Quantum computation

Introduction

Jérémie Roland

Université Libre de Bruxelles

Quantum Information & Communication

Outline

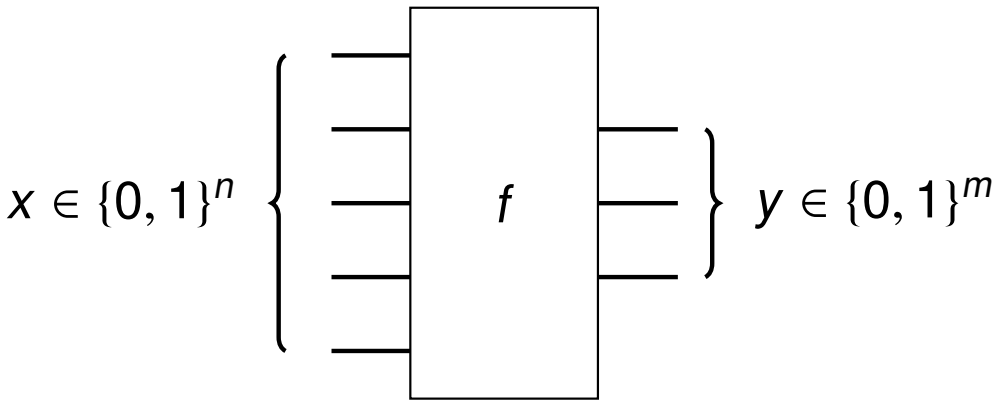
Outline

What is an algorithm?

- A computational procedure that
  - given as input a value or a set of values
  - produces as output a value or a set of values

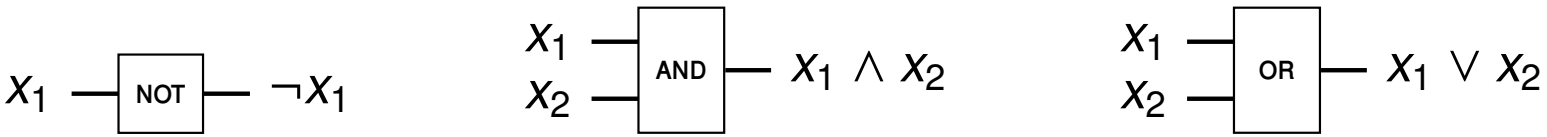
Bits

- Wlog: inputs and outputs may be expressed as bit strings
  - Input: $x = x_0 x_1 \dots x_{n-1} \in \{0,1\}^n$
  - Output: $y = y_0 y_1, \dots y_{m-1} \in \{0,1\}^m$
- An algorithm computes a function
  - $f : \{0,1\}^n \to \{0,1\}^m : x \mapsto y = f(x)$

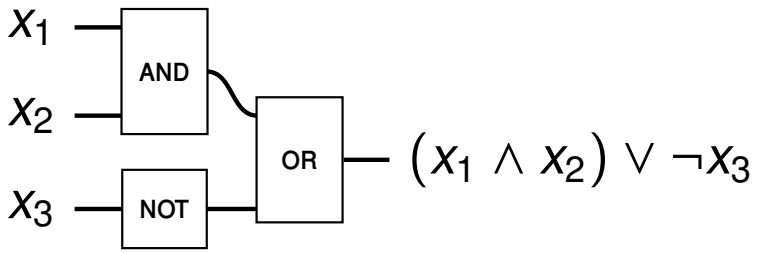


Circuit model

- Building blocks: logical gates
  - Examples: NOT, AND, OR



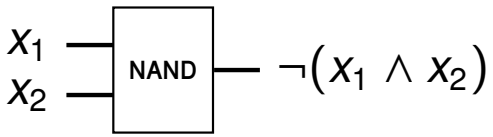
- Circuit



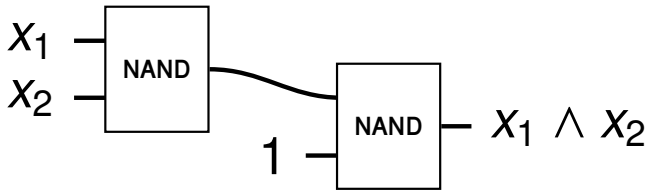
Universal set of gates

- A universal set of gates can simulate any logical gate (hence any function)
  - Example 1: NOT, AND, OR, FANOUT and SWAP

  - Example 2: NAND, FANOUT and SWAP



- Ancilla: extra bit with a fixed value
  - Example: Simulate an AND gate from two NAND gates

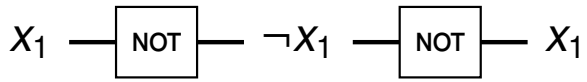


Outline

Reversibility of logical gates

Observation

- Some logical gates are reversible
  - Example: NOT



- Many others are not
  - Examples: AND, XOR

- Irreversible gates erase some information

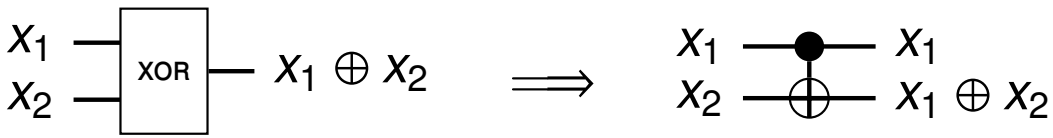
Reversible computation [Ben73]

Landauer's principle [Lan61]

When a computer erases a single bit of information, the amount of energy dissipated into the environment is at least $k_B T \ln 2$.

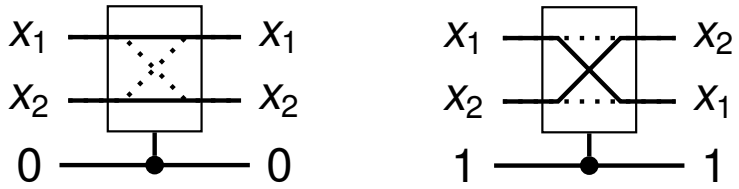
How to make a computation reversible?

- For each gate: additional output bit(s) holding erased information
  - Example: XOR gate $\Longrightarrow$ Controlled-NOT gate (C-NOT)

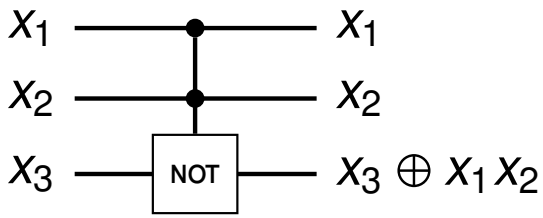


Universal set of gates

- Universal (set of) gate(s) for reversible computation [FT82]
  - Example 1: Fredkin gate (Controlled-SWAP)



  - Example 2: Toffoli gate ("Controlled-Controlled-NOT")

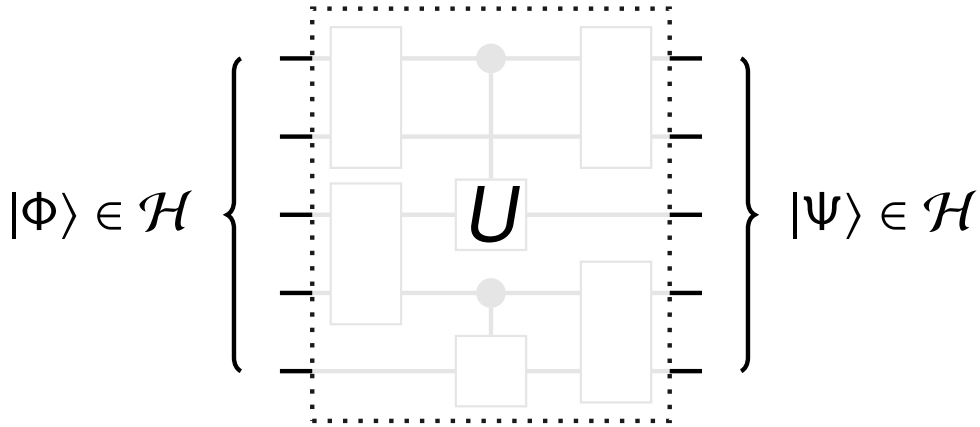


- Can simulate NOT, AND, OR, SWAP and FANOUT (with help of ancillas)
  - and therefore any circuit

Outline

Quantum circuits

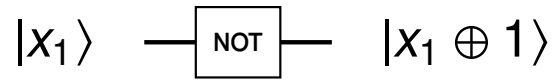
- A quantum circuit transforms a quantum state $|\Phi\rangle \in \mathcal{H}$ into $|\Psi\rangle = U|\Phi\rangle \in \mathcal{H}$
  - where U is a unitary operation



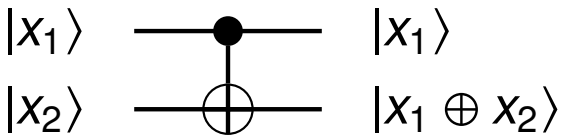
- Each wire carries a qubit
  - n qubits $\Longrightarrow \dim \mathcal{H} = 2^n$
- What elementary gates to implement any unitary U over $\mathcal{H}$?

Quantum gates

- Quantum evolution is reversible
  - Number of qubits is preserved
  - Reversible classical gates have quantum analogues
  - Example 1: NOT gate: $U_{\text{NOT}} : \mathcal{H}_2 \to \mathcal{H}_2 : |x_1\rangle \mapsto |x_1 \oplus 1\rangle$



  - Example 2: c-NOT gate: $U_{\text{c-NOT}} : \mathcal{H}_2 \otimes \mathcal{H}_2 \to \mathcal{H}_2 \otimes \mathcal{H}_2 : |x_1\rangle \otimes |x_2\rangle \mapsto |x_1\rangle \otimes |x_1 \oplus x_2\rangle$



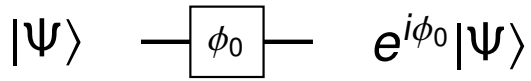
- This is not enough: quantum evolution is unitary
  - For n qubits, a quantum circuit implements a unitary $U \in U(2^n)$ (unitary group)
  - Note: global phases being irrelevant, we can restrict to $SU(2^n)$

Question

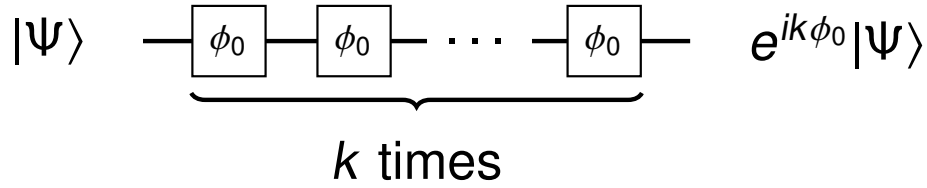
Can we implement all operations in $SU(2^n)$ from a finite set of elementary gates?

$U(1)$: global phase

- Suppose we want to implement all operations in $U(1) \simeq \{e^{i\phi} : \phi \in [0, 2\pi)\}$
  - Global phases
- From a single element $e^{i\phi_0}$



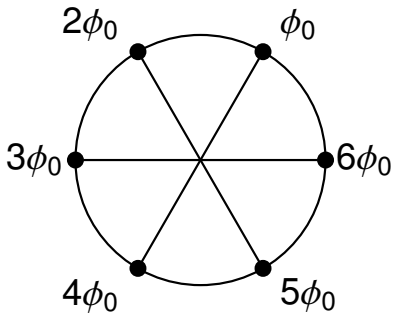
- The only option is to repeat the gate



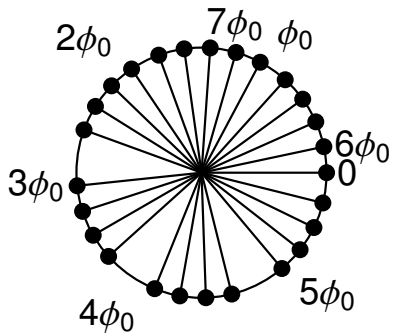
- Therefore, we can implement the set of phases $\{e^{ik\phi_0} : k \in \mathbb{N}\}$
  - How does this compare with all possible phases $\{e^{i\phi} : \phi \in [0, 2\pi)\}$?

$U(1)$: global phase

- Case 1: $\frac{\phi_0}{2\pi} \in \mathbb{Q}$
  - Example: $\phi_0 = \pi/3$



- Case 2: $\frac{\phi_0}{2\pi} \in \mathbb{R} \setminus \mathbb{Q}$



  - Any phase $\phi \in [0, 2\pi)$ can be approximated within arbitrary precision
  - The same idea will be used to approximate any operator in $U(2^n)$

$SU(2)$: one-qubit gates

- A one-qubit gate $U \in SU(2)$ can be written
  - in the computational basis

$$U : \mathcal{H}_2 \to \mathcal{H}_2 : \begin{cases} |0\rangle & \mapsto & u_{00}|0\rangle + u_{10}|1\rangle \\ |1\rangle & \mapsto & u_{01}|0\rangle + u_{11}|1\rangle \end{cases} \quad \text{or} \quad U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$$

  - where unitarity imposes $U^\dagger U = I \Leftrightarrow \sum_k u_{kl}^* u_{km} = \delta_{lm}$
- Some special gates
  - NOT-gate U_{NOT}, Hadamard gate H and phase gate U_ϕ

$$U_{\text{NOT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad U_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

- Each one-qubit gate can be represented (up to a global phase) as

$$R_{\hat{n}}(\theta) = e^{-i\frac{\theta}{2}\hat{n}\cdot\hat{\sigma}} = \cos\tfrac{\theta}{2}\, I + \sin\tfrac{\theta}{2}\, (n_x X + n_y Y + n_z Z)$$

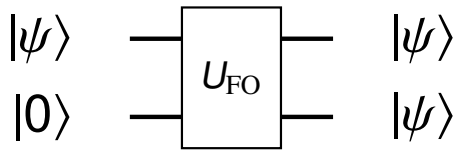
  - for some angle θ and some unit vector $\hat{n} = (n_x, n_y, n_z)$
  - where $\hat{\sigma} = (X, Y, Z)$ are the Pauli matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

A quantum FANOUT gate?

- In classical circuits, SWAP and FANOUT gates are usually assumed to be available

- In quantum circuits, no problem for SWAP (unitary operation)
- However, a quantum FANOUT should act as



  - For computational basis states ($|\psi\rangle = |0\rangle$ or $|1\rangle$), we have

$$|0\rangle \otimes |0\rangle \xrightarrow{U_{\mathrm{FO}}} |0\rangle \otimes |0\rangle \qquad |1\rangle \otimes |0\rangle \xrightarrow{U_{\mathrm{FO}}} |1\rangle \otimes |1\rangle$$

  - Therefore, we have by linearity for superpositions $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

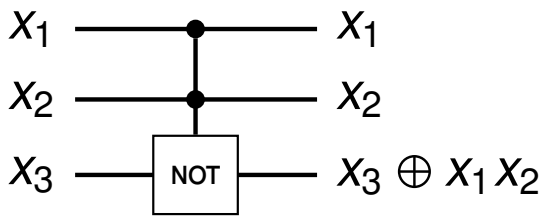
$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle = \alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |0\rangle \xrightarrow{U_{\mathrm{FO}}} \alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |1\rangle$$
$$\neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

  - No quantum FANOUT (cf. no-cloning theorem)

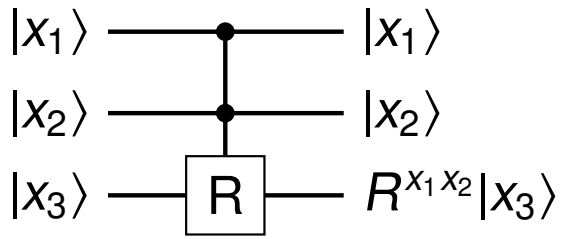
Outline

A universal quantum gate

- Recall: The Toffoli gate is universal for reversible classical computation



- We define the Deutsch gate as



  - where $R = -iR_x(\theta) = -ie^{-i\frac{\theta}{2}X}$, for $\theta \in \mathbb{R} \setminus \mathbb{Q}$

Theorem [Deu89]

The Deutsch gate is universal for quantum computation

Proof of universality (sketch)

- Since $R = -iR_x(\theta) = -ie^{-i\frac{\theta}{2}X}$, we have $R^4 = R_x(4\theta) = e^{-2i\theta X}$
  - Powers of R can approximate any operator generated by X
  - in particular, we can approximate X itself, which is the NOT-gate
- Since powers of R can approximate NOT
  - Powers of c-c-R (Deutsch) can approximate c-c-NOT (Toffoli)
  - Therefore, the Deutsch gate is (at least) universal for reversible computation
  - In particular, we can swap any two computational basis states
- By combining X operations, and swaps of computational basis states
  - we can also generate Y and Z operations
- By combining X, Y, Z operations, and swaps of computational basis states
  - We can generate all of $SU(2^n)$

A universal 2-qubit quantum gate

Note

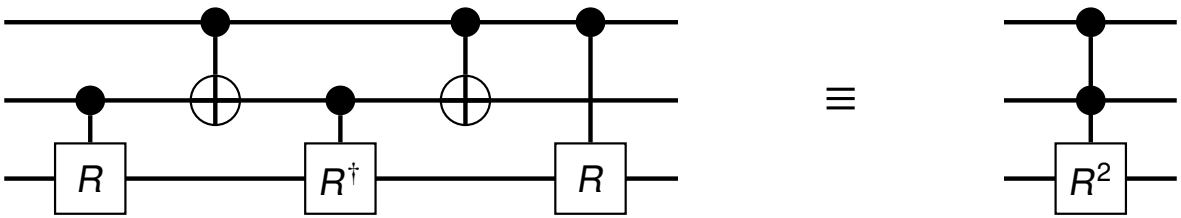
- The Toffoli gate (3-bit gate) is universal for reversible computation
- There is no universal 2-bit gate for reversible computation

Theorem

The controlled-R gate is universal for quantum computation

Proof

- Powers of c-R can approximate c-NOT (cf. above) and c-$R^\dagger$
- c-R, c-$R^\dagger$ and c-NOT can simulate c-c-R^2



- c-c-R^2 is a Deutsch gate, and therefore universal

More universal 2-qubit quantum gates

Theorem [DBE95, Llo95]

Any *generic* 2-qubit quantum gate is universal for quantum computation

Notes

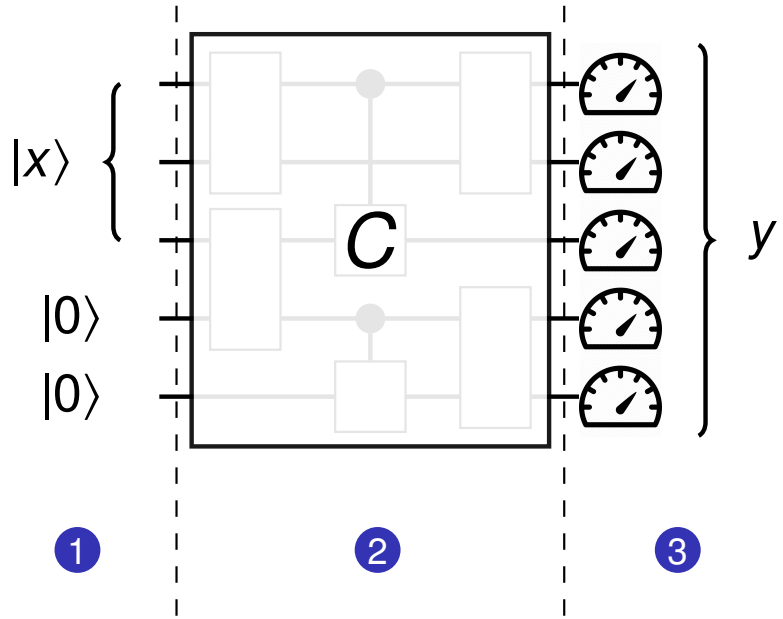
- *Generic* essentially means that all the involved phases are irrational
- Excellent news for implementations
  - Any generic interaction between two qubits is sufficient for universal quantum computation

Outline

Quantum algorithm

Quantum algorithm

1. Preparation of an n-qubit computational basis state
2. Quantum circuit C made of gates from a universal set
3. Measurement in the computational basis



Generality

Generality of this definition

- Preparation of another state?
  - Include the preparation of the state in the circuit
- Measurement in another basis?
  - Include the change of basis in the circuit
- POVM instead of projective measurement?
  - Can be simulated by a projective measurement using ancillas
- Intermediate measurements in the circuit?
  - All measurements can be postponed to the end
  - Requires ancilla if subsequent gates dependent on measurement outcome

Classical complexity

Notion of complexity and efficient algorithm

- **Complexity of an algorithm**: (Asymptotic behavior of the) number of elementary gates in the circuit
- **Efficient algorithm**: Algorithm with a complexity that grows at most polynomially in n (input size).

Basic classical complexity classes

- ***P*** (Polynomial): Problems accepting an efficient (deterministic) algorithm
- ***BPP*** (Bounded-error Probabilistic Polynomial) : Problems that can be solved with probability at least 2/3 by an efficient probabilistic algorithm.
- ***PSPACE*** (Polynomial Space): Problems that can be solved by an algorithm using at most a polynomial amount of space (i.e., memory).

$$P \subseteq BPP \subseteq PSPACE$$

Quantum complexity

Definition:

- ***BQP*** (Bounded-error Quantum Polynomial) : Problems that can be solved with probability at least $2/3$ by an efficient **quantum** algorithm.

Note

- This definition does **not** depend on the choice of universal set of gates
  - Any universal set of gates can approximate another set of gates
  - Controlling errors only incurs a polynomial overhead

How powerful is quantum computation?

Theorem

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE$$

Proof (sketch)

- $P \subseteq BQP$
  - Classical circuits can be made reversible
  - Reversible circuits are special cases of quantum circuits
- $BPP \subseteq BQP$
  - Quantum circuits can generate random bits
  - Measurement of $\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$ in the computational basis
- $BQP \subseteq PSPACE$
  - Quantum circuits can be simulated by classical circuits with polynomial space (but possibly exponential time)

How powerful is quantum computation?

Theorem

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE$$

Proof (sketch)

- $BQP \subseteq PSPACE$
  - Quantum circuits can be simulated by classical circuits with polynomial space (but possibly exponential time)
  - Let $U = U_t U_{t-1} \cdots U_2 U_1$ be the unitary realized by the quantum circuit
  - The probability to measure outcome y if the input of the circuit was $|x\rangle$ is

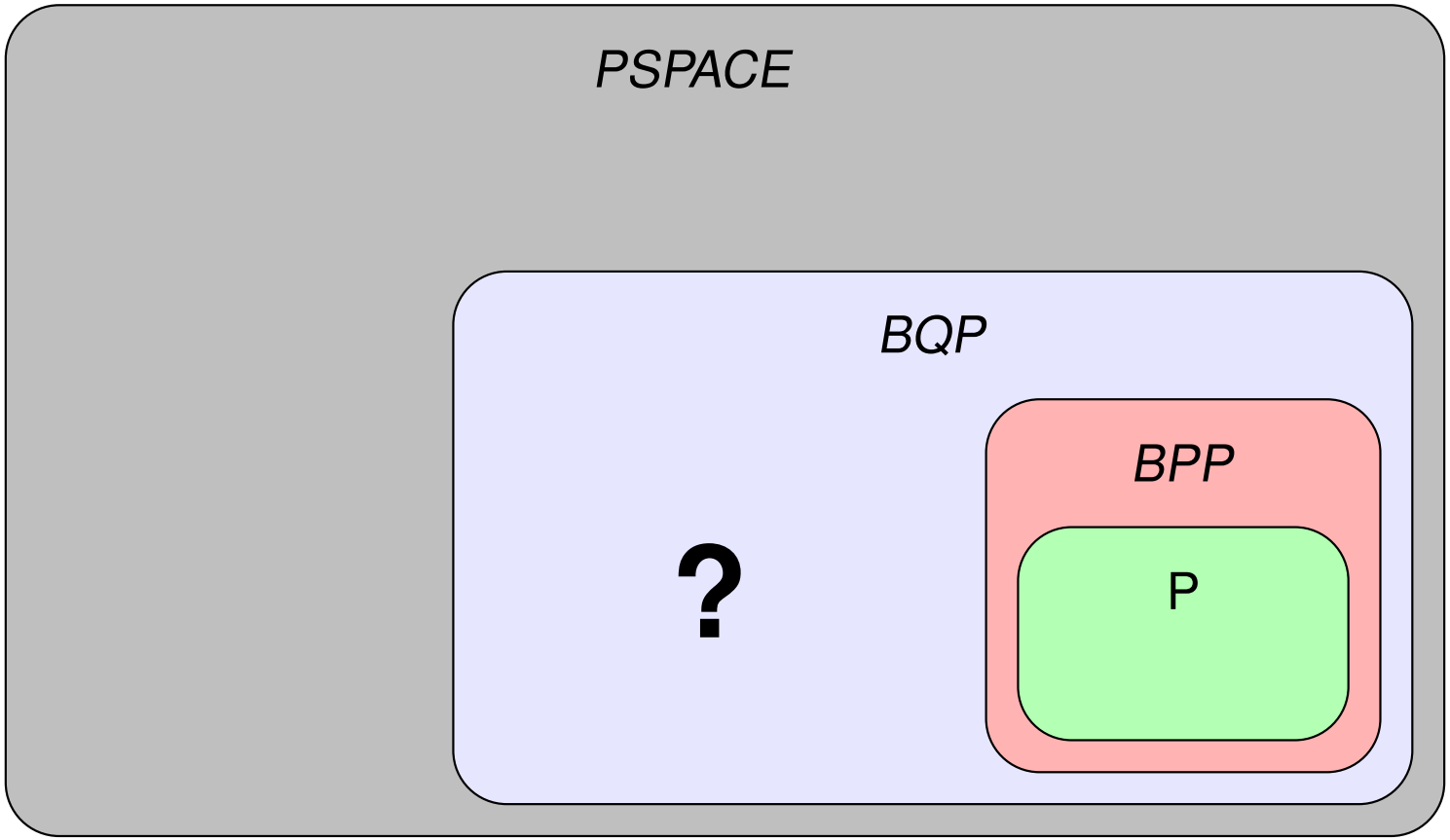
$$p_y = |\langle y|U|x\rangle|^2$$

  - The amplitude can be expanded as (cf. path integral)

$$\langle y|U|x\rangle = \sum_{x^{(1)},\cdots,x^{(t-1)}} \langle y|U_t|x^{(t-1)}\rangle\langle x^{(t-1)}|U_{t-1}|x^{(t-2)}\rangle \cdots \langle x^{(2)}|U_2|x^{(1)}\rangle\langle x^{(1)}|U_1|x\rangle$$

  - U_i's are 2-qubit gates so each factor can be computed in constant time
  - There are $2^{n(t-1)}$ terms, but each term can be computed in polynomial time

Classical and quantum complexity classes



Motivation for quantum computation

- Problems efficiently solvable by quantum computers, but not by classical computers
  - Would imply $BQP \neq BPP$
  - Statement still unknown: it is even unknown if $PSPACE \neq P$

Quantum speed-ups

Evidence of the power of quantum computation

- Non-exponential speed-ups
  - Example: Grover's algorithm for unstructured search (quadratic speed-up) [Gro96]
- Relativized exponential speed-ups (in the presence of some oracle O, see later)
  - $BQP^O \neq BPP^O$
  - Example: Simon's algorithm for period finding [Sim94]
- Exponential speed-up over the best *known* classical algorithm
  - Example: Shor's algorithm for factoring (problem in BQP, not known if in BPP) [Sho94]

References I

[Ben73] Charles H. Bennett.
Logical reversibility of computation.
IBM J. Res. Dev., 17(6):525–532, 1973.

[DBE95] David Deutsch, Adriano Barenco, and Artur Ekert.
Universality in quantum computation.
Proc. R. Soc. London A, 449:669–677, 1995.

[Deu89] David Deutsch.
Quantum computational networks.
Proc. R. Soc. London A, 425:73, 1989.

[FT82] Edward Fredkin and Tommaso Toffoli.
Conservative logic.
Int. J. Theor. Phys., 21(3/4):219–253, 1982.

[Gro96] Lov K. Grover.
A fast quantum mechanical algorithm for database search.
In Proc. 28th STOC, pages 212–219, 1996.

[Lan61] Rolf Landauer.
Irreversibility and heat generation in the computing process.
IBM J. Res. Dev., 5:183, 1961.

[Llo95] Seth Lloyd.
Almost any quantum logic gate is universal.
Phys. Rev. Lett., 75(2):346, 1995.

References II

[Sho94] Peter W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
In Proc. 35th FOCS, pages 124–134, 1994.
arXiv:quant-ph/9508027.

[Sim94] Daniel R. Simon.
On the power of quantum computation.
In Proc. 35th FOCS, pages 116–123, 1994.