

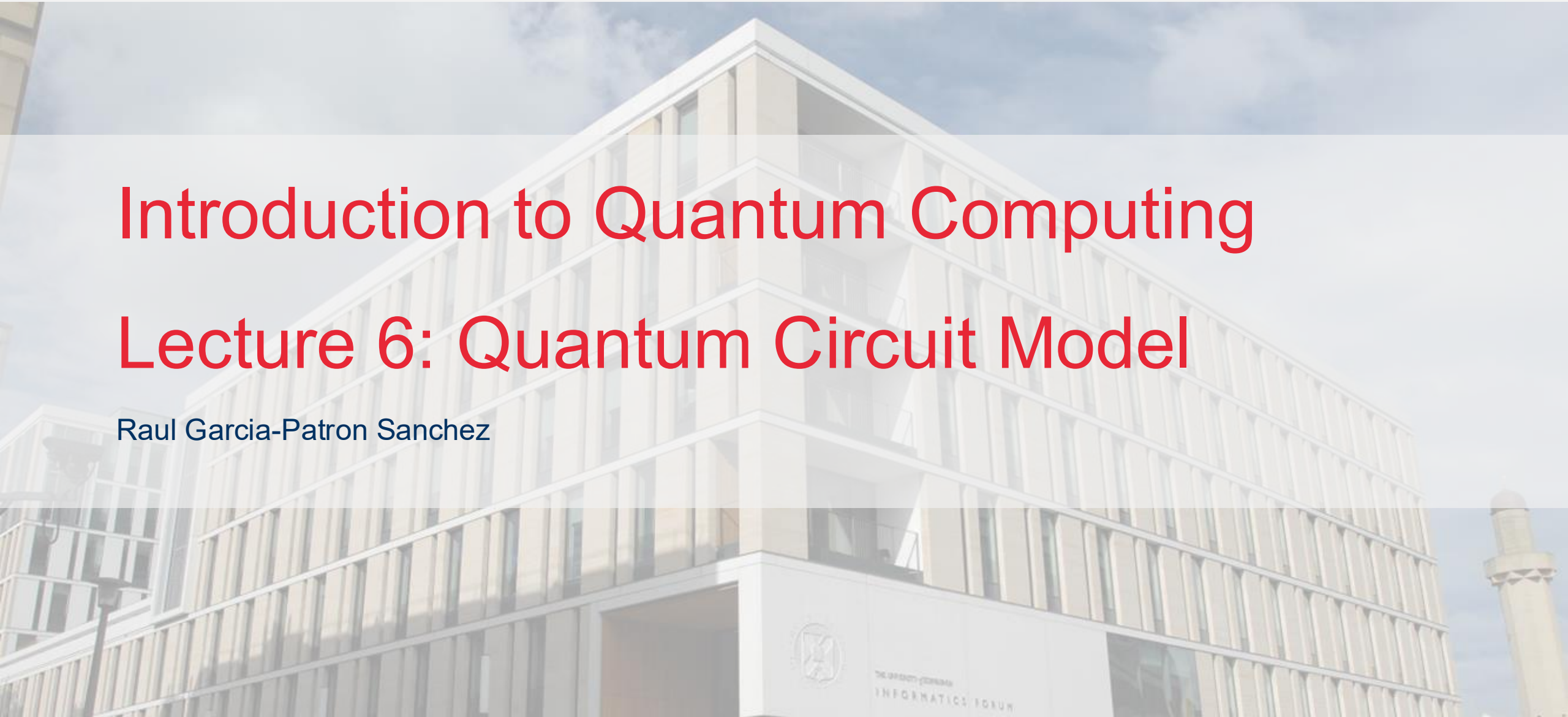


THE UNIVERSITY of EDINBURGH
informatics

Introduction to Quantum Computing

Lecture 6: Quantum Circuit Model

Raul Garcia-Patron Sanchez



Postulate I: Quantum states

A quantum state with d degrees of freedom is represented by a vector in a complex vector space with inner-product (Hilbert space)

$$|\psi\rangle \in \mathcal{H} \equiv \mathbb{C}^d \qquad \langle\psi|\psi\rangle = 1$$

Hilbert space = Complex Vector Space + Inner-product

State vector $|\psi\rangle \equiv \begin{bmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{d-1} \end{bmatrix}$

A d -dimensional vector of complex numbers

- Qubit: $d = 2$
- Qudit: $d > 2$
- N qubits: $d = 2^N$

$\psi_i \in \mathbb{C}$: Probability amplitude of degree of freedom i

$$P(i) = |\psi_i|^2$$

Postulate II: Quantum operations

The evolution of a quantum system $|\psi\rangle \in \mathcal{H} \equiv \mathbb{C}^d$ is given by a unitary transformation $U : \mathcal{H} \rightarrow \mathcal{H}$, s.t. $|\psi_{out}\rangle = U|\psi_{in}\rangle$

Unitary matrices

$$UU^\dagger = U^\dagger U = I_d$$

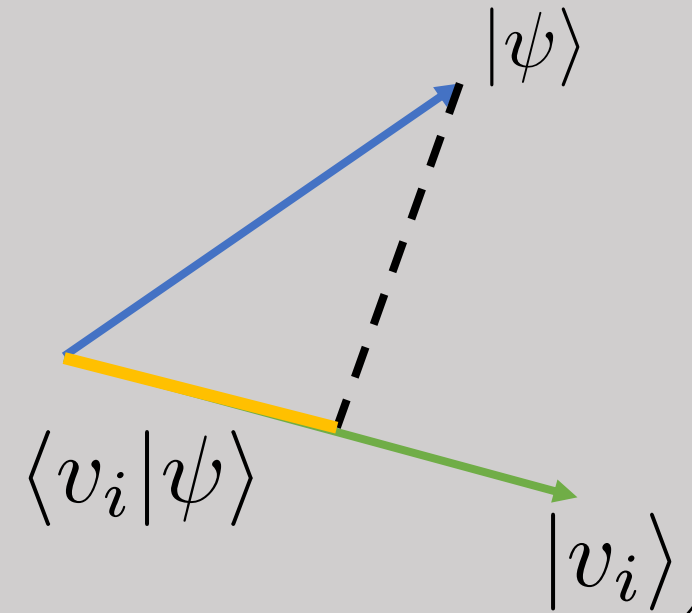
- Linear operator $U : \mathcal{H} \rightarrow \mathcal{H}$
- Preserves the inner-product
- Equivalent of orthogonal matrices on real vector spaces

Measurement of orthonormal basis

Any orthonormal basis $\{|v_i\rangle\}$ that span $\mathcal{H}$ has an associated measurement

Probability of outcome i reads: $P(i) = |\langle v_i | \psi \rangle|^2$

The quantum state is updated to $|v_i\rangle$



Composition of quantum systems

Two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ can form a new Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ s.t. $\dim \mathcal{H}_{AB} = \dim \mathcal{H}_A \times \dim \mathcal{H}_B$.

A basis of $\mathcal{H}_{AB}$ is built via tensor product of basis of $\mathcal{H}_A$ and $\mathcal{H}_B$.

An operator $\mathcal{L}(\mathcal{H}_{AB})$ is built via linear combinations of tensor product of operators from $\mathcal{L}(\mathcal{H}_A)$ and $\mathcal{L}(\mathcal{H}_B)$.

$$\forall |\psi_{AB}\rangle \in \mathcal{H}_{AB} : |\psi_{AB}\rangle = \sum_{i,j} \psi_{i,j} |i\rangle \otimes |j\rangle$$

$$\forall U \in \mathcal{L}(\mathcal{H}_{AB}), \exists \{V_i\} \in \mathcal{L}(\mathcal{H}_A) \text{ and } \{W_i\} \in \mathcal{L}(\mathcal{H}_B) : U = \sum_i V_i \otimes W_i$$



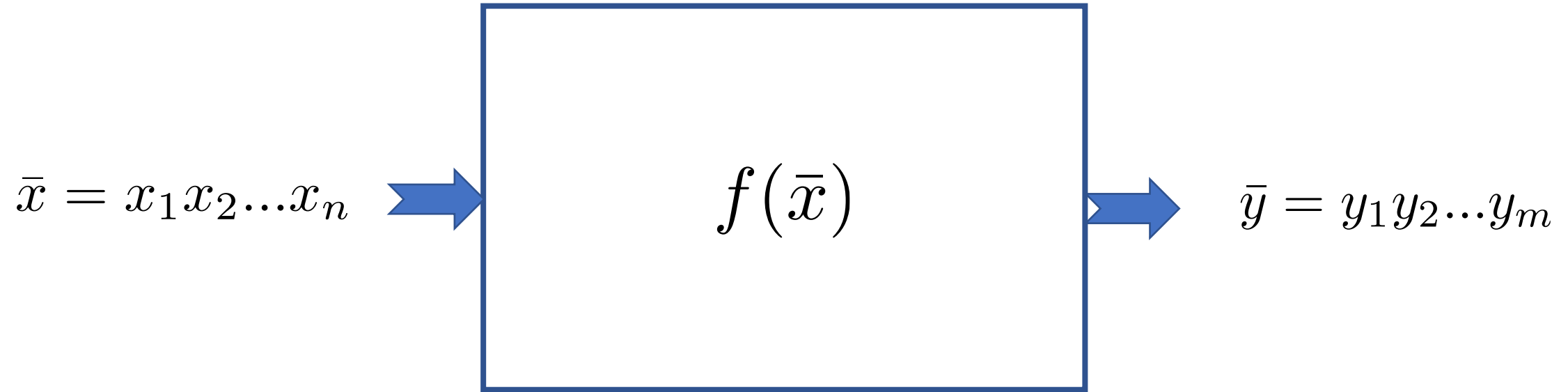
THE UNIVERSITY of EDINBURGH
informatics

Circuit Model



Classical Circuit Model

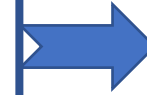
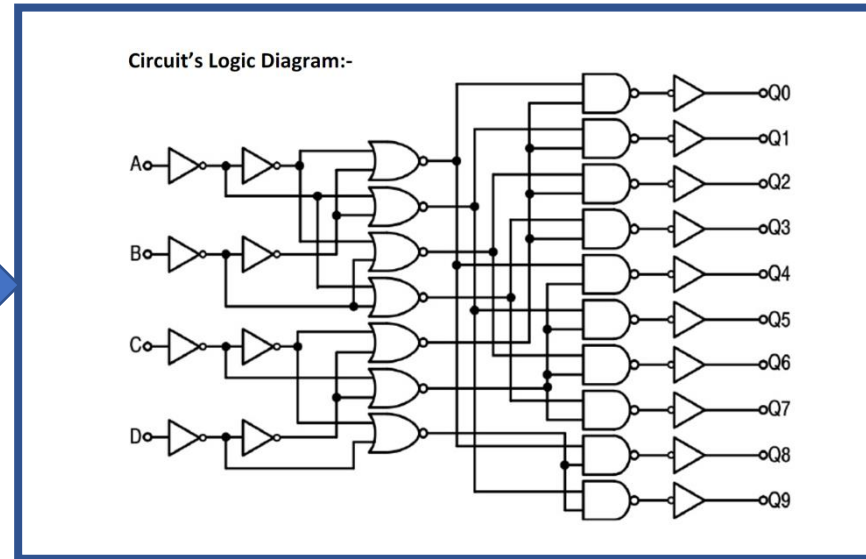
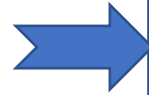
- Classical circuits compute Boolean functions: $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$



Classical Circuit Model

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

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



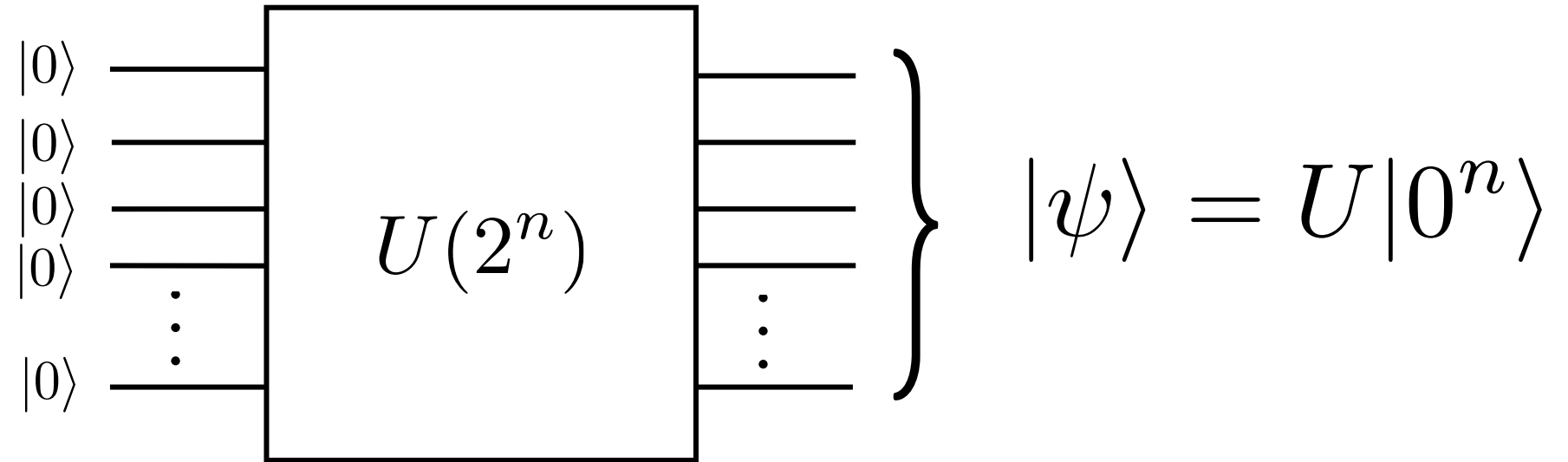
$$\bar{y} = y_1 y_2 \dots y_m$$

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

All Boolean functions can be generated with NAND gates.

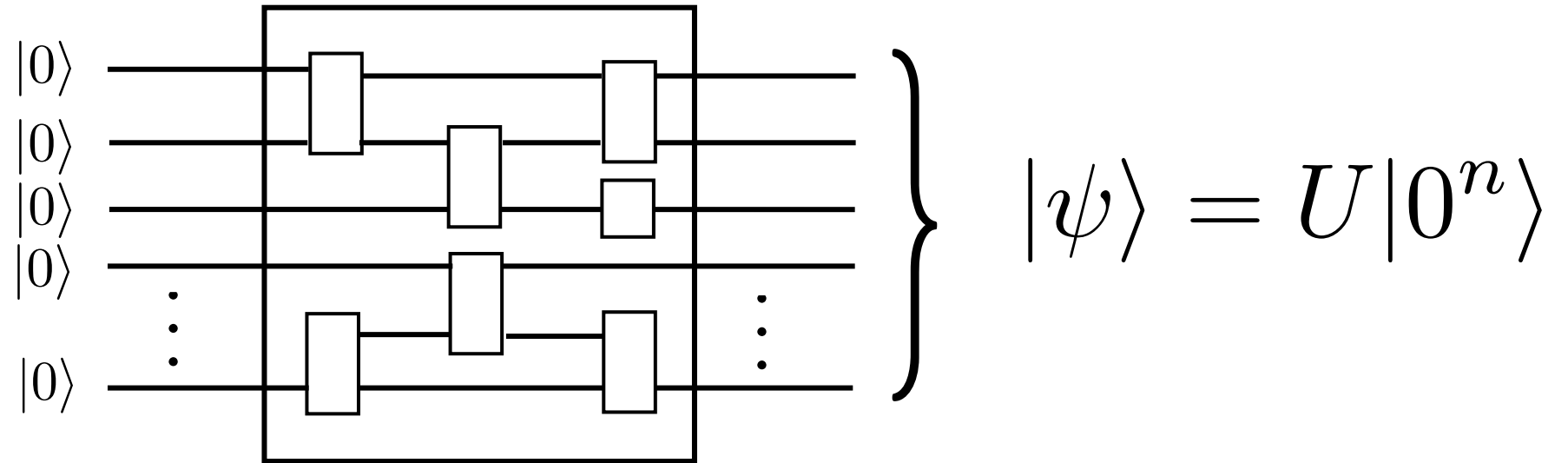
Quantum Circuit Model

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



Quantum Circuit Model

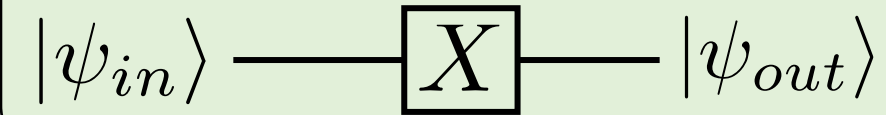
- Quantum circuits implement unitaries, $U : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n}$



- $\exists$ 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.

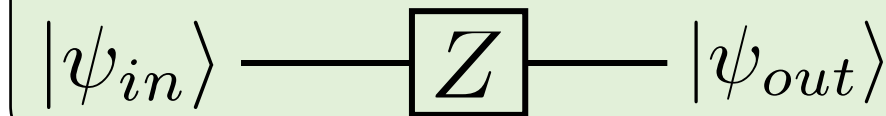
1-qubit gates

NOT gate



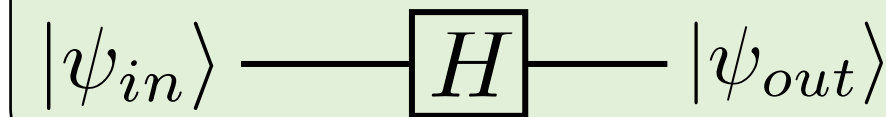
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

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

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

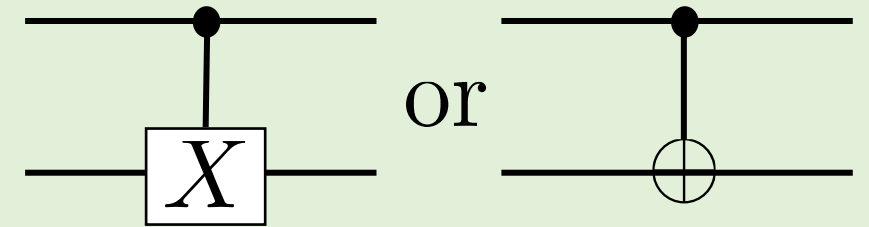
$$R_{\theta} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

Entangling operations

- $\exists U_{AB} \in \mathcal{L}(\mathcal{H}_{AB})$ s.t. $\nexists U_A \in \mathcal{L}(\mathcal{H}_A)$ and $U_B \in \mathcal{L}(\mathcal{H}_B) : U_{AB} = U_A \otimes U_B$

Controlled-NOT gate (CNOT gate):

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



- $\forall U \in \mathcal{L}(\mathcal{H}_{AB}), \exists \{V_i\} \in \mathcal{L}(\mathcal{H}_A)$ and $\{W_i\} \in \mathcal{L}(\mathcal{H}_B) : U = \sum_i V_i \otimes W_i$

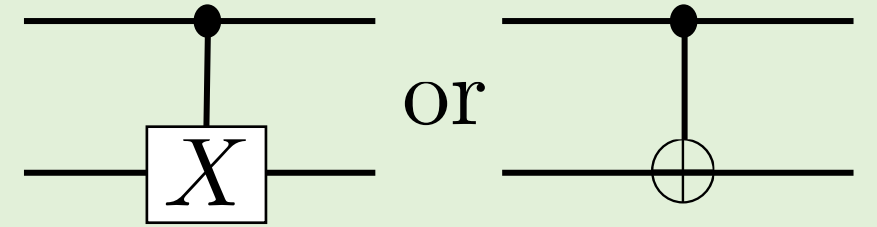
Outer-products (Dirac notation)

$$\begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} = a_{00} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + a_{01} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + a_{10} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + a_{11} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$
$$= a_{00}|0\rangle\langle 0| + a_{01}|0\rangle\langle 1| + a_{10}|1\rangle\langle 0| + a_{11}|1\rangle\langle 1|$$

$ 0\rangle\langle 0 \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$	$ 0\rangle\langle 1 \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$
$ 1\rangle\langle 0 \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$	$ 1\rangle\langle 1 \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Entangling operations

Controlled-not gate (cnot gate):



$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes I + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes X = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

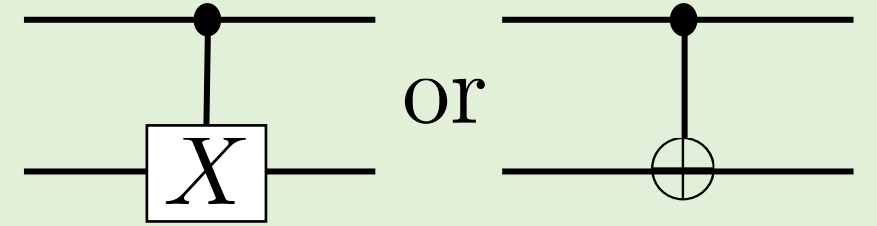
$$|0\rangle\langle 0| \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$|1\rangle\langle 1| \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Gates: 2-qubit

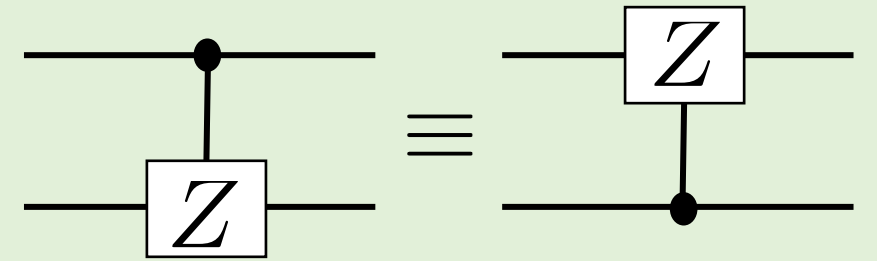
Controlled-not gate (cnot gate):

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



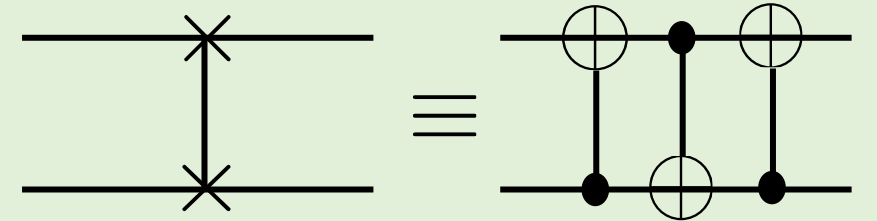
Controlled-Z gate:

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



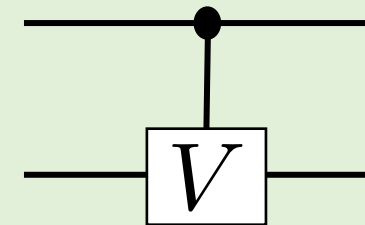
SWAP (permutation) gate

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



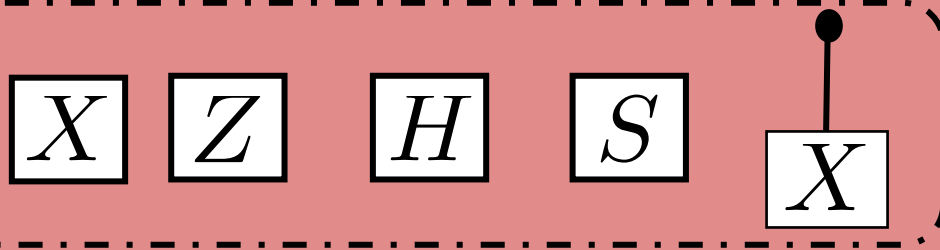
Controlled-V gate:

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



Universal sets of gates – Clifford + T gates

Clifford Gates

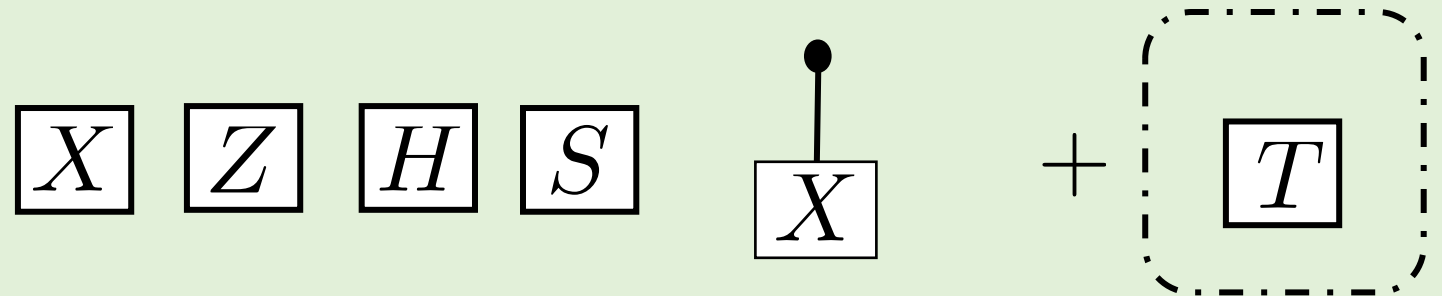


Very important role in QC: QEC
(Quantum Error Correction)

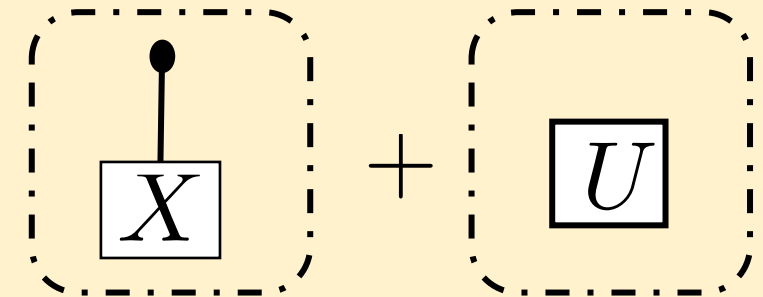
Map chain of Pauli to another

Can be classically simulated! (Gottesman-Knill Th)

Clifford gates + T



CNOT + Almost any 1-qubit gate



Almost any 2-qubit gate

Certainly not practical!

Universal sets of gates – CNOT and General Phase gates + Hadamard

CNOT and Phase Gates



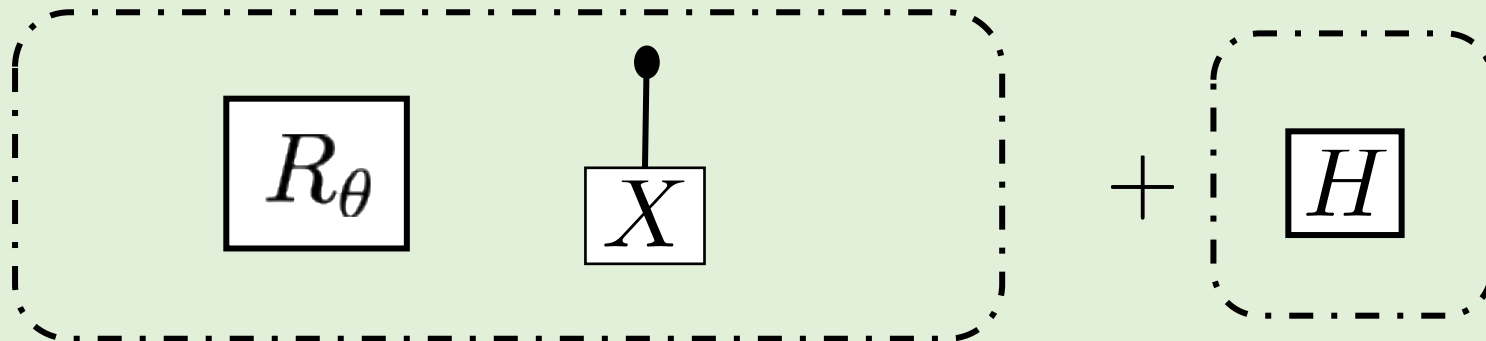
$$U : |\bar{x}\rangle \rightarrow e^{i\phi(\bar{x})} |L\bar{x}\rangle$$

General Phase Gates

$$R_\theta$$

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

CNOT and Phase Gates + Hadamard



Hardness of General U

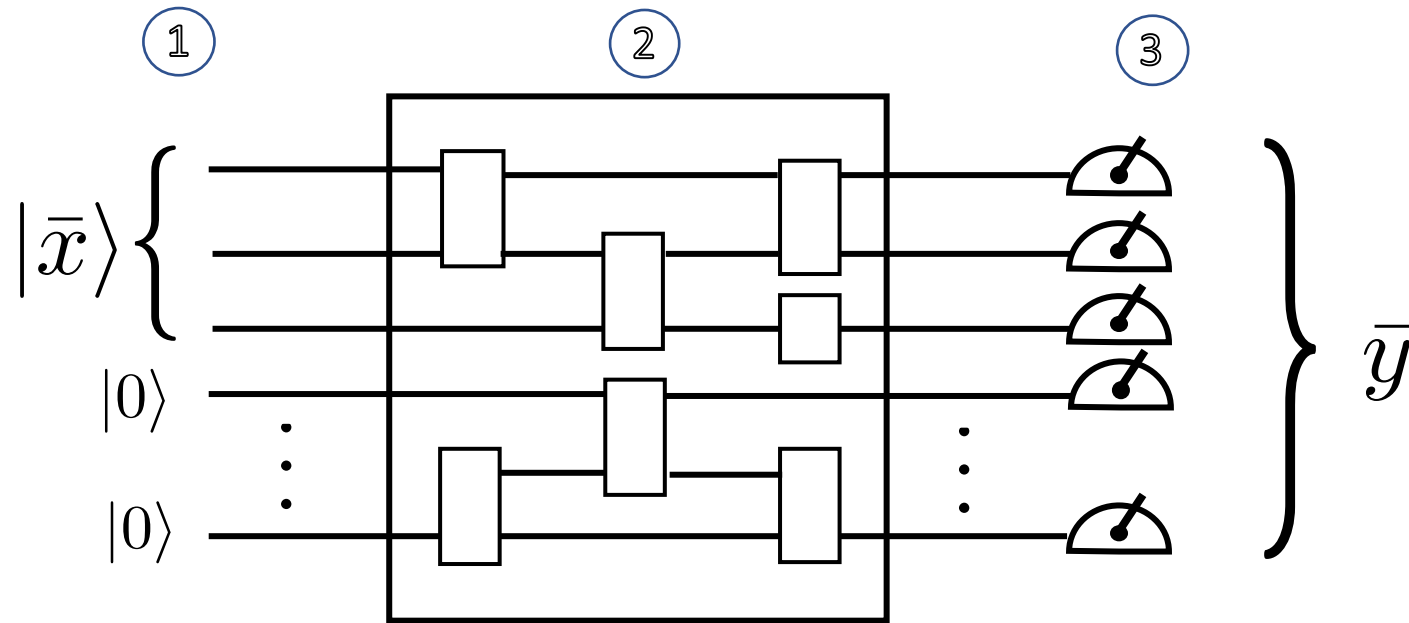
Shannon: almost all Boolean function require $\approx 2^n$ gates.

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 $\text{poly}(n)$ gates.

Quantum Algorithms

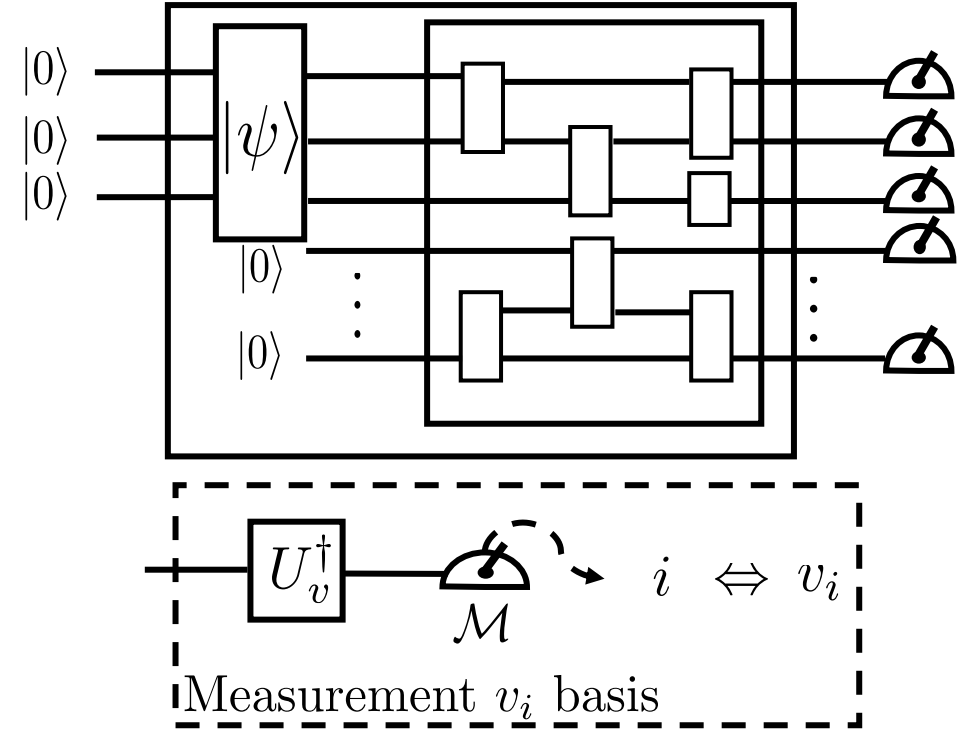


- ① Preparation of an n qubit computational state
- ② Quantum circuit from a universal set of gates
- ③ Measurement in the computational basis

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?



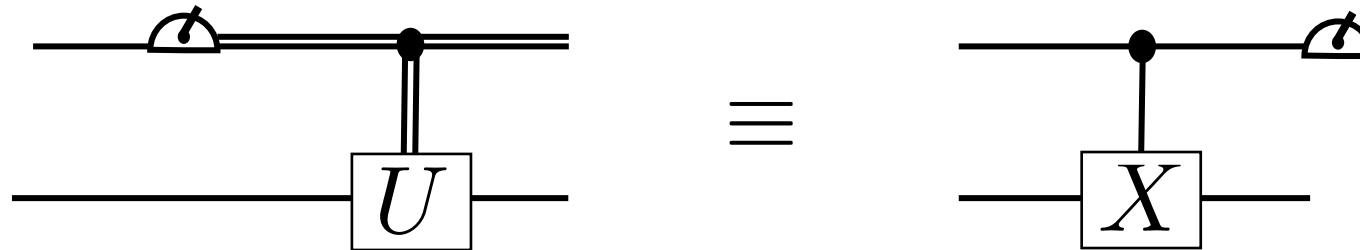
- General measurement?
Additional extra qubits, gates and computational measurement.

- 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



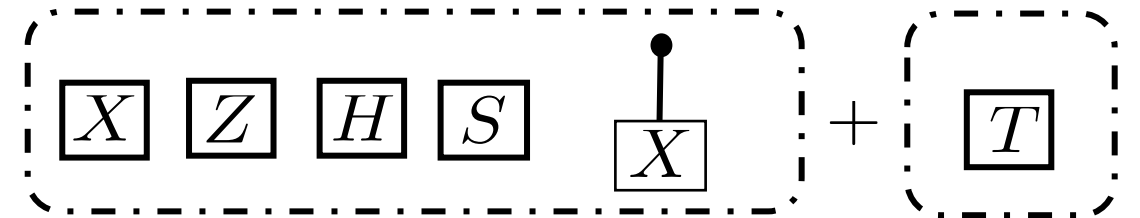
- Initialization to a pure state

$$|000\dots 0\rangle$$

- Long coherence times

$$\frac{1}{\sqrt{2}}(|000\dots 0\rangle + |111\dots 1\rangle)$$

- 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 $\equiv$ Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information
Cambridge University Press (2010)