The Quantum Circuit Model

Andreas Klappenecker
Department of Computer Science
Texas A&M University

A Quantum Bit

A 2-level quantum system can store a single quantum bit.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The state space is a 2-dimensional complex vector space

$$a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

Coin Flip

If we measure

$$a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

with respect to the computational basis $|0\rangle$, $|1\rangle$ then we get

Result	**Post-Measurement-State**	**Probability**
0	$\|0\rangle$	$\frac{\|a\|^2}{\|a\|^2 + \|b\|^2}$
1	$\|1\rangle$	$\frac{\|b\|^2}{\|b\|^2 + \|b\|^2}$

Quantum States

The states

$$a|0\rangle + b|1\rangle \qquad \text{and} \qquad \lambda a|0\rangle + \lambda b|1\rangle$$

are considered as **equivalent**, since they cannot be distinguished by a measurement.

Many authors assume that $|a|^2 + |b|^2 = 1$.

Operations on a Quantum Computer

Apart from measurements, all operations are linear and length preserving, hence **unitary** operators, $UU^\dagger = \mathbf{1}$.

All operations on a quantum computer, apart from measurements (I/O operations), are **deterministic**.

Single Bit Operations

matrix	effect	in	out
$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$X \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}$	$a\lvert 0\rangle + b\lvert 1\rangle$	$a\lvert 1\rangle + b\lvert 0\rangle$
$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$Z \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -b \end{pmatrix}$	$a\lvert 0\rangle + b\lvert 1\rangle$	$a\lvert 0\rangle - b\lvert 1\rangle$
$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$H \begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} a+b \\ a-b \end{pmatrix}$	$\lvert 0\rangle$	$\frac{1}{\sqrt{2}}\lvert 0\rangle + \frac{1}{\sqrt{2}}\lvert 1\rangle$

Infinitely many operations are available:

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a\cos\theta + b\sin\theta \\ -a\sin\theta + b\cos\theta \end{pmatrix}$$

Entanglement

Let A and B be quantum systems with state spaces H_A and H_B

The state space of the joint quantum system is $H_A \otimes H_B$.

Adding a single quantum bit doubles the memory

Two Quantum Bits

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Tensor Product Structure

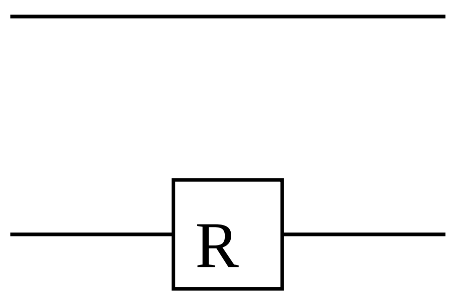
$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

An operation on a single qubit will in general effect **all** coefficients of the joint state vector.

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes X \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ad \\ ac \\ bd \\ bc \end{pmatrix}$$

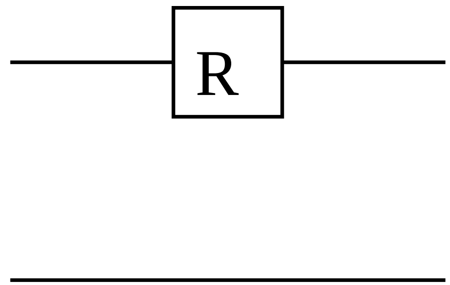
A single qubit operation is a **highly parallel** operation!

Parallelism



$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta & . & . \\ -\sin\theta & \cos\theta & . & . \\ . & . & \cos\theta & \sin\theta \\ . & . & -\sin\theta & \cos\theta \end{pmatrix}$$

Parallelism



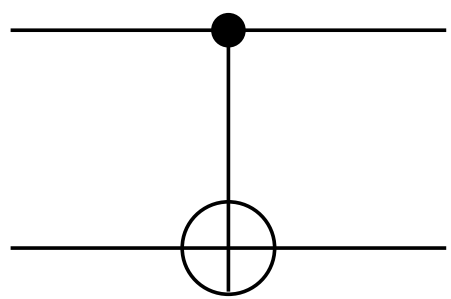
$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \cos\theta & . & \sin\theta & . \\ . & \cos\theta & . & \sin\theta \\ -\sin\theta & . & \cos\theta & . \\ . & -\sin\theta & . & \cos\theta \end{pmatrix}$$

XOR Operation

The **XOR** operation or **controlled NOT** operation is an interaction between two quantum bits.

$$|x\,y\rangle \longmapsto |x\,x \oplus y\rangle$$

in		**out**
$\|00\rangle$	$\mapsto$	$\|00\rangle$
$\|01\rangle$	$\mapsto$	$\|01\rangle$
$\|10\rangle$	$\mapsto$	$\|11\rangle$
$\|11\rangle$	$\mapsto$	$\|10\rangle$



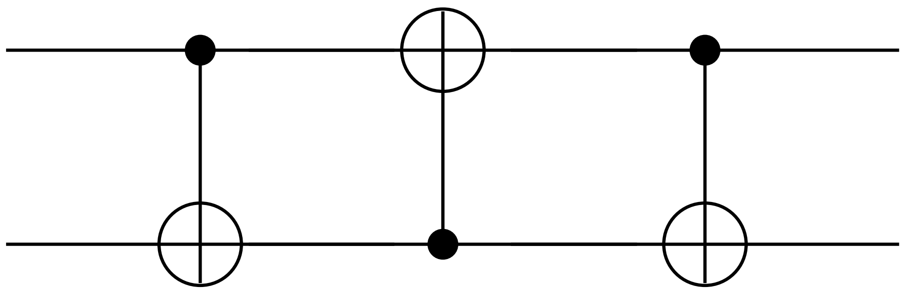
XOR Operation

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

in		**out**
$\|00\rangle$	$\mapsto$	$\|00\rangle$
$\|01\rangle$	$\mapsto$	$\|01\rangle$
$\|10\rangle$	$\mapsto$	$\|11\rangle$
$\|11\rangle$	$\mapsto$	$\|10\rangle$

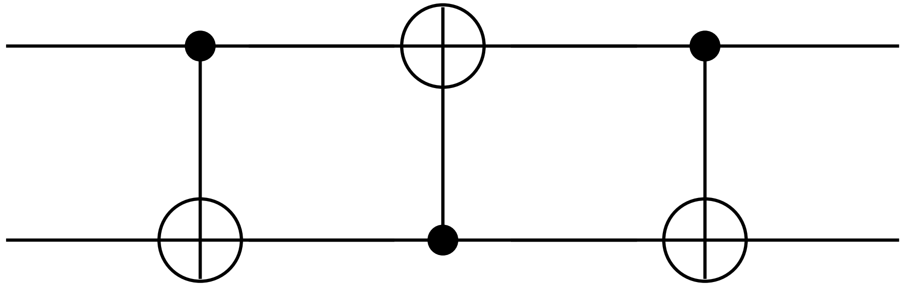
$$\begin{pmatrix} 1 & . & . & . \\ . & 1 & . & . \\ . & . & . & 1 \\ . & . & 1 & . \end{pmatrix}$$

Swap Operation



in		gate 1		gate 2		gate 3		out
$\|00\rangle$	$\mapsto$	$\|00\rangle$	$\mapsto$	$\|00\rangle$	$\mapsto$	$\|00\rangle$	$=$	$\|00\rangle$
$\|01\rangle$	$\mapsto$	$\|01\rangle$	$\mapsto$	$\|11\rangle$	$\mapsto$	$\|10\rangle$	$=$	$\|10\rangle$
$\|10\rangle$	$\mapsto$	$\|11\rangle$	$\mapsto$	$\|01\rangle$	$\mapsto$	$\|01\rangle$	$=$	$\|01\rangle$
$\|11\rangle$	$\mapsto$	$\|10\rangle$	$\mapsto$	$\|10\rangle$	$\mapsto$	$\|11\rangle$	$=$	$\|11\rangle$

Swap Operation



$$(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = (ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle)$$

do swap operation

$$(ac|00\rangle + bc|01\rangle + ad|10\rangle + bd|11\rangle)$$

$$(c|0\rangle + d|1\rangle) \otimes (a|0\rangle + b|1\rangle) = (ca|00\rangle + cb|01\rangle + da|10\rangle + db|11\rangle)$$

Lopsided Complexity

The single qubit operations are easier to implement

The sparser XOR operation is considered costly

[The implementation of the XOR operation is currently the major challenge in most technologies. The difficulties basically result from the fact that an interaction between different quantum systems is difficult to control.]

Quantum Teleportation

Suppose that Alice and Bob are on different planets and Alice wants to communicate a quantum state to Bob.

We assume that they have only classical communication media available but they also share an EPR pair.

How can Alice teleport the quantum state to Bob?

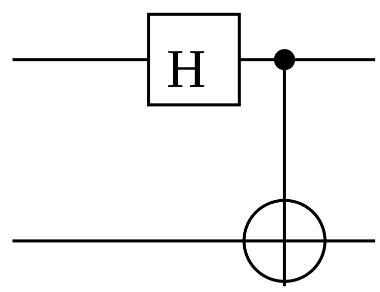
[**Quantum teleportation has been demonstrated in the Lab**]

Einstein-Podolsky-Rosen Pairs

The state

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

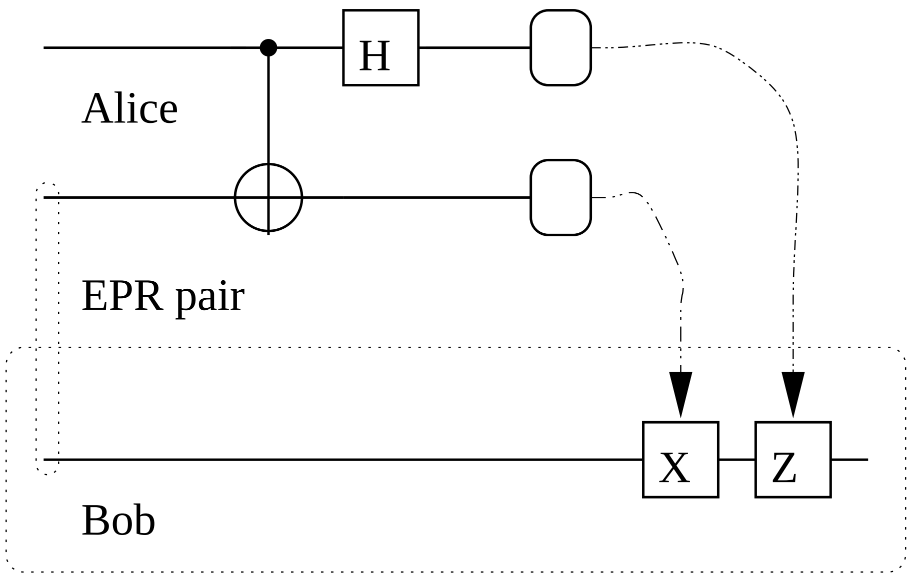
is called an **EPR pair** or a **Bell state**. Engineering this state is not all that difficult:



$$|00\rangle \quad \mapsto \quad \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle \quad \mapsto \quad \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Teleportation

The upper two quantum systems belong to Alice



The least significant bit is owned by Bob. Alice communicates the results of the measurements to Bob by phone.

Teleportation

Alice has a quantum state $|\psi\rangle = a|0\rangle + b|1\rangle$. Alice and Bob share $|\beta\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

Initially, the complete system is in the state

$$|\psi\rangle \otimes |\beta\rangle = (a|0\rangle + b|1\rangle) \otimes \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

this state is equal to

$$\frac{1}{\sqrt{2}}\Big[a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|00\rangle + |11\rangle)\Big]$$

Apply the XOR operation

$$\frac{1}{\sqrt{2}}\Big[a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|10\rangle + |01\rangle)\Big]$$

Teleportation

$$\frac{1}{\sqrt{2}}\Big[a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|10\rangle + |01\rangle)\Big]$$

Alice applies the Hadamard gate H

$$\frac{1}{2}\Big[a(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + b(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle)\Big]$$

Regrouping terms gives

$$\begin{aligned}\frac{1}{2}\Big[|00\rangle(a|0\rangle + b|1\rangle) \quad &+ \quad |01\rangle(a|1\rangle + b|0\rangle) + \\ |10\rangle(a|0\rangle - b|1\rangle) \quad &+ \quad |11\rangle(a|1\rangle - b|0\rangle)\Big]\end{aligned}$$

Teleportation

Alice measures her system, i.e., the 2 most significant bits of

$$\frac{1}{2}\Big[|00\rangle(a|0\rangle + b|1\rangle) \quad + \quad |01\rangle(a|1\rangle + b|0\rangle) + \\ |10\rangle(a|0\rangle - b|1\rangle) \quad + \quad |11\rangle(a|1\rangle - b|0\rangle)\Big]$$

Result	**Bob's State**	**Action**
00	$a\|0\rangle + b\|1\rangle$	none
01	$a\|1\rangle + b\|0\rangle$	X
10	$a\|0\rangle - b\|1\rangle$	Z
11	$a\|1\rangle - b\|0\rangle$	ZX