

Quantum Computation

Michael A. Nielsen

University of Queensland



Goals:

1. To explain the quantum circuit model of computation.
2. To explain Deutsch's algorithm.
3. To explain an alternate model of quantum computation based upon measurement.

What does it mean to compute?

Church-Turing thesis: An algorithmic process or computation is what we can do on a Turing machine.



Deutsch (1985):

Can we justify C-T thesis using laws of physics?

Quantum mechanics seems to be very hard to simulate on a classical computer.

Might it be that computers exploiting quantum mechanics are not efficiently simulatable on a Turing machine?

Violation of strong C-T thesis!

Might it be that such a computer can solve some problems faster than a probabilistic Turing machine?

Candidate universal computer: quantum computer

The Church-Turing-Deutsch principle

Church-Turing-Deutsch principle: Any physical process can be efficiently simulated on a quantum computer.

Research problem: Derive (or refute) the Church-Turing-Deutsch principle, starting from the laws of physics.

Models of quantum computation

There are many models of quantum computation.

Historically, the first was the **quantum Turing machine**, based on classical Turing machines.

A more convenient model is the **quantum circuit** model.

The quantum circuit model is mathematically equivalent to the quantum Turing machine model, but, so far, human intuition has worked better in the quantum circuit model.

There are also many other interesting alternate models of quantum computation!

Quantum circuit model

Classical


Unit: bit

1. Prepare n -bit input
2. 1- and 2-bit logic gates
3. Readout value of bits

Quantum

Unit: qubit

1. Prepare n -qubit input in the computational basis.
2. Unitary 1- and 2-qubit quantum logic gates
3. Readout partial information about qubits

$$|x_1, x_2, \dots, x_n\rangle$$




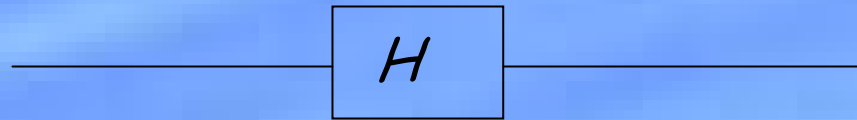
External control by a classical computer.

Single-qubit quantum logic gates

Pauli gates

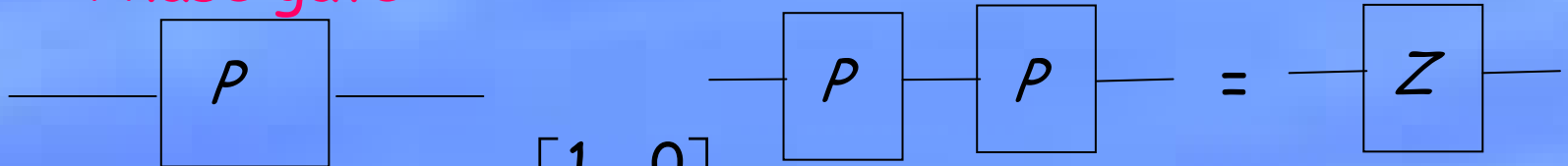
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Hadamard gate



$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}; \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}; \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

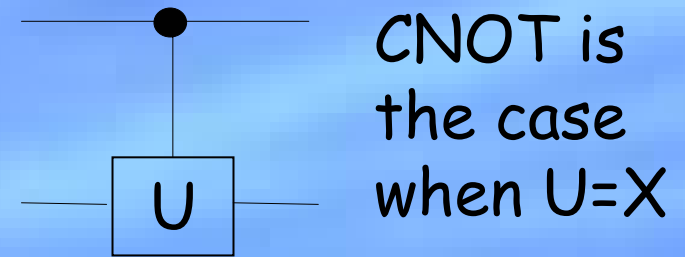
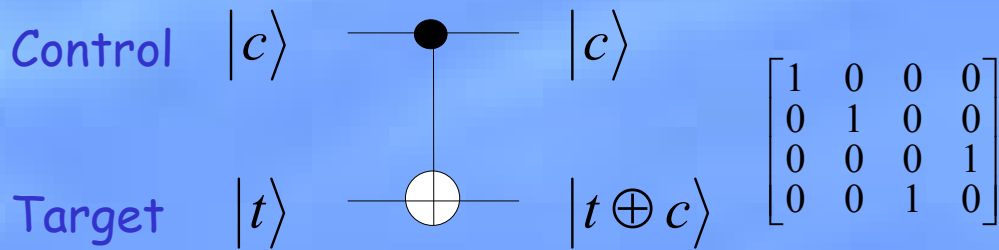
Phase gate



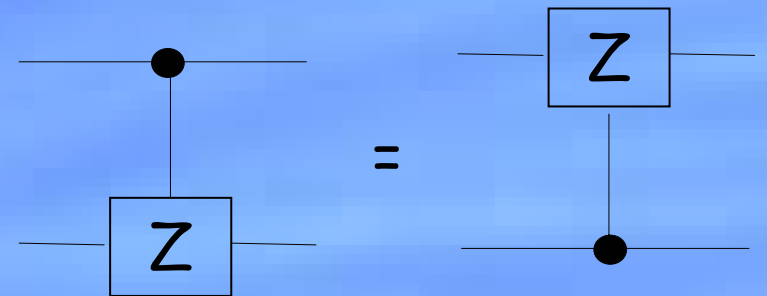
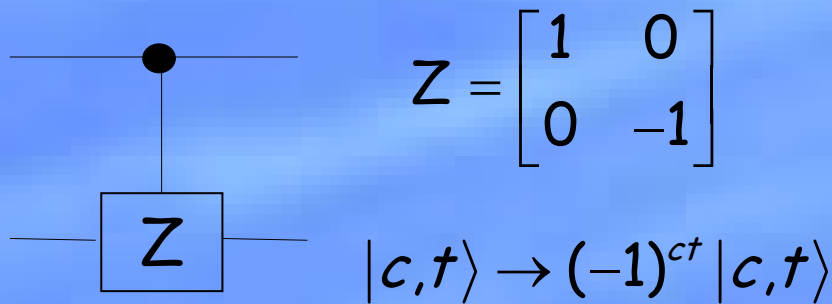
$$P|0\rangle = |0\rangle; \quad P|1\rangle = i|1\rangle \quad P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$P^2 = Z$$

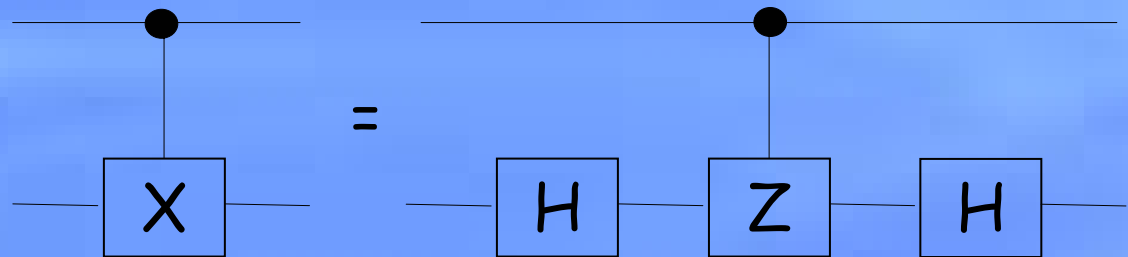
Controlled-not gate



Controlled-phase gate

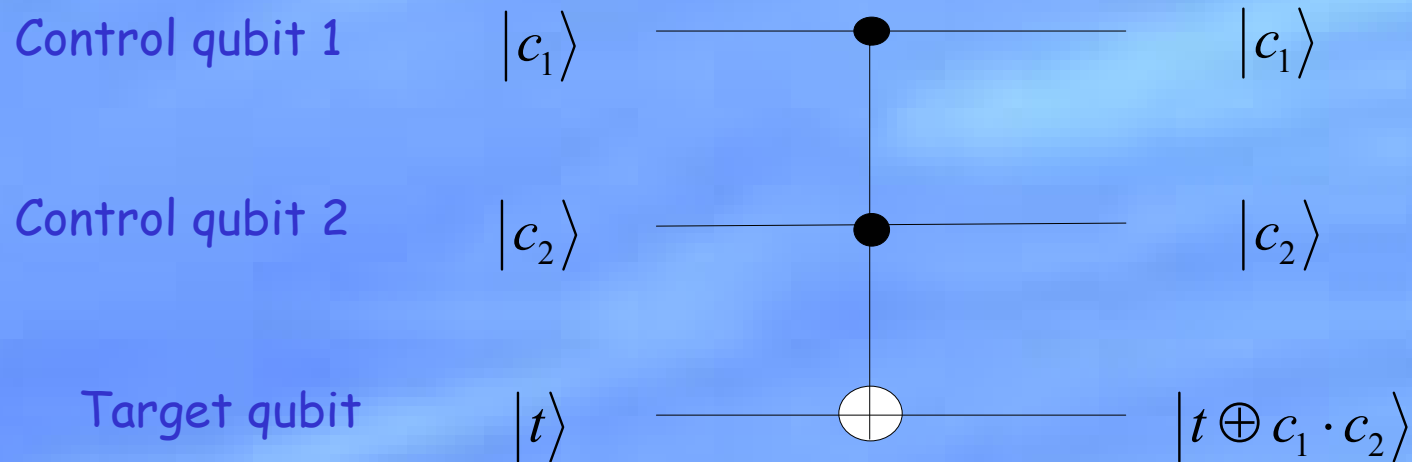


Symmetry makes the controlled-phase gate more natural for implementation!



Exercise: Show that $HZH = X$.

Toffoli gate



Worked Exercise: Show that all permutation matrices are unitary. Use this to show that any classical reversible gate has a corresponding unitary quantum gate.

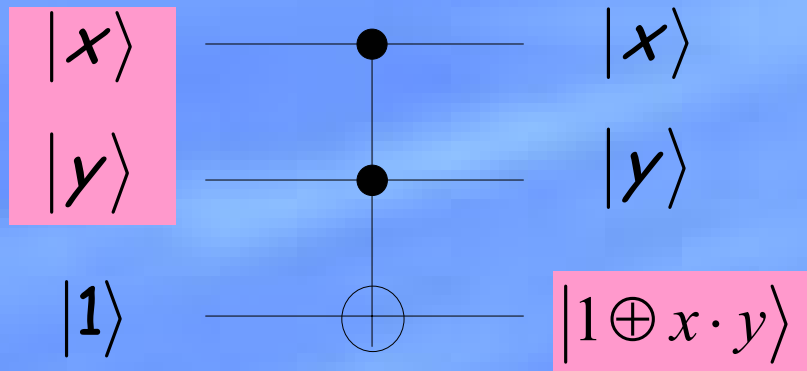
Challenge exercise: Show that the Toffoli gate can be built up from controlled-not and single-qubit gates.

Cf. the classical case: it is not possible to build up a Toffoli gate from reversible one- and two-bit gates.

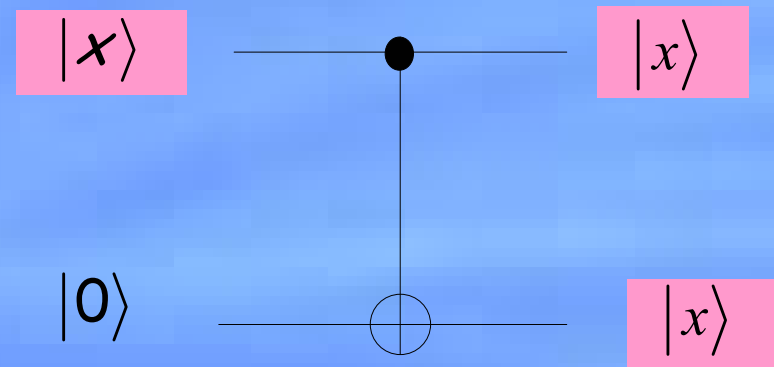
How to compute classical functions on quantum computers

Use the quantum analogue of classical reversible computation.

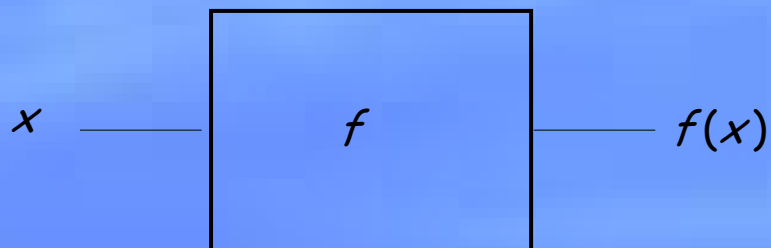
The quantum NAND



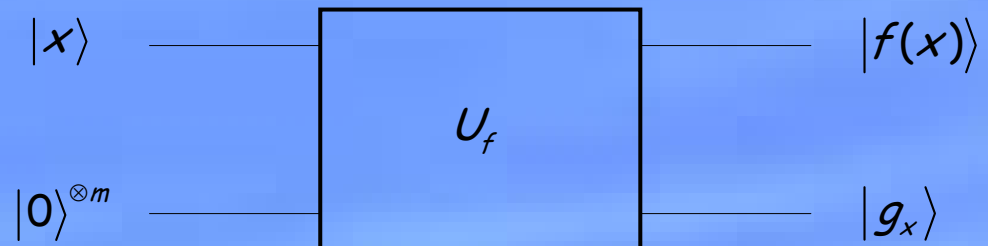
The quantum fanout



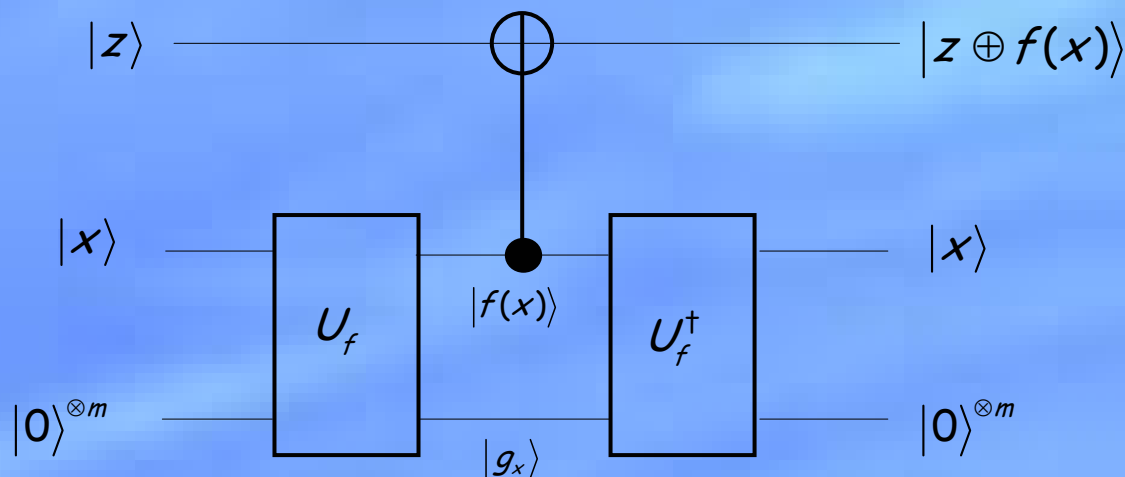
Classical circuit



Quantum circuit



Removing garbage on quantum computers



Canonical form: $|x\rangle|z\rangle \rightarrow |x\rangle|z \oplus f(x)\rangle$

Example: $|x\rangle|z\rangle \rightarrow |x\rangle|z \oplus \text{parity}(x)\rangle$

Given an "easy to compute" classical function, there is a routine procedure we can go through to translate the classical circuit into a quantum circuit computing the canonical form.

Example: Deutsch's problem

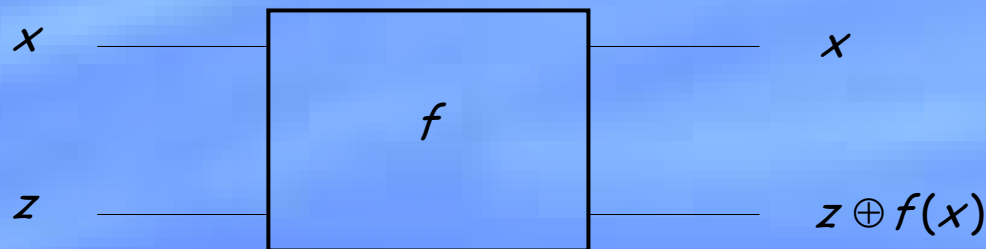
Given a **black box** computing a function $f : \{0,1\} \rightarrow \{0,1\}$

Our task is to determine whether f is **constant** or **balanced**?

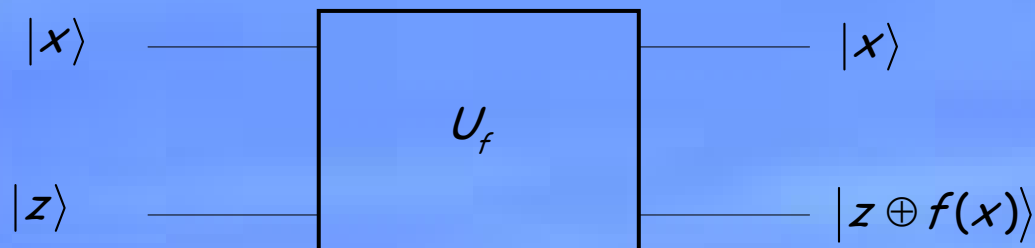
Classically we need to evaluate **both** $f(0)$ and $f(1)$.

Quantumly we need only use the black box for $f(\bullet)$ **once**!

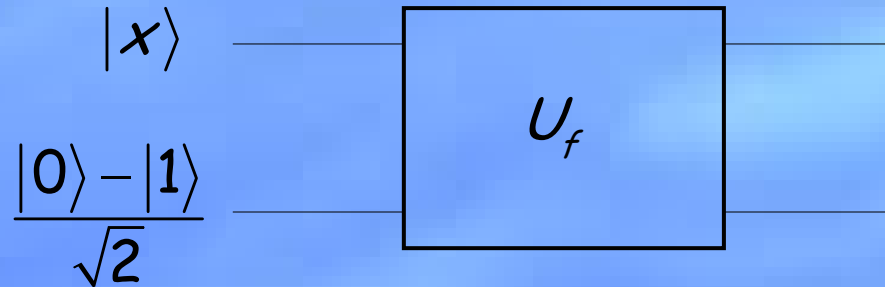
Classical black box



Quantum black box



Putting information in the phase



$f(x) = 0$:

$$|x\rangle(|0\rangle - |1\rangle) \rightarrow |x\rangle(|0\rangle - |1\rangle)$$

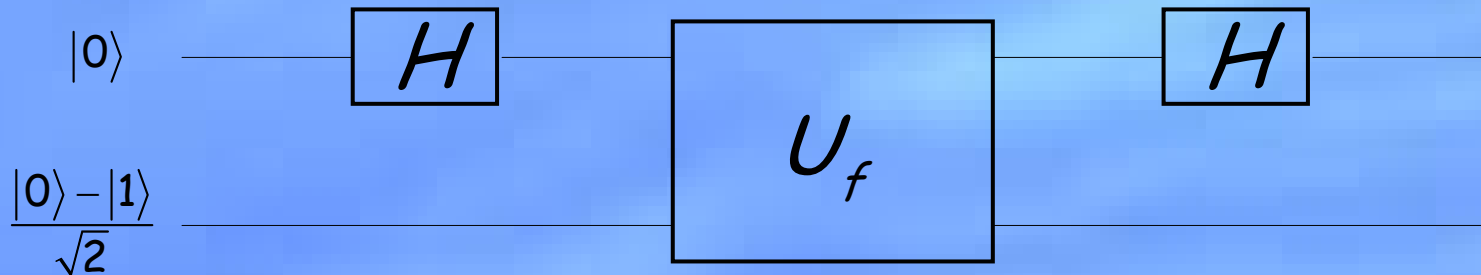
$f(x) = 1$:

$$|x\rangle(|0\rangle - |1\rangle) \rightarrow |x\rangle(|1\rangle - |0\rangle) = -|x\rangle(|0\rangle - |1\rangle)$$

$$|x\rangle(|0\rangle - |1\rangle) \rightarrow (-1)^{f(x)} |x\rangle(|0\rangle - |1\rangle)$$

$$|x\rangle \rightarrow (-1)^{f(x)} |x\rangle$$

Quantum algorithm for Deutsch's problem



Quantum parallelism

$$|0\rangle \rightarrow |0\rangle + |1\rangle$$

$$\rightarrow (-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle$$

$$\rightarrow (-1)^{f(0)} (|0\rangle + |1\rangle) + (-1)^{f(1)} (|0\rangle - |1\rangle)$$

$$= \left[(-1)^{f(0)} + (-1)^{f(1)} \right] |0\rangle + \left[(-1)^{f(0)} - (-1)^{f(1)} \right] |1\rangle$$

f constant \Rightarrow all amplitude in $|0\rangle$.

f balanced \Rightarrow all amplitude in $|1\rangle$.

Research problem: What makes quantum computers powerful?

Universality in the quantum circuit model

Classically, any function $f(x)$ can be computed using just nand and fanout; we say those operations are **universal** for classical computation.

Suppose U is an **arbitrary** unitary transformation on n qubits.

Then U can be composed from controlled-not gates and single-qubit quantum gates.

Just as in the classical case, a counting argument can be used to show that there are unitaries U that take exponentially many gates to implement.

Research problem: Explicitly construct a class U_n of unitary operations taking exponentially many gates to implement.

Summary of the quantum circuit model

Input: An n -bit string, x , representing an instance of some problem.

Example: x is a number to be factored.

Initial state: $|0\rangle^{\otimes m}$, where m is some computable function of n .

Circuit: A circuit of single-qubit and controlled-not gates is applied to the qubits. The sequence of gates applied is under the control of an external classical computer, and may depend upon the problem instance x .

Readout: Some fixed subset of the qubits is measured in the computational basis at the end of the computation, and the output constitutes the solution to the problem.

Example: For a decision problem, just the first qubit would be read out, to indicate "yes" or "no".

QP: The class of decision problems soluble by a quantum circuit of polynomial size, with polynomial classical overhead.

Quantum complexity classes

How does QP compare with P?

BQP: The class of decision problems for which there is a polynomial quantum circuit which outputs the correct answer ("yes" or "no") with probability at least $\frac{3}{4}$.

BPP: The analogous classical complexity class.

Research problem: Prove that BQP is strictly larger than BPP.

Research problem: What is the relationship of BQP to NP?

What is known: $BPP \subseteq BQP \subseteq PSPACE$

When will quantum computers be built?

Alternate models for quantum computation

Standard model: prepare a computational basis state, then do a sequence of one- and two-qubit unitary gates, then measure in the computational basis.

Research problem: Find alternate models of quantum computation.

Research problem: Study the relative power of the alternate models. Can we find one that is physically realistic and more powerful than the standard model?

Research problem: Even if the alternate models are no more powerful than the standard model, can we use them to stimulate new approaches to implementations, to error-correction, to algorithms (“high-level programming languages”), or to quantum computational complexity?

Overview:

Alternate models for quantum computation

Topological quantum computer: One creates pairs of “quasiparticles” in a lattice, moves those pairs around the lattice, and then brings the pair together to annihilate. This results in a unitary operation being implemented on the state of the lattice, an operation that depends only on the topology of the path traversed by the quasiparticles!

Quantum computation via entanglement and single-qubit measurements: One first creates a particular, fixed entangled state of a large lattice of qubits. The computation is then performed by doing a sequence of single-qubit measurements.

Overview:

Alternate models for quantum computation

Quantum computation as equation-solving: It can be shown that quantum computation is actually equivalent to counting the number of solutions to certain sets of quadratic equations (modulo 8)!

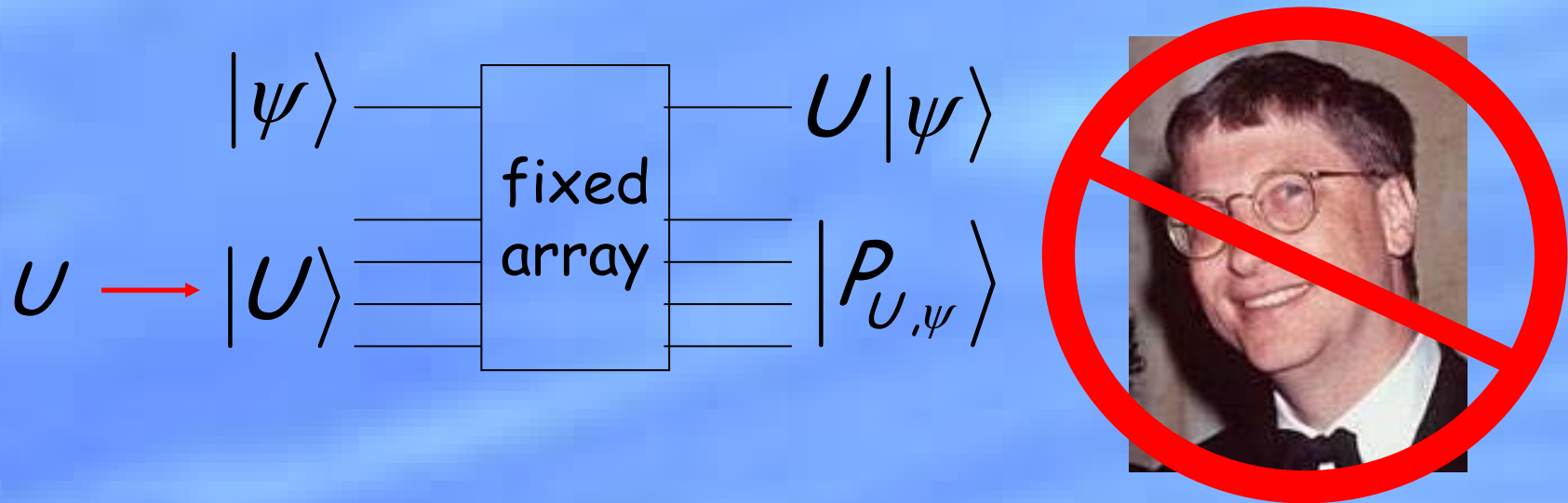
Quantum computation via measurement alone:

A quantum computation can be done simply by a sequence of two-qubit measurements. (No unitary dynamics required, except quantum memory!)

Further reading on the last model:

D. W. Leung, <http://xxx.lanl.gov/abs/quant-ph/0111122>

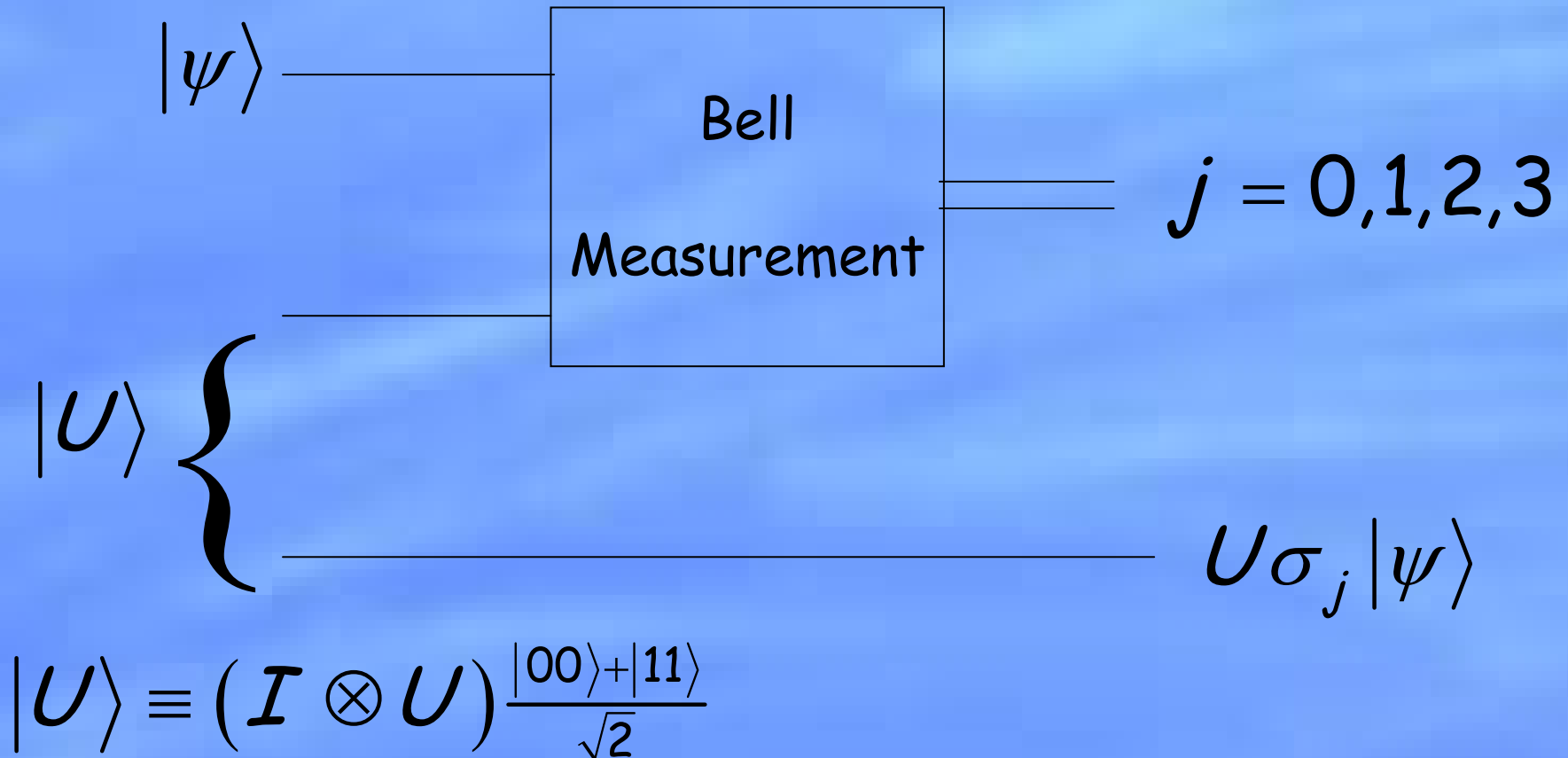
Can we build a programmable quantum computer?



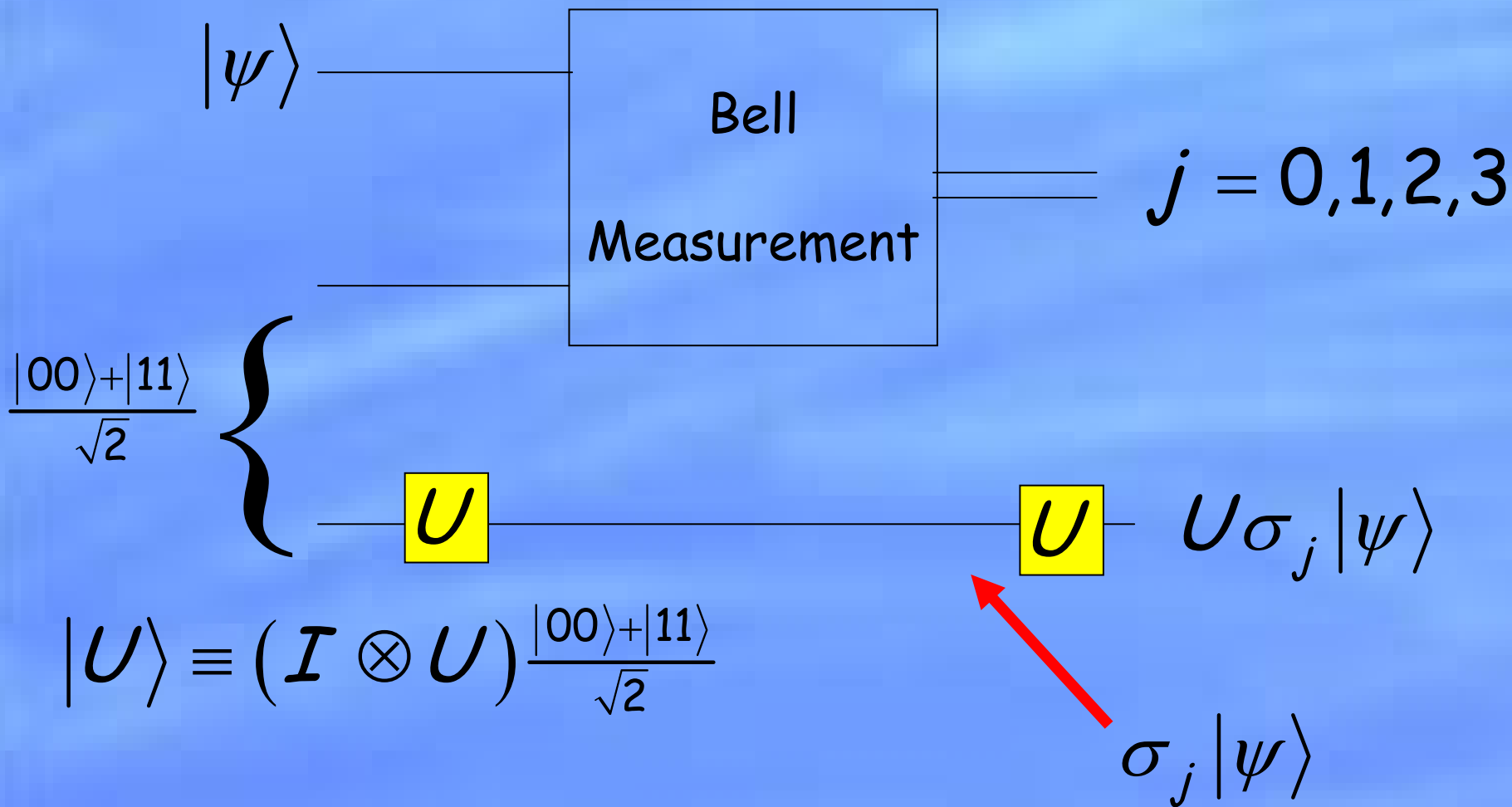
No-programming theorem: Unitary operators U_1, \dots, U_n which are distinct, even up to global phase factors, require orthogonal programs $|U_1\rangle, \dots, |U_n\rangle$.

Challenge exercise: Prove the no-programming theorem.

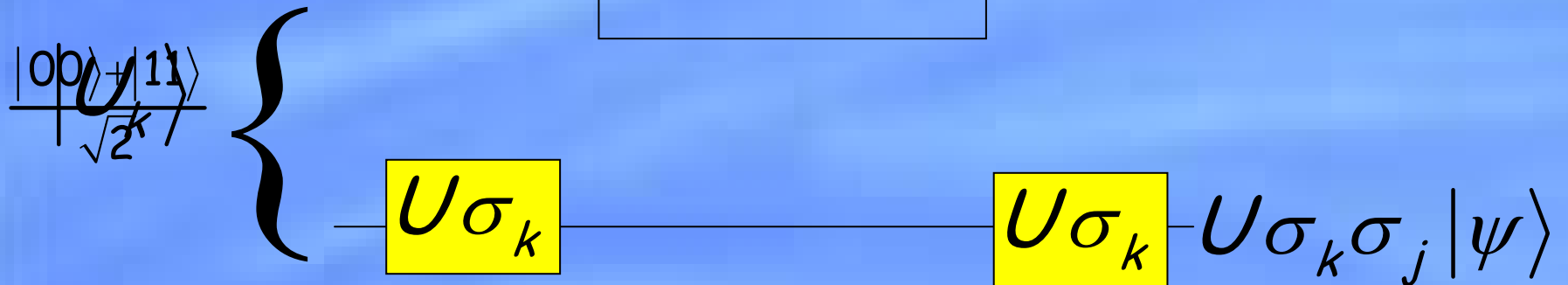
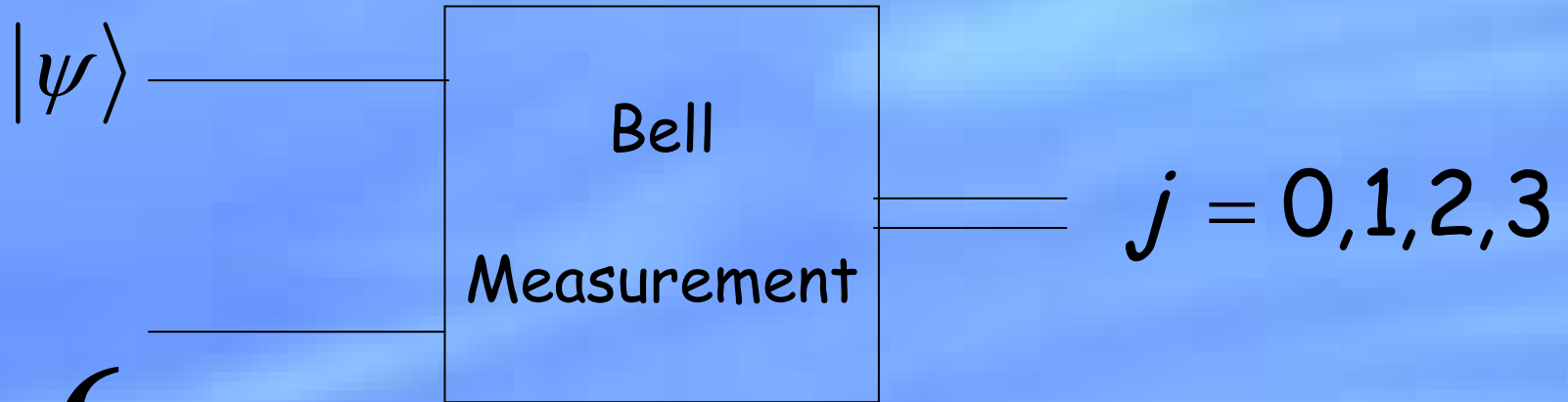
A stochastic programmable quantum computer



Why it works



How to do single-qubit gates using measurements alone



$$|U_k\rangle \equiv (\mathbf{I} \otimes U\sigma_k) \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

With probability $\frac{1}{4}$, $j = k$, and the gate succeeds.

Coping with failure

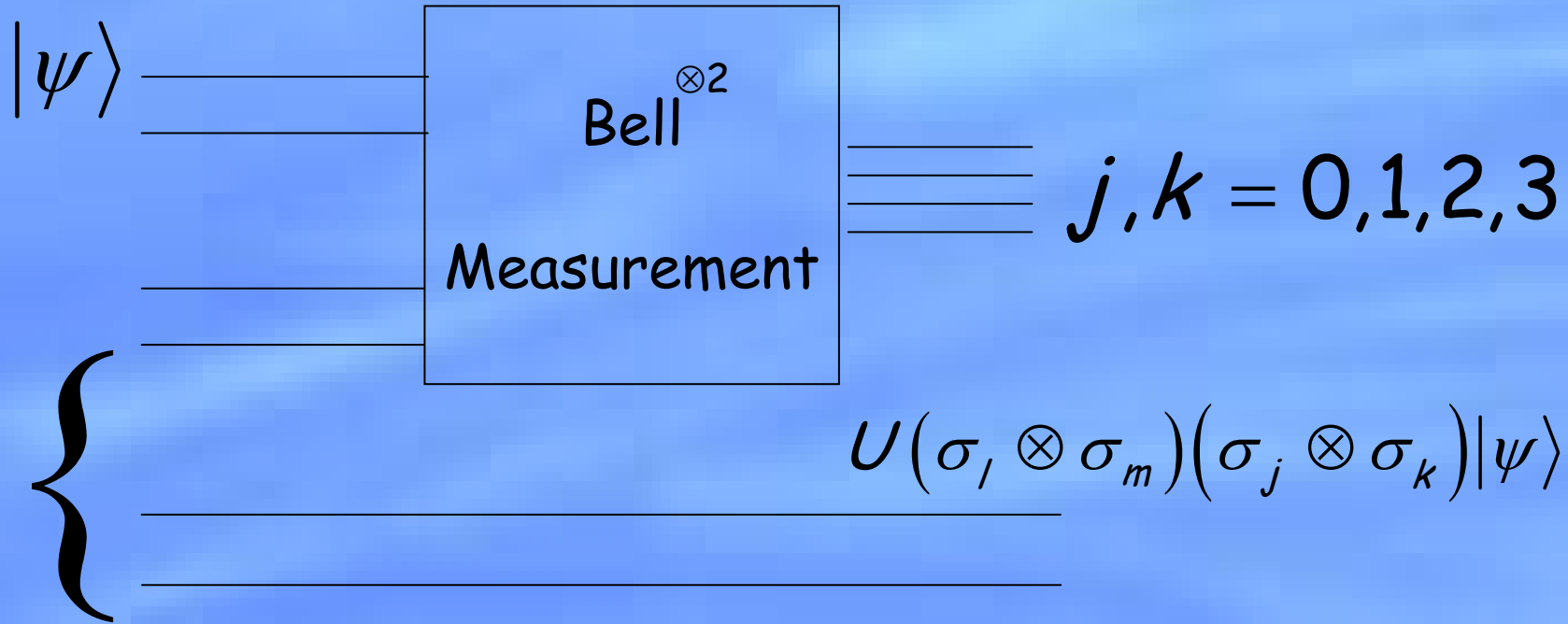
Action was $U\sigma_k\sigma_j, j \neq k$ - a **known unitary error**.

Now attempt to apply the gate $U(U\sigma_k\sigma_j)^\dagger$ to the qubit, using a similar procedure based on measurements alone.

Successful with probability $\frac{1}{4}$, otherwise repeat.

Failure probability ε can be achieved with **$O(\log \frac{1}{\varepsilon})$ repetitions**.

How to do the controlled-not



$$|U_{lm}\rangle \equiv (\mathbf{I} \otimes U_{\sigma_l} \otimes \sigma_m) |\text{Bell}\rangle^{\otimes 2}$$

With probability $\frac{1}{16}$, $j = l, k = m$, and the gate succeeds.

Discussion

Measurement is now recognized as a powerful tool in many schemes for the implementation of quantum computation.

Research problem: Is there a practical variant of this scheme?

Research problem: What sets of measurement are sufficient to do universal quantum computation?

Research problem: Later in the week I will talk about attempts to quantify the “power” of different entangled states. Can a similar quantitative theory of the power of quantum measurements be developed?