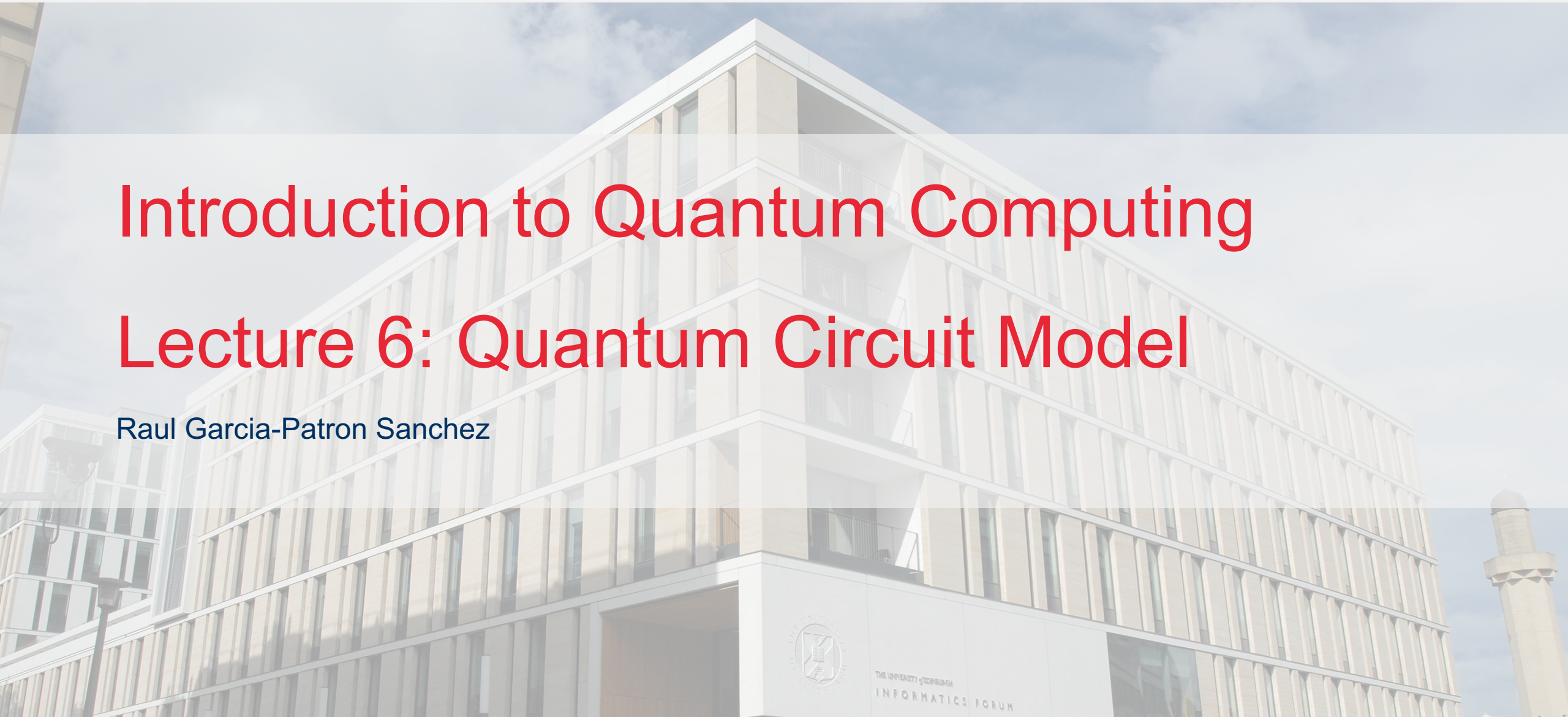


THE UNIVERSITY of EDINBURGH
informatics

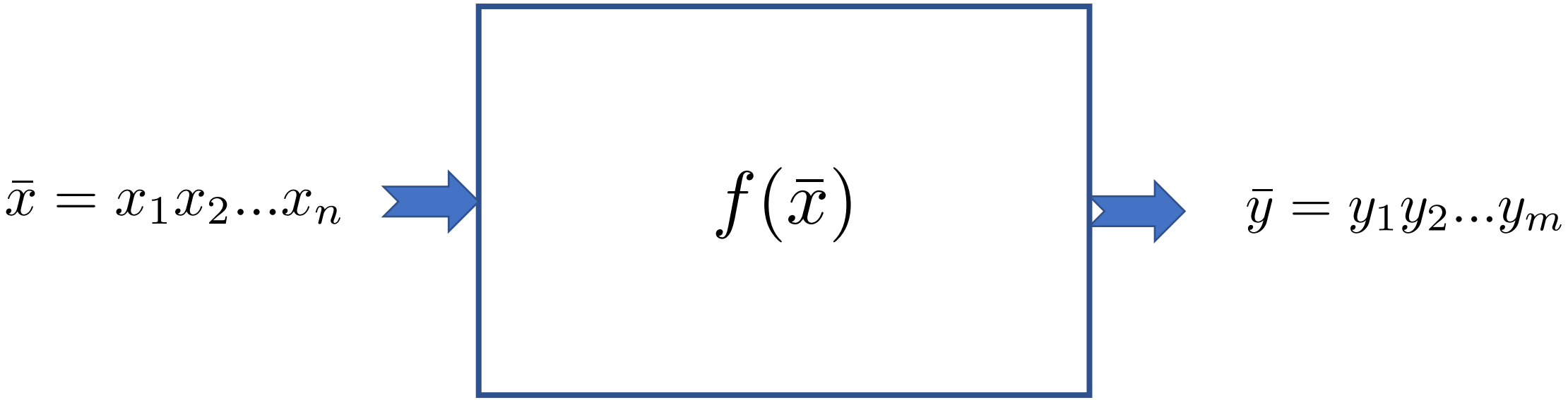
Introduction to Quantum Computing

Lecture 6: Quantum Circuit Model

Raul Garcia-Patron Sanchez

Classical Circuit Model

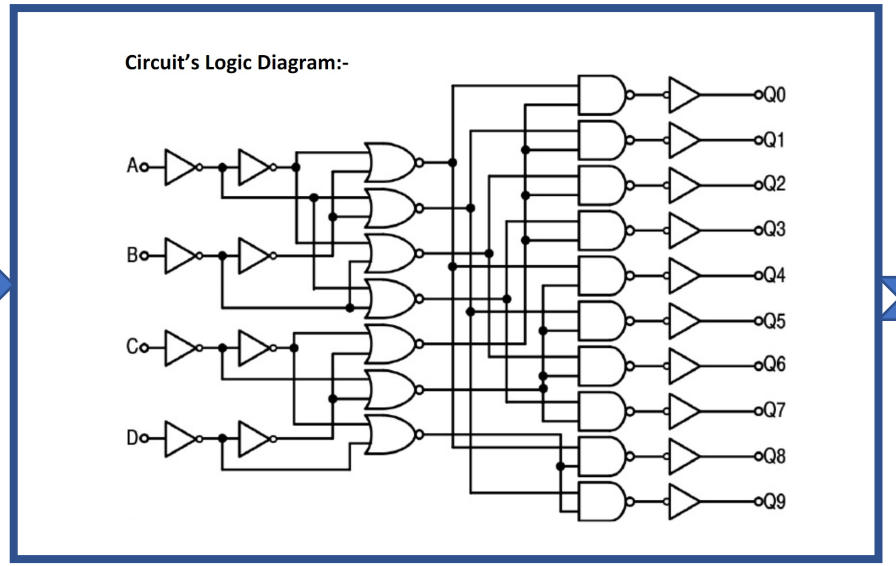
- Classical circuits compute Boolean functions: $f : \{0,1\}^n \rightarrow \{0,1\}^m$



Classical Circuit Model

- Classical circuits compute Boolean functions: $f : \{0,1\}^n \to \{0,1\}^m$

$\bar{x} = x_1 x_2 \ldots x_n$



$\bar{y} = y_1 y_2 \ldots y_m$

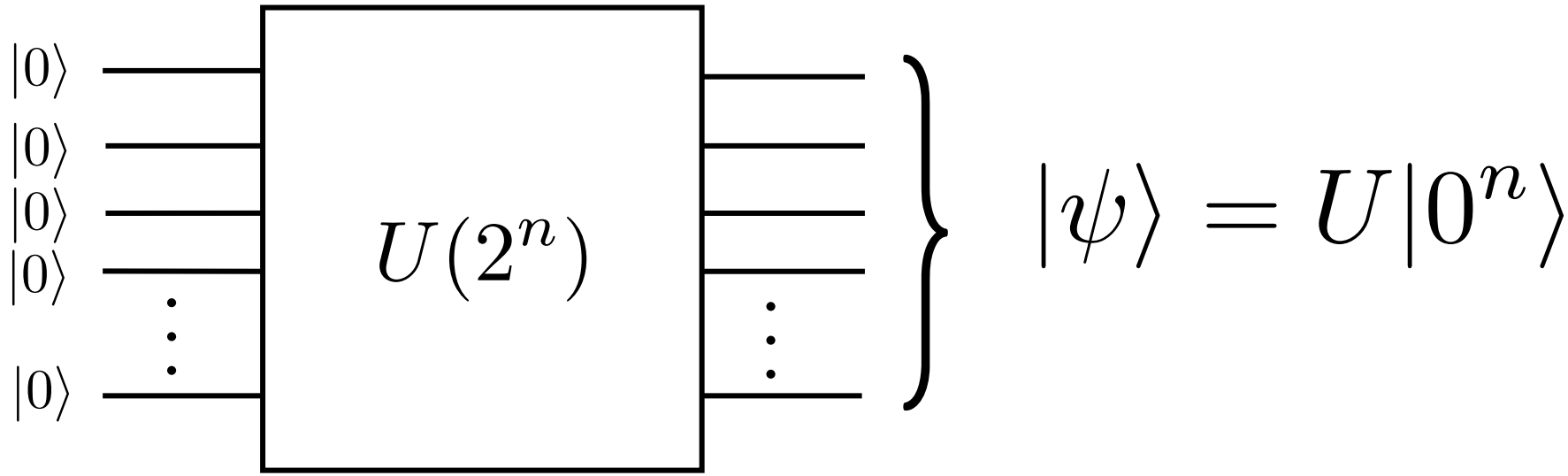
- NAND gates are UNIVERSAL

All Boolean functions can be generated with NAND gates.

- Most circuits are irreversible.
- Resource count: # gates, depth of circuit (# layers of gates).
- Most Boolean functions need exponential number of gates.

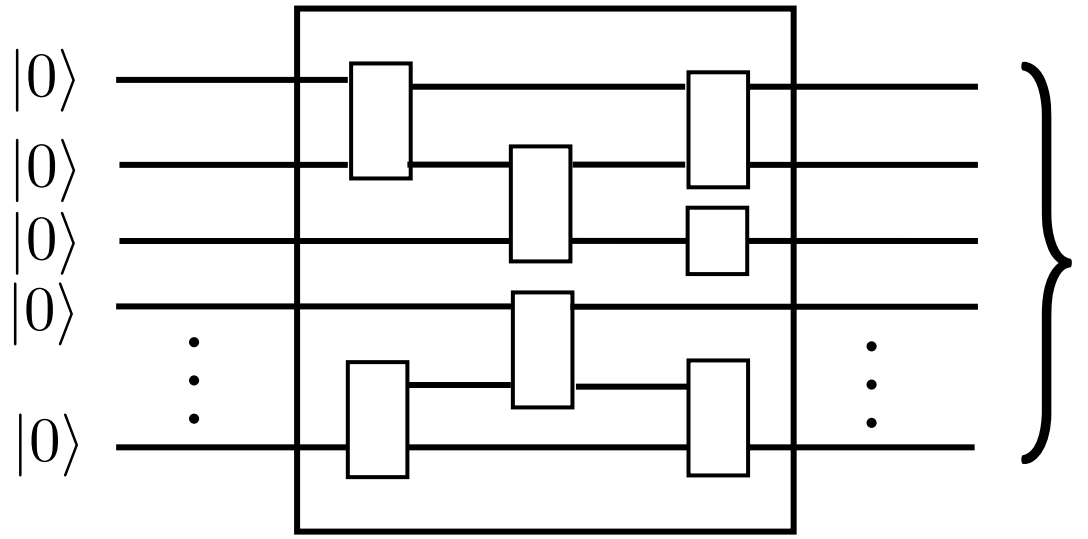
Quantum Circuit Model

- Quantum circuits implement unitaries, $U : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n}$



Quantum Circuit Model

- Quantum circuits implement unitaries, $U : \mathcal{H}^{\otimes n} \to \mathcal{H}^{\otimes n}$

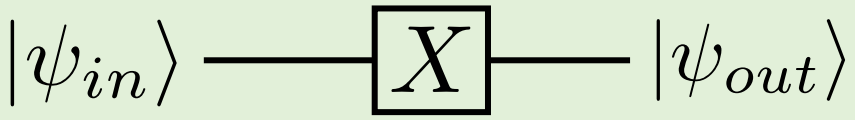


$$|\psi\rangle = U|0^n\rangle$$

- $\exists$ sets of 1 and 2 qubit gates that are UNIVERSAL
- (Ideal) quantum circuits are reversible.
- Resource count: # gates, depth of circuit (# layers of gates).
- Most unitaries need exponential number of gates.

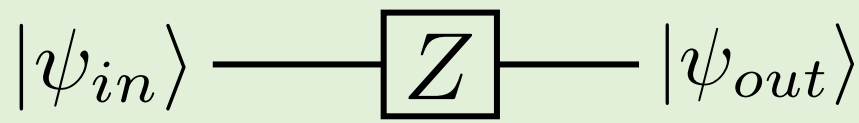
1-qubit gates

NOT gate



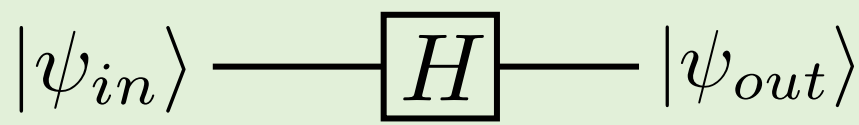
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Z gate



$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Hadamard gate



$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Phase gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

T gate

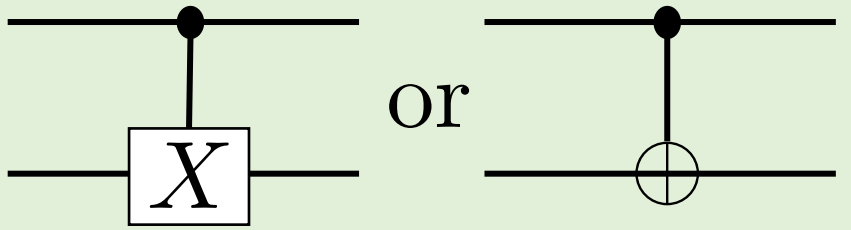
$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

Gates: 2-qubit

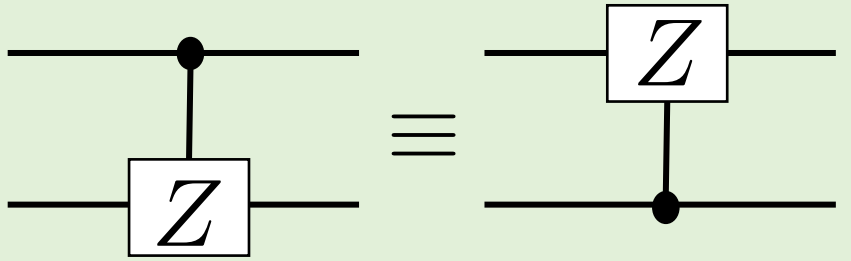
Controlled-not gate (cnot gate):

$$U_{\wedge X} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$



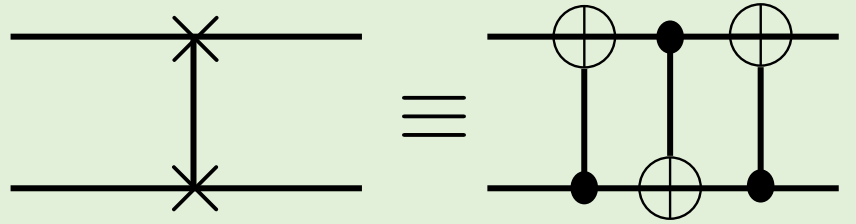
Controlled-Z gate:

$$U_{\wedge Z} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z = \mathrm{diag}(1, 1, 1, -1)$$



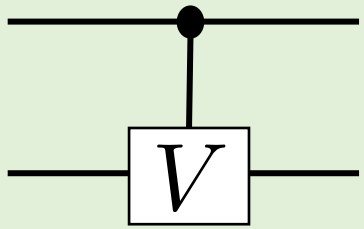
SWAP (permutation) gate

$$\Pi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



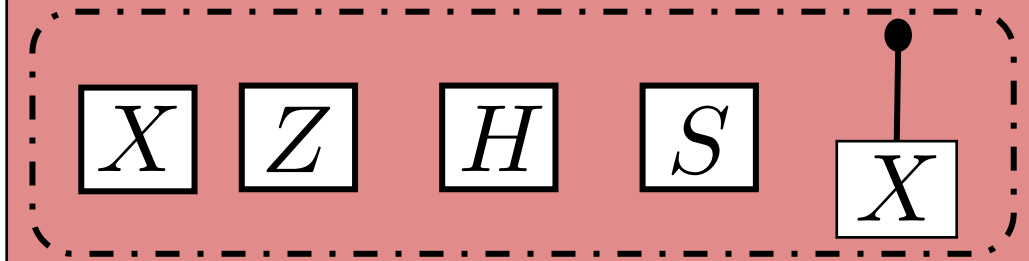
Controlled-V gate:

$$U_{\wedge V} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes V$$



Universal sets of gates

Clifford Gates

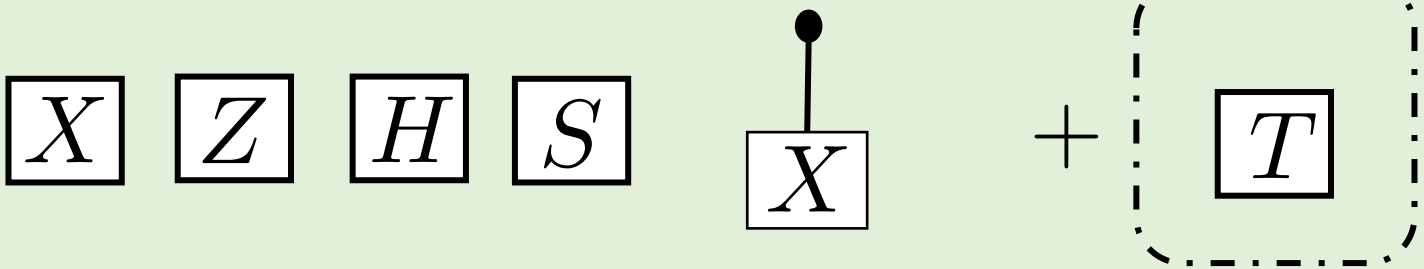


Very important role in QC: QEC
(Quantum Error Correction)

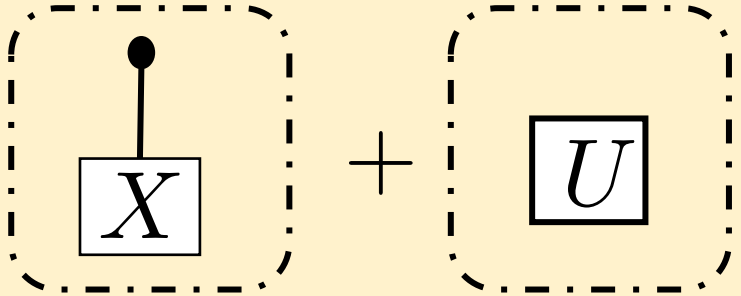
Map chain of Pauli to another

Can be classically simulated! (Gottesman-Knill Th)

Clifford gates + T



CNOT + Almost any 1-qubit gate



Almost any 2-qubit gate

Certainly not practical!

Hardness of General U

Shannon: almost all Boolean function require $\approx 2^n$ gates.

Solovay-Kitaev Theorem

$\exists$quantum circuits that require $\Omega(2^n \log(1/\epsilon)/\log(n))$ gates.

We will be interested in those

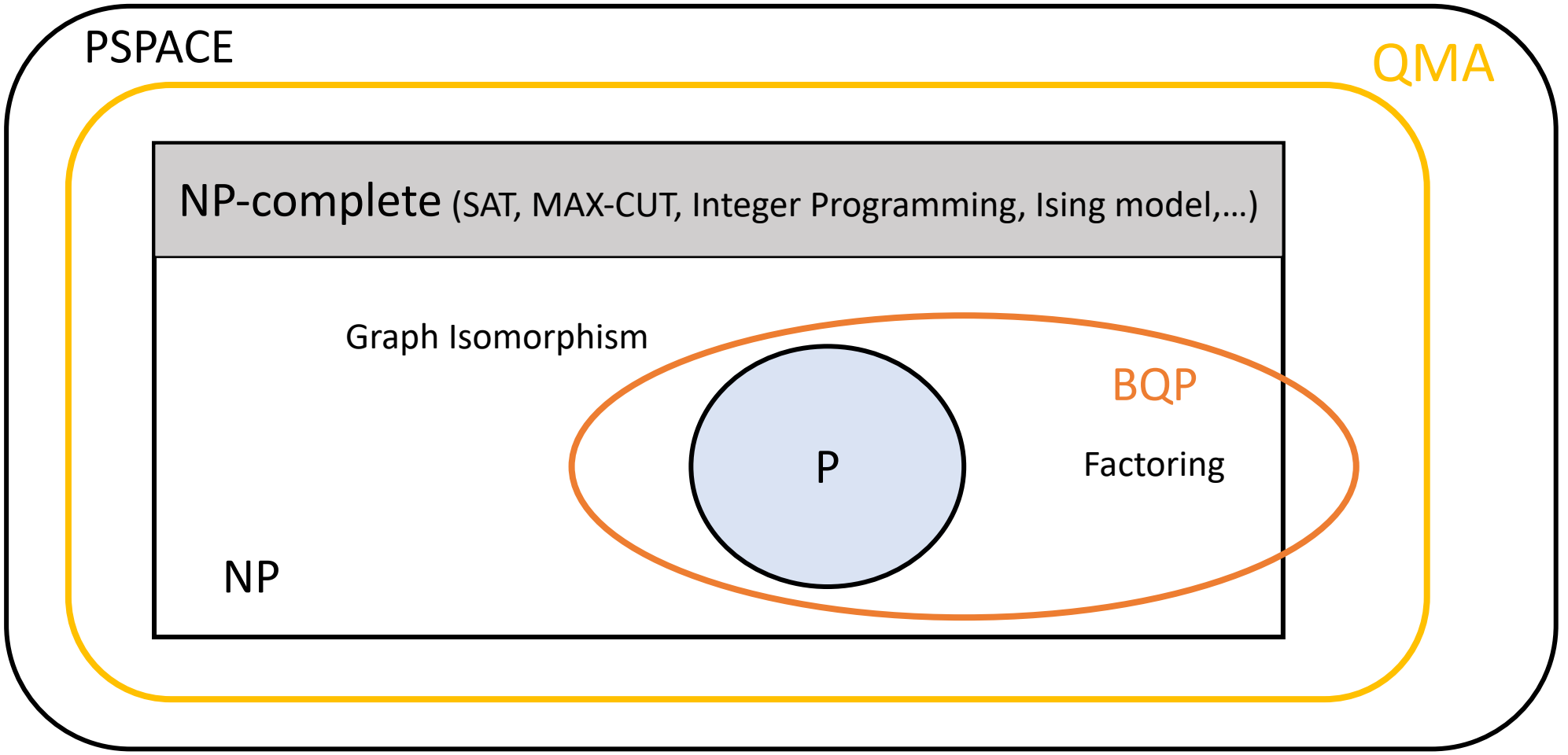
that can be generated with poly(n) gates.

Hardness of General U

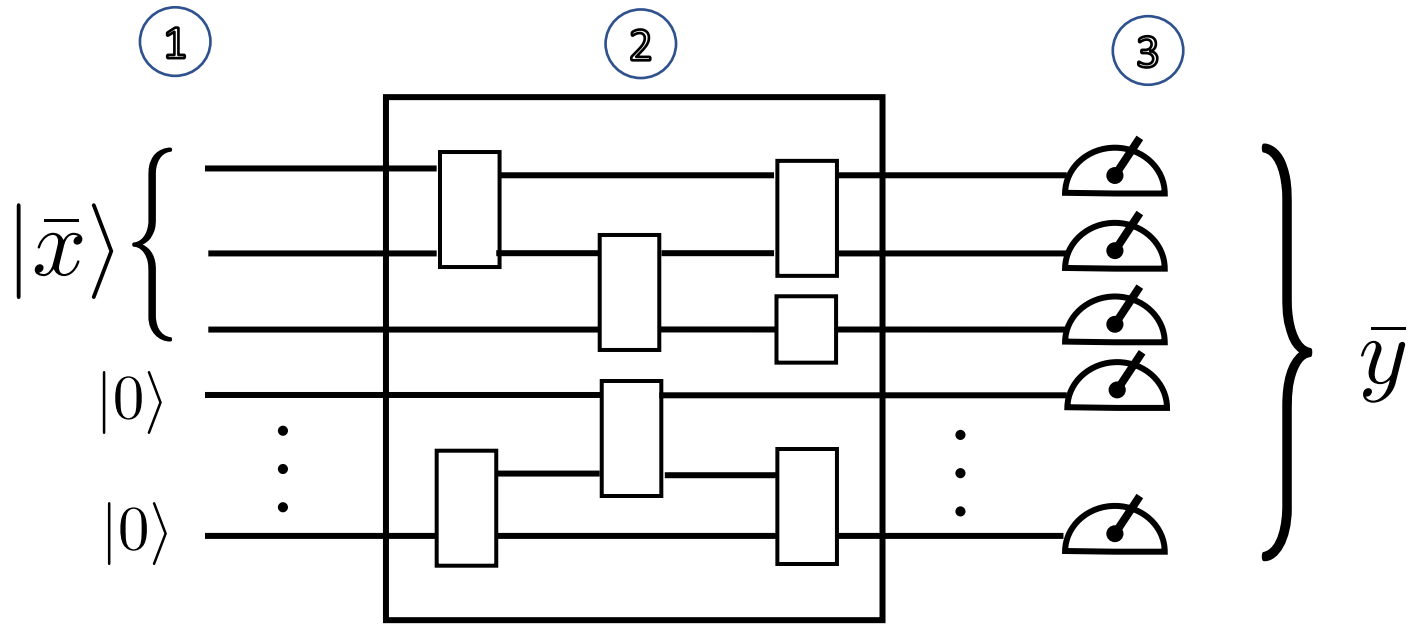
QMA: A quantum analogue of NP

Verifying that $|\psi\rangle$ satisfies a property can be done efficinetly.

Generating the state that satisfies it is hard.



Quantum Algorithms

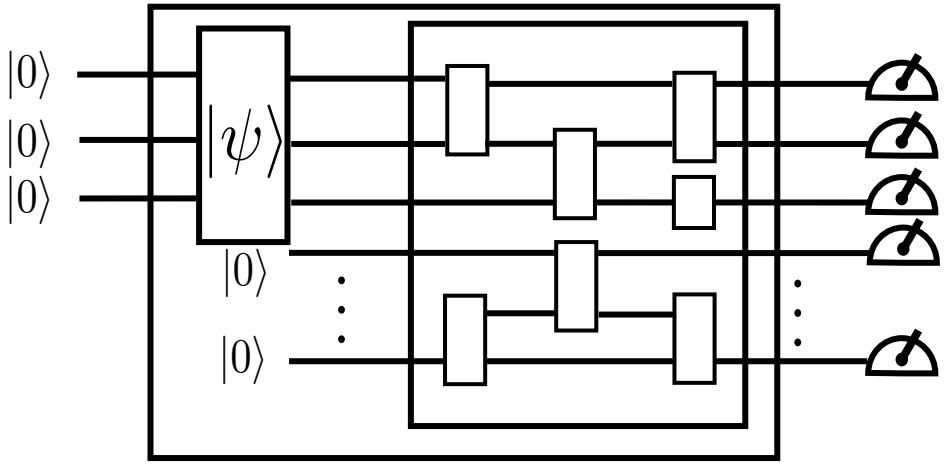


1. Preparation of an n qubit computational state
2. Quantum circuit from a universal set of gates
3. Measurement in the computational basis

Efficient if #gates is $O(\text{poly}(n))$.

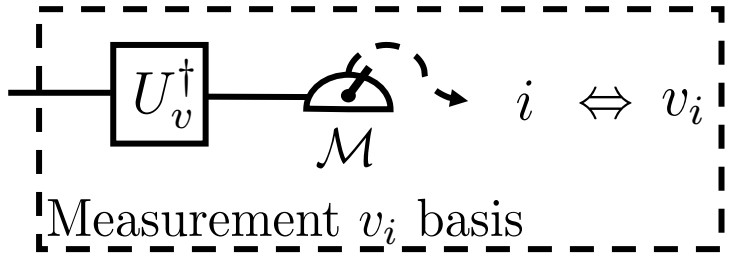
Generality of the model

- Preparation of another state?
  Include the preparation in the circuit



- Qubit not measured
  Measure and forget

- Measurement in another basis?



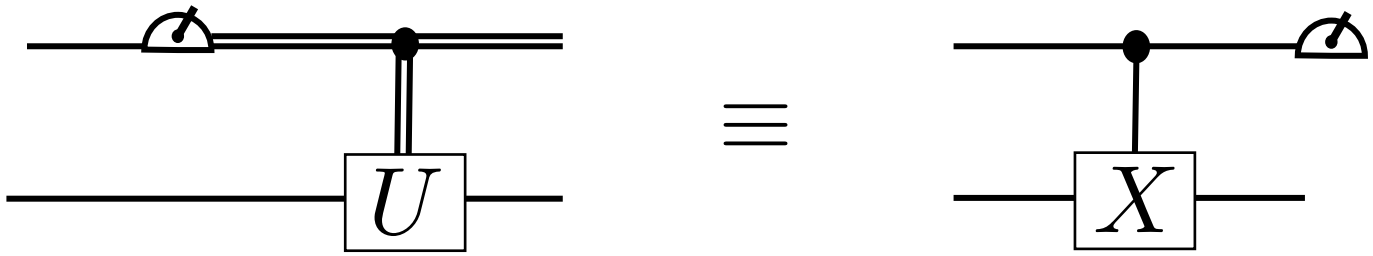
- General measurement?
  Additional extra qubits, gates and computational measurement.

- Intermediate measurement in the circuit?
  Postpone measurements to the end

- Irreversible quantum operations?
  Equivalent to reversible operation with an additional quantum system (environment).

Principle of deferred measurement

An intermediate measurement, even if its classical outcome controls further operations, can always be postponed to the end of the circuit.



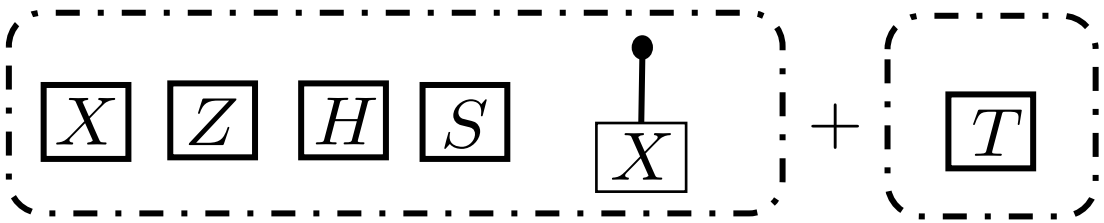
We will discuss quantum algorithms in an ideal framework without error. Then both are equivalent.

In practice you want your quantum circuit as small as short.

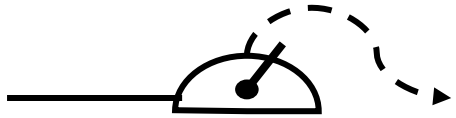
DiVincenzo criteria for Quantum Computation

- Well-defined qubits

- Initialization to a pure state $|000...0\rangle$
- Long coherence times $\frac{1}{\sqrt{2}}(|000...0\rangle + |111...1\rangle)$
- Universal set of gates



- Single qubit measurements



References

This lecture is supposed to be self-contained and there is no associate reading to it. Nonetheless, we provide references for those wanting to explore further the topic.

Further references

1. Quantum circuit model NC 4.2-4.4
2. Universal quantum gates NC 4.5; David Deutsch, Adriano Barenco, and Artur Ekert, Universality in quantum computation, Proc. R. Soc. London A, 449:669–677, 1995.
3. Principle of deferred measurement NC page 186 + Exercise 4.35
4. DiVincenzo criteria for QC: D. P. Divincenzo, Mesoscopic Electron Transport, chapter Topics in Quantum Computers, pages 657–677 (1997), arXiv:cond-mat/9612126.
5. For QMA start with Wikipedia
    1. Quantum NP - A Survey, Dorit Aharonov and Tomer Naveh, arXiv:quant-ph/0210077v1
    2. Watrous, John (2009). "Quantum Computational Complexity", arXiv:0804.3401.

NC ≡ Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information
Cambridge University Press (2010)