Science offers the boldest metaphysics of the age. It is a thoroughly, human construct, driven by the faith that if we dream, press to discover, explain, and dream again, thereby plunging repeatedly into new terrain, the world will somehow come clearer and we will grasp the true strangeness of the universe. And the strangeness will all prove to be connected, and make sense.

Edward O. Wilson

Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

Contents II

- 1.4 Quantum algorithms
  - Quantum parallelism
  - Deutsch's algorithm
  - The Deutsch-Josza algorithm
  - Quantum algorithms summarised
- 1.5 Experimental quantum information processing
  - Prospects for practical quantum information processing
- 1.6 Quantum information
  - Quantum information theory

Contents I

- 1.1 Global perspectives (notation)
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

LUND
UNIVERSITY

What is quantum information

- Quantum information concerns the use of quantum mechanical processes and quantum mechanical systems for transmitting, storing or processing information
- Quantum information introduces new non-classical resources like superposition and entanglement into the field of information science

What is superposition and entanglement?

In quantum information data is represented by quantum bits (qubits)

- A qubit is a quantum mechanical systems with two states $|0\rangle$ and $|1\rangle$ that can be in any arbitrary superposition

$$|\Psi\rangle = \alpha|0\rangle+\beta\,|1\rangle$$

of those states

Dirac notation

For a wave function Ψ.
The expectation value for an operator **P** may be denoted <**P**> where

$$< \mathbf{P} >= \int \psi^{*} \mathbf{P} \psi \, d\tau$$

In the Dirac notation the integral is replaced by <**P**> = <ψ| **P** |ψ>
Where < ψ | can be seen as corresponding to ψ * and | ψ > to ψ

Instead of the symbol ψ a symbol characterising the actual state is often used,
For example, |0> eller |1> to describe whether the system is in state 0 or state 1.

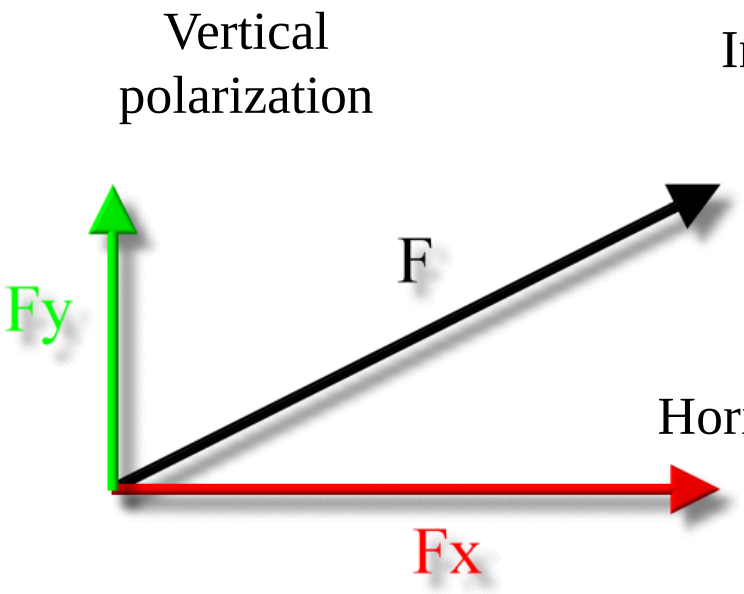
The postulates of quantum mehanics

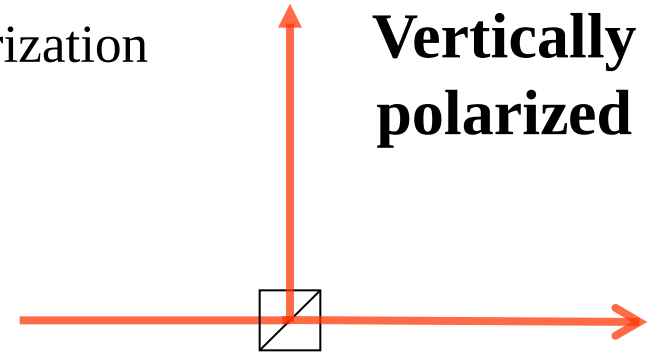
(Chapter 2.2)

- Any isolated physical system is associated to a Hilbert space. The system is described by a unit vector in this Hilbert space
- The evolution of a closed quantum system is described by a unitary transformation
- ≈A measurement will project a system onto the measurement operator basis system

What does this mean?

Polarizing beam splitter





Vertically polarized

Polarizing Beam splitter

Horisontally polarized

The postulates of quantum mehanics
(Chapter 2.2)

- Any isolated physical system is associated to a Hilbert space. The system is described by a unit vector in this Hilbert space
- The evolution of a closed quantum system is described by a unitary transformation
- ≈A measurement will project a system onto the measurement operator basis system
- The state of a composite physical system is the tensor product of all the state spaces of all the individual physical systems

Tensor product examples

Tensor product of two matrices

$$\begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \otimes \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} = \begin{bmatrix} a_{1,1}\begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} & a_{1,2}\begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \\ a_{2,1}\begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} & a_{2,2}\begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_{1,1}b_{1,1} & a_{1,1}b_{1,2} & a_{1,2}b_{1,1} & a_{1,2}b_{1,2} \\ a_{1,1}b_{2,1} & a_{1,1}b_{2,2} & a_{1,2}b_{2,1} & a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1} & a_{2,1}b_{1,2} & a_{2,2}b_{1,1} & a_{2,2}b_{1,2} \\ a_{2,1}b_{2,1} & a_{2,1}b_{2,2} & a_{2,2}b_{2,1} & a_{2,2}b_{2,2} \end{bmatrix}.$$

Wave function of two two-level system (*e.g.* two particles with spin)

2-dimensional $\Rightarrow$ 4-dimensional Hilbert space

(The Hilbert space of n two-level particles is 2^n –dimensional)

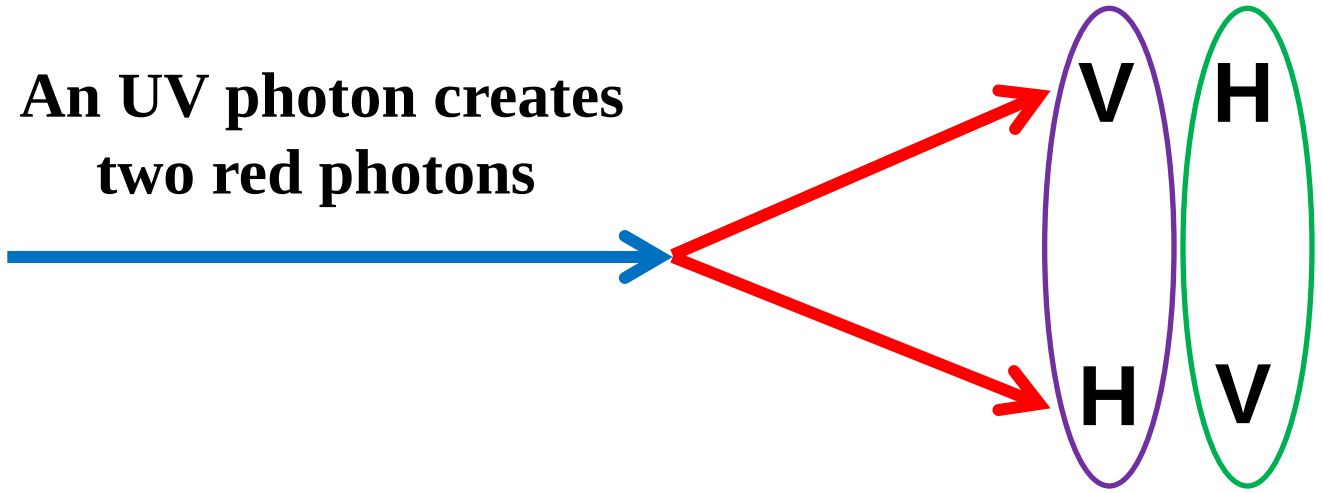
Dirac notation for several particles

- According to the fourth postulat of quantum mechanics the joint wave function for a system of two particles , a and b, may be written as the product of each of their wave functions, e. g., $|1\rangle_a|0\rangle_b$, or by suppressing the indices more briefly just as $|10\rangle$.

Entanglement

- If two systems, a and b, described by a wave function $\Psi(a,b)$ are entangled, then it is not possible to rewrite $\Psi(a,b)$ as a product of two wavefunctions $\Psi_1(a)^* \Psi_2(b)$
- Explicit example
- Discuss the EPR paradox

The wave function does not collapse until there is a measurement



Which one of the red photons that is vertically polarized is not determined until the polarization is measured

Polarising beam splitters*

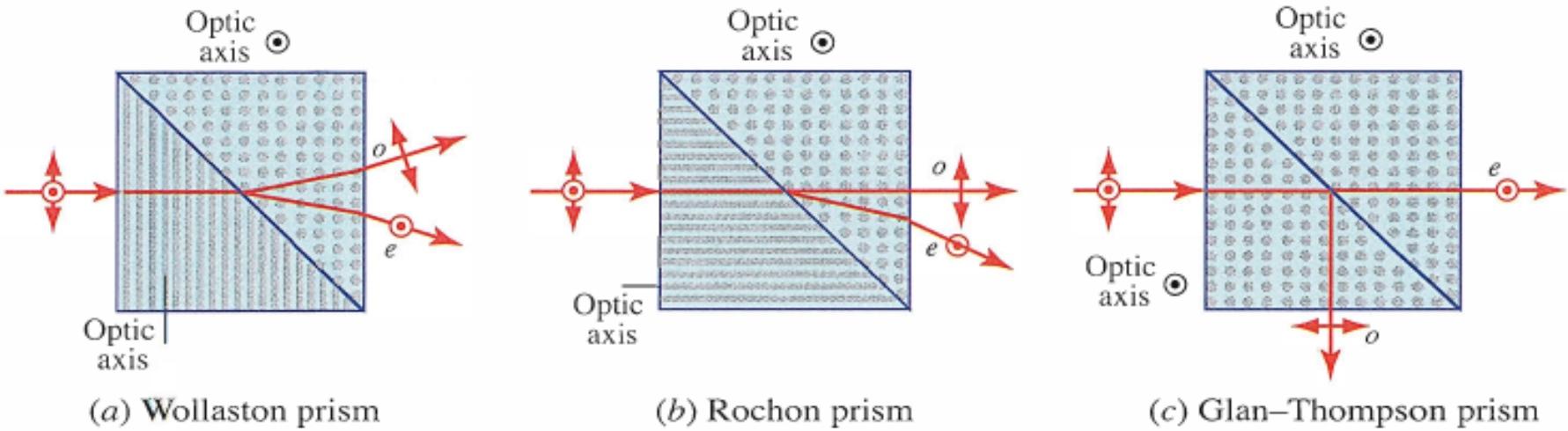
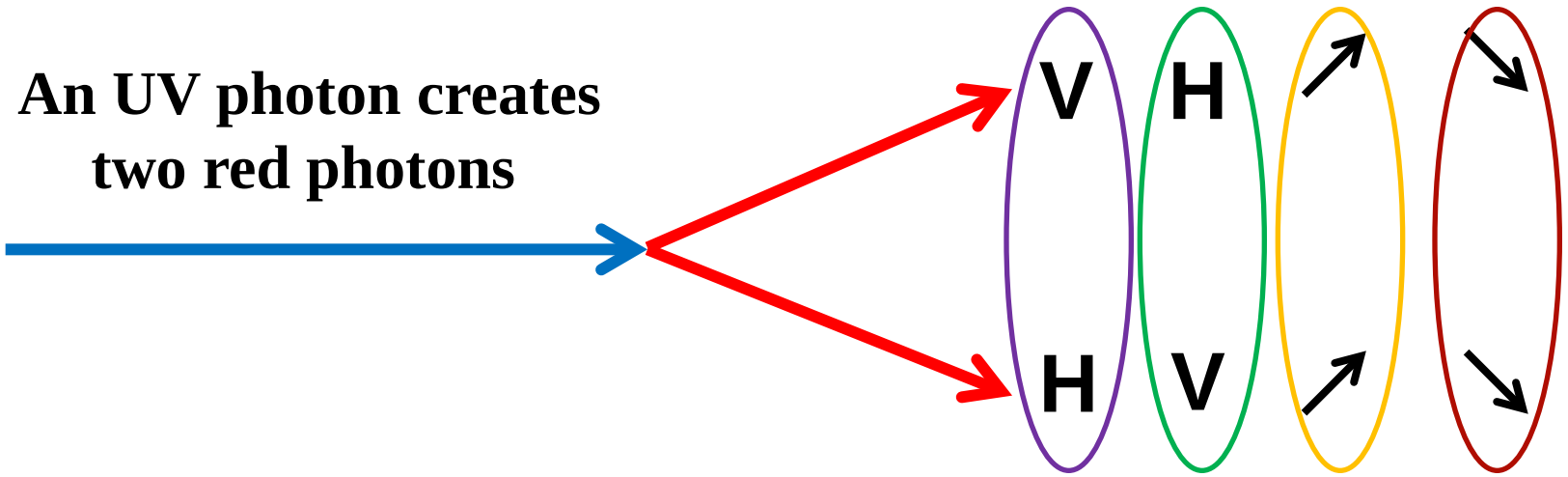


Figure 6.6-3 Polarizing beamsplitters. The directions and polarizations of the waves that exit differ for the three prisms. In this illustration, the crystals are negative uniaxial (e.g., calcite). The Glan–Thompson device has the merit of providing a large angular separation between the emerging waves.

- **45° and -45° states are measured in the same way by turning the base 45 degrees!**

*Photonics, Teich & Saleh,

The wave function does not collapse until there is a measurement

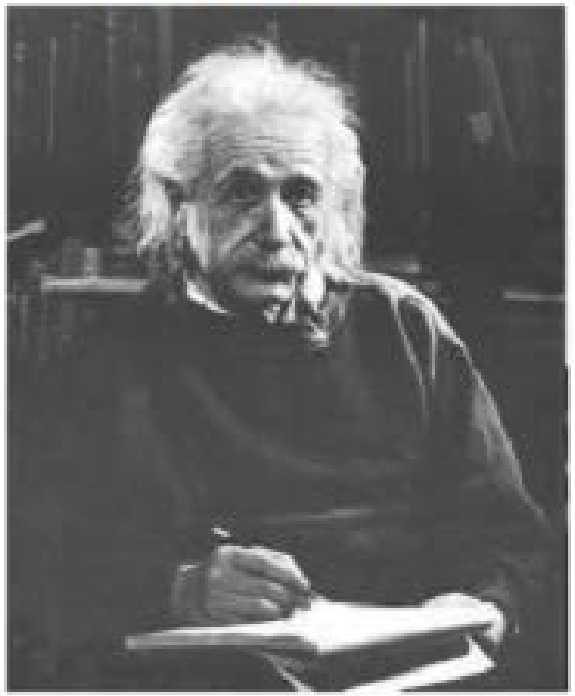


Depending on our measurement the resulting polarization will be different

So what is our interpretation?

LUND UNIVERSITY

Albert Einstein



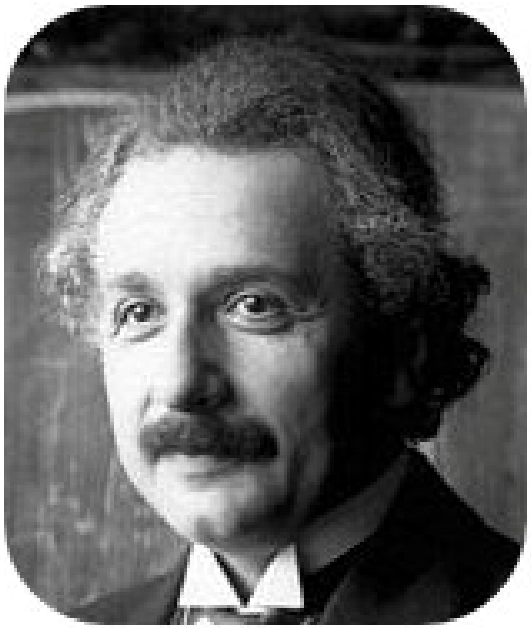
"God does not play dice with the universe."

Niels Bohr

"Anyone who is not shocked by Quantum Theory has not understood it."

https://hunt4truth.wordpress.com/tag/stephen-hawking/

The Einstein-Podolsky-Rosen paradox (1935)



A. Einstein

B. Podolsky

N. Rosen

http://physicsforme.com/2012/03/08/epr-before-epr-a-1930-einstein-bohr-thought-experiment-revisited/

The Bohr Einstein dialogue

How can it be possible that a measurement on the earth immediately can change the physical reality in an other part of the universe?

http://thelifeofpsi.com/2013/10/28/bertlmanns-socks/

Hidden variables

How can it be possible that a measurement on the earth immediately can change the physical reality in an other part of the universe?

http://thelifeofpsi.com/2013/10/28/bertlmanns-socks/

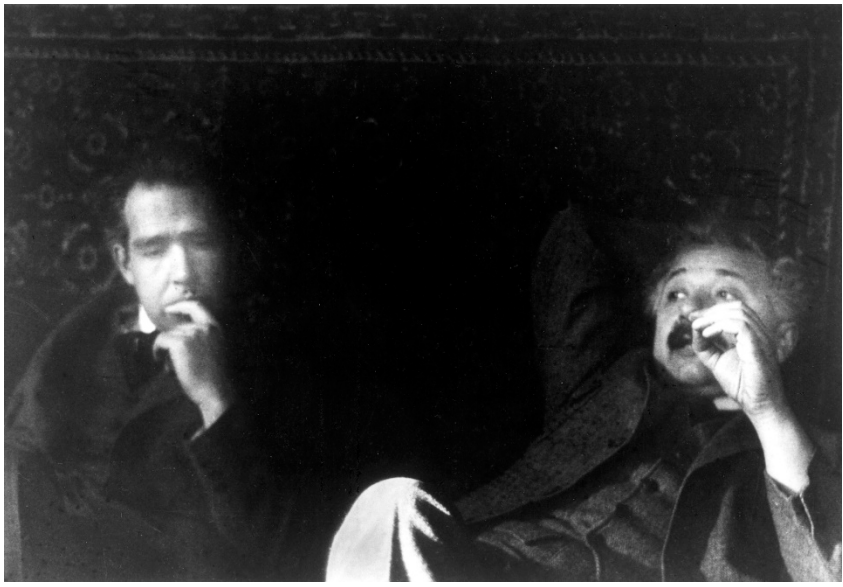
Bell´s inequality

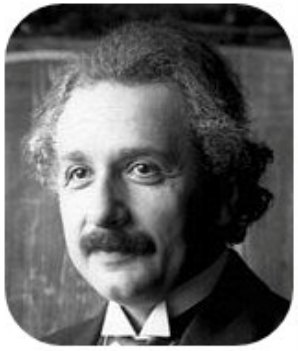
In 1964 John Stewart Bell showed that it is possible to design a measurement that gives different results for quantum mechanics and the hidden variable theory

http://en.wikipedia.org/wiki/John_Stewart_Bell

Can the Einstein-Podolsky-Rosen paradox be explained by superluminal communication?

LUND UNIVERSITY





A. Einstein

B. Podolsky

N. Rosen

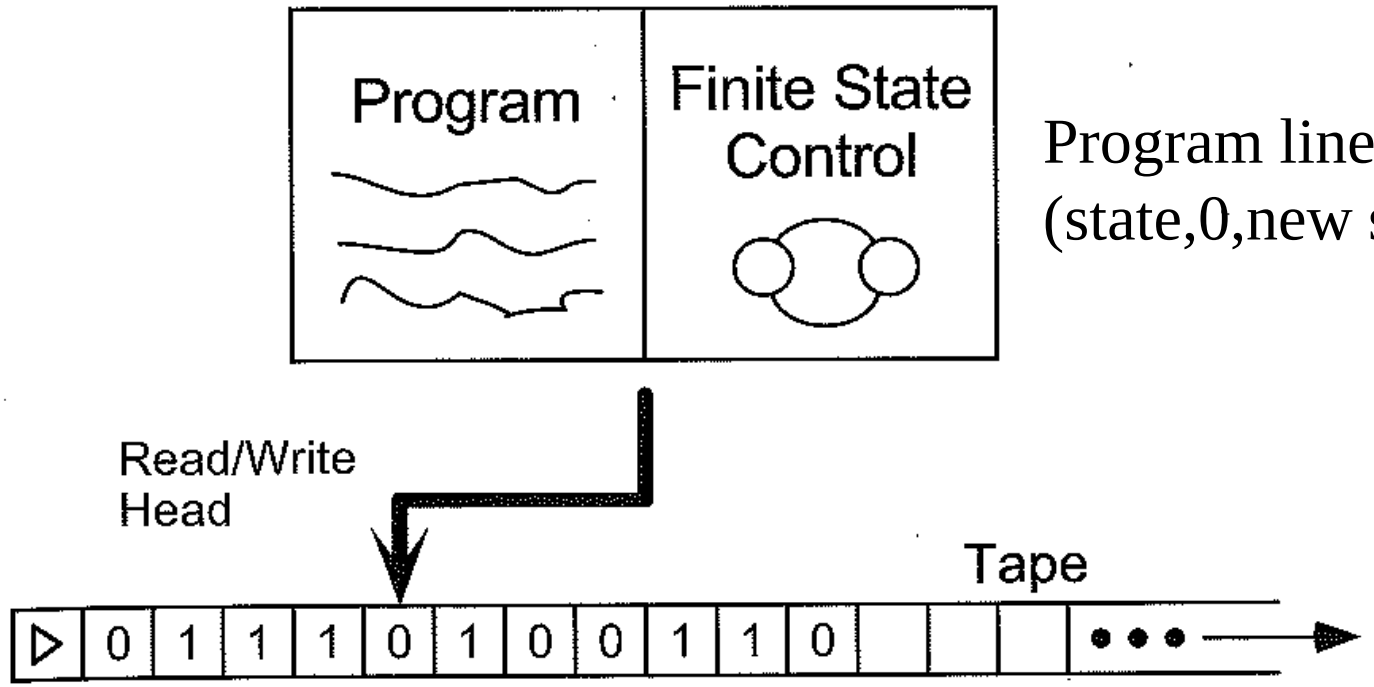
In principle, but there is no experimental support and it would contradict theory of relativity

Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

Computing, history

- There is a universal Turing machine that can simulate any other Turing machine
  - Alan Turing 1936



Program line example
(state,0,new state,b,+1)

Figure 3.1. Main elements of a Turing machine. In the text, blanks on the tape are denoted by a 'b'. Note the ▷ marking the left hand end of the tape.

Computing, history (I)

- There is a universal Turing machine (Fig 3.1, p. 123) that can simulate any other Turing machine
  - Alan Turing 1936
- If an algorithm can be performed at any class of hardware, then there is an equivalently efficient algorithm for a Turing machine
  - Church-Turing thesis (strong version)

See notes

LUND UNIVERSITY

(Quantum) computing, history

- Rolf Landauer, IBM, 1960ies
  - From an entropy point of view a computation consumes an energy >kT*ln(2) (~$3*10^{-21}$ J) per bit information erased or discarded
  - A reversible computer, which after the computations just prints the answer and then reverse its operations going back to the original state, could give a much lesser entropy change and thus could be much more energy efficient

SMIL 1956

Information is physical

Rolf Landauer

LUND UNIVERSITY

(Quantum) computing, history

- Charles Bennett, IBM, 1973
  - It is in principle possible to construct a reversible Turing machine with essentially the same performance as a Turing machine

LUND UNIVERSITY

Regarding operations on quantum systems

- Generally a quantum system, Ψ, at time t_2 can be related to its state at some earlier time, t_1, by a unitary transformation U
- $\Psi(t_2)=U\Psi(t_1)$
- Clearly, if we expose the system at time t_2 to U^{-1}, the original state is obtained
- $U^{-1}\,\Psi(t_2) = U^{-1}\,U\,\Psi(t_1) = \Psi(t_1)$

LUND UNIVERSITY

Quantum computing, history

- Paul Benioff, Argonne National Lab., 1982
  - For any arbitrary Turing machine carrying out a calculation, Q, in N steps, there is a set of states, Ψ, and a hamiltonian, H, such that the time development of Ψ under H reproduces the calculation of Q by the Turing machine.
  - Benioff also shows that a quantum mechanical implementation of a Turing machine is as least as efficient as a classical Turing machine and it would in principle not need to consume any energy for its calculations

LUND
UNIVERSITY

Quantum computing, history

- David Deutsch, Oxford, 1985
  - Deutsch argues (and shows) that, as for a normal computers, it should be possible to program a quantum computer to carry out arbitrary operations
  - Such quantum computers would have properties different from classical computers, *e. g.*, quantum computers would be faster on certain calculations due to 'quantum parallelism'

In quantum information data is represented by quantum bits (qubits)

- A qubit is a quantum mechanical systems with two states $|0\rangle$ and $|1\rangle$ that can be in any arbitrary superposition

$$|\Psi\rangle = \alpha|0\rangle+\beta\,|1\rangle$$

of those states

Superposition of states makes a quantum computer (QC) powerful

Input data (4 bits)

Input data (4 qubits)

$(|0>+|1>)/\sqrt{2}$ 0

$(|0>+|1>)/\sqrt{2}$ 1

$(|0>+|1>)/\sqrt{2}$ 1

$(|0>+|1>)/\sqrt{2}$ 0

Quantum Computer

Input ≡ (|1>+|0>) (|0>+|1>) (|0>+|1>) (|0>+|1>)/4=

=(|0000>+|0001>+|0010>+|0011> . . . +|1111>)/4

Quantum parallelism

- Consider an operation, *f*, performing the operation *f(x)* on a state *x* and putting the resultat in *y*. For a system $|x, y\rangle$ we obtain for $x = (|0\rangle + |1\rangle)/\sqrt{2}$
- $|x,y\rangle = [|0,f(0)\rangle + |1,f(1)\rangle]/\sqrt{2}$.
- By performing the operation *f* on state *x*, *f*(0) and *f*(1) have been calculated in one operation.

See notes

Quantum parallelism

- More generally, if *x is* represented by *n* quantum bits it can be a superposition of 2^n values. The function *f* is then evaluated in 2^n points in one step.

Quantum parallelism

- Such ’quantum parallelism' is not automatically useful beacuse a measurement on system $|x,y\rangle$ will collapse the superposition $[|0,f(0)\rangle+|1,f(1)\rangle]/\sqrt{2}$ to either the first or the second term
- You need a problem and an algorithm which can utilize that all values have been calculated

LUND
UNIVERSITY

Quantum computing, history

- Peter Shor, ATT Bell laboratories, 1994
  - Quantum algorithms for factorisation into prime numbers much more efficient than the best known algorithms for classical computers
  - Encryption, security protocols on the internet and elsewhere

Computationally hard problems

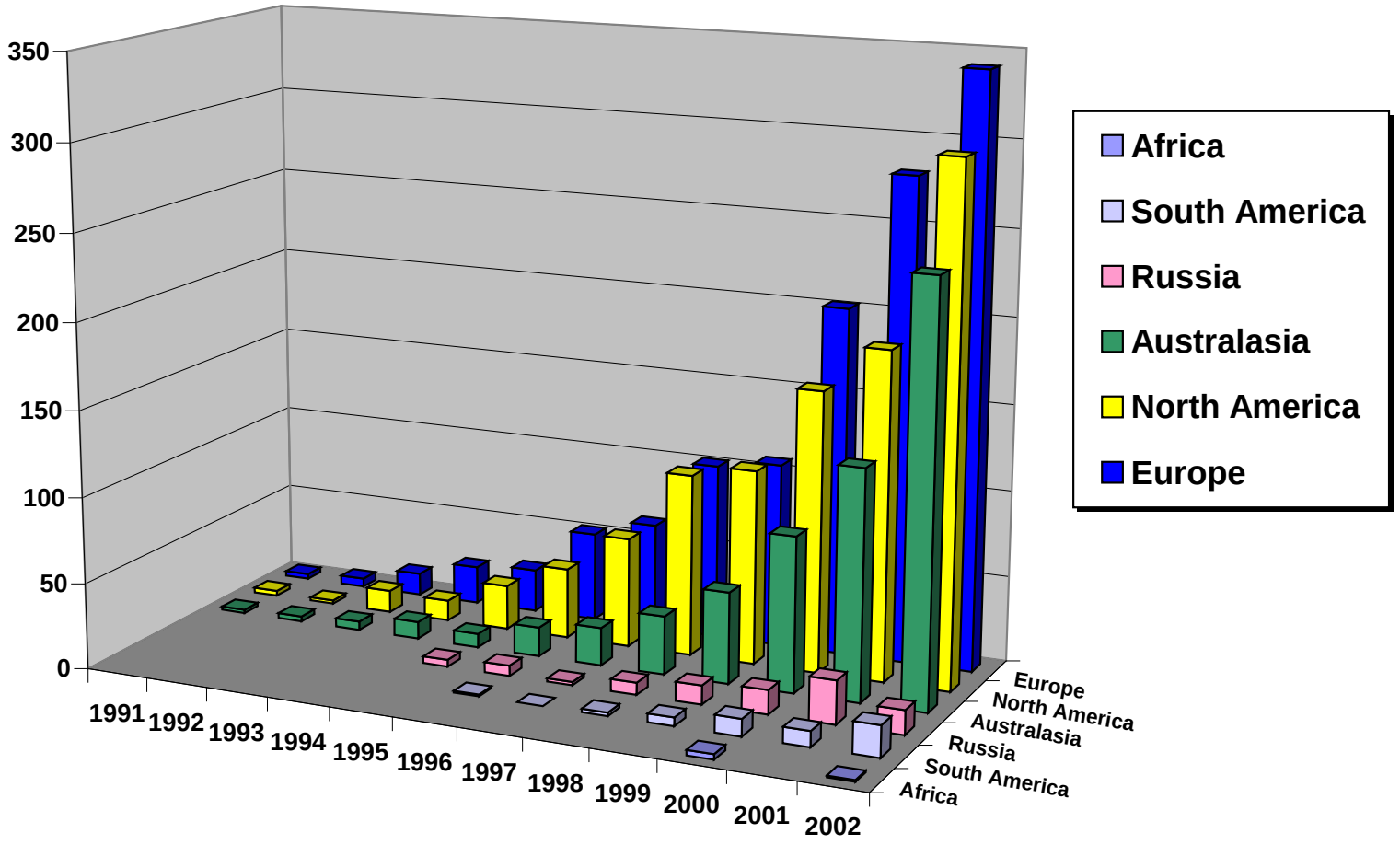
- The number of steps required to solve the problem using the best known algorithms on classical computers increase exponentially with the size of the problem
- For some of these problems there are, however, quantum algorithms where the number of steps only increase polynomially

LUND UNIVERSITY

Computationally hard problems

- Consider a computationally hard problem with an input represented by n=25 bits that takes 1 hour to solve on a classical computer (computation time goes as 2^n)
- How long time would it take to solve a problem requiring n=50 bits?
  - 1000 years!
- While on a quantum computer (*e.g.* assuming computation time goes as n^2) the time would go from 1 hour to 4 hours.

Papers published in quantum information science



Quantum computing changes the landscape of computer science

- QC algorithms challenge the strong version of the Church-Turing thesis
- If an algorithm can be performed at any class of hardware, then there is an equivalent efficient algorithm for a Turing machine

Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

In quantum information data is represented by quantum bits (qubits)

- A qubit is a quantum mechanical systems with two states |0> and |1> that can be in any arbitrary superposition

$$\Psi = \alpha|0\rangle+\beta\,|1\rangle$$

of those states

- What can we say about α and β?

Qubit representation

$$\left|\Psi\right\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}\left|0\right\rangle + e^{i\varphi}\sin\frac{\theta}{2}\left|1\right\rangle\right)$$

The Bloch sphere

$$|\Psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$

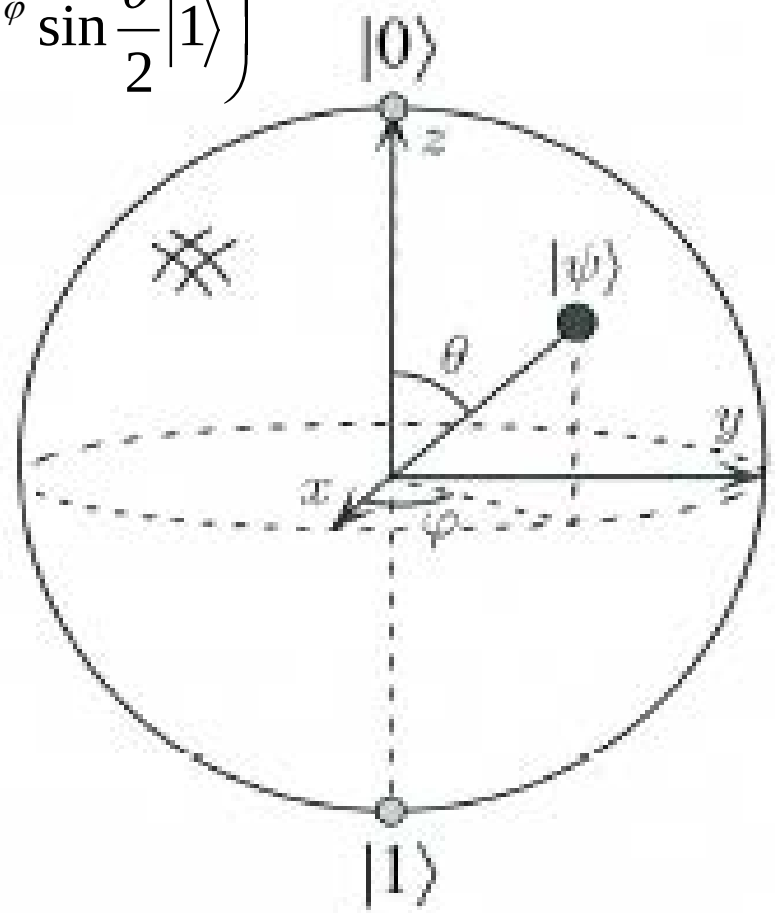
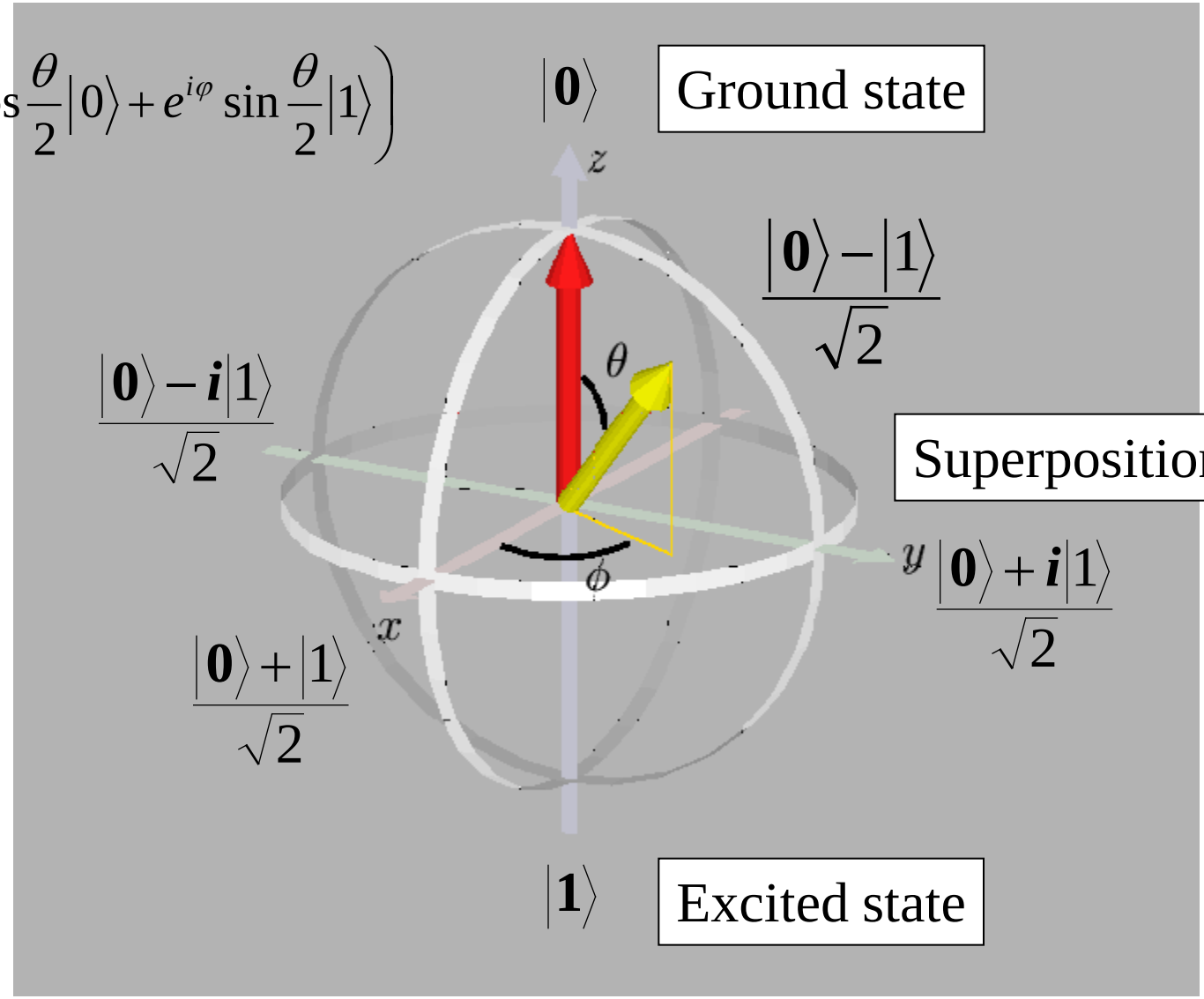


Figure 1.3. Bloch sphere representation of a qubit.

The Bloch sphere

$$|\Psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$



Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

1.3.1 Single qubit gates (1)

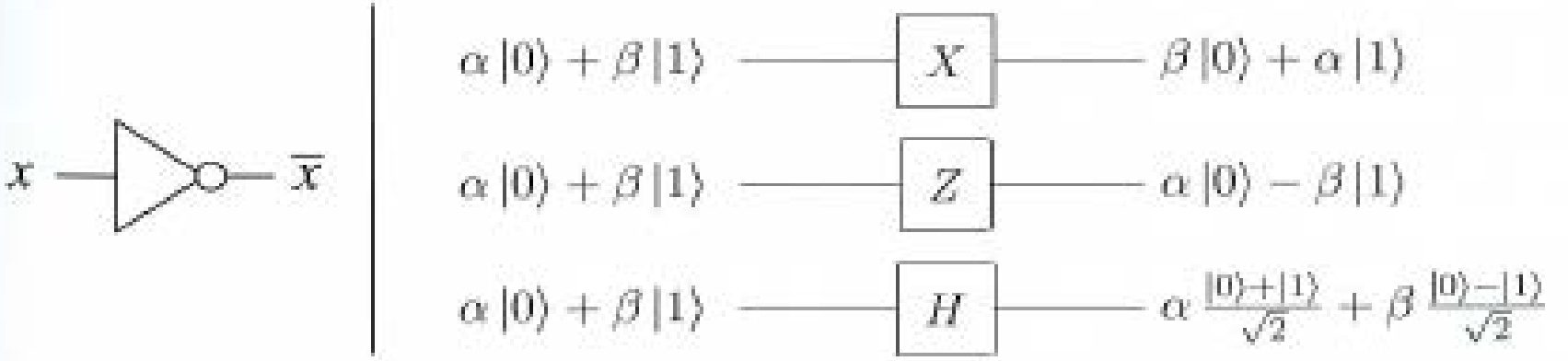


Figure 1.5. Single bit (left) and qubit (right) logic gates.

The Bloch sphere

$$|\Psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$

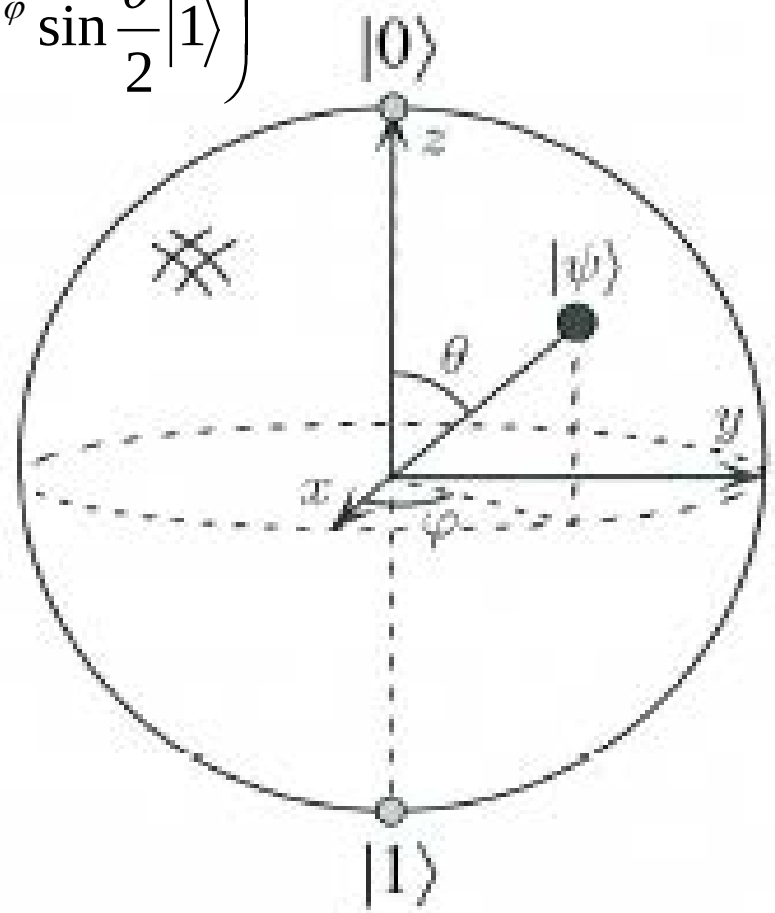


Figure 1.3. Bloch sphere representation of a qubit.

LUND UNIVERSITY

Regarding operations on quantum systems

- Generally a quantum system, Ψ, at time t_2 can be related to its state at some earlier time, t_1, by a unitary transformation U
- $\Psi(t_2)=U\Psi(t_1)$
- Clearly, if we expose the system at time t_2 to U^{-1}, the original state is obtained
- $U^{-1}\,\Psi(t_2) = U^{-1}\,U\,\Psi(t_1) = \Psi(t_1)$

Single qubit vector representation

- Single qubit, x
- $\Psi = \alpha|0\rangle + \beta\,|1\rangle$
- Base functions |0>, |1>
- Vector representation $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

1.3.1 Single qubit gates (2)

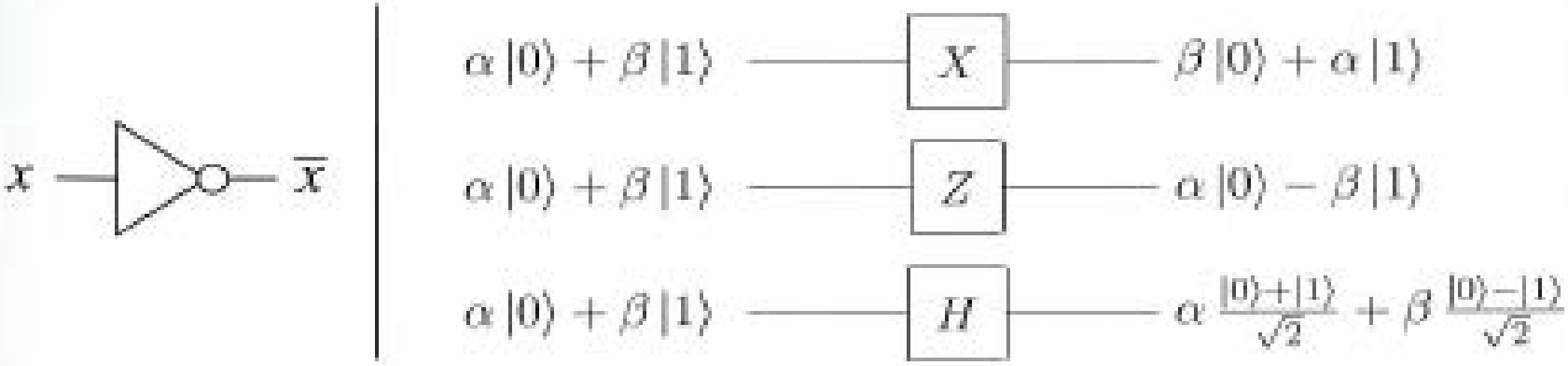


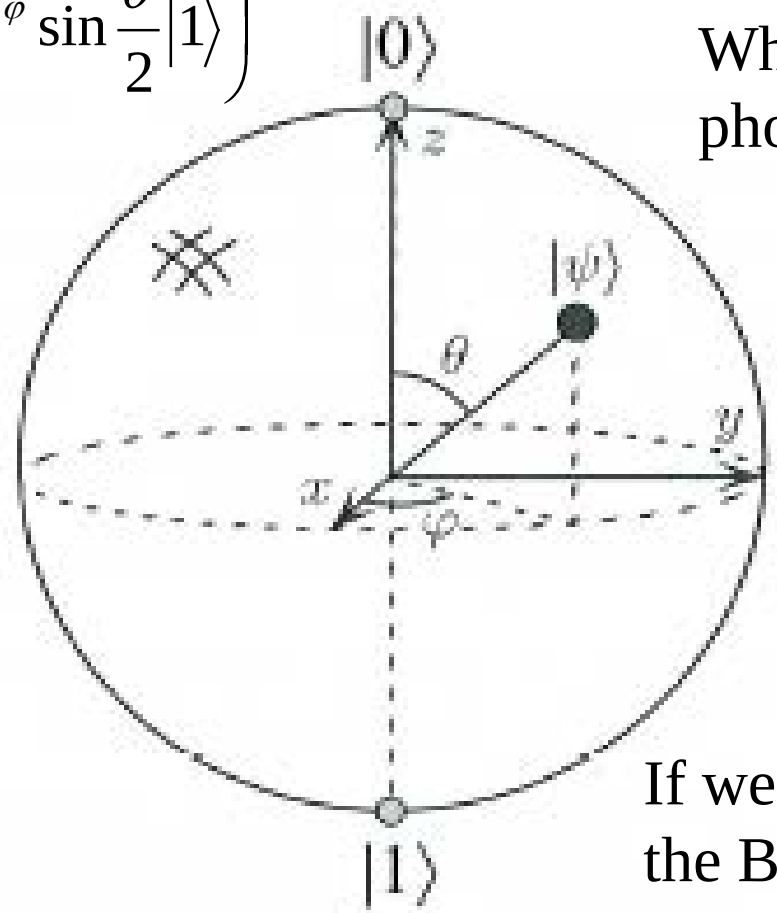
Figure 1.5. Single bit (left) and qubit (right) logic gates.

There are infinitely many two by two unitary matrices, and thus infinitely many single **qubit operations**

Write down initial and final vector and find the operation matrix

The Bloch sphere

$$|\Psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$



What happens when a photon passes an atom?

If we start at |0>, where on the Bloch sphere could we add up?

Figure 1.3. Bloch sphere representation of a qubit.

Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

Multiple qubit vector representation

- Two qubits, x_1, x_2
- Computational base $|x_1,x_2\rangle$
- What are the base functions?
- Base functions $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$
- $\Psi = \alpha|00\rangle+\beta\,|01\rangle+\gamma|10\rangle+\delta|11\rangle$

- What is the vector representation?

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$$

1.2.1 multiple qubits

- N qubits span a computational basis $|x_1,x_2,x_3 \ldots ,x_N\rangle$
- The quantum state is specified by 2^N amplitudes
- Lets say $N \approx 500$ would it be difficult to store these amplitudes in a classical memory?
- The number of amplitudes is larger than the estimated number of atoms in the universe

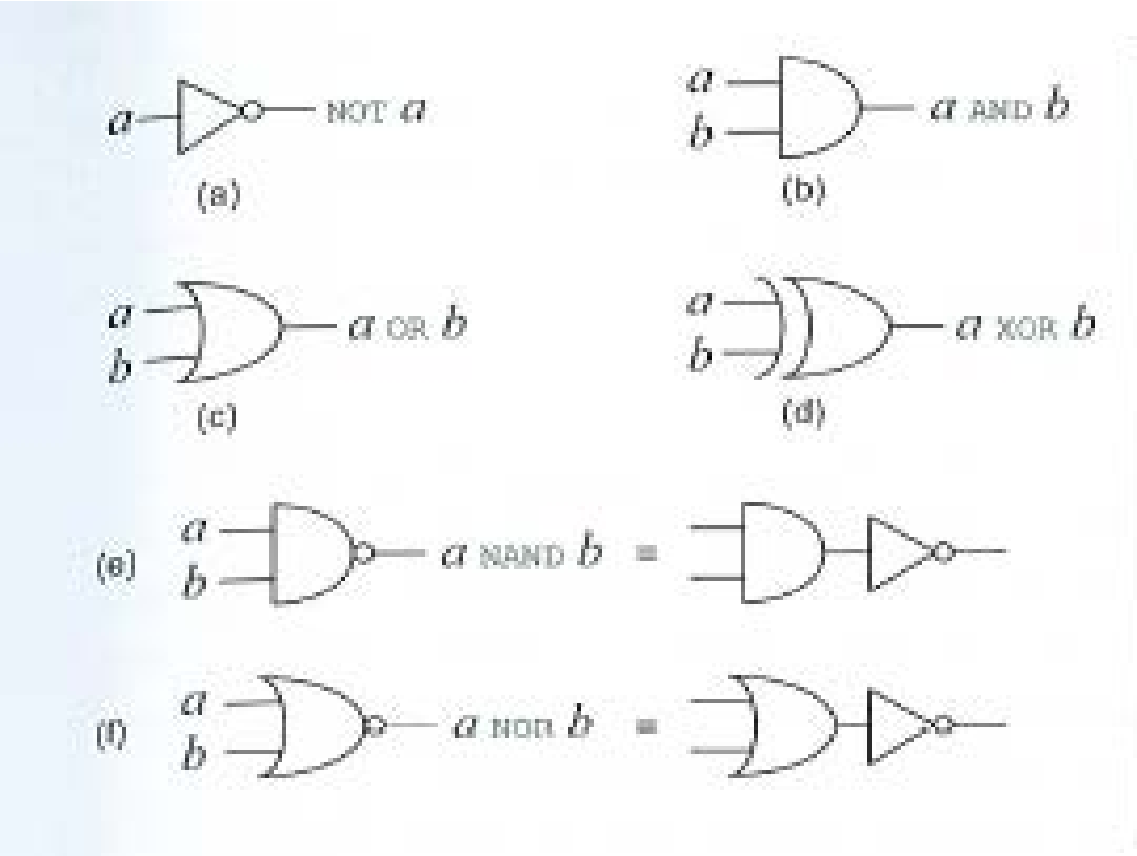
Hilbert space is a big place

Carlton Caves

Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

Two (qu)bit gates



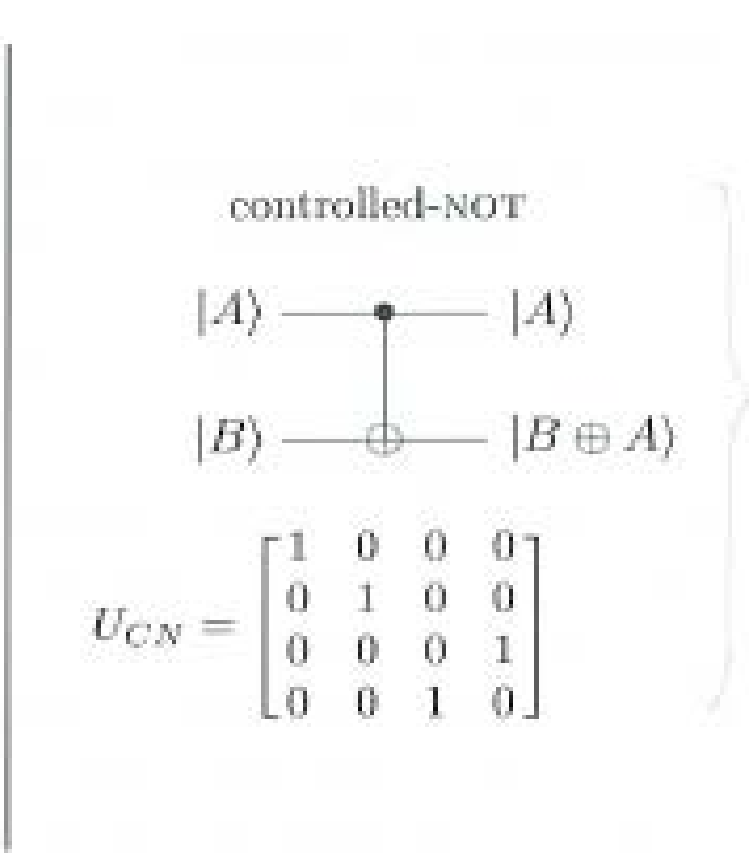


Figure 1.6. On the left are some standard single and multiple bit gates, while on the right is the prototypical multiple qubit gate, the controlled-NOT. The matrix representation of the controlled-NOT, U_{CN}, is written with respect to the amplitudes for $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, in that order.

CNOT gate

- Control $|\Psi_c> = \alpha|0\rangle+\beta\ |1\rangle$
- Target $|\Psi_t> = \gamma|0\rangle+\delta|1\rangle$
- What is the product state wave function?
- How is it changed by the CNOT operation?
- Do the same thing in the vector/matrix representation

Multiple qubit gates 1.3.2

- Any multiple qubit gates can be constructed from CNOT and single-qubit gates
- Quantum gates are reversible
- What would be the inverse of a CNOT gate?

Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

Polarising beam splitters

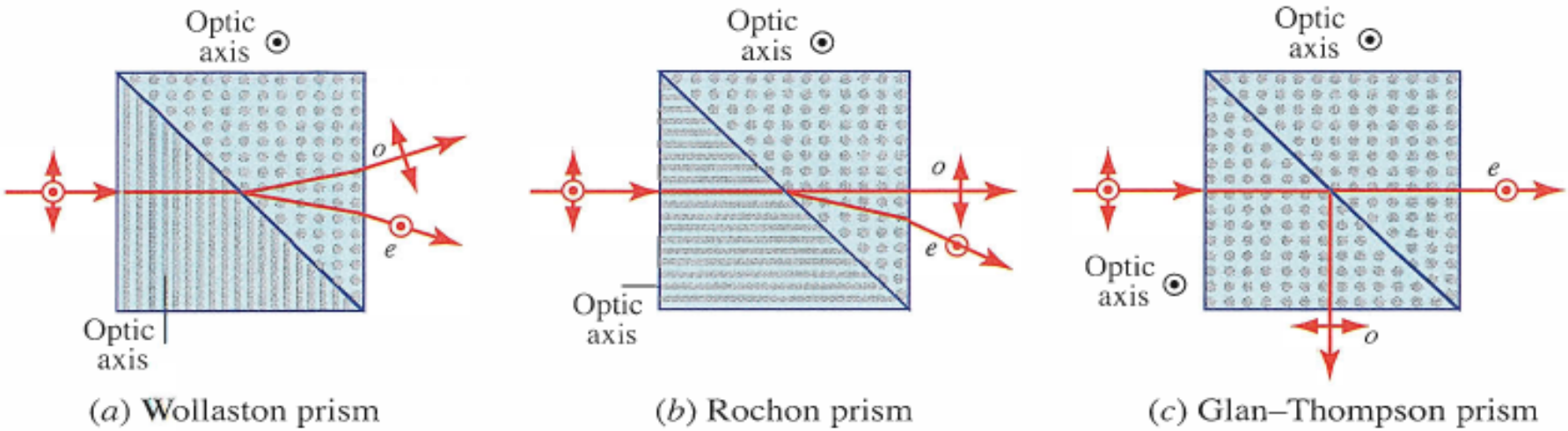
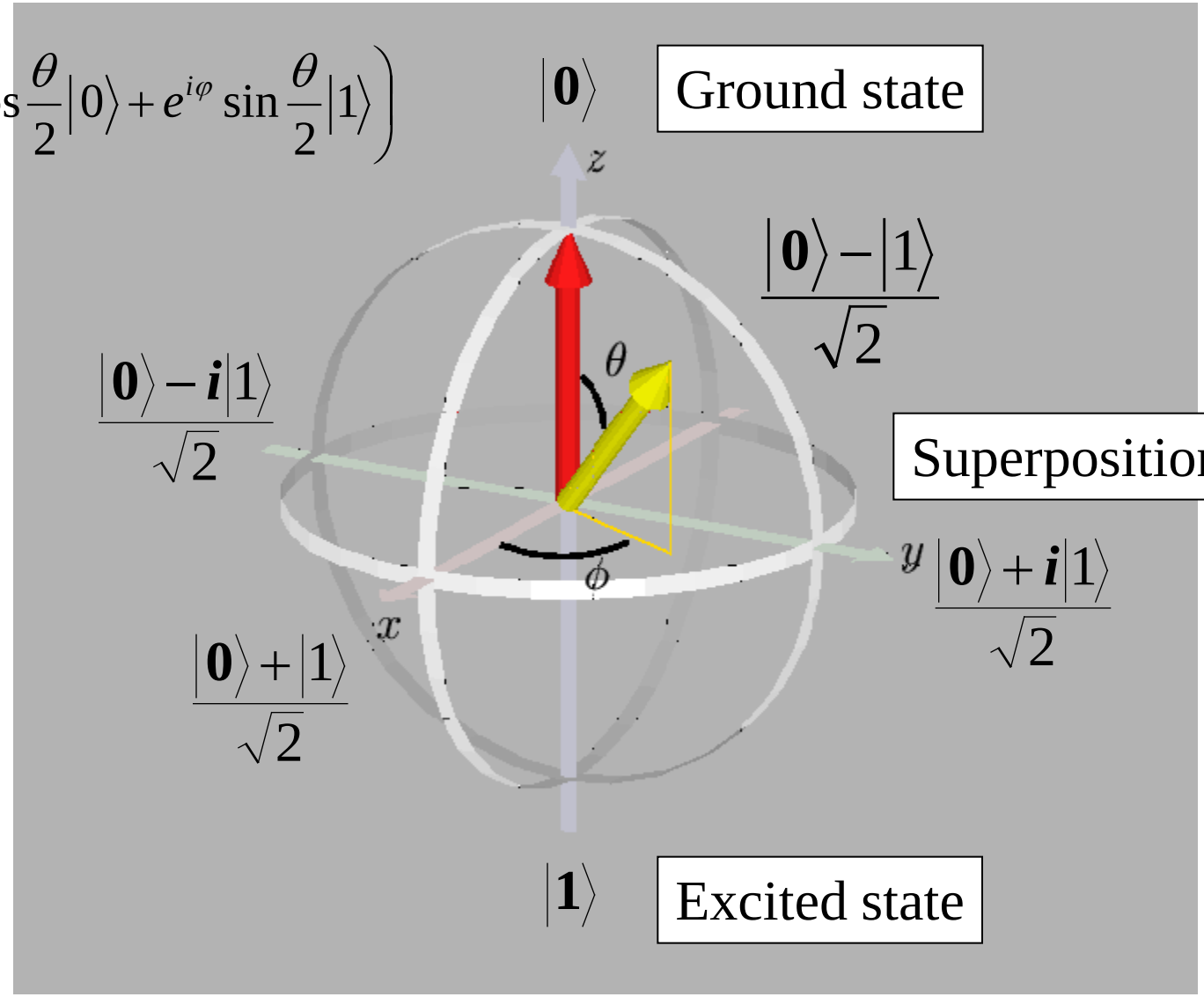


Figure 6.6-3 Polarizing beamsplitters. The directions and polarizations of the waves that exit differ for the three prisms. In this illustration, the crystals are negative uniaxial (e.g., calcite). The Glan–Thompson device has the merit of providing a large angular separation between the emerging waves.

- **45° and -45° states are measured in the same way by turning the base 45 degrees!**

The Bloch sphere

$$|\Psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$



Opposite states on the Bloch sphere constitute an orthonormal base

Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits (Chapter 4)
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

1.3.4 Quantum circuits

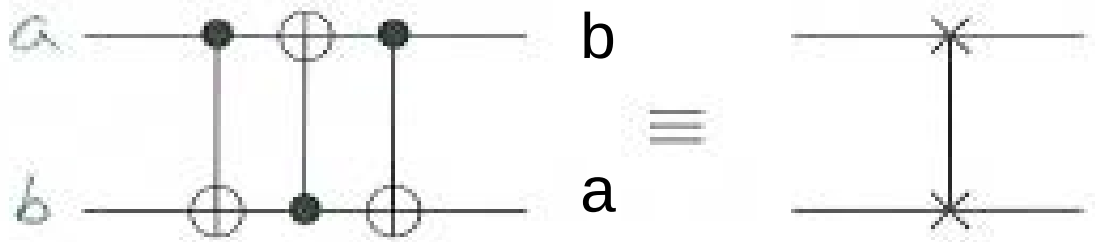


Figure 1.7. Circuit swapping two qubits, and an equivalent schematic symbol notation for this common and useful circuit.

Show that 1.7 indeed is a swap gate

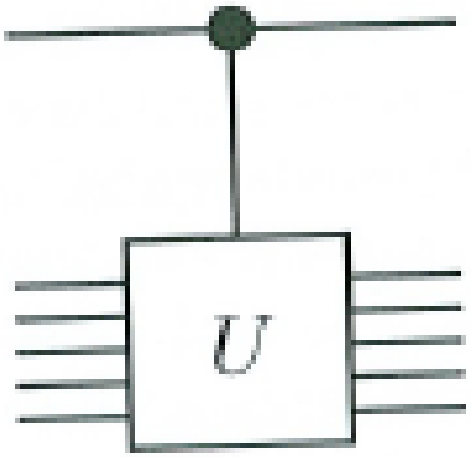


Figure 1.8. Controlled-U gate.

Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

1.3.5 Qubit copying circuit?

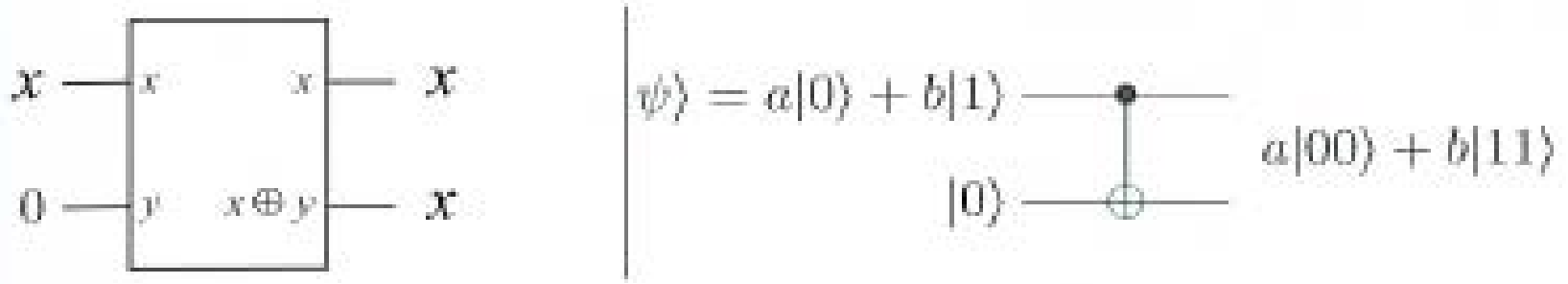


Figure 1.11. Classical and quantum circuits to 'copy' an unknown bit or qubit.

The resulting state is entangled

1.3.5 The no cloning theorem

We would like to turn the known state $|0\rangle$ into a clone of the unknown state $|\alpha\rangle$

The joint state of this system is $|\alpha\rangle|0\rangle$.
Suppose there exists a universal cloning operator, U, that performs the operation $U|\alpha\rangle|0\rangle=|\alpha\rangle|\alpha\rangle$ for any state α.

It thereby also performs $U|\beta\rangle|0\rangle=|\beta\rangle|\beta\rangle$ for a state $\beta\neq\alpha$.

However if we consider the state $|\gamma\rangle=(|\alpha\rangle+|\beta\rangle)/\sqrt{2}$ we may write
$U|\gamma\rangle|0\rangle=U((|\alpha\rangle+|\beta\rangle)/\sqrt{2})|0\rangle= U(|\alpha\rangle|0\rangle+|\beta\rangle|0\rangle)/\sqrt{2}=(|\alpha\rangle|\alpha\rangle+|\beta\rangle|\beta\rangle)/\sqrt{2}$.

However, $U|\gamma\rangle|0\rangle$ can also be calculated as
$U|\gamma\rangle|0\rangle=|\gamma\rangle|\gamma\rangle=(|\alpha\rangle+|\beta\rangle)/\sqrt{2}(|\alpha\rangle+|\beta\rangle)/\sqrt{2}=(|\alpha\rangle|\alpha\rangle+|\alpha\rangle|\beta\rangle+|\beta\rangle|\alpha\rangle+|\beta\rangle|\beta\rangle)/2$
Which is completely different from above

Thus there can not exist a universal cloning operation U.

1.3.5 Qubit copying circuit?

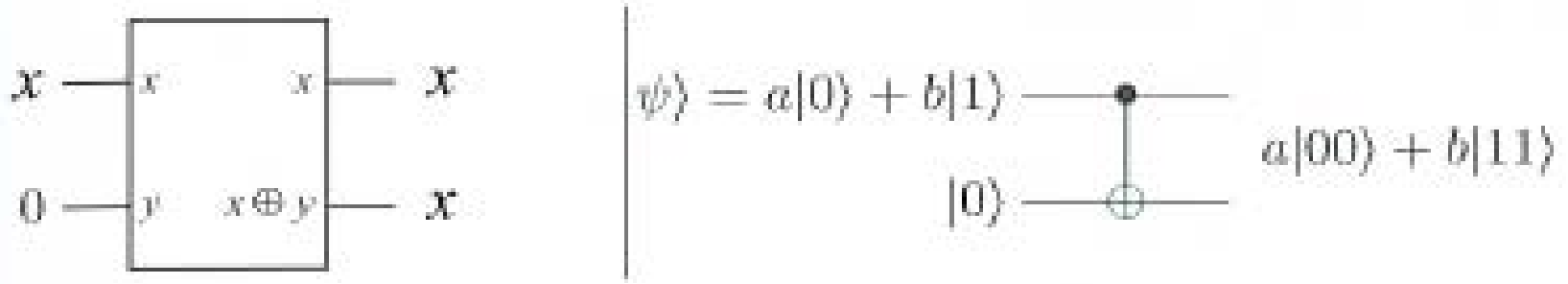


Figure 1.11. Classical and quantum circuits to 'copy' an unknown bit or qubit.

The resulting state is entangled

Is it possible to disentangle it?

Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

1.3.6 Bell states (EPR states)

- An entangled state basis

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}; \quad (1.23)$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}; \quad (1.24)$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}; \text{ and} \quad (1.25)$$

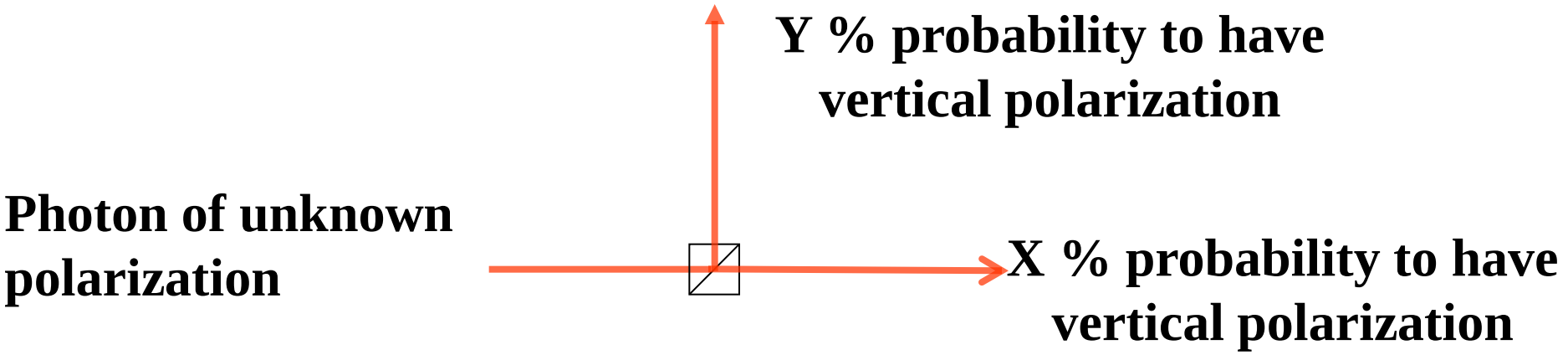
$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \quad (1.26)$$

Contents I

- 1.1 Global perspectives
  - History of quantum computation
- 1.2 Quantum bits
  - Multiple qubits
- 1.3 Quantum computation
  - Single qubit gates
  - Multiple qubit gates
  - Measurement bases
  - Quantum circuits
  - Qubit copying circuit
  - Bell states
  - Quantum teleportation

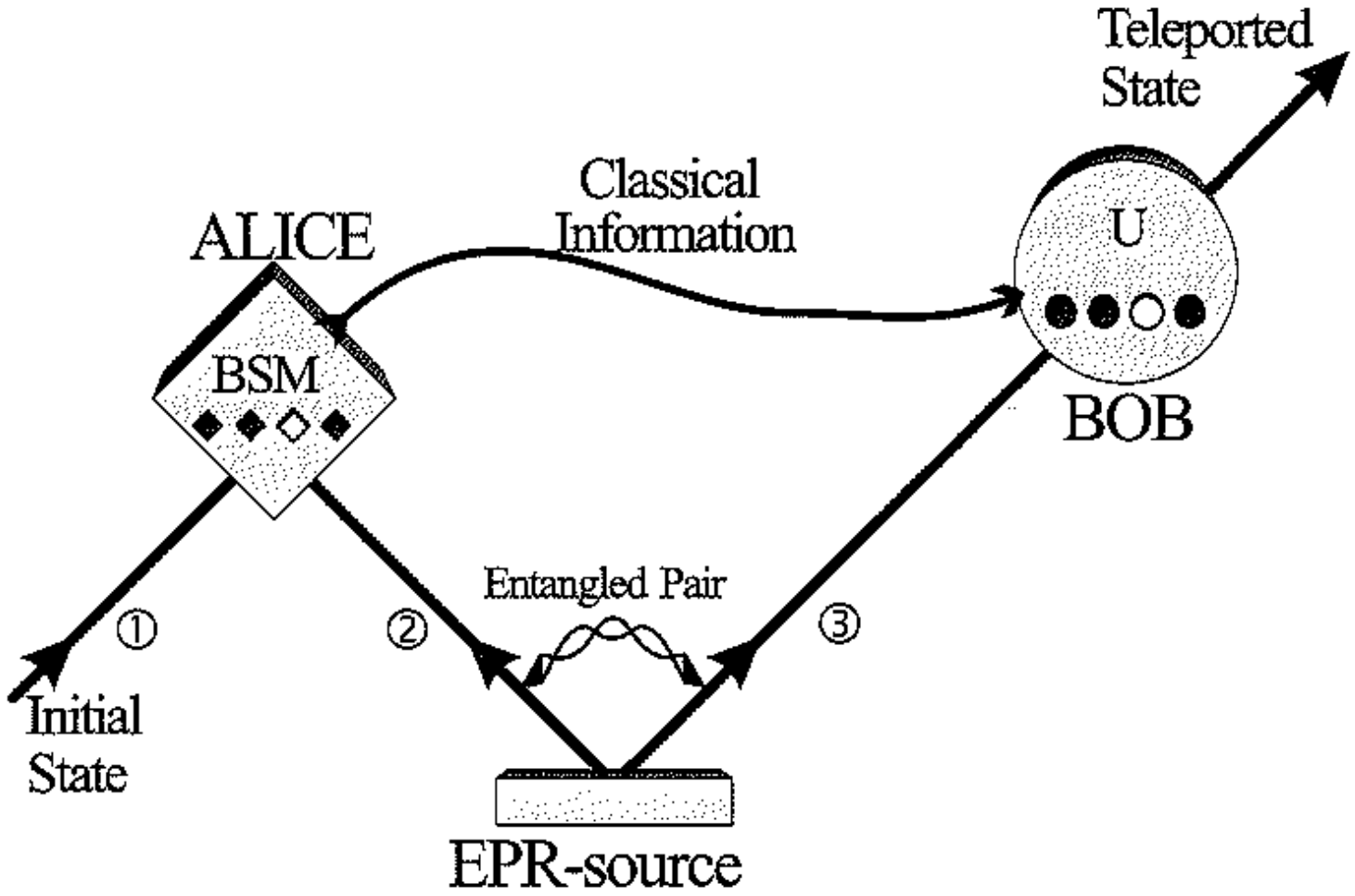
Concerning sending information about a quantum state?

- We cannot generally obtain complete information about an initially unknown quantum state



- An ability to copy an unknown quantum state would lead to faster than light communication?

1.3.7 Quantum teleportation



The Physics of Quantum Information,

Bouwmeester, Ekert, Zeilinger, Springer, 2000

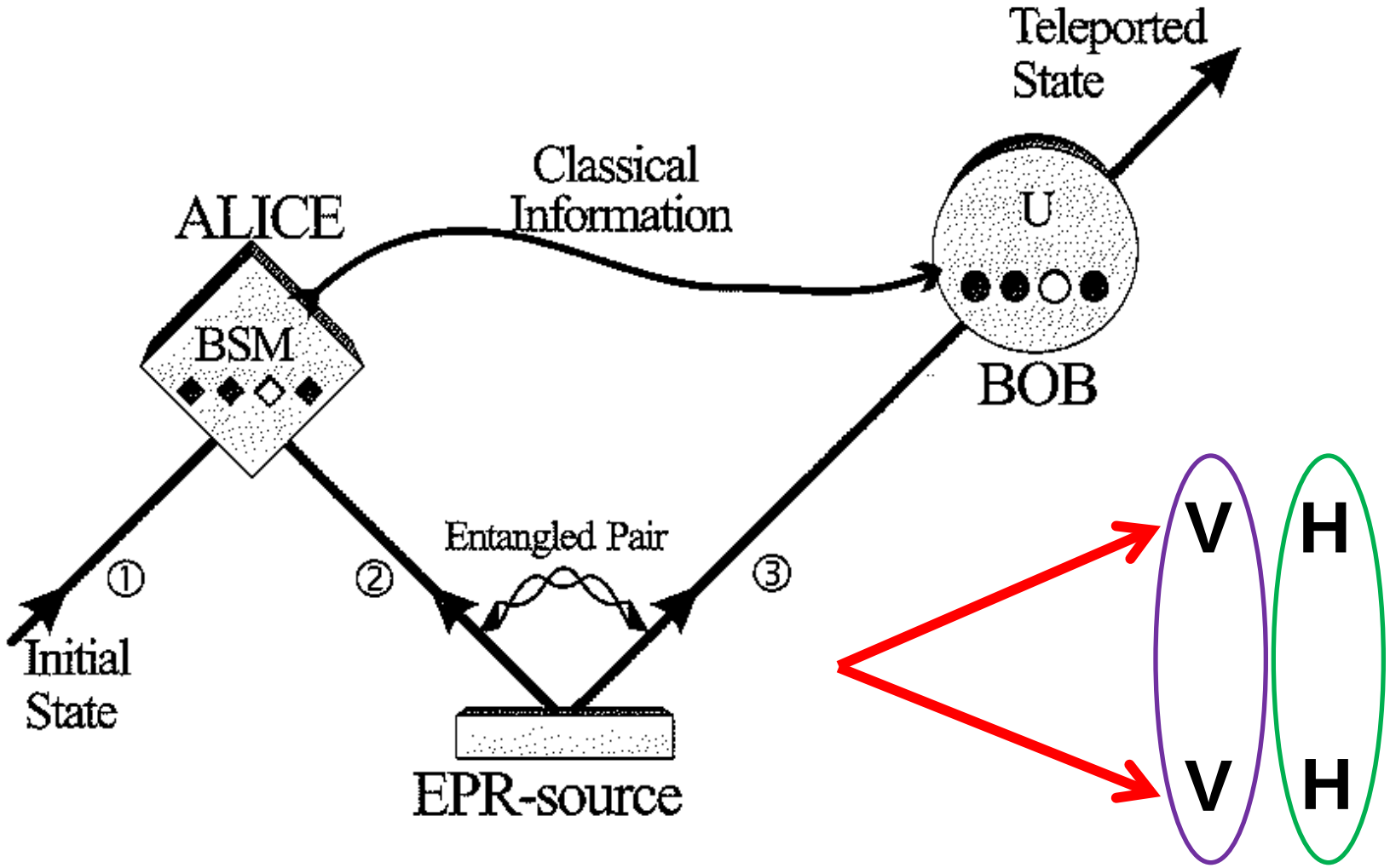
Why Alice and Bob

LUND UNIVERSITY

http://www.zap2it.com/tv/bob-the-builder/SH003260870000

http://www.thebarefootbeat.com/wp-content/uploads/2013/10/alice_in_wonderland17.jpg

1.3.7 Quantum teleportation



The Physics of Quantum Information,

Bouwmeester, Ekert, Zeilinger, Springer, 2000

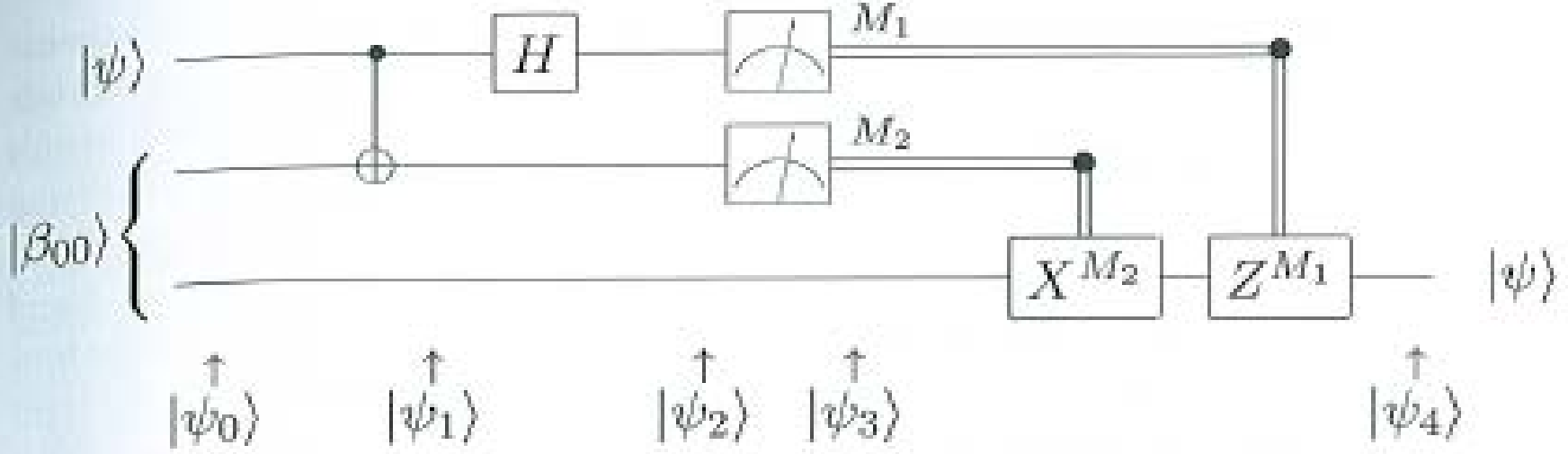


Figure 1.13. Quantum circuit for teleporting a qubit. The two top lines represent Alice's system, while the bottom line is Bob's system. The meters represent measurement, and the double lines coming out of them carry classical bits (recall that single lines denote qubits).

$$|\psi_2\rangle = \frac{1}{2}\Big[|00\rangle\,(\alpha|0\rangle + \beta|1\rangle) + |01\rangle\,(\alpha|1\rangle + \beta|0\rangle) + |10\rangle\,(\alpha|0\rangle - \beta|1\rangle) + |11\rangle\,(\alpha|1\rangle - \beta|0\rangle)\Big]\,. \tag{1.32}$$

$$00 \longmapsto |\psi_3(00)\rangle \equiv \Big[\alpha|0\rangle + \beta|1\rangle\Big] \tag{1.33}$$

$$01 \longmapsto |\psi_3(01)\rangle \equiv \Big[\alpha|1\rangle + \beta|0\rangle\Big] \tag{1.34}$$

$$10 \longmapsto |\psi_3(10)\rangle \equiv \Big[\alpha|0\rangle - \beta|1\rangle\Big] \tag{1.35}$$

$$11 \longmapsto |\psi_3(11)\rangle \equiv \Big[\alpha|1\rangle - \beta|0\rangle\Big]\,. \tag{1.36}$$

Quantum teleportation

Contents II

- 1.4 Quantum algorithms
  - Quantum parallelism
  - Deutsch's algorithm
  - The Deutsch-Josza algorithm
  - Quantum algorithms summarised
- 1.5 Experimental quantum information processing
  - Prospects for practical quantum information processing
- 1.6 Quantum information
  - Quantum information theory

Superposition of states makes a quantum computer (QC) powerful

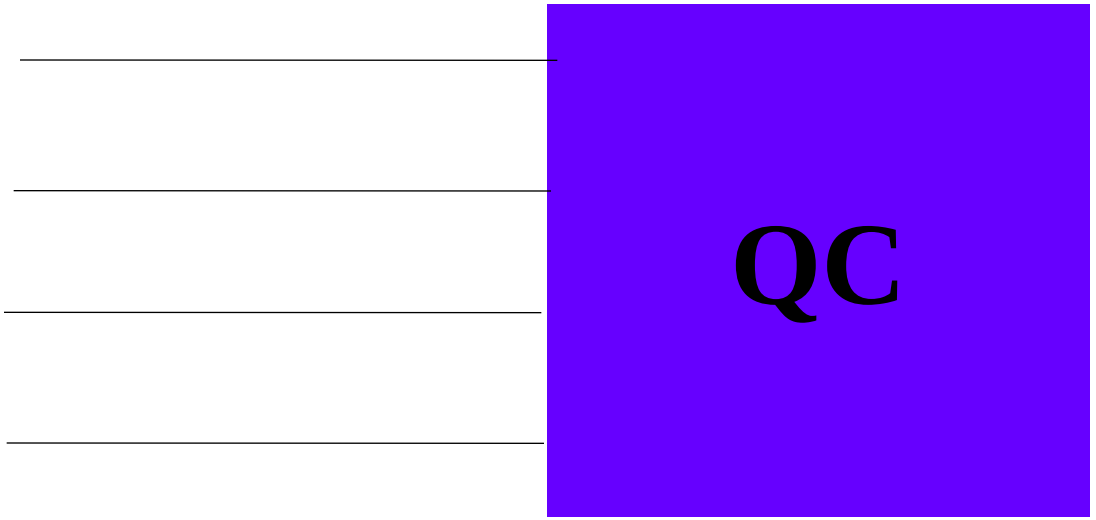
Input data

$(|0>+|1>)/\sqrt{2}$

$(|0>+|1>)/\sqrt{2}$

$(|0>+|1>)/\sqrt{2}$

$(|0>+|1>)/\sqrt{2}$



Input = (|0>+|1>) (|0>+|1>) (|0>+|1>) (|0>+|1>)/4=

=(|0000>+|0001>+|0010>+|0011> . . . +|1111>)/4

Quantum parallelism

- Consider an operation, *f*, performing the operation *f(x)* on a state *x* and putting the result in *y*. For a system $|x, y\rangle$ we obtain for $x = (|0\rangle + |1\rangle)/\sqrt{2}$
- $|x,y\rangle = [|0,f(0)\rangle + |1,f(1)\rangle]/\sqrt{2}$.

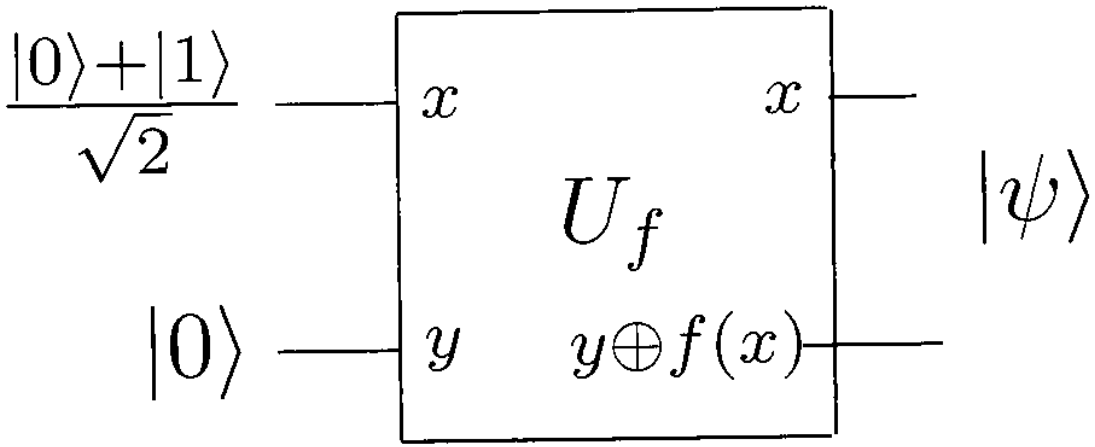
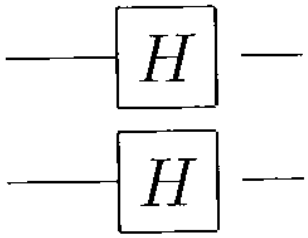


Figure 1.17. Quantum circuit for evaluating $f(0)$ and $f(1)$ simultaneously. U_f is the quantum circuit which takes inputs like $|x, y\rangle$ to $|x, y \oplus f(x)\rangle$.

Fig 1.18



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

Figure 1.18. The Hadamard transform $H^{\otimes 2}$ on two qubits.

$$|0> \Rightarrow \frac{|0>+|1>}{\sqrt{2}}$$

$$|1> \Rightarrow \frac{|0>-|1>}{\sqrt{2}}$$

- Start with 0 inputs
- What is the input product state? |00>
- What is the output state? (|00>+|01>+|10>+|11>)/2

For n inputs we get an equal superposition of 0 to (2^n-1)

Contents II

- 1.4 Quantum algorithms
  - Quantum parallelism
  - Deutsch's algorithm
  - The Deutsch-Josza algorithm
  - Quantum algorithms summarised
- 1.5 Experimental quantum information processing
  - Prospects for practical quantum information processing
- 1.6 Quantum information
  - Quantum information theory

1.4.3 Deutsch's algorithm

- Calculates $f(0) \oplus f(1)$

Work on board

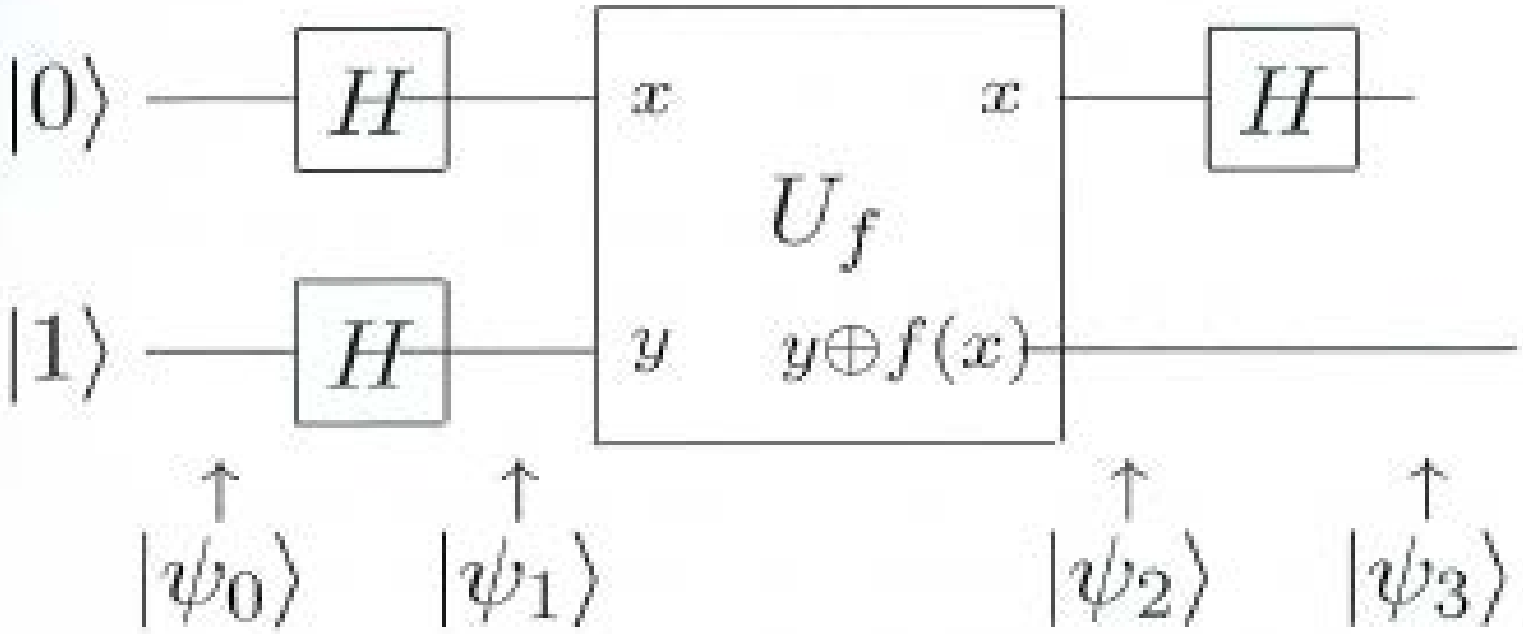


Figure 1.19. Quantum circuit implementing Deutsch's algorithm.

Contents II

- 1.4 Quantum algorithms
  - Quantum parallelism
  - Deutsch's algorithm
  - The Deutsch-Josza algorithm
  - Quantum algorithms summarised
- 1.5 Experimental quantum information processing
  - Prospects for practical quantum information processing
- 1.6 Quantum information
  - Quantum information theory

1.4.4 Deutsch-Jozsa algorithm

- Alice selects a number between 0 and 2^n-1. Bob evaluates it with a function (which may be very difficult to evaluate but) which is constant or balanced.

The Deutsch-Jozsa algorithm

Lets say n=20

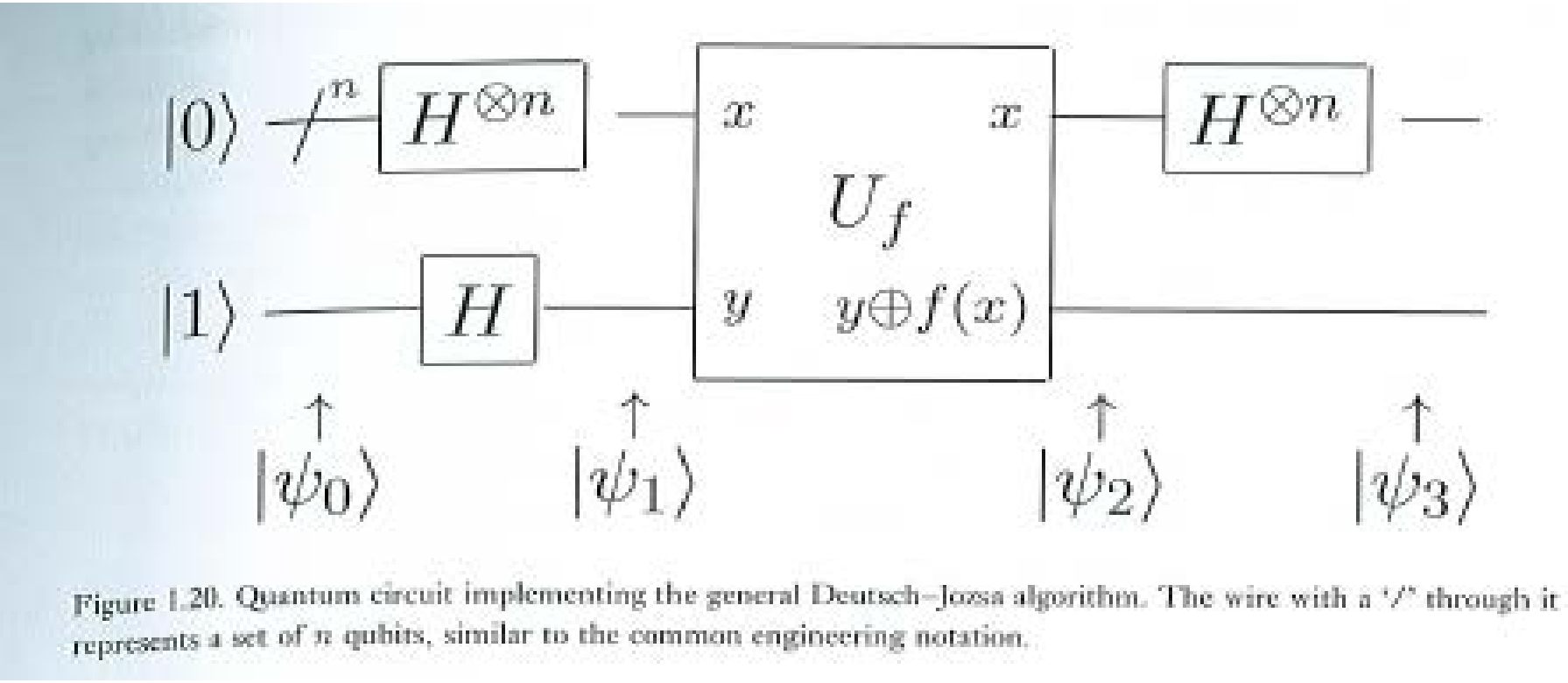


Figure 1.20. Quantum circuit implementing the general Deutsch–Jozsa algorithm. The wire with a '/' through it represents a set of n qubits, similar to the common engineering notation.

If all output bits in the query (x output) register are zero the function is constant, otherwise it is balanced

Classically Alice may need up to $2^n/2 + 1$ calls to tell whether it is constant or balanced.

1.4.4 Deutsch-Jozsa algorithm

- The problem is not so important and a probabilistic classical computer could solve it fast with a good accuracy.
- Finding important/relevant algorithms is challenging

Contents II

- 1.4 Quantum algorithms
  - Quantum parallelism
  - Deutsch's algorithm
  - The Deutsch-Josza algorithm
  - Quantum algorithms summarised
- 1.5 Experimental quantum information processing
  - Prospects for practical quantum information processing
- 1.6 Quantum information
  - Quantum information theory

1.4.5 Quantum algorithms

- We will treat three classes of superior quantum algorithms
  - The quantum Fourier transform (Chapter 5) GJ
    - Hidden subgroup problem
  - Search problems (Chapter 6) GJ
  - Quantum simulations (Chapter 4) SK

Contents II

- 1.4 Quantum algorithms
  - Quantum parallelism
  - Deutsch's algorithm
  - The Deutsch-Josza algorithm
  - Quantum algorithms summarised
- 1.5 Experimental QI processing (Andreas Walther)
  - Prospects for practical quantum information processing
    - (Some random statements)
- 1.6 Quantum information
  - Quantum information theory

1.5.2 Prospects for quantum information processing

- A quantum computer can solve some problems which are untractable with conventional computers, such as, certain computationally hard problems
- **QC is a structured way to learn how to control quantum systems and how to design fully controllable quantum systems**

1.5.2 Prospects for quantum information processing

- Building quantum information processors is a great challenge for scientists and engineers in the third millenium

Power of quantum computers

- The quantum corollary to Moore's law could essentially be something like "a single qubit will be added to quantum computers every 18 months"

Quantum error correction (Chapter 10)

- Digital and analog computers
- There are efficient error correction algorithms for correcting errors in quantum computer operations when the error per operation is $< 10^{-4}$
- If quantum operations can be performed with a fractional error of less than 10^{-4} we can for example keep arbitrary large quantum systems in superposition for arbitrary long time!

Contents II

- 1.4 Quantum algorithms
  - Quantum parallelism
  - Deutsch's algorithm
  - The Deutsch-Josza algorithm
  - Quantum algorithms summarised
- 1.5 Experimental quantum information processing
  - Prospects for practical quantum information processing
- 1.6 Quantum information (chapters 8, 9, 12)
  - Quantum information theory

Quantum Communication

Secure Data Transmission

Data security of the future?

→ communication based on quantum physics

quantum physics:

An eavesdropper influences information.

Alice and Bob will detect the eavesdropping.

LUND UNIVERSITY

The ”one time pad” is the only known perfectly safe classical cryptosystem

If we choose a very simple digital alphabet, in which we use only capital letters and some punctuation marks, such as

A	B	C	D	E	...	...	X	Y	Z		?	,	.
00	01	02	03	04	...	...	23	24	25	26	27	28	29

we can illustrate the secret-key encrypting procedure by the following simple example (we refer to the dietary requirements of 007): In order to obtain

	S	H	A	K	E	N		N	O	T		S	T	I	R	R	E	D
	18	07	00	10	04	13	26	13	14	19	26	18	19	08	17	17	04	03
Key	15	04	28	13	14	06	21	11	23	18	09	11	14	01	19	05	22	07
	03	11	28	23	18	19	17	24	07	07	05	29	03	09	06	22	26	10
	D	L	,	X	S	T	P	Y	H	H	F	.	C	J	G	W		K

From ”*Quantum information*”, Zeilinger . . .

LUND
UNIVERSITY

Quantum cryptography

- Safe transmission of key
- Quantum key distribution

Quantum Communication

Secure Data Transmission

Data security of the future?

→ communication based on quantum physics

quantum physics:

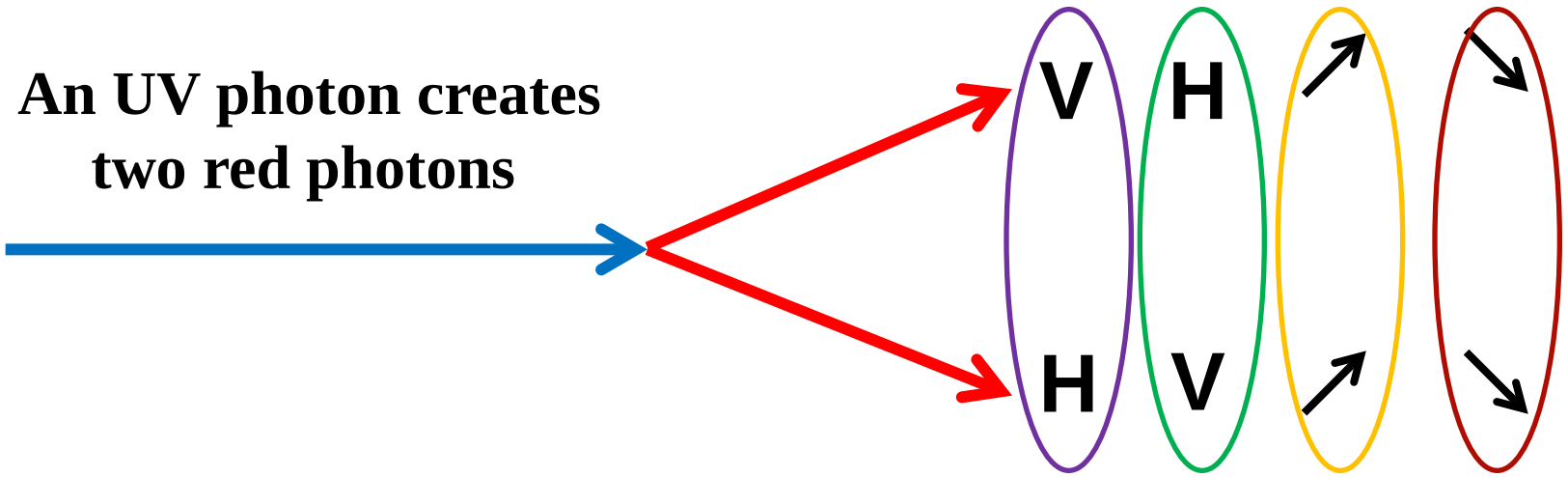
An eavesdropper influences information.

Alice and Bob will detect the eavesdropping.

Quantum distinguishability

- Ability to distinguish non-orthogonal states would lead to faster than light communication

The wave function does not collapse until there is a measurement

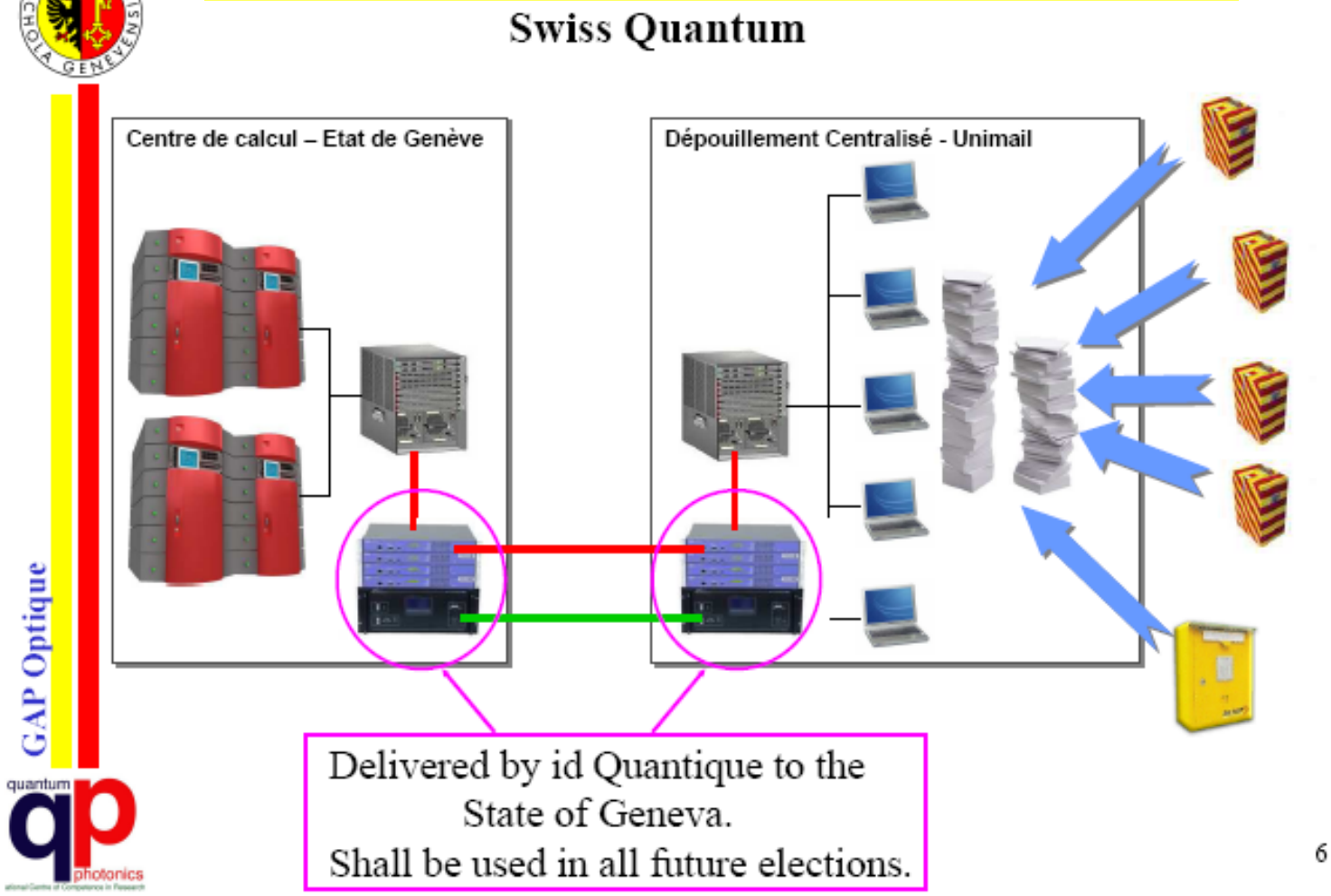


Depending on our measurement the resulting polarization will be different

Geneva University, Gisin group

Gisin, Ribordy, Tittel, Zbinden, Rev. Mod. Phys. **74**, 145 (2002)

Swiss Federal Elections, Nov'07



Courtesy: Nicolas Gisin, University of Geneva

LUND
UNIVERSITY

What is quantum information

- Quantum information concerns the use of quantum mechanical processes and quantum mechanical systems for transmitting, storing or processing information
- Quantum information introduces new non-classical resources like superposition and entanglement into the field of information science


Photons as quantum information carriers

Goals for quantum information

- Develop tools which sharpen our intuition of quantum mechanics, and makes its predictions more transparent to human minds

Science offers the boldest metaphysics of the age. It is a thoroughly, human construct, driven by the faith that if we dream, press to discover, explain, and dream again, thereby plunging repeatedly into new terrain, the world will somehow come clearer and we will grasp the true strangeness of the universe. And the strangeness will all prove to be connected, and make sense.

Edward O. Wilson