classical Circuits → Reversible Circuits

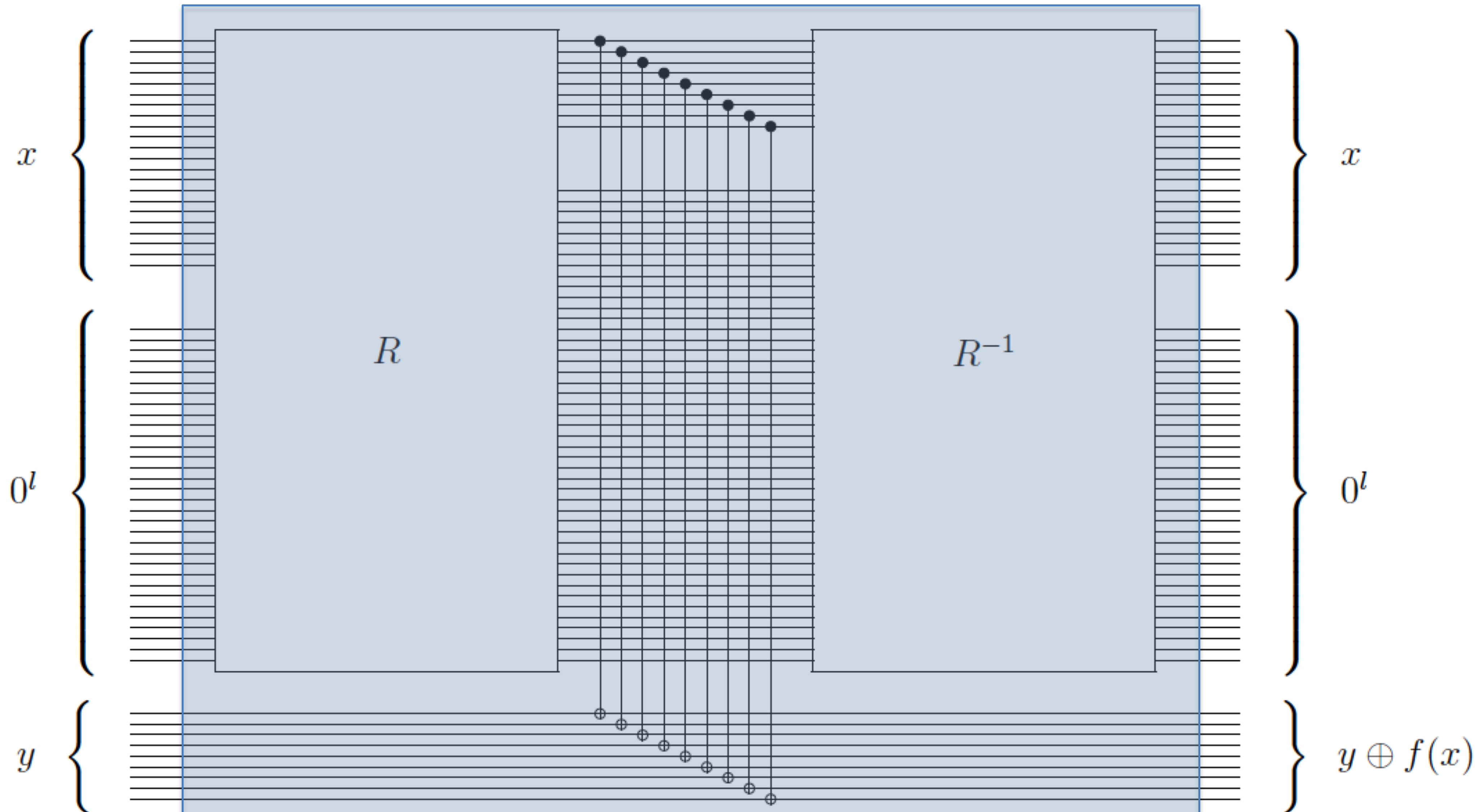


Classical Circuits → Reversible Circuits



$$S_C\,|x\rangle\,|y\rangle\,|0^l\rangle = |x\rangle\,|y \oplus f(x)\rangle\,|0^l\rangle$$

Classical Circuits → Reversible Circuits



$$S_C \quad |x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle$$

(ignoring ancilla bits)

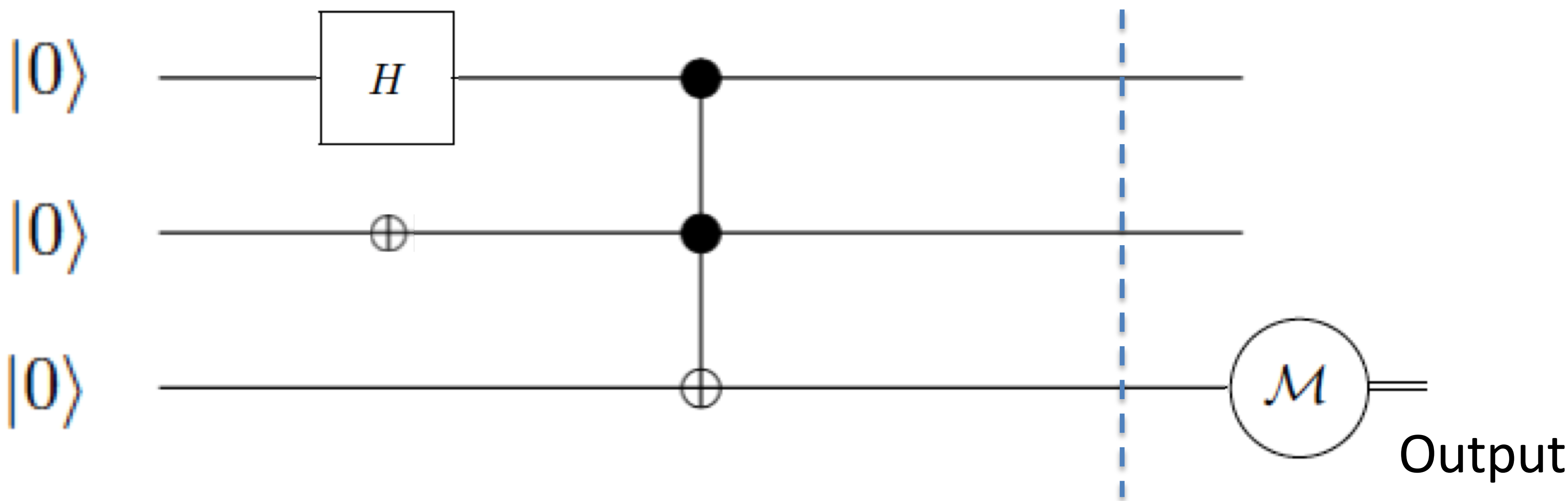
Simulating Classical Circuits: summary

- If f: $\{0,1\}^n \rightarrow \{0,1\}^m$ can be computed by a classical circuit C, then our simulation procedure generates a *reversible* circuit S_C that satisfies

$$S_C \left|x\right\rangle \left|y\right\rangle \left|0^l\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle \left|0^l\right\rangle$$

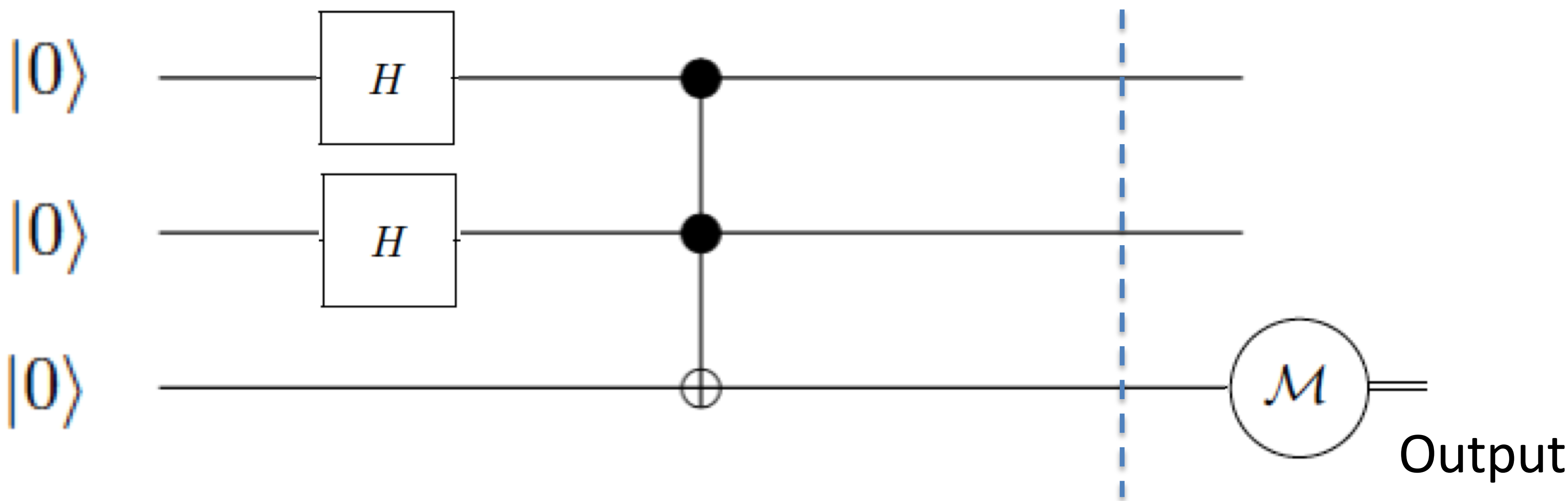
- The size of S_C is polynomial in the size of C

Exercise



- What is the superposition at the blue dotted line?
- What is the probability of measuring 1?

Exercise



- What is the superposition at the blue dotted line?
- What is the probability of measuring 1?

Recall: Circuit Complexity Classes

- *Input*: binary string x
- *Universal gate sets (bases)*: NOT, AND gates
- *Uniformity*
- *Acceptance*

Recall: Circuit Complexity Classes

- *Input*: binary string x
- *Universal gate sets (bases)*: NOT, AND gates

Recall: Circuit Complexity Classes

- *Input*: binary string x
- *Universal gate sets (bases)*: NOT, AND gates
- *Uniformity*

Recall: Circuit Complexity Classes

- *Input*: binary string x
- *Universal gate sets (bases)*: NOT, AND gates
- *Uniformity*

  $\{C_n \mid n \geq 0\}$ is a *uniform family of poly-size Boolean circuits* if

  – C_n has n input bits and one designated output bit

  – there is a polynomial time algorithm that can produce C_n, given 1^n as input

Recall: Circuit Complexity Classes

- *Input*: binary string x
- *Universal gate sets (bases)*: NOT, AND gates
- *Uniformity*: poly(n)-time algorithm to produce C_n

Recall: Circuit Complexity Classes

- *Input*: binary string x
- *Universal gate sets (bases)*: NOT, AND gates
- *Uniformity*: poly(n)-time algorithm to produce C_n
- *Acceptance*: designated output bit is 1

Recall: Circuit Complexity Classes

- *Input*: binary string x
- *Universal gate sets (bases)*: NOT, AND gates
- *Uniformity*: poly(n)-time algorithm to produce C_n
- *Acceptance*: designated output bit is 1

A language is in P iff there is a uniform family $\{C_n\}$ of poly-size circuits such that

- If $x \in L$ then C_n accepts input x
- If $x \notin L$ then C_n does not accept input x

BPP as a Circuit Complexity Class

- *Input*: binary string x and coin flip bits
- *Universal gate sets (bases)*: NOT, AND gates
- *Uniformity*: poly(n)-time algorithm to produce C_n
- *Acceptance*: designated output bit is 1

BPP as a Circuit Complexity Class

- *Input*: binary string x and coin flip bits
- *Universal gate sets (bases)*: NOT, AND gates
- *Uniformity*: poly(n)-time algorithm to produce C_n
- *Acceptance*: designated output bit is 1

A language is in BPP iff there is a uniform family $\{C_n\}$ of poly-size circuits such that

- If $x \in L$ then C_n accepts input x with probability $\geq 2/3$
- If $x \notin L$ then C_n accepts input x with probability $\leq 1/3$

Reversible Circuit Complexity Classes

Reversible Circuit Complexity Classes

- *Initial state*
- *Universal gate sets (bases)*
- *Uniformity*
- *Acceptance*

Reversible Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*
- *Uniformity*
- *Acceptance*

Reversible Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*: Toffoli, NOT
- *Uniformity*
- *Acceptance*

Reversible Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*: Toffoli. NOT
- *Uniformity*: as for classical circuits
- *Acceptance*:

Reversible Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*: Toffoli, NOT
- *Uniformity*: as for classical circuits
- *Acceptance*: output bit measurement is 1

Reversible Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*: Toffoli, NOT
- *Uniformity*: as for classical circuits
- *Acceptance*: output bit measurement is 1

A language is in Reversible-P iff there is a uniform family $\{C_n\}$ of poly-size reversible circuits such that

- If $x \in L$ then C_n accepts input x
- If $x \notin L$ then C_n does not accept input x

Reversible-P = P

- Reversible-P ⊆ P: follows since any gates (including Toffoli gates) can be simulated by NOT and AND gates
- P ⊆ Reversible-P: follows from our simulation of classical circuits by reversible circuits

Quantum Circuit Complexity Classes

Quantum Circuit Complexity Classes

- *Initial state*: $|x\rangle|0\ldots0\rangle$ (actual input plus ancilla bits)

Quantum Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*

Quantum Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*

For quantum computation, we can work with *real-valued* sets of quantum gates/unitary operators

Such a basis set is universal for quantum computation if any real unitary operator can be approximated with arbitrary precision by a circuit involving only the basis gates

Quantum Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*

Quantum Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*

Yaoyun Shi (2002) showed that Toffoli, NOT, and Hadamard gates form a universal set

Solovay-Kitaev: Any universal set of gates can simulate any other universal set with at most a polynomial increase in the number of gates

Quantum Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*: Toffoli, NOT, Hadamard

Quantum Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*: Toffoli, NOT, Hadamard
- *Uniformity*: as for classical circuits

Quantum Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*: Toffoli, NOT, Hadamard
- *Uniformity*: as for classical circuits
- *Acceptance:* output bit measurement is 1

In quantum circuits, the measurement is probabilistic

Quantum Circuit Complexity Classes

- *Initial state*: $|x\rangle|0...0\rangle$ (actual input plus ancilla bits)
- *Universal gate sets (bases)*: Toffoli, NOT, Hadamard
- *Uniformity*: as for classical circuits
- *Acceptance*: output bit measurement is 1

A language is in BQP iff there is a uniform family $\{C_n\}$ of poly-size quantum circuits such that

- If $x \in L$ then C_n accepts input x with probability $\geq 2/3$
- If $x \notin L$ then C_n accepts input x with probability $\leq 1/3$

BQP versus Traditional Classes

BPP is contained in BQP

Let C be a "BPP" circuit:

- Input: binary string x plus coin flips
- Gate set: NOT and AND
- Accept: if output bit is 1

BPP is contained in BQP

Obtain an equivalent quantum circuit as follows:

- Apply the classical → reversible gate conversion, (adding the needed ancilla bits)
- Replace each coin flip input by a qubit that is initialized to $|0\rangle$
- Add a Hadamard gate as the first operation that is applied to each coin flip qubit

Why does this work?

Evidence that BPP $\subsetneq$ BQP

- Factoring: given a positive integer N, output a prime factorization of N
- The best classical algorithms take time exponential in log N
- *Shor's algorithm* takes time $O((\log N)^3)$
- Prior to Shor's algorithm, *Simon's algorithm* was an interesting example of the power of quantum computation

BQP is in EXP

BQP is in EXP

- Evaluate a “BQP” circuit using matrix calculations, where the matrices are exponentially large in the number of input and ancilla bits.
- Or use Dirac notation, keeping track after every operation of the current superposition, using a sum that is exponential in the number of input and ancilla bits.

BQP is in PSPACE

- Adapt the argument that BPP is in PSPACE
- Let L be in BQP, x an instance of L, and Qx a circuit that with high probability outputs 1 if x is in L and 0 if x is not in L

BQP is in PSPACE

Consider the *state tree* of circuit Qx:

- Nodes are classical superpositions, with initial node $|x\rangle|0^l\rangle|0\rangle$ (and rightmost bit being output bit)
- Each level i corresponds to application of either a Hadamard or Toffoli operation
  - If Toffoli, one edge from each node at level i to node at level i+1
  - If Hadamard, two edges
- Each edge has an associated +/- *sign*
  - sign is "-" iff the edge corresponds to a Hadamard operation in which a 1-valued bit remains 1

BQP is in PSPACE

- We can write the final superposition of the qubits of Qx as a sum over all paths in the tree:

$$|final\rangle = \sum_p amp(p)\,|p\rangle$$
$$= \left(\frac{1}{\sqrt{2}}\right)^h \sum_p sign(p)\,|p\rangle$$

where sign(p) is the product of signs along path p and h is the number of Hadamard matrices

BQP is in PSPACE

- The amplitude of some fixed superposition |s⟩ is

$$\left(\frac{1}{\sqrt{2}}\right)^h \sum_{p:|p\rangle=|s\rangle} sign(p)$$

- The probability of measuring output |s⟩ is

$$Pr(s) = 2^{-h} \sum_{p,p'} sign(p) sign(p')$$

where the sum is over all p, p’ with |p⟩ = |p’⟩= |s⟩

- The probability of measuring output bit 1 is the sum of Pr(s), for all |s⟩ having rightmost bit 1.

Summary

- BPP $\subseteq$ QBP $\subseteq$ PSPACE

- It's conjectured that BPP $\subsetneq$ BQP: the fact that Factoring is in BQP is strong evidence

Next class

- Overview of Simon’s algorithm