INTRODUCTION TO QUANTUM COMPUTING 1.

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

March 5, 2008

1. INTRODUCTION

In the first lecture we deal with reasons why to study quantum computing and with very basic experiments, principles, formalism and some basic outcomes of Quantum Information Processing and Communication.

We deal also, at the beginning, in some details, with classical reversible computations, as a special case of quantum computation.

INTRODUCTORY OBSERVATIONS

In quantum computing we witness a merge of two of the most important areas of science of 20th century: quantum physics and informatics.

This merge is bringing new aims, challenges and potentials for informatics and also new approaches for physics to explore quantum world.

In spite of the fact that it is hard to predict particular impacts of quantum computing on computing in general, it is quite safe to expect that the merge will lead to important outcomes.

A VIEW of HISTORY

19th century was mainly influenced by the first industrial revolution that had its basis in the classical mechanics discovered, formalized and developed in the 18th century.

20th century was mainly influenced by the second industrial revolution that had its basis in electrodynamics discovered, formalized and developed in the 19th century.

21th century can be expected to be mainly developed by quantum mechanics and informatics discovered, formalized and developed in the 20th century.

QUANTUM PHYSICS

is

is an **excellent theory** to predict probabilities of quantum events.

Quantum physics is an elegant and conceptually simple theory that describes with astounding precision a large spectrum of the phenomena of Nature.

The predictions made on the base of quantum physics have been experimentally verified to 14 orders of precision. No conflict between predictions of theory and experiments is known.

Without quantum physics we cannot explain properties of superfluids, functioning of laser, the substance of chemistry, the structure and function of DNA, the existence and behaviour of solid bodies, color of stars, ...

QUANTUM PHYSICS — SUBJECT I

Quantum physics deals with fundamentals entities of physics — particles like

- protons, electrons and neutrons (from which matter is built);
- photons (which carry electromagnetic radiation) - they are the only particles we can directly observe;
- various “elementary particles” which mediate other interactions of physics.

We call them **particles** in spite of the fact that some of their properties are totally unlike the properties of what we call particles in our ordinary world.

Indeed, it is not clear in what sense these “particles” can be said to have properties at all.

QUANTUM MECHANICS

is, in spite of its quality, from the point of view of explaining quantum phenomena, a very unsatisfactory theory.

Quantum mechanics is a theory with either some hard to accept principles or a theory leading to mysteries and paradoxes.

> *Quantum theory seems to lead to philosophical standpoints that many find deeply unsatisfying.*
>
> *At best, and taking its descriptions at their most literal, it provides us with a very strange view of the world indeed.*
>
> *At worst, and taking literally the proclamations of some of its most famous protagonists, it provides us with no view of the world at all.*
>
> Roger Penrose

You have nothing to do but mention the quantum theory, and people will take your voice for the voice of science, and believe anything

Bernard Shaw (1938)

WHAT QUANTUM PHYSICS TELL US?

Quantum physics

tells us

WHAT happens

but does not tell us

WHY it happens

and does not tell us either

HOW it happens

nor

HOW MUCH it costs

QUANTUM PHYSICS UNDERSTANDING

I am going to tell you what Nature behaves like......

However do not keep saying to yourself, if you can possibly avoid it,

BUT HOW CAN IT BE LIKE THAT?

because you will get “down the drain” into a blind alley from which nobody has yet escaped.

NOBODY KNOWS HOW IT CAN BE LIKE THAT.

Richard Feynman (1965): The character of physical law.

QUANTUM MECHANICS - ANOTHER VIEW

- Quantum mechanics is not physics in the usual sense - it is not about matter, or energy or waves, or particles - it is about information, probabilities, probability amplitudes and observables, and how they relate to each other.
- Quantum mechanics is what you would inevitably come up with if you would started from probability theory, and then said, let's try to generalize it so that the numbers we used to call ”probabilities” can be negative numbers.

  As such, the theory could be invented by mathematicians in the 19th century without any input from experiment. It was not, but it could have been (Aaronson, 1997).

WHY is QIPC so IMPORTANT?

There are five main reasons why QIPC is increasingly considered as of (very) large importance:

- QIPC is believed to lead to new Quantum Information Processing Technology that could have deep and broad impacts.
- Several sciences and technology are approaching the point at which they badly need expertise with isolation, manipulating and transmission of particles.
- It is increasingly believed that new, quantum information processing based, understanding of (complex) quantum phenomena and systems can be developed.
- Quantum cryptography seems to offer new level of security and be soon feasible.
- QIPC has been shown to be more efficient in interesting/important cases.
- TCS and Information theory got new dimension and impulses.

WHY WE SHOULD TRY to have QUANTUM COMPUTERS?

When you try to reach for stars you may not quite get one, but you won’t come with a handful of mud either.

Leo Burnett

WHY von NEUMANN

DID (COULD) NOT DISCOVER QUANTUM COMPUTING?

- No computational complexity theory was known (and needed).
- Information theory was not yet well developed.
- Progress in physics and technology was far from what would be needed to make even rudimentary implementations.
- The concept of randomized algorithms was not known.
- No public key cryptography was known (and needed).

DEVELOPMENT of BASIC VIEWS

on the role of information in physics:

- Information is information, nor matter, nor energy.

  Norbert Wiener

- Information is physical

  Ralf Landauer

  Should therefore information theory and foundations of computing (complexity theory and computability theory) be a part of physics?

- Physics is informational

  Should (Hilbert space) quantum mechanics be a part of Informatics?

WHEELER's VIEW

I think of my lifetime in physics as divided into three periods

- In the first period ...I was convinced that

  EVERYTHING IS PARTICLE

- I call my second period

  EVERYTHING IS FIELDS

- Now I have new vision, namely that

  EVERYTHING IS INFORMATION

WHEELER's "IT from BIT"

IT FROM BIT symbolizes the idea that every item of the physical world has at the bottom - at the very bottom, in most instances - an immaterial source and explanation.

Namely, that which we call reality arises from posing of yes-no questions, and registering of equipment-invoked responses.

In short, that things physical are information theoretic in origin.

TWO BASIC WORLDS

BASIC OBSERVATION: All information processing and transmissions are done in the physical world.

Our basic standpoint is that:

The goal of physics is to study elements, phenomena, laws and limitations of the physical world.

The goal of informatics is to study elements, phenomena, laws and limitations of the information world.

TWO WORLDS - BASIC QUESTIONS

- **Which of the two worlds, physical and information, is more basic?**
- **What are the main relations between the basic concepts, principles, laws and limitations of these two worlds?**

Quantum physics is an elementary theory of information. *Č. Brückner, A. Zeilinger*

MAIN PARADOX

- Quantum physics is extremely elaborated theory, full of paradoxes and mysteries. It takes any physicist years to develop a feeling for quantum mechanics.
- Some (theoretical) computer scientists/mathematicians, with almost no background in quantum physics, have been able to make crucial contributions to theory of quantum information processing.

PERFORMANCE OF PROCESSORS

1. There are no reasons why the increase of performance of processors should not follow **Moore law** in the near future.
2. A long term increase of performance of processors according to **Moore law** seems to be possible only if, at the performance of computational processes, we get more and more on atomic level.

An extrapolation of the curve depicting the number of electrons needed to store a bit of information shows that around 2020 we should need one electron to store one bit.

MOORE LAW

It is nowadays accepted that information processing technology has been developed for the last 50 years according the so-called Moore law. This law has now three forms.

Economic form: Computer power doubles, for constant cost, every two years or so.

Physical form: The number of atoms needed to represent one bit of information should halves every two years or so.

Quantum form: For certain application, quantum computers need to increase in the size only by one qubit every two years or so, in order to keep pace with the classical computers performance increase.

PRE-HISTORY

1970 Landauer demonstrated importance of reversibility for minimal energy computation;

1973 Bennett showed the existence of universal reversible Turing machines;

1981 Toffoli-Fredkin designed a universal reversible gate for Boolean logic;

1982 Benioff showed that quantum processes are at least as powerful as Turing machines;

1982 Feynman demonstrated that quantum physics cannot be simulated effectively on classical computers;

1984 Quantum cryptographic protocol BB84 was published, by Bennett and Brassard, for absolutely secure generation of shared secret random classical keys.

1985 Deutsch showed the existence of a universal quantum Turing machine.

1989 First cryptographic experiment for transmission of photons, for distance 32.5cm was performed by Bennett, Brassard and Smolin.

1993 Bernstein-Vazirani-Yao showed the existence of an efficient universal quantum Turing machine;

1993 Quantum teleportation was discovered, by Bennett et al.

1994 Shor discovered a polynomial time quantum algorithm for factorization;

Cryptographic experiments were performed for the distance of 10km (using fibers).

1994 Quantum cryptography went through an experimental stage;

1995 DiVincenzo designed a universal gate with two inputs and outputs;

1995 Cirac and Zoller demonstrated a chance to build quantum computers using existing technologies.

1995 Shor showed the existence of quantum error-correcting codes.

1996 The existence of quantum fault-tolerant computation was shown by P. Shor.

REVERSIBILITY

QUANTUM PROCESSES ARE REVERSIBLE

An operation is reversible if its outputs uniquely determine its inputs.

$$(a,b) \longrightarrow a+b$$

a non-reversible operation

$$(a,b) \longrightarrow (a+b, a-b)$$

a reversible operation

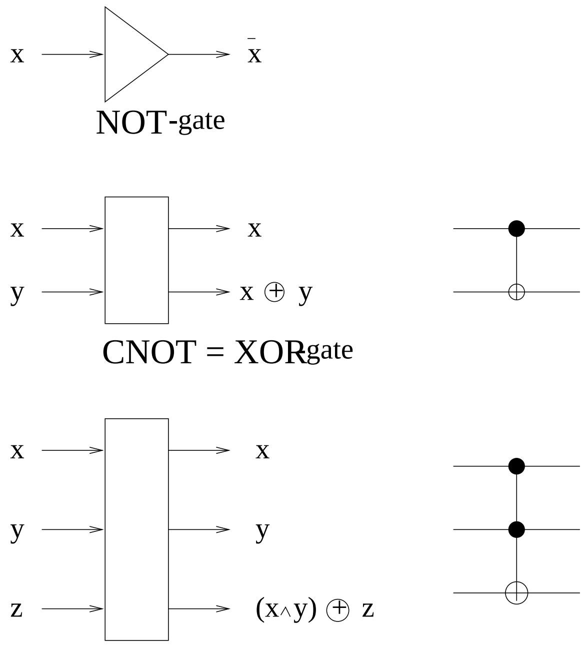
$$a \longrightarrow f(a)$$

A mapping that can but does not have to be reversible

$$(a,0) \longrightarrow (a, f(a))$$

a surely reversible operation

REVERSIBLE GATES



NOT-gate

CNOT = XOR-gate

CCNOT-gate

A universal reversible gate for
Boolean logic

Three reversible classical gates: NOT gate, XOR or CNOT gate and Toffoli or CCNOT gate.

GARBAGE REMOVAL

In order to produce reversible computation one needs to produce garbage (information). Its removal is possible and important.

Bennett (1973) has shown that if a function f is computable by a one-tape Turing machine in time $t(n)$, then there is a 3-tape reversible Turing machine computing, with constant time overhead, the mapping

$$a \longrightarrow (a, g(a), f(a))$$

Bennett (1973) has also shown that there is an elegant reversible way how to remove garbage:

Basic computation: of f: $a \rightarrow (a, g(a), f(a))$.

Fanout: $(a, g(a), f(a)) \rightarrow (a, g(a), f(a), f(a))$

Uncomputing of f : $(a, g(a), f(a), f(a)) \rightarrow (a, f(a))$

BILLIARD BALL REVERSIBLE COMPUTER

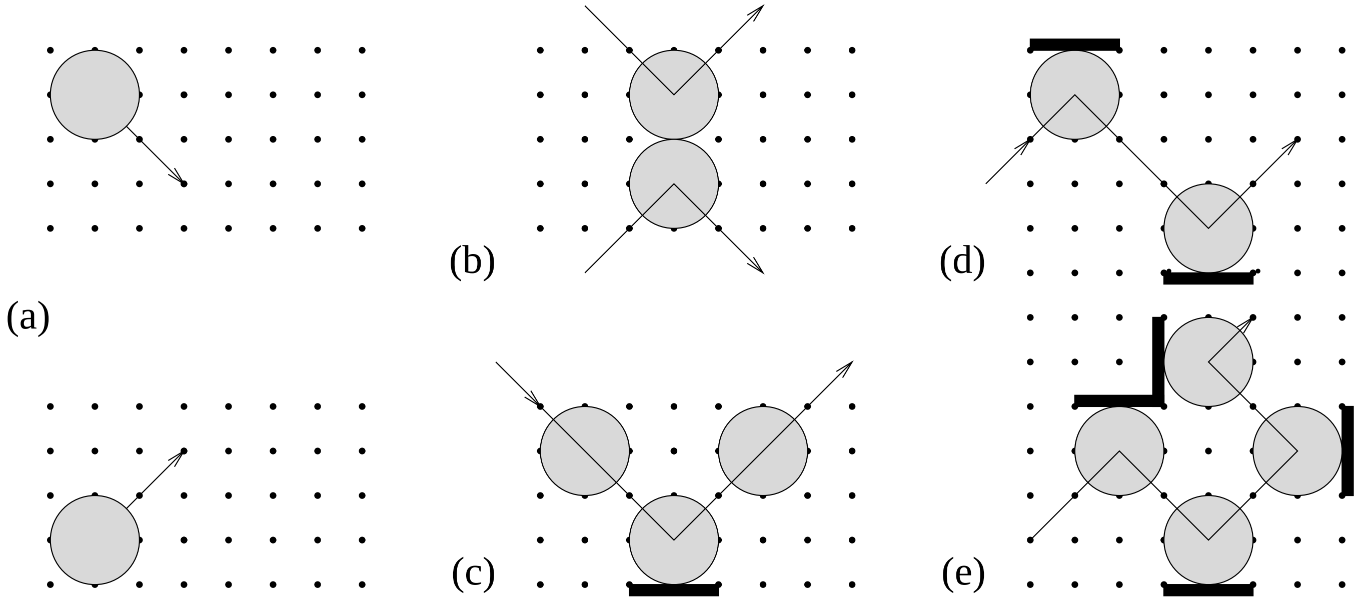


Figure 1: Billiard ball model of reversible computation

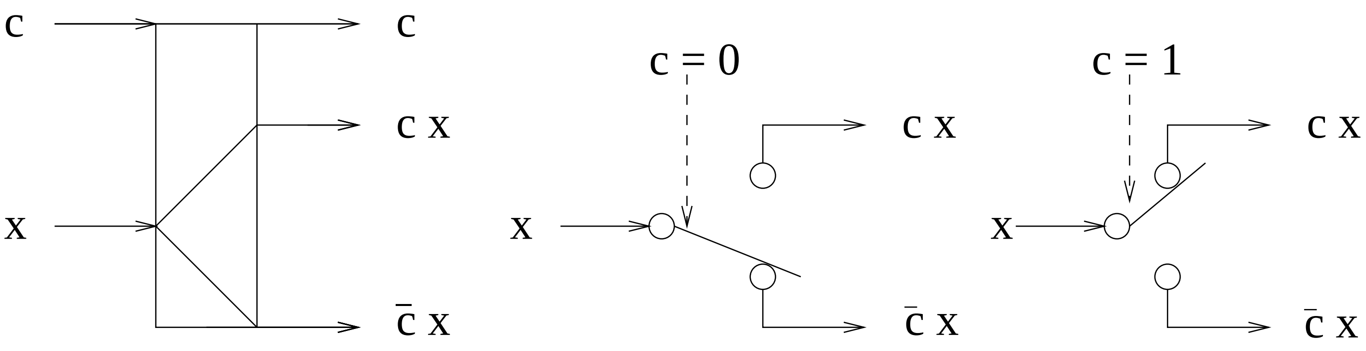


Figure 2: Switch gate

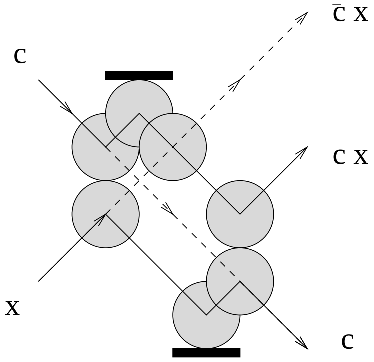


Figure 3: A billiard ball implementation of the switch gate

CLASSICAL EXPERIMENTS

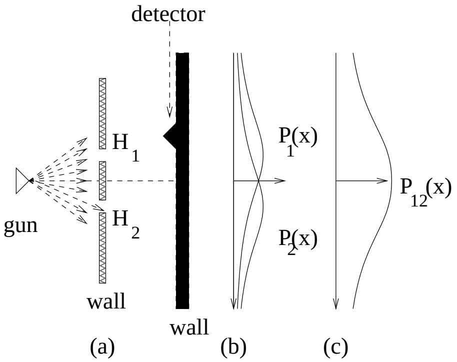


Figure 4: Experiment with bullets

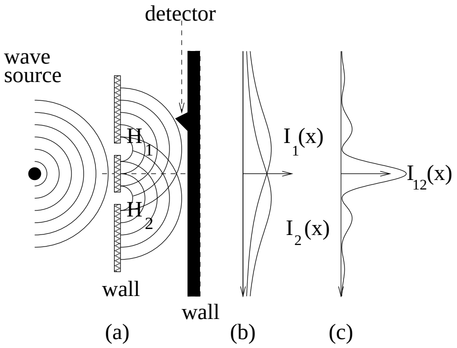


Figure 5: Experiments with waves

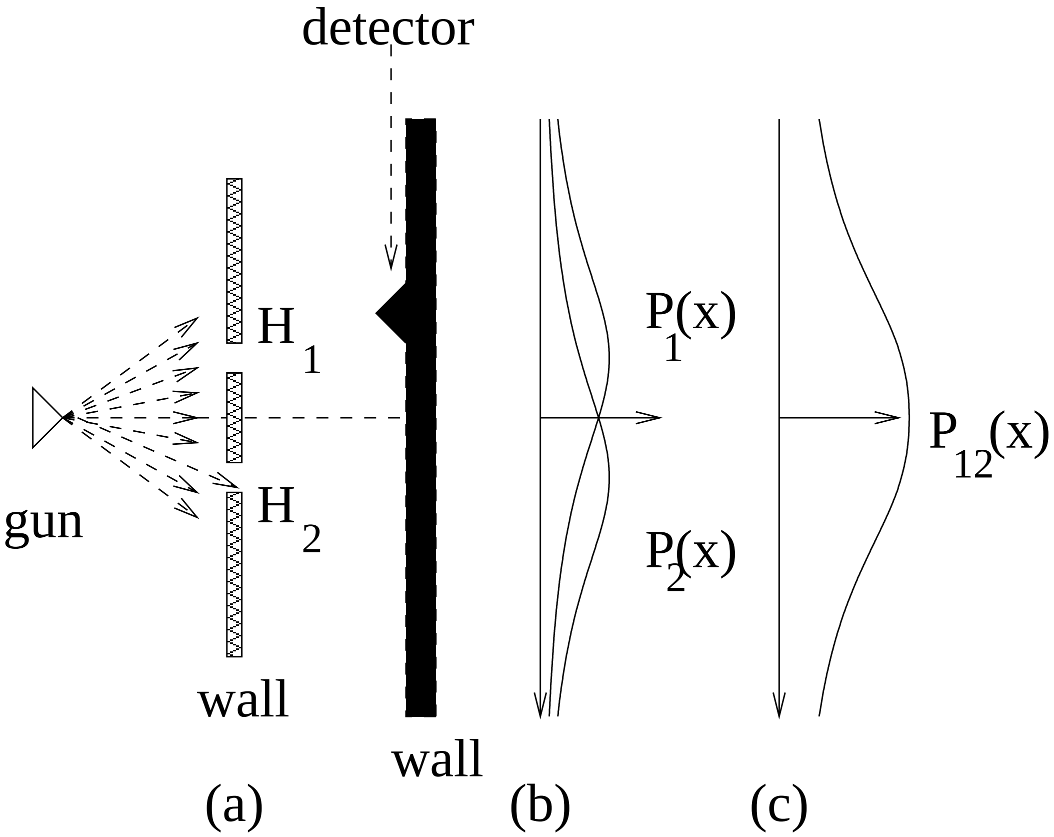


Figure 6: Experiment with bullets

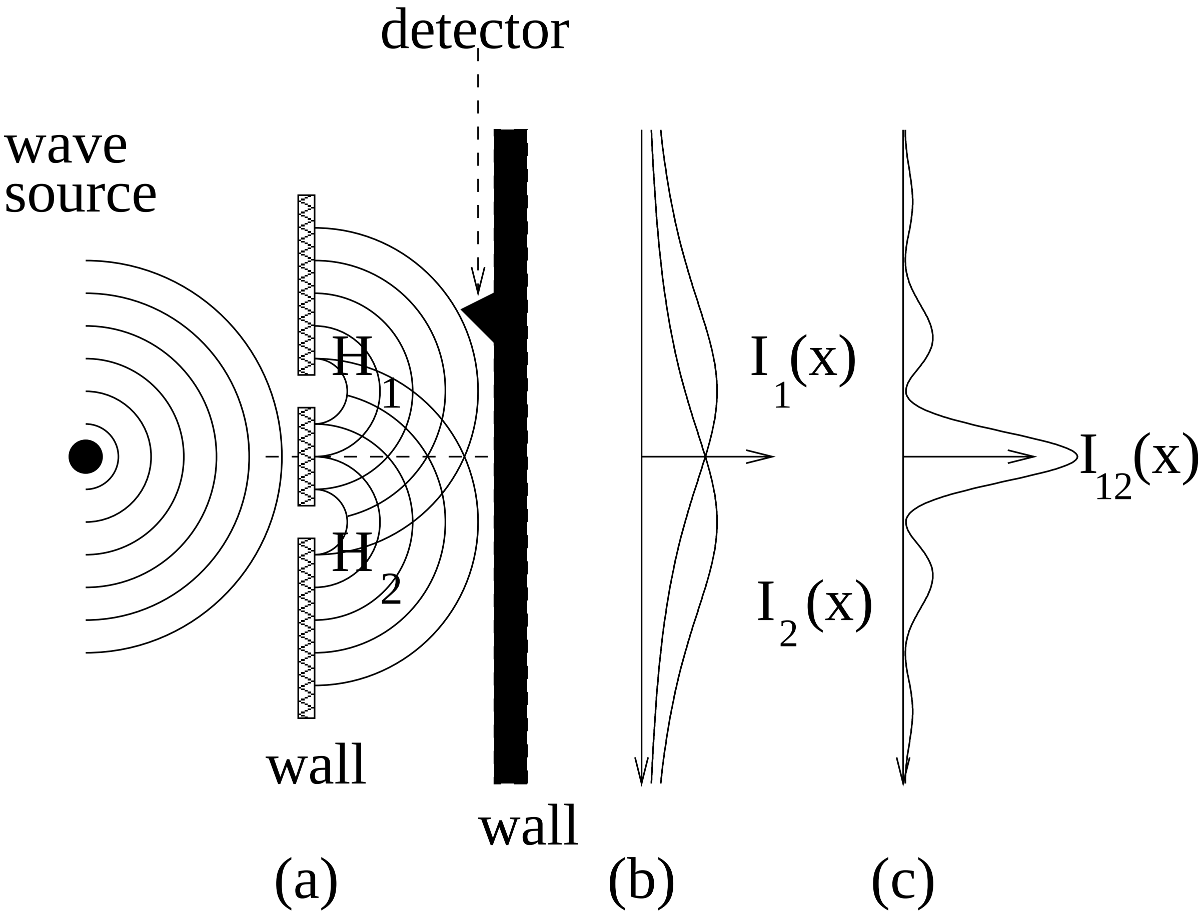


Figure 7: Experiments with waves

QUANTUM EXPERIMENTS

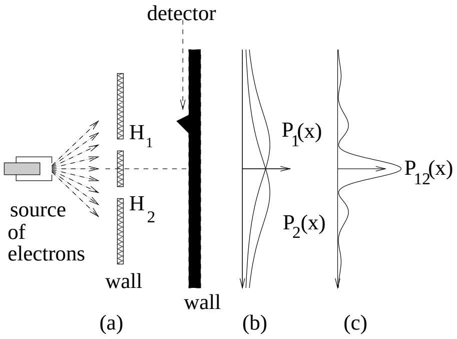


Figure 8: Two-slit experiment

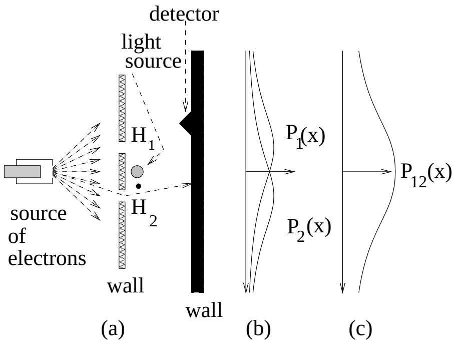


Figure 9: Two-slit experiment with an observation

QUANTUM EXPERIMENTS

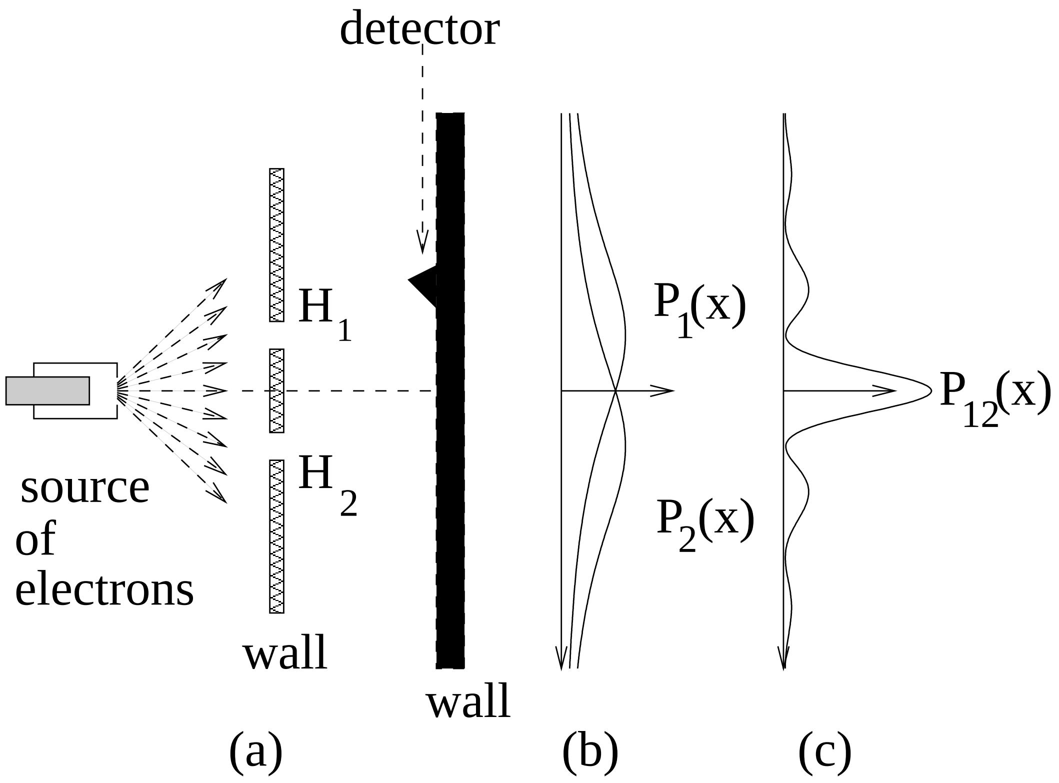


Figure 10: Two-slit experiment

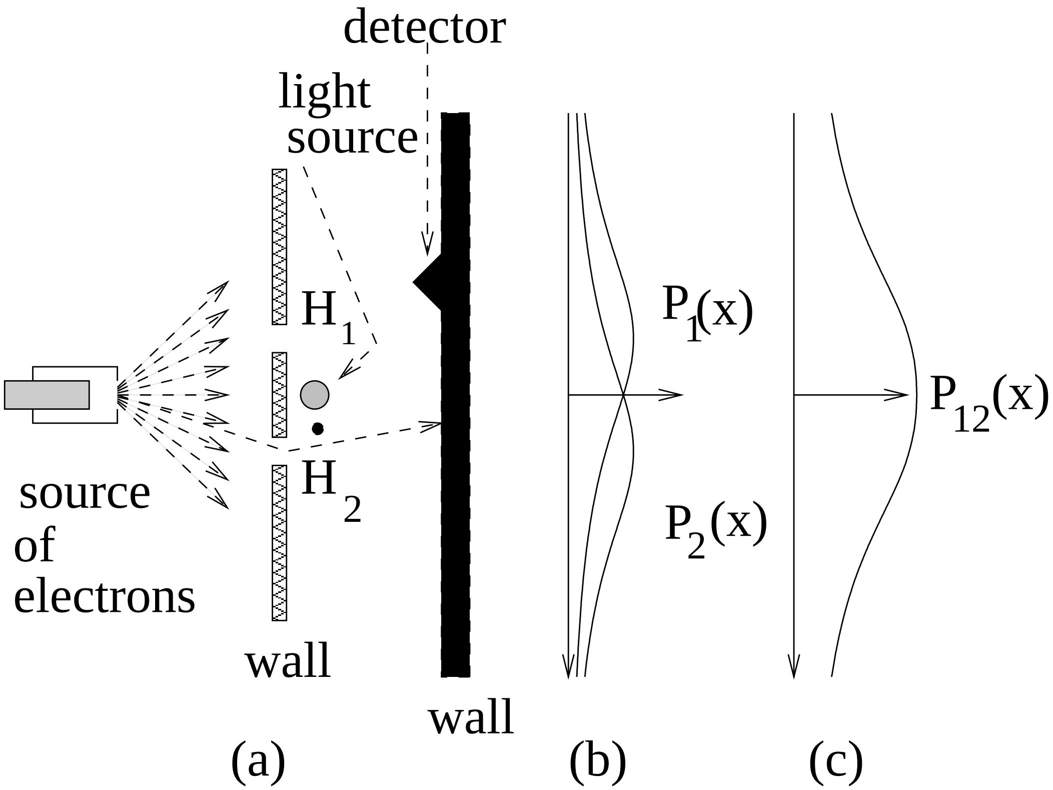


Figure 11: Two-slit experiment with an observation

TWO-SLIT EXPERIMENT – OBSERVATIONS

- Contrary to our intuition, at some places one observes fewer electrons when both slits are open, than in the case only one slit is open.
- Electrons — particles, seem to behave as waves.
- Each electron seems to behave as going through both holes at once.
- Results of the experiment do not depend on frequency with which electrons are shot.
- Quantum physics has no explanation where a particular electron reaches the detector wall. All quantum physics can offer are statements on the probability that an electron reaches a certain position on the detector wall.

BOHR's WAVE-PARTICLE DUALITY PRINCIPLES

- Things we consider as waves correspond actually to particles and things we consider as particles have waves associated with them.
- The wave is associated with the position of a particle - the particle is more likely to be found in places where its wave is big.
- The distance between the peaks of the wave is related to the particle's speed; the smaller the distance, the faster particle moves.
- The wave's frequency is proportional to the particle's energy. (In fact, the particle's energy i s equal exactly to its frequency times Planck's constant.)

QUANTUM MECHANICS

- **Quantum mechanics is a theory that describes atomic and subatomic particles and their interactions.**
- **Quantum mechanics was born around 1925.**
- **A physical system consisting of one or more quantum particles is called a quantum system.**
- **To completely describe a quantum particle an infinite-dimensional Hilbert space is needed.**
- **For quantum computational purposes it is sufficient a partial description of particle(s) given in a finite-dimensional Hilbert (inner-product) space.**
- **To each isolated quantum system we associate an inner-product vector space elements of which of norm 1 are called (pure) states.**

THREE BASIC PRINCIPLES

P1 To each transfer from a quantum state ϕ to a state ψ a complex number

$$\langle\psi|\phi\rangle$$

is associated, which is called the **probability amplitude** of the transfer, such that

$$|\langle\psi|\phi\rangle|^2$$

is the **probability** of the transfer.

P2 If a transfer from a quantum state ϕ to a quantum state ψ can be decomposed into two subsequent transfers

$$\psi \leftarrow \phi' \leftarrow \phi$$

then the resulting amplitude of the transfer is the **product** of amplitudes of sub-transfers: $\langle\psi|\phi\rangle = \langle\psi|\phi'\rangle\langle\phi'|\phi\rangle$

P3 If the transfer from ϕ to ψ has two independent alternatives, with amplitudes α and β

$$\begin{tikzcd}\psi & \varphi \arrow[l, bend right] \arrow[l, bend left]\end{tikzcd}$$

then the resulting amplitude is the sum $\alpha + \beta$ of amplitudes of two sub-transfers.

QUANTUM SYSTEM = HILBERT SPACE

Hilbert space $\mathcal{H}_n$ is n-dimensional complex vector space with

scalar product

$$\langle\psi|\phi\rangle = \sum_{i=1}^{n} \phi_i\psi_i^* \textbf{ of vectors } |\phi\rangle = \begin{vmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{vmatrix}, |\psi\rangle = \begin{vmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{vmatrix},$$

norm of vectors

$$||\phi|| = \sqrt{|\langle\phi|\phi\rangle|}$$

and the metric

$$\textbf{dist}(\phi,\psi) = ||\phi - \psi||.$$

This allows us to introduce on $\mathcal{H}$ a topology and such concepts as continuity.
Elements (vectors) of a Hilbert space $\mathcal{H}$ are usually called **pure states** of H.

ORTHOGONALITY of PURE STATES

Two quantum states $|\phi\rangle$ and $|\psi\rangle$ are called orthogonal if their scalar product is zero, that is if

$$\langle\phi|\psi\rangle = 0.$$

Two pure quantum states are physically perfectly distinguishable only if they are orthogonal.

In every Hilbert space there are so-called orthogonal bases all states of which are mutually orthogonal.

BRA-KET NOTATION

Dirac introduced a very handy notation, so called bra-ket notation, to deal with amplitudes, quantum states and linear functionals $f : H \rightarrow \mathbf{C}$.

If $\psi, \phi \in H$, then

$\langle\psi|\phi\rangle$ — a number - a scalar product of ψ and ϕ
(an amplitude of going from ϕ to ψ).

$|\phi\rangle$ — **ket-vector** — a column vector - an equivalent to ϕ

$\langle\psi|$ — **bra-vector** – a row vector - the conjugate transpose of $|\psi\rangle$ – a linear functional on H

such that $\langle\psi|(|\phi\rangle) = \langle\psi|\phi\rangle$

Example If $\phi = (\phi_1, \ldots, \phi_n)$ and $\psi = (\psi_1, \ldots, \psi_n)$, then

$$\text{ket vector - } |\phi\rangle = \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix} \quad \text{and} \quad \langle\psi| = (\psi_1^*, \ldots, \psi_n^*) \quad - \text{bra-vector}$$

and

$$\text{inner product - scalar product: } \langle\phi|\psi\rangle = \sum_{i=1}^{n} \phi_i^* \psi_i$$

$$\text{outer product: } |\phi\rangle\langle\psi| = \begin{pmatrix} \phi_1\psi_1^* & \ldots & \phi_1\psi_n^* \\ \vdots & \ddots & \vdots \\ \phi_n\psi_1^* & \vdots & \phi_n\psi_n^* \end{pmatrix}$$

It is often said that physical counterparts of vectors of n-dimensional Hilbert spaces are n-level quantum systems.

QUBITS

A **qubit** - a two-level quantum system is a quantum state in H_2

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where $\alpha, \beta \in \mathbf{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$ and

$\{|0\rangle, |1\rangle\}$ is a **(standard) basis** of H_2

EXAMPLE: Representation of qubits by

(a) electron in a Hydrogen atom — (b) a spin-$\frac{1}{2}$ particle

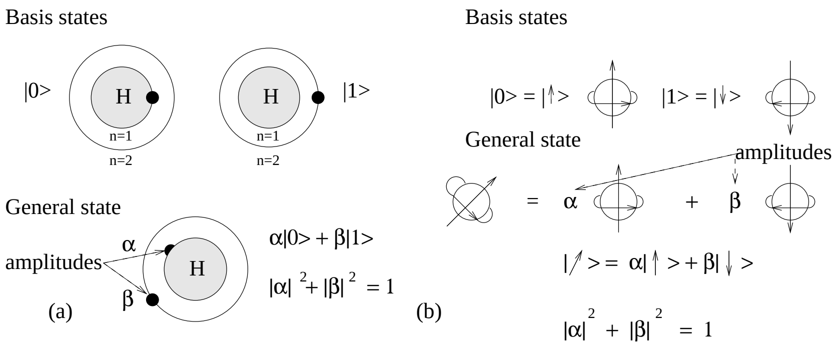


Figure 12: Qubit representations by energy levels of an electron in a hydrogen atom and by a spin-$\frac{1}{2}$ particle. The condition $|\alpha|^2 + |\beta|^2 = 1$ is a legal one if $|\alpha|^2$ and $|\beta|^2$ are to be the probabilities of being in one of two basis states (of electrons or photons).

x

HILBERT SPACE H_2

STANDARD (COMPUTATIONAL) BASIS

$$|0\rangle, |1\rangle$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

DUAL BASIS

$$|0'\rangle, |1'\rangle$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Hadamard matrix (Hadamard operator in the standard basis)

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

has properties

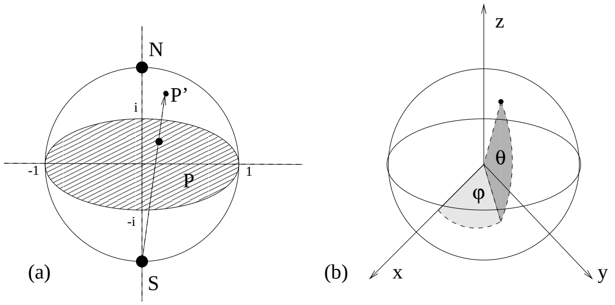
$$H|0\rangle = |0'\rangle \qquad H|0'\rangle = |0\rangle$$

$$H|1\rangle = |1'\rangle \qquad H|1'\rangle = |1\rangle$$

transforms one of the basis into another one.

QUBIT REPRESENTATION

There are several ways to represent qubits as points on a unit sphere:



One way to represent states of qubits is as points on the surface of a unit Riemann sphere, where North and South poles correspond to the basis states (bits) (see Figure a).[1]

Qubits can be represented also by points on a Bloch sphere (called also Poincaré sphere), and (see Figure b), using the spherical coordinate system.

This representation is based on the fact that any qubit can be represented as

$$\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

.

A qubit unitary operation = rotation

[1] The Riemann sphere is a sphere of unit radius whose equatorial plane is the complex plane whose center is the origin of the plane. One qubit state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be represented by a point on a Riemann sphere as follows. If $\beta \neq 0$ we mark in the complex plane the point P that represents the number $\frac{\alpha}{\beta}$ and then we project P from the South Pole onto the sphere to get the point P' that then represents $|\phi\rangle$. If $\alpha = 0$ one gets the North Pole this way; if $\beta = 0$ the South Pole is the limit (Penrose, 1994).

REALISATION of ROTATION on SPIN-$1/2$ PARTICLES

- For states of standard and dual basis of spin-$1/2$ particles one often uses the following notation:
$$|0\rangle = |\uparrow\rangle,\ |1\rangle = |\downarrow\rangle,\ |\rightarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |\leftarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
- If such a particle is put into a magnetic field it starts (its spin-orientation) to rotate. Let t be time for a full rotation.
- After rotation time $t/4$ the particle will be in the state
$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle);$$
- After rotation time $t/2$ the particle will be in the state
$$|1\rangle = |\downarrow\rangle.$$
- After rotation time $3t/4$ the particle will be in the state
$$|\leftarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
;
- In all other times the particle will be in all other potential superpositions of two basis states.

STERN-GERLACH MEASUREMENT EXPERIMENT

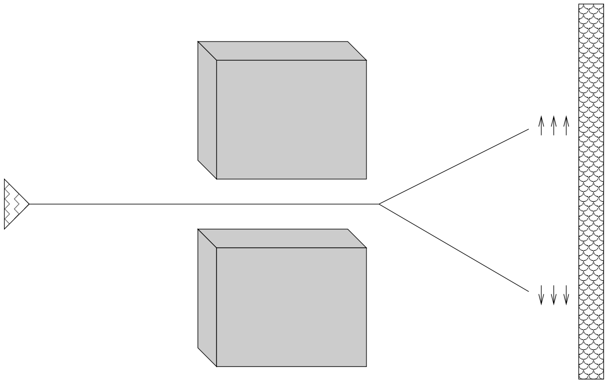


Figure 13: Stern-Gerlach experiment with spin-$\frac{1}{2}$ particles

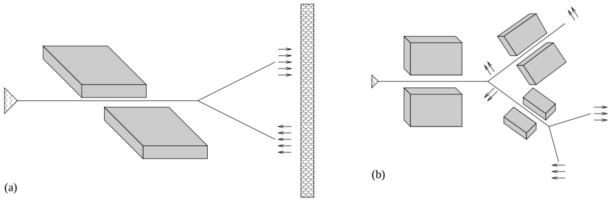


Figure 14: Several Stern-Gerlach magnets

Stern-Gerlach experiment indicated that a measurement of an n-level quantum state makes the state to collapse to one of the basis states and produces only one of n-possible classical outcomes.

QUANTUM (PROJECTION) MEASUREMENTS

A quantum state is observed (measured) with respect to an **observable** — a decomposition of a given Hilbert space into orthogonal subspaces (such that each vector can be uniquely represented as a sum of vectors of these subspaces).

There are two outcomes of a projection measurement of a state $|\phi\rangle$:

1. Classical information into which subspace projection of $|\phi\rangle$ was made.
2. A new quantum state $|\phi'\rangle$ into which the state $|\phi\rangle$ collapses.

The subspace into which projection is made is chosen **randomly** and the corresponding probability is uniquely determined by the amplitudes at the representation of $|\phi\rangle$ at the basis states of the subspace.

QUANTUM STATES and PROJECTION MEASUREMENT

In case an orthonormal basis $\{\beta_i\}_{i=1}^n$ is chosen in $\mathcal{H}_n$, any state $|\phi\rangle \in \mathcal{H}_n$ can be expressed in the form

$$|\phi\rangle = \sum_{i=1}^{n} a_i|\beta_i\rangle, \quad \sum_{i=1}^{n} |a_i|^2 = 1,$$

where

$a_i = \langle\beta_i|\phi\rangle$ are called probability amplitudes

and

their squares, $|a_i|^2$, provide probabilities

that if the state $|\phi\rangle$ is measured with respect to the basis $\{\beta_i\}_{i=1}^n$, then the state $|\phi\rangle$ collapses into the state $|\beta_i\rangle$ with probability $|a_i|^2$.

The classical “outcome” of a measurement of the state $|\phi\rangle$ with respect to the basis $\{\beta_i\}_{i=1}^n$ is the index i of that state $|\beta_i\rangle$ into which the state $|\phi\rangle$ collapses.

PHYSICAL VIEW of QUANTUM MEASUREMENT

In case an orthonormal basis $\{\beta_i\}_{i=1}^n$ is chosen in $\mathcal{H}_n$, it is said that an observable was chosen.

In such a case, a measurement, or an observation, of a state

$$|\phi\rangle = \sum_{i=1}^{n} a_i|\beta_i\rangle, \quad \sum_{i=1}^{n} |a_i|^2 = 1,$$

with respect to a basis (observable), $\{\beta_i\}_{i=1}^n$, is seen as saying that the state $|\phi\rangle$ has property $|\beta_i\rangle$ with probability $|a_i|^2$.

In general, any decomposition of a Hilbert space $\mathcal{H}$ into mutually orthogonal subspaces, with the property that any quantum state can be uniquely expressed as the sum of the states from such subspaces, represents an observable (a measuring device). There are no other observables.

WHAT ARE ACTUALLY QUANTUM STATES? - TWO VIEWS

- In so called “relative state interpretation” of quantum mechanics a quantum state is interpreted as an objective real physical object.
- In so called “information view of quantum mechanics” a quantum state is interpreted as a specification of (our knowledge or beliefs) probabilities of all experiments that can be performed with the state - the idea that quantum states describe the reality is therefore abounded.

A quantum state is a useful abstraction which frequently appears in the literature, but does not really exists in nature.

A. Peres (1993)

QUBIT MEASUREMENT

A qubit state can "contain" unbounded large amount of information. However, a quantum state cannot be fully identified.

By a measurement of the qubit state

$$\alpha|0\rangle + \beta|1\rangle$$

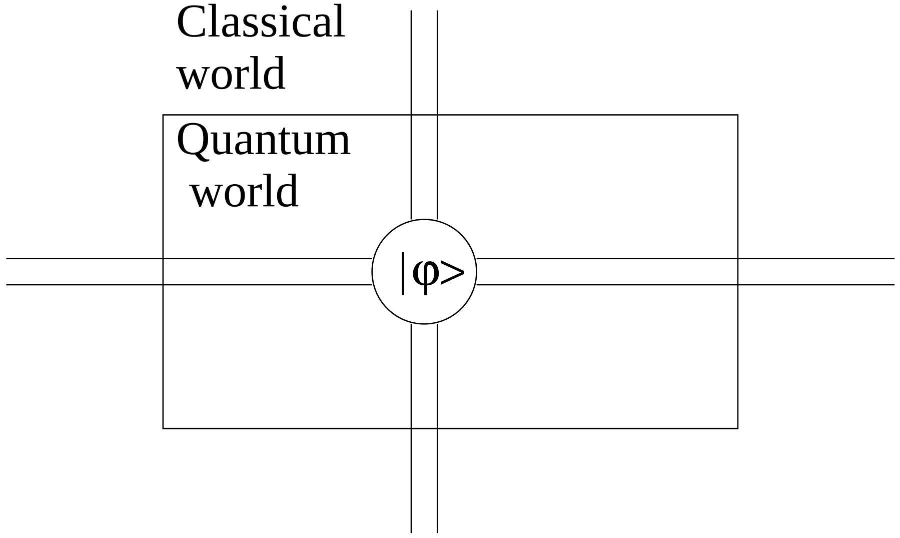
with respect to the basis

$$|0\rangle, |1\rangle$$

we can obtain only classical information and only in the following random way:

$$0 \ \textbf{ and } |0\rangle \ \textbf{ with probability } \ |\alpha|^2$$

$$1 \ \textbf{ and } |1\rangle \ \textbf{ with probability } \ |\beta|^2$$



measurement wrt. {|0>,|1>}

Classical
world

Quantum
world

|φ>

measurement wrt.
{|0’’’>,|1’’’>}

measurement wrt. {|0’>,|1’>|

measurement wrt. {|0’’>,|1’’>|

$|\varphi> = \alpha\ |0> + \beta|1>$

$= \alpha\ ,|0\ ,> + \beta\ \ |'1\ \ '>$

$= \alpha\ ''|0\ ''>+\beta\ ''|1\ \ ''>$

$= \alpha'''|0\ '''>+\beta\ '''|1\ \ '''>$

EXAMPLE 1

If the state

$$|0\rangle$$

is measured with respect to the standard (called also Boolean or computational) basis $\{|0\rangle, |1\rangle\}$**, then we get as the outcome**

$$0$$

with probability 1 **and the state collapses**

to itself.

If the state

$$|0\rangle$$

is measured with respect to the dual basis $\{|0'\rangle, |1'\rangle\}$**, then we get as the outcome**

0 **with probability** $\frac{1}{2}$ $\quad$ 1 **with probability** $\frac{1}{2}$

and the state collapses into the state

$|0'\rangle$ **or** $|1'\rangle$

because

$$|0\rangle = \frac{1}{\sqrt{2}}(|0'\rangle + |1'\rangle).$$

EXAMPLE 2

If the qubit

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

is measured with respect to the standard basis $\{|0\rangle, |1\rangle\}$**, then we get**

0 **-** $|0\rangle$ **with probability** $|\alpha|^2$ **or** 1 **-** $|1\rangle$ **with probability** $|\beta|^2$

Let us now try to measure $|\phi\rangle$ **with respect to the dual basis** $\{|0'\rangle, |1'\rangle\}$**. Since**

$$|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

and therefore

$$|0\rangle = \frac{1}{\sqrt{2}}(|0'\rangle + |1'\rangle) \qquad |1\rangle = \frac{1}{\sqrt{2}}(|0'\rangle - |1'\rangle)$$

we have

$$|\phi\rangle = \frac{1}{\sqrt{2}}((\alpha + \beta)|0'\rangle + (\alpha - \beta)|1'\rangle)$$

what implies that measurement of $|\phi\rangle$ **with respect to the dual basis provides**

$0 - |0'\rangle$ **with probability** $\frac{1}{2}|\alpha + \beta|^2$

or

$1 - |1'\rangle$ **with probability** $\frac{1}{2}|\alpha - \beta|^2$

HEISSENBERG's UNCERTAINTY PRINCIPLE

- Heissenberg's uncertainty principle says that if the value of a physical quantity is certain, then the value of a complementary quality is uncertain.
- Example. Measurement with respect to standard basis of states $|0\rangle$ and $|1\rangle$ gives certain outcome and therefore measurement of the same states according to the dual basis provides uncertain (random) outcomes.
- Another pair of complementary quantities are position and speed.

WHAT ARE QUANTUM STATES?

- In the classical world we see a state as consisting of all information needed to describe completely the system at an instant of time.
- Due to Heissenberg's principle of uncertainty, such an approach is not possible in quantum world - for example, we cannot describe exactly both position and velocity (momentum).

BEAM-SPLITTERS and MACH-ZEHNDER INTERFEROMETER

The following picture illustrate one-particle interference using so-called Mach-Zehnder interferometer.

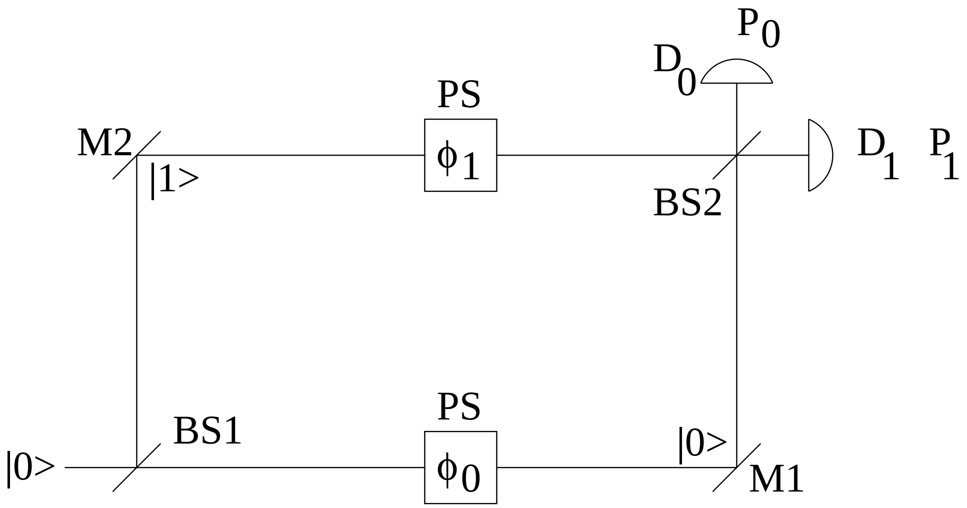


Figure 15: Mach-Zehnder interferometer, BS - beam-splitters, M -mirrors, PS - phase-shifter, D - detectors

Action of a beam-splitter is as that of the Hadamard gate

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

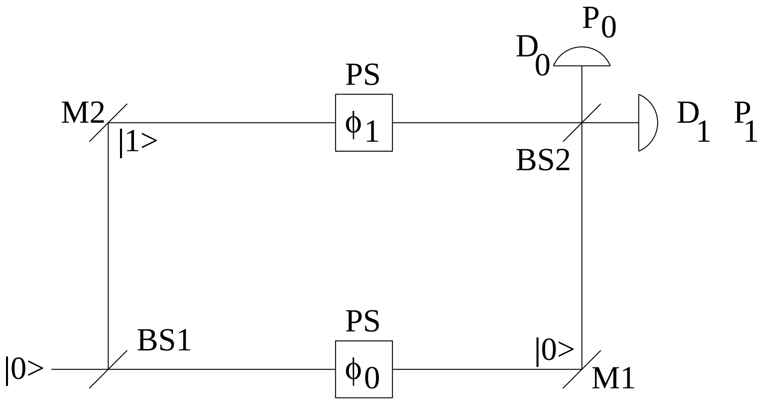


Figure 16: Mach-Zehnder interferometer, BS - beam-splitters, M -mirrors, PS - phase-shifter, D - det ectors

Action of Mach-Zehnder interferometer can be described as follows

$$|0\rangle \overset{BS1}{\rightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \overset{PS}{\rightarrow} \frac{1}{\sqrt{2}}(e^{i\phi_0}|0\rangle + e^{i\theta_1}|1\rangle) \tag{1}$$

$$= e^{i\frac{\theta_0+\theta_1}{2}}\frac{1}{\sqrt{2}}(e^{i\frac{\theta_0-\theta_1}{2}}|0\rangle + e^{i\frac{-\theta_0+\theta_1}{2}}|1\rangle) \tag{2}$$

$$\overset{BS2}{\rightarrow} e^{i\frac{\theta_0+\theta_1}{2}}(\cos\frac{1}{2}(\phi_0-\phi_1)|0\rangle + i\sin\frac{1}{2}(\phi_0-\phi_1)|1\rangle) \tag{3}$$

Two detectors detect a particle with probabilities

$$P_0 = \cos^2\frac{\phi_0-\phi_1}{2} \text{ and } \quad P_1 = \sin^2\frac{\phi_0-\phi_1}{2}$$

and therefore if $\phi_0 = \phi_1$ only the detector D_0 can detect a particle.

OBSERVATION on INTERFERENCE EXPERIMENTS

- **Single particle experiments are not restricted to photons.**
- **One can repeat such an experiment with electrons, atoms or even some molecules.**
- **When it comes to atoms both internal and external degrees of freedom can be used**

CLASSICAL versus QUANTUM COMPUTING

The essence of the difference
between
classical computers and **quantum computers**

is in the way information is stored and processed.

In **classical computers**, information is represented on **macroscopic level** by **bits**, which can take one of the two values

$$0 \quad \text{or} \quad 1$$

In **quantum computers**, information is represented on **microscopic level** using **qubits**, which can take on any from uncountable many values

$$\alpha|0\rangle + \beta|1\rangle$$

where α, β are arbitrary complex numbers such that

$$|\alpha|^2 + |\beta|^2 = 1.$$

QUANTUM EVOLUTION/COMPUTATION

EVOLUTION	COMPUTATION
in	in
QUANTUM SYSTEM	HILBERT SPACE

is described by

Schrödinger linear equation

$$i\hbar\frac{\partial\psi(t)}{\partial t} = H(t)\psi(t),$$

where $H(t)$ is a quantum analogue of a Hamiltonian of the classical system, from which it follows that $\psi(t) = e^{-\frac{i}{\hbar}H(t)}$ and therefore that an discretized evolution (computation) step of a quantum system is performed by a multiplication by a **unitary operator** and a step of such an evolution we can see as a multiplication of a **unitary matrix** A with a vector $|\psi\rangle$, i.e.

$$A|\psi\rangle$$

A matrix A is **unitary** if for A and its adjoint matrix $A^\dagger$ (with $A^\dagger_{ij} = (A_{ji})^*$) it holds:

$$A \cdot A^\dagger = A^\dagger \cdot A = I$$

HAMILTONIANS

The Schrödinger equation tells us how a quantum system evolves

subject to the Hamiltonian

However, in order to do quantum mechanics, one has to know how to pick up the Hamiltonian.

The principles that tell us how to do so are real bridge principles of quantum mechanics.

Each quantum system is actually uniquely determined by a Hamiltonian.

UNITARY MATRICES — EXAMPLES

In the following there are examples of unitary matrices of degree 2

Pauli matrices $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Hadamard matrix $= \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$ $\frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix} = \sqrt{\sigma_x}$ – matrix

$$\begin{pmatrix} i\cos\theta & \sin\theta \\ \sin\theta & i\cos\theta \end{pmatrix} \quad \begin{pmatrix} e^{i\alpha}\cos\theta & -ie^{i(\alpha-\theta)}\sin\theta \\ -ie^{i(\alpha+\theta)}\sin\theta & e^{i\alpha}\cos\theta \end{pmatrix}$$

Pauli matrices play a very important role in quantum computing.

A UNIVERSAL SET of QUANTUM GATES

The main task at quantum computation is to express solution of a given problem P as a unitary matrix U_P and then to construct a circuit C_{U_P} with elementary quantum gates from a universal se ts of quantum gates to realize U. That is

$$P \rightarrow U_P \rightarrow C_{U_P}.$$

A simple universal set of quantum gates consists of gates

$$\textbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \sigma_z^{1/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi}{4}i} \end{pmatrix}$$

SOLVING SCHRÖDINGER EQUATION

For the Hamiltonian

$$H = \frac{\pi\hbar}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix} = \frac{\pi\hbar}{2}V$$

the Schödinger equation

$$i\hbar\frac{\partial U(t)}{\partial t} = HU(t)$$

has the solution

$$U(t) = e^{-\frac{i}{\hbar}Ht} = \sum_{k=1}^{\infty}\frac{(-\frac{i\pi}{2})^k V^k t^k}{k!} = I + \frac{1}{2}\sum_{k=0}^{\infty}\frac{(-\pi i t)^k}{k!}V$$

and therefore for $t = 1$,

$$e^{-\frac{i\pi}{2}V} = I + \frac{1}{2}(e^{-i\pi} - 1)V = I - V = CNOT.$$

CLASSICAL versus QUANTUM MECHANICS

A crucial difference between quantum theory and classical mechanics is perhaps this: whereas classical states are essentially **descriptive**, quantum states are essentially **predictive**; they encapsulate predictions concerning the values that measurements of physical quantities will yield, and these predictions are in terms of probabilities.

The state of a classical particle is given by its position $q = (q_x, q_y, q_z)$ and momentum $p = (p_x, p_y, p_z)$.

The state of n particles is therefore given by $6n$ numbers.

Hamiltonian, or total energy $H(p, q)$ of a system of n particles is then a function of $3n$ coordinates p^i_u, $i = 1, \ldots,$, $u \in \{x, y, z\}$ and $3n$ coordinates q^i_u.

Time evolution of such a system is then described by a system of $3n$ pairs of Hamiltonian equations

$$\frac{dq^i_u}{dt} = \frac{\partial H}{\partial p^i_u} \qquad \frac{dp^i_u}{dt} = -\frac{\partial H}{\partial q^i_u}$$

MEASUREMENT

in CLASSICAL versus QUANTUM physics

BEFORE QUANTUM PHYSICS

it was taken for granted that when physicists measure something, they are gaining knowledge of a pre-existing state — a knowledge of an independent fact about the world.

QUANTUM PHYSICS

says otherwise. Things are not determined except when they are measured, and it is only by being measured that they take on specific values.

A quantum measurement forces a previously indeterminate system to take on a definite value.

TENSOR PRODUCTS

of vectors $(x_1,\ldots,x_n)\otimes(y_1,\ldots,y_m)=(x_1y_1,\ldots,x_1y_m,x_2y_1,\ldots,x_2y_m,\ldots,x_ny_1,\ldots,x_ny_m$

of matrices $$A\otimes B=\begin{pmatrix} a_{11}B & \ldots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \ldots & a_{nn}B\end{pmatrix}$$ where $$A=\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & & \ldots \\ a_{n1} & \ldots & a_{nn}\end{pmatrix}$$

Example

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\otimes\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}=\begin{pmatrix}a_{11} & a_{12} & 0 & 0\\ a_{21} & a_{22} & 0 & 0\\ 0 & 0 & a_{11} & a_{12}\\ 0 & 0 & a_{21} & a_{22}\end{pmatrix} \quad \begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\otimes\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}a_{11} & 0 & a_{12} & 0\\ 0 & a_{11} & 0 & a_{12}\\ a_{21} & 0 & a_{22} & 0\\ 0 & a_{21} & 0 & a_{22}\end{pmatrix}$$

of Hilbert spaces $H_1\otimes H_2$ is the complex vector space spanned by tensor products of vectors from H_1 and H_2, that corresponds to the quantum system composed of the quantum systems corresponding to Hilbert spaces H_1 and H_2.

An important difference between classical and quantum systems

A state of a compound classical (quantum) system can be (cannot be) always composed from the states of the subsystems.

QUANTUM REGISTERS

Any ordered sequence of n quantum qubit systems creates so-called quantum n-qubit register.

Hilbert space corresponding to an n-qubit register is n-fold tensor product of two-dimensional Hilbert spaces

$$\mathcal{H}_{2^n} = \bigotimes_{i=1}^{n} \mathcal{H}_2.$$

Since vectors $|0\rangle$ and $|1\rangle$ form a basis of H_2, one of the basis of $\mathcal{H}_{2^n}$, so-called computational basis, consists of all possible n-fold tensor products where $b_i \in \{0,1\}$ for all i.

$$|b_1\rangle \otimes |b_2\rangle \otimes \ldots \otimes |b_n\rangle = |b_1 b_2 \ldots b_n\rangle.$$

Example A two-qubit register has as a computational basis vectors

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

PAULI MATRICES

Very important one-qubit unary operators are the following *Pauli operators*, expressed in the standard basis as follows;

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Observe that Pauli matrices transform a qubit state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ as follows

$$\sigma_x(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle \quad \sigma_z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

and for $\sigma_y' = \sigma_x \sigma_z$ we have

$$\sigma_y'(|\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle - \alpha|1\rangle.$$

Operators σ_x, σ_z and σ_y' represent therefore a *bit error*, a *sign error* and a *bit-sign error*.

MIXED STATES - DENSITY MATRICES

A probability distribution $\{(p_i, |\phi_i\rangle\}_{i=1}^k$ on pure states is called a mixed state to which it is assigned a density operator

$$\rho = \sum_{i=1}^{k} p_i|\phi_i\rangle\langle\phi_i|.$$

One interpretation of a mixed state $\{p_i, |\phi_i\rangle\}_{i=1}^k$ is that a source X produces the state $|\phi_i\rangle$ with probability p_i.

Any matrix representing a density operator is called density matrix.

To two different mixed states can correspond the same density matrix.

Two mixed states with the same density matrix are physically undistinguishable.

DENSITY MATRICES

Density matrices are exactly matrices that are Hermitian, positive and have trace 1.

Eigenvalues of a density matrix are real, nonnegative and sum up to one - density matrices can be seen as a generalisation of probability distributions.

For any pure state $|\phi\rangle$, $|\phi\rangle\langle\phi|$ is a density matrix (representing $|\phi\rangle$).

Density matrices represent a class of similar mixed states and are also often called states.

MAXIMALLY MIXED STATES

To the maximally mixed state

$$(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)$$

which represents a random bit corresponds the density matrix

$$\frac{1}{2}\begin{pmatrix}1\\0\end{pmatrix}(1,0)+\frac{1}{2}\begin{pmatrix}0\\1\end{pmatrix}(0,1)=\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\frac{1}{2}I_2$$

Surprisingly, many other mixed states have as their density matrix that one of the maximally mixed state.

QUANTUM ONE-TIME PAD CRYPTOSYSTEM

CLASSICAL ONE-TIME PAD cryptosystem

plaintext: an n-bit string p
shared key: an n-bit string k
cryptotext: an n-bit string c
encoding: $c = p \oplus k$
decoding: $p = c \oplus k$

QUANTUM ONE-TIME PAD cryptosystem:

plaintext: an n-qubit string $|p\rangle = |p_1\rangle \ldots |p_n\rangle$
shared key: two n-bit strings k, k'
cryptotext: an n-qubit string $|c\rangle = |c_1\rangle \ldots |c_n\rangle$
encoding: $|c_i\rangle = \sigma_x^{k_i}\sigma_z^{k'_i}|p_i\rangle$
decoding: $|p_i\rangle = \sigma_z^{k'_i}\sigma_x^{k_i}|c_i\rangle$ where $|p_i\rangle = \begin{pmatrix} a_i \\ b_i \end{pmatrix}$ and $|c_i\rangle = \begin{pmatrix} d_i \\ e_i \end{pmatrix}$ are qubits and

$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with $\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are Pauli matrices.

UNCONDITIONAL SECURITY of QUANTUM ONE-TIME PAD

In the case of encryption of a qubit

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

by QUANTUM ONE-TIME PAD cryptosystem what is being transmitted is the mixed state

$$(\frac{1}{4}, |\phi\rangle), (\frac{1}{4}, \sigma_x|\phi\rangle).(\frac{1}{4}, \sigma_z|\phi\rangle), (\frac{1}{4}, \sigma_x\sigma_z|\phi\rangle)$$

whose density matrix is

$$\frac{1}{2}I_2.$$

This density matrix is identical to the density matrix corresponding to that of a random bit, that is to the mixed state

$$(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)$$

UNCONDITIONAL SECURITY of QUANTUM ONE-TIME PAD

In the case of encryption of a qubit

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

by QUANTUM ONE-TIME PAD cryptosystem what is being transmitted is the mixed state

$$(\frac{1}{4}, |\phi\rangle), (\frac{1}{4}, \sigma_x|\phi\rangle).(\frac{1}{4}, \sigma_z|\phi\rangle), (\frac{1}{4}, \sigma_x\sigma_z|\phi\rangle)$$

whose density matrix is

$$\frac{1}{2}I_2.$$

This density matrix is identical to the density matrix corresponding to that of a random bit, that is to the mixed state

$$(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)$$

SHANNON's THEOREMS

Shannon classical encryption theorem says that n bits are necessary and sufficient to encrypt securely n bits.

Quantum version of Shannon encryption theorem says that $2n$ classical bits are necessary and sufficient to encrypt securely n qubits.

TWO QUBIT REGISTERS

A general state of a 2-qubit register is:

$$|\phi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

where

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

and $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ are vectors of the “standard” basis of H_4, i.e.

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

Important unitary matrices of degree 4, to transform states of 2-qubit registers are C-NOT (CNOT) or controlled not matrix:

$$\color{red}{CNOT}\color{black} = XOR = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

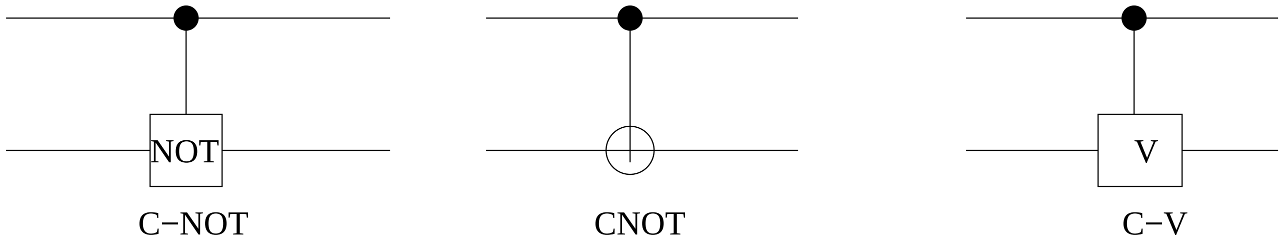
for which it holds:

$$CNOT : |x, y\rangle \Longrightarrow |x, x \oplus y\rangle$$

and C-V, or control V, matrix

$$\color{red}{C - V}\color{black} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$$

For the gates corresponding to the above matrices we use notation:



$$V = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

NO-CLONING THEOREM

INFORMAL VERSION: Unknown quantum state cannot be cloned.

FORMAL VERSION: There is no unitary transformation U such that for any qubit state $|\psi\rangle$

$$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

PROOF: Assume U exists and for two different states $|\alpha\rangle$ and $|\beta\rangle$

$$U(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle \quad U(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$$

Let

$$|\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)$$

Then

$$U(|\gamma\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle) \neq |\gamma\rangle|\gamma\rangle = \frac{1}{2}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle + |\alpha\rangle|\beta\rangle + |\beta\rangle|\alpha\rangle)$$

STRONG NO-CLONING THEOREM

General form of no-cloning theorem: If $\{|\psi_i\rangle\}$ is a set of pure states containing at least one non-orthogonal pair then no physical operation can achieve transformation

$$|\psi_i\rangle \rightarrow |\psi_i\rangle|\psi_i\rangle.$$

Natural question: How much additional information to $|\psi_i\rangle$ would be sufficient to do cloning? **Answer**: not less than $|\psi_i\rangle$.

Strong no-cloning theorem Let $\{|\psi_i\rangle\}$ be any finite set of pure states containing no orthogonal pair of states. Let $\{\rho_i\}$ be any other set of (generally mixed) states indexed by the same labels. Then there is a physical operation

$$|\psi_i\rangle \otimes \rho_i \rightarrow |\psi_i\rangle|\psi_i\rangle$$

if and only if there is a physical operation

$$\rho_i \rightarrow |\psi_i\rangle,$$

i.e. the full information of the clone must already be provided in the ancilla state ρ_i alone.

NO-DELETION THEOREM

Pati-Braunstein discovered so-called *no-deletion* theorem.

Let Let $\{|\psi_i\rangle\}$ be any finite set of pure states containing no orthogonal pair of states. There is no (trace preserving) physical operation to do

$$|\psi_i\rangle|\psi_i\rangle \rightarrow |\psi_i\rangle|0\rangle.$$

A more general form says that if for an environment $|A\rangle$ there is a physical operation to perform

$$|\psi_i\rangle|\psi_i\rangle|A\rangle \rightarrow |\psi_i\rangle|0\rangle|A_i\rangle$$

then $|A_i\rangle \rightarrow |\psi_i\rangle$.
No-cloning theorem therefore says that quantum information cannot be created from nothing and strong no-deletion theorem says that if quantum information is removed (from one place), it has to be put somewhere else.

PERMANENCE of INFORMATION

- Classical information is physical, but has no *permanence*.
- Permanence refers to the fact that to duplicate quantum information, it (second copy) must exist somewhere else in the universe and to eliminate quantum information, it must be moved to somewhere else in the universe, where it still exists.

ANALYSIS of NO-CLONING and NO-DELETION THEOREMS

- Possibility of cloning or deleting would allow superluminal communication.
- The same is true for strong versions of no-cloning theorem - see Chakrabarthy, Pati and Adhikar 2006.

TRACING OUT OPERATION

One of the profound differences between the quantum and classical systems lies in the relation between systems and their subsystems.

As discussed below, a state of a Hilbert space $H = H_A \otimes H_B$ cannot be always decomposed into states of its subspaces H_A and H_B. We also cannot define any natural mapping from the space of linear operators on H into the space of linear operators on H_A (or H_B).

However, density operators are much more robust and that is also one reason for their importance. A density operator ρ on H can be "projected" into H_A by the operation of **tracing out** H_B, to give the following density operator (for finite dimensional Hilbert spaces):

$$\rho_{H_A} = Tr_{H_B}(\rho) = \sum_{|\phi\rangle,|\phi'\rangle \in \mathcal{B}_{H_A}} |\phi\rangle \left(\sum_{|\psi\rangle \in \mathcal{B}_{H_B}} \langle \phi\psi|\rho|\phi'\psi\rangle \right) \langle \phi'|,$$

where $\mathcal{B}_{H_A}$ ($\mathcal{B}_{H_B}$) is an orthonormal basis of the Hilbert space H_A (of the Hilbert space H_B).

TRACING OUT OPERATION II

The rule to compute ρ_A given on the previous slide is neither very transparent nor easy to use.

In the following an easier to use rule is will be introduced.

A meaning of the tracing out operation. If *dim*$(A) = n$, *dim*$(B) = m$, then a density matrix ρ on $A \otimes B$, is an $nm \times nm$ matrix which can be seen as an $n \times n$ matrix consisting of $m \times m$ blocks ρ_{ij} as follows:

$$\rho = \begin{pmatrix} \rho_{11} & \dots & \rho_{1n} \\ \vdots & \ddots & \\ \rho_{n1} & \dots & \rho_{nn} \end{pmatrix}$$

and in such a case

$$\rho_A = \begin{pmatrix} \mathit{Tr}(\rho_{11}) & \dots & \mathit{Tr}(\rho_{1n}) \\ \vdots & \ddots & \vdots \\ \mathit{Tr}(\rho_{n1}) & \dots & \mathit{Tr}(\rho_{nn}) \end{pmatrix}$$

This can be easily seen from the formula for computing ρ_A once one realizes that

$$\mathit{Tr}(\rho_{ij}) = \sum_{|\psi\rangle \in \mathcal{B}_B} \langle \phi, \psi | \rho | \phi', \psi \rangle,$$

where $|\phi\rangle$ and $|\phi'\rangle$ are ith and jth vectors of $\mathcal{B}_A$.

EXAMPLES

Let ρ be a density matrix of $A \otimes B$ of the form

$$\rho = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}.$$

In such a case

$$\rho_A = \mathrm{Tr}_B \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} = \begin{pmatrix} a_{11} + a_{22} & a_{13} + a_{24} \\ a_{31} + a_{42} & a_{33} + a_{44} \end{pmatrix}.$$

Moreover,

$$\rho_B = \mathrm{Tr}_A \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} = \begin{pmatrix} a_{11} + a_{33} & a_{12} + a_{34} \\ a_{21} + a_{43} & a_{22} + a_{44} \end{pmatrix}.$$

TRACING OUT OPERATION – A SIMPLE WAY OUT

Perhaps the simplest way to introduce tracing out operation is to say that it is a linear operation such that for any bipartite system $A \otimes B$ and any states $|\phi_1\rangle$ and $|\phi_2\rangle$ of A and any states $|\psi_1\rangle$ and $|\psi_2\rangle$ of B

$$\mathit{Tr}_B(|\phi_1\rangle\langle\phi_2| \otimes |\psi_1\rangle\langle\psi_2|) = |\phi_1\rangle\langle\phi_2|\mathit{Tr}(|\psi_1\rangle\langle\psi_2|) = \langle\psi_2|\psi_1\rangle|\phi_1\rangle\langle\phi_2|.$$

ANOTHER VIEW of MEASUREMENT

A self-adjoint operator A of a finite dimensional Hilbert space H has the so-called **spectral representation**. If $\lambda_1, \ldots, \lambda_k$ are its distinct eigenvalues, then A can be expressed in the form

$$A = \sum_{i=1}^{k} \lambda_i P_i,$$

where P_i is the projection operator into the subspace of H spanned by the eigenvectors corresponding to λ_i.

In a special case when all eigenvalues are distinct and $|\phi_i\rangle$ is the eigenstate/eigenvector corresponding to the eigenvalue λ_i, then

$$A = \sum_{i=1}^{n} \lambda_i |\phi_i\rangle\langle\phi_i|$$

In this case eigenvectors of A form an orthonormal basis and measurement with respect to this basis is often said to be the measurement given by the observable A.

IS TRACING OUT a REASONABLE OPERATION?

It is. It is a single operation with the following properties.

If we have a composed quantum system $A \otimes B$ and we measure a state (density matrix) ρ on $A \otimes B$ with respect to an observable $O \otimes I_B$, where O is an observable on A,

then

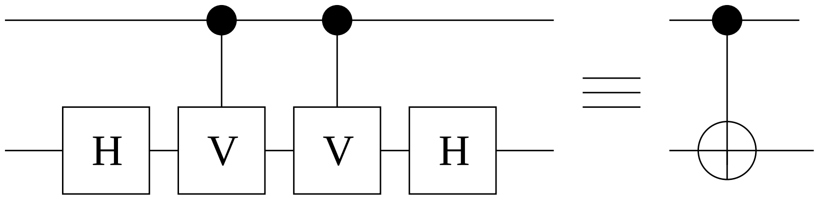
we get the same, in average, as if we measure $\rho_A = \mathrm{Tr}_B(\rho)$ only on A and with respect only to the observable O.

QUANTUM CIRCUITS - EXAMPLES

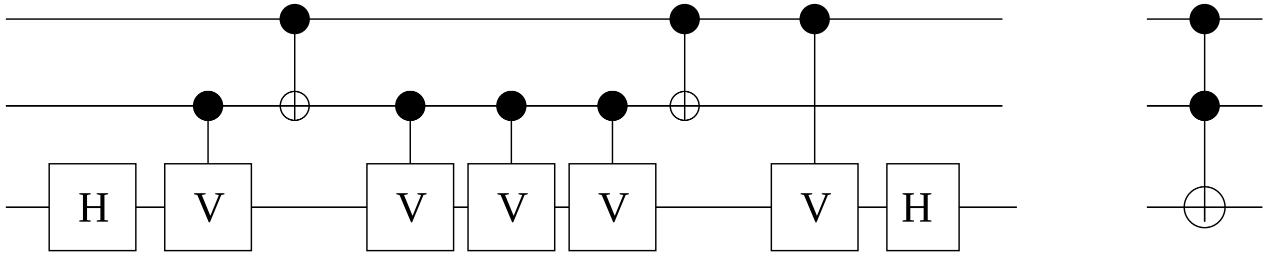
Quantum circuits are defined in a similar way as classical only its gates are either unitary operations or measurements.

Hadamard gate and C-V gate form a universal set of unitary gates - using these gates one can for any unitary operation U and $\varepsilon > 0$ design a quantum circuit C_U that approximates U with precision ε.

Two examples of quantum circuits for the CNOT gate and for Toffoli gate:



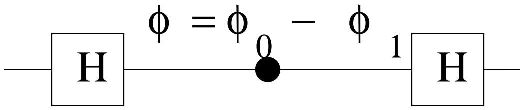
CNOT gate



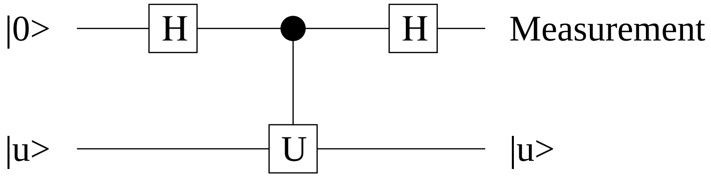
Toffoli gate

GENERALIZATION of MACH-ZEHNDER INTERFEROMETER

Mach-Zehnder interferometer can be represented by the following circuit



Its modification is the following circuit where $|u\rangle$ is eigenvector of U that maps $U|u\rangle = e^{i\phi}|u\rangle$.



This circuit “kick back” eigenvalue $e^{i\phi}$ in the front of the $|1\rangle$-component in the first qubit. The first qubit evolves as follows:

$$|0\rangle|u\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|u\rangle \xrightarrow{c-U} \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle|1\rangle)|u\rangle \xrightarrow{H} (\cos\frac{\phi}{2}|0\rangle + i\sin\frac{\phi}{2}|1\rangle)|u\rangle.$$

A QUANTUM EVOLUTION STEP

A quantum evolution step consists formally of a quantum state (vector) multiplication by a unitary operator. That is

$$A|\phi\rangle = |\psi\rangle$$

For example,

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} a_{11}b_1 + a_{12}b_2 + a_{13}b_3 + a_{14}b_4 \\ a_{21}b_1 + a_{22}b_2 + a_{23}b_3 + a_{24}b_4 \\ a_{31}b_1 + a_{32}b_2 + a_{33}b_3 + a_{34}b_4 \\ a_{41}b_1 + a_{42}b_2 + a_{43}b_3 + a_{44}b_4 \end{pmatrix}.$$

A better insight into such a process can be obtained using different notation at which it is assumed that all rows and columns are labeled by the states of the standard basis of H_4.

$$\begin{pmatrix} a_{00,00} & a_{00,01} & a_{00,10} & a_{00,11} \\ a_{01,01} & a_{01,01} & a_{01,10} & a_{01,11} \\ a_{10,00} & a_{10,01} & a_{10,10} & a_{10,11} \\ a_{11,00} & a_{11,01} & a_{11,10} & a_{11,11} \end{pmatrix} \begin{pmatrix} b_{00} \\ b_{01} \\ b_{10} \\ b_{11} \end{pmatrix} = \begin{pmatrix} a_{00,00}b_{00} + a_{00,01}b_{01} + a_{00,10}b_{10} + a_{00,11}b_{11} \\ a_{01,00}b_{00} + a_{01,01}b_{01} + a_{01,10}b_{10} + a_{01,11}b_{11} \\ a_{10,00}b_{00} + a_{10,01}b_{01} + a_{10,10}b_{10} + a_{10,11}b_{11} \\ a_{11,00}b_{00} + a_{11,01}b_{01} + a_{11,10}b_{10} + a_{11,11}b_{11} \end{pmatrix} = \begin{pmatrix} d_{00} \\ d_{01} \\ d_{10} \\ d_{11} \end{pmatrix}.$$

IMPLICATIONS FOR SECURE TRANSMISSION of QUANTUM STATES

Let us assume that an eavesdropper Eve knows that Alice is sending to Bob one quantum state from a set $\{\phi_1, \phi_2, \ldots, \phi_n\}$ of non-orthogonal quantum states. What she can do?

- Eve cannot make copy of the transmitted state.
- There is no measurement Eve can find out reliably which state is being transmitted.
- She can only measure the state being transmitted, but each such a measurement will, with large probability, destroy the state being transmitted.

Intuitive conclusion There is nothing an eavesdropper can do without having large probability of being detected.

BELL STATES and BASIS

States

$$|\beta_{00}\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle, \quad |\beta_{10}\rangle = |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\beta_{01}\rangle = |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle, \quad |\beta_{11}\rangle = |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

form an orthogonal (Bell) basis in H_4 and play an important role in quantum computing.

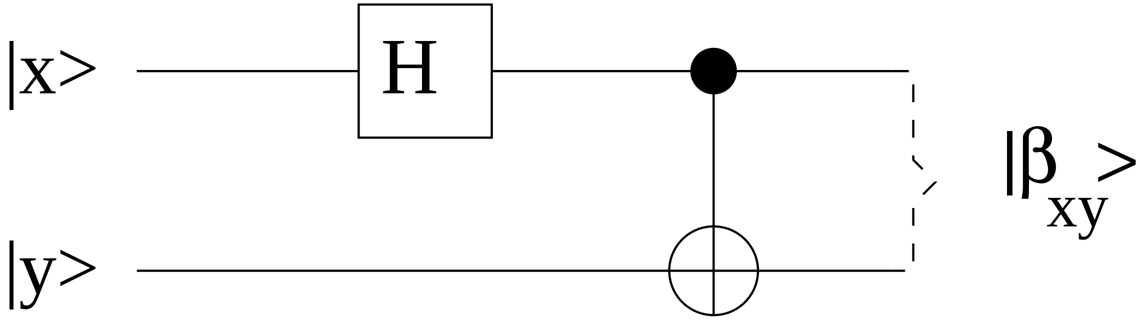
Theoretically, there is an observable for this basis. However, no one has been able to construct a measuring device for Bell measurement using linear elements only.

DESIGN of BELL STATES

Bell states can be defined concisely by formula

$$|\beta_{xy}\rangle = \frac{|0y\rangle + (-1)^x|1\bar{y}\rangle}{\sqrt{2}}.$$

and constructed easily by the circuit



MAGIC BASIS

It is the basis of $\mathcal{H}_4$ with basis states

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\psi_1\rangle = \frac{i}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \quad |\psi_3\rangle = \frac{i}{\sqrt{2}}(|00\rangle - |11\rangle)$$

Transformation rule to change a unitary U_s in the standard basis into U_m in the magic basis is through the rule

$$U_m = Q^\dagger U_s Q,$$

where

$$Q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & i \\ 0 & i & 1 & 0 \\ 0 & i & -1 & 0 \\ 1 & 0 & 0 & -i \end{pmatrix}.$$

The matrix Q represents also an isomorphism between $SU(2) \otimes SU(2)$ and $SO(4)$.

QUANTUM MEASUREMENT

of the states of 2-qubit registers

$$|\phi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

1. Measurement with respect to the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ provides the results:

$$\begin{array}{llll} 00 & \text{and} & |00\rangle & \text{with probability} & |\alpha_{00}|^2 \\ 01 & \text{and} & |01\rangle & \text{with probability} & |\alpha_{01}|^2 \\ 10 & \text{and} & |10\rangle & \text{with probability} & |\alpha_{10}|^2 \\ 11 & \text{and} & |11\rangle & \text{with probability} & |\alpha_{11}|^2 \end{array}$$

2. Measurement of particular qubits provides the results:

By measuring the first qubit we get

0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$

and $|\phi\rangle$ is reduced to the vector $\dfrac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

1 with probability $|\alpha_{10}|^2| + |\alpha_{11}|^2$

and $|\phi\rangle$ is reduced to the vector $\dfrac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$

MEASUREMENT — EXAMPLE

A photon with linear polarization along a direction θ to the vertical axis (to vector $|1\rangle$) is represented by the state

$$|\theta\rangle = \cos\theta|1\rangle + \sin\theta|0\rangle$$

A photon with orthogonal polarization has then the state

$$|\theta^\perp\rangle = \sin\theta|1\rangle - \cos\theta|0\rangle$$

From that it follows that:

$$|1\rangle = \cos\theta|\theta\rangle + \sin\theta|\theta^\perp\rangle$$

$$|0\rangle = \sin\theta|\theta\rangle - \cos\theta|\theta^\perp\rangle$$

If another photon is prepared with linear polarization ϕ, then

$$\begin{aligned} |\phi\rangle &= \cos\phi|1\rangle + \sin\phi|0\rangle \qquad (4) \\ &= \cos\phi[\cos\theta|\theta\rangle + \sin\theta|\theta^\perp\rangle] + \sin\phi[\sin\theta|\theta\rangle - \cos\theta|\theta^\perp\rangle] \qquad (5) \\ &= \cos(\theta-\phi)|\theta\rangle + \sin(\theta-\phi)|\theta^\perp\rangle \qquad (6) \end{aligned}$$

If the above state is measured with respect to the basis $\{\theta\rangle, |\theta^\perp\rangle\}$ (or using the calcite crystal oriented with its axis at an angle θ), then the outcome is θ with probability

$$\cos^2(\theta-\phi).$$

MEASUREMENT of TWO PHOTONS

Let us assume that two photons in the state

$$|\psi\rangle = \alpha|10\rangle - \beta|01\rangle$$

are much separated, see Figure, and then one is measured with respect to the polarization θ and the other one with respect to the polarization ϕ.

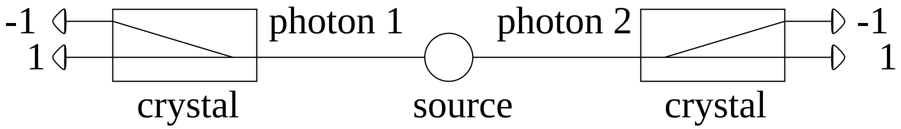


Figure 17: Two entangled photons are measured for orientations θ and ϕ

$$\begin{aligned}
|\psi\rangle &= \alpha|10\rangle - \beta|01\rangle && (7)\\
&= \alpha[\cos\theta|\theta\rangle + \sin\theta|\theta^{\perp}\rangle][\sin\phi|\phi\rangle - \cos\phi|\phi\rangle] - \beta[\sin\theta|\theta\rangle - \cos\theta|\theta^{\perp}\rangle][\cos\phi|\phi\rangle + \sin\phi|\phi^{\perp}\rangle] && (8)\\
&= [\alpha\cos\theta\sin\phi - \beta\sin\theta\cos\phi]|\theta\rangle|\phi\rangle + [\alpha\cos\theta\cos\theta - \beta\sin\theta\sin\phi]|\theta\rangle|\phi^{\perp}\rangle && (9)\\
&+ [\alpha\sin\theta\sin\phi + \beta\cos\theta\cos\phi]|\theta^{\perp}\rangle|\phi\rangle + [-\alpha\sin\theta\cos\phi + \beta\cos\theta\sin\phi]|\theta^{\perp}\rangle|\phi^{\perp}\rangle && (10)
\end{aligned}$$

The probability that the state $|\psi\rangle$ collapses into the state $|\theta\rangle|\phi^{\perp}\rangle$ is therefore

$$|\alpha\cos\theta\cos\phi - \beta\sin\theta\sin\phi|^2.$$

QUANTUM ENTANGLEMENT I

The concept of entanglement is primarily concerned with states of multipartite systems.

For a bipartite quantum system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, we say that its state $|\Phi\rangle$ is *an entangled state* if it cannot be decomposed into a tensor product of a state from $\mathcal{H}_A$ and a state from $\mathcal{H}_B$.

For example, it is easy to verify that a two-qubit state

$$|\phi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle,$$

is not entangled, that is

$$|\phi\rangle = (x_1|0\rangle + y_1|1\rangle) \otimes (x_2|0\rangle + y_2|1\rangle)$$

if and only if $\frac{a}{b} = \frac{x_2}{y_2} = \frac{c}{d}$, that is if

$$ad - bc = 0.$$

Therefore, all Bell states are entangled, and they are important examples of entangled states.

QUANTUM ENTANGLEMENT - BASIC DEFINITIONS

The concept of entanglement is primarily concerned with the states of multipartite systems.

For a bipartite quantum system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, a pure state $|\Phi\rangle$ is called entangled if it cannot be decomposed into a tensor product of a state from $\mathcal{H}_A$ and a state from $\mathcal{H}_B$.

A mixed state (density matrix) ρ of $\mathcal{H}$ is called entangled if ρ cannot be written in the form

$$\rho = \sum_{i=1}^{k} p_i \rho_{A,i} \otimes \rho_{B,i}$$

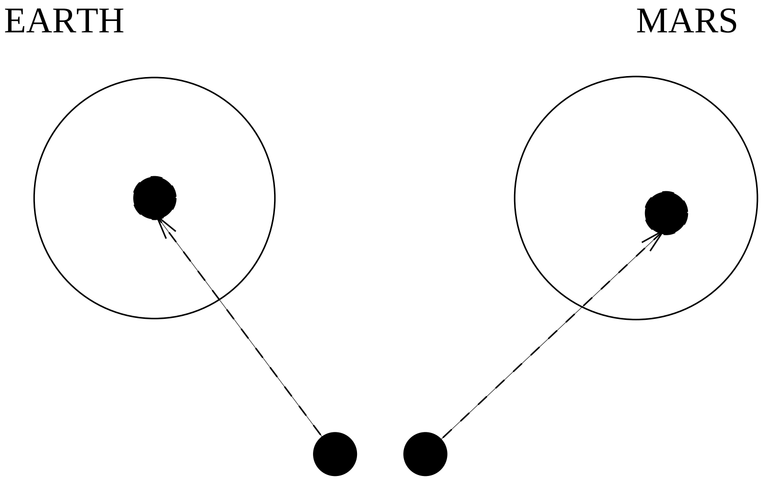
where $\rho_{A,i}$ ($\rho_{B,i}$) are density matrices in $\mathcal{H}_A$ (in $\mathcal{H}_B)$ and $\Sigma_{i=1}^{k} p_i = 1$, $p_i > 0$.

Basic importance of entanglement comes from the following facts demonstrating that entanglement implies the existence of non-local correlations.

Let two particles originally in the EPR-state

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

move far from each other



then measurement of any one of these particles makes the EPR-state to collapse, randomly, either to one of the states $|00\rangle$ or $|11\rangle$. As the classical outcomes both parties get at their measurements, no matter when they make them, the same outcomes.

Einstein called this phenomenon "spooky action at a distance" because measurement in one place seems to have an instantaneous (non-local) effect at the other (very distant) place.

CREATION of ENTANGLED STATES

Entangled states are gold mine for QIPC, but their creation is very difficult. This is natural because particles in an entangled states should exhibit non-local correlations no matter how far they are.

Basic methods to create entangled states:

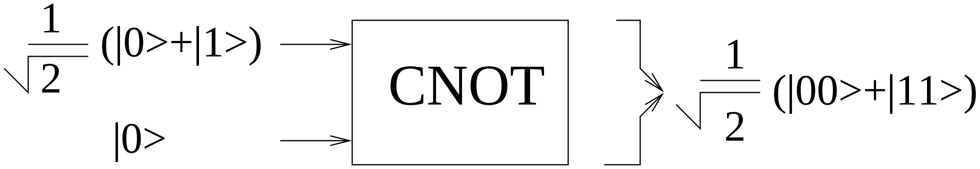
- Using special physical processes, for example parametric down-conversion. (Nowadays one can create in one second million maximally entangled states with 99% "precision" (fidelity)).
- Using "entangling" quantum operations. For example

$$\text{CNOT}((\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- Using entanglement swapping.

HOW TO CREATE ENTANGLED STATES?

$$\mathbf{CNOT}\left(\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes |0\rangle\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



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

|0>

CNOT

$\frac{1}{\sqrt{2}}$ (|00>+|11>)

ENTANGLEMENT SWAPPING

If particles P_1 and P_2 are in the EPR-state and so are particles P_3 and P_4, then Bell measurement of particles P_2 and P_3, makes particles P_1 and P_4, that have never interacted before, to be in the maximally entangled EPR-state:

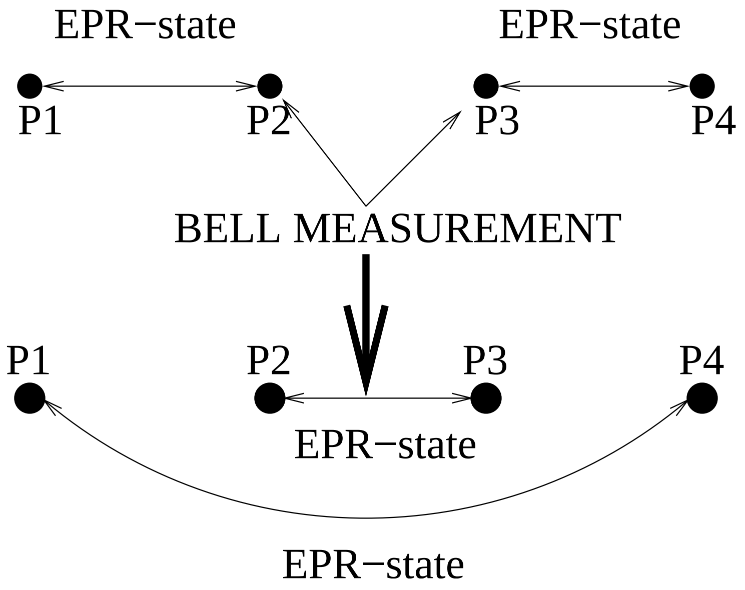


Figure 18: Entanglement swapping

QUANTUM NON-LOCALITY

- Physics was non-local since Newton's time, with exception of the period 1915-1925.
- Newton has fully realized counter-intuitive consequences of the non-locality his theory implied.
- Einstein has realized the non-locality quantum mechanics imply, but it does not seem that he realized that entanglement based non-locality does not violate no-signaling assumption.
- Recently, attempts started to study stronger non-signaling non-locality than the one quantum mechanics allows.

NON-LOCALITY in NEWTON's THEORY

Newton realized that his theory concerning gravity allows non-local effect. Namely, that

> **if a stone is moved on the moon, then weight of all of us, here on the earth, is immediately modified.**

NEWTON's words

The *consequences of current theory that implies that* gravity should be innate, inherent and essential to Matter, so that any Body may act upon another at a Distance throw a Vacuum, without the mediation of any thing else, by and through which their Action and Force may be conveyed from one to another, is to me so great an Absurdity, that I believe no Man who has in philosophical Matters a competent Faculty of thinking, can ever fall unto it.

Gravity must be caused by an Agent acting constantly according certain Laws, but whether this Agent be material or immaterial, I have left to the Consideration of my Readers.

POWER of ENTANGLEMENT

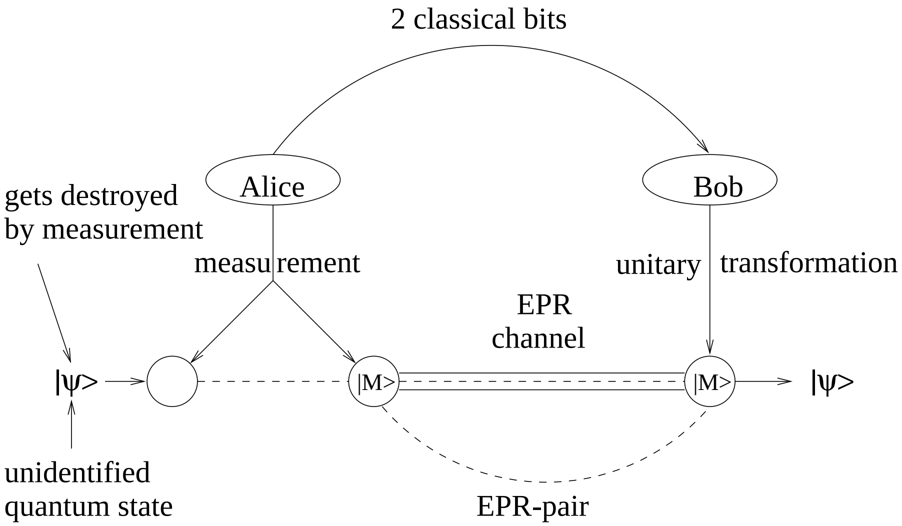
After its discovery, entanglement and its non-locality impacts have been seen as a peculiarity of the existing quantum theory that needs some modification to get rid of them, as a source of all kind mysteries and counter-intuitive consequences.

Currently, after the discovery of quantum teleportation and of such powerful quantum algorithms as Shor's factorization algorithm, entanglement is seen and explored as a new and powerful quantum resource that allows

- to perform tasks that are not possible otherwise;
- to speed-up much some computations and to economize (even exponentially) some communications;
- to increase capacity of (quantum) communication channels;
- to implement perfectly secure information transmissions;
- to develop a new, better, information based, understanding of the key quantum phenomena and by that, a deeper, information processing based, understanding of Nature.

QUANTUM TELEPORTATION

Quantum teleportation allows to transmit unknown quantum information to a very distant place in spite of impossibility to measure or to broadcast information to be transmitted.



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |EPR-pair\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Total state

$$|\psi\rangle|EPR-pair\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

Measurement of the first two qubits is then done with respect to the “Bell basis”.

BELL BASES

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

QUANTUM TELEPORTATION I

Total state of three particles:

$$|\psi\rangle|EPR-state\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

can be expressed as follows:

$$\begin{aligned}|\psi\rangle|EPR-state\rangle &= \frac{1}{2}|\Phi^+\rangle(\alpha|0\rangle+\beta|1\rangle)+\frac{1}{2}|\Psi^+\rangle(\alpha|1\rangle+\beta|0\rangle)\\ &\quad +\frac{1}{2}|\Phi^-\rangle(\alpha|0\rangle-\beta|1\rangle)+\frac{1}{2}|\Psi^-\rangle(\alpha|1\rangle-\beta|0\rangle)\end{aligned}$$

and therefore the measurement of the first two particles projects the state of the Bob's particle into a “small modification ” $|\psi_1\rangle$ of the unknown state $|\psi\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)$.

The unknown state $|\psi\rangle$ can therefore be obtained from $|\psi_1\rangle$ by applying one of the four operations

$$\sigma_x, \sigma_x\sigma_z, \sigma_z, I$$

and the result of the Bell measurement provides two bits specifying which of the above four operations should be applied.

These four bits Alice needs to send to Bob using a classical channel (by email, for example).

QUANTUM TELEPORTATION II

If the first two particles of the state

$$\begin{aligned}|\psi\rangle|EPR-state\rangle &= \frac{1}{2}|\Phi^+\rangle(\alpha|0\rangle+\beta|1\rangle)+\frac{1}{2}|\Psi^+\rangle(\alpha|1\rangle+\beta|0\rangle)\\ &+\frac{1}{2}|\Phi^-\rangle(\alpha|0\rangle-\beta|1\rangle)+\frac{1}{2}|\Psi^-\rangle(\alpha|1\rangle-\beta|0\rangle)\end{aligned}$$

are measured with respect to the Bell basis then Bob's particle gets into the mixed state

$$(\frac{1}{4},\alpha|0\rangle+\beta|1\rangle)\oplus(\frac{1}{4},\alpha|0\rangle-\beta|1\rangle)\oplus(\frac{1}{4},\beta|0\rangle+\alpha|1\rangle)\oplus(\frac{1}{4},\beta|0\rangle-\alpha|1\rangle)$$

to which corresponds the density matrix

$$\frac{1}{4}\begin{pmatrix}\alpha\\ \beta*\end{pmatrix}(\alpha^*,\beta^*)+\frac{1}{4}\begin{pmatrix}\alpha\\ -\beta\end{pmatrix}(\alpha^*,-\beta^*)+\frac{1}{4}\begin{pmatrix}\beta\\ \alpha\end{pmatrix}(\beta^*,\alpha^*)+\frac{1}{4}\begin{pmatrix}\beta\\ -\alpha\end{pmatrix}(\beta^*,-\alpha^*)=\frac{1}{2}.I$$

The resulting density matrix is identical to the density matrix for the mixed state corresponding to the random bit:

$$(\frac{1}{2},|0\rangle)\oplus(\frac{1}{2},|1\rangle).$$

Indeed, the density matrix for the last mixed state has the form:

$$\frac{1}{2}\begin{pmatrix}1\\ 0\end{pmatrix}(1,0)+\frac{1}{2}\begin{pmatrix}0\\ 1\end{pmatrix}(0,1)=\frac{1}{2}I.$$

QUANTUM TELEPORTATION — COMMENTS

- **Alice can be seen as dividing information contained in $|\psi\rangle$ into**

  quantum information - transmitted through EPR channel

  and

  classical information - transmitted through a classical channel

- **In a quantum teleportation an unknown quantum state $|\phi\rangle$ can be disassembled into, and later reconstructed from, two classical bit-states and an maximally entangled pure quantum state.**

- **Using quantum teleportation an unknown quantum state can be *teleported* from one place to another by a sender who does not need to know — for teleportation itself — neither the state to be teleported nor the location of the intended receiver.**

- **One can also see quantum teleportation as a protocol that allows one to teleport all characteristics of an object, embedded in some matter and energy, and localized at one place to another piece of energy and matter located at a distance.**

- **The teleportation procedure cannot be used to transmit information faster than light**

  but

  it can be argued that quantum information presented in unknown state is transmitted instantaneously (except two random bits to be transmitted at the speed of light at most).
- **EPR channel is irreversibly destroyed during the teleportation process.**
- **One can also see quantum teleportation as a protocol that allows one to teleport all characteristics of an object embedded in some matter and energy localized at one place to another piece of energy and matter located at a distance.**

QUANTUM TELEPORTATION - GENERALISATIONS

- One can teleport also qudits from $\mathcal{H}_d$. In such a case Alice and Bob have to share a maximally entangled state in $\mathcal{H}_d$ (a natural generalisation of the EPR-state) and measurement is performed in a (naturally) generalised Bell basis.
- Teleportation can be done also if the state Alice and Bob share is not maximally entangled or even a mixed state. In such a case there is a price to pay, either concerning fidelity (quality of teleportation) or probability (of perfect result (see Agrawal. Pati - quant-ph/0611115.

QUANTUM SUPER DENSE CODING

A process inverse to teleportation, in which one qubit is used to send two bits, is called **superdense quantum coding**.

Assume again that Alice and Bob share two particles in the EPR-state: If now Alice wants to send to Bob bits $b_1 b_2$, she performs on her particle a Pauli operations according to the columns 1 and 2 of the following table 19:

Alice's bits	Pauli's rotations	Alice's particle: new state	$\rightarrow$	Bob's XOR transformation	Bob's bases $\mathcal{D}, \mathcal{B}$	Bob's bits
00	I	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\|0\rangle$	00	00
01	σ_x	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\|1\rangle$	01	01
11	σ'_y	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\|1\rangle$	11	11
10	σ_z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\|0\rangle$	10	10

Figure 19: Superdense coding steps

The overall state of two particles is then depicted in column 3. If Alice sends then her particle to Bob (we say that she sends one qubit) and Bob performs on his, now two, particles the XOR operation, then his two particles get into the state shown in column 4. If now Bob measures his old particle in the standard basis and the newly obtained particle in the dual basis, he can determine, see columns 5 and 6, the two bits Alice tried to send him.

Observe, that in both examples it was the EPR state that allowed extraordinary powerful transmission of quantum or classical information.

QUANTUM PSEUDO-TELEPATHY

Using entangled states various effects can be produced that resemble telepathy.

Example - Stage telepathy

Two players, Alice and Bob, are on a stage, see Figure 20, very far from each other (so far that they cannot communicate), and they are simultaneously, but independently and randomly asked again and again, by a moderator, either a “food question” or a “color question”.

- **FOOD question**: What is your favorite meal?

  ANSWER has to be either **carrot** or **peas**.

- **COLOR question**: What is your favorite color?

  ANSWER has to be either **green** or **red**.

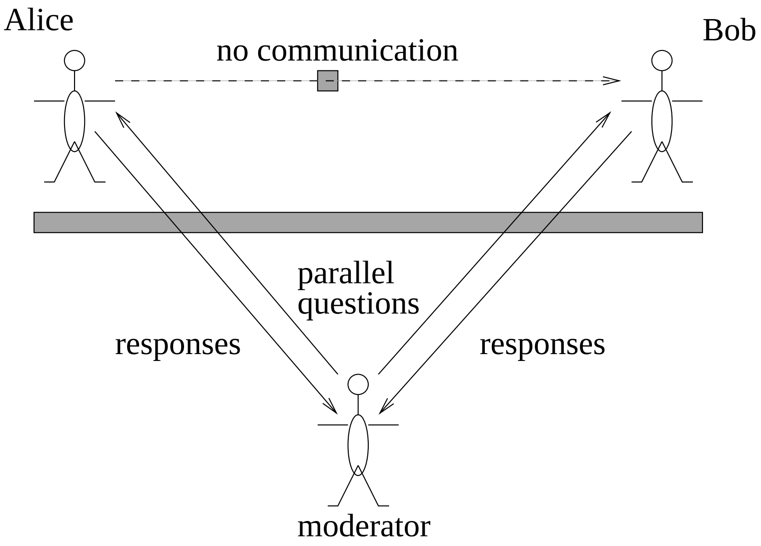


Figure 20: Setting for "colour-food" game

The audience observes that their answers satisfy the following conditions:

- If both players are asked color-questions then in about 9% of cases they answer **green**.
- If one of the players is asked the color-question and answers **green** and the other is asked the food-question, then (s)he answers **peas**.
- If both are asked food-questions they never both answer **peas**.

It is not difficult to show that within the classical physics there is no way that Alice and Bob could invent a strategy for their answers, before they went to the stage, in such a way that the above mentioned behavior of them would be observed. However, there is a quantum solution, and actually quite a simple one.

SOLUTION

Let $|p\rangle$ and $|c\rangle$ be two arbitrary orthogonal states in the two-dimensional Hilbert space H_2, and let

$$|r\rangle = a|p\rangle + b|c\rangle,$$

$$|g\rangle = b|p\rangle - a|c\rangle$$

be two new (orthogonal) states.

Let Alice and Bob, at the very beginning, before they go to the stage, create a large number of pairs of particles in the state

$$|\psi\rangle = N(|r\rangle|r\rangle - a^2|p\rangle|p\rangle),$$

where N is a normalization factor, and let later each of them takes his/her particle from each pair with him/her to the stage.

If any of them is asked the color-question, then (s)he measures his/her particle with respect to the $\{|r\rangle, |g\rangle\}$-basis and answers in accordance with the result of measurement.

If any of them is asked the food-question (s)he measures his/her particle with respect to the $\{|p\rangle, |c\rangle\}$-basis and responds in accordance with the result of measurement.

It is a not difficult exercise to show that in this way Alice's and Bob's responses follow the rules described above (9% comes from an optimization in one case).

ANSWER YOUR QUESTION PUZZLE — SOLUTION—PROOF

Case 1. Both are asked colour question. By substitution we get.

$$|\psi\rangle = N(|r\rangle|r\rangle - a^2(a|r\rangle + b|g\rangle)(a|r\rangle + b|g\rangle))$$

The coefficient at $|g\rangle|g\rangle$ is Na^2b^2 with maximum at about 9%.

Case 2. Alice is asked colour-question, Bob is asked food question.

$$|\psi\rangle = N(|r\rangle(a|p\rangle + b|c\rangle) - a^2(a|r\rangle + b|g\rangle)|p\rangle$$

There is no $|g\rangle|c\rangle$ term. This implies that probability that Alice answers green and Bob carrot is 0.

Case 3. Alice is asked colour-question, Bob is asked food question.

Solution is as above, due to the symmetry of the cases.

Case4 4. Both are asked food questions. By substitution we get

$$|\psi\rangle = N((a|p\rangle + b|c\rangle 0(a|p\rangle + b|c\rangle) - a^2|p\rangle|p\rangle)$$

Since $|p\rangle|p\rangle$ terms cancel the probability is 0 that both answers **peas**.

WHAT ARE QUANTUM OPERATIONS?

The main question we deal with in this section is very fundamental. What are physically realizable operations one can perform (at least theoretically) on (mixed) states (to get again (mixed) states)?

In closed quantum systems unitary operations are actually the only quantum operations that are available. Measurements are actually outside of the closed system framework, an interface from quantum to classical world, but surely they are operations we consider as physically realizable.

Of main importance are quantum operations in open quantum systems. Actually, all actions that are performed in open quantum systems are quantum operations: unitary operations, measurements, channel transmissions, flow of time, noise impacts, ...

The concept of quantum operations is therefore very general and very fundamental.

It is perhaps a bit surprising, but actually nice, useful and natural, that we can actually study and consider open quantum systems in the framework of closed quantum systems.We can consider as the basic setting that our (principal) quantum system and its environment form a closed quantum system in which we operate.

The requirement to consider only physically realizable (at least theoretically) operation is, of course, logical. As we shall see this question has, in a sense and at least theoretically, clear and simple answer. They are, as discussed later, trace preserving completely positive linear maps.

THREE APPROACHES

There are basically three main approaches to define what are “physically realizable quantum operations” (superoperators) $\mathcal{E}$.

A physically motivated axiomatic approach says that for a Hilbert space $\mathcal{H}$ we should consider as physically realizable operations maps $\mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$ which are *consistent with the (statistical) interpretation of quantum theory*. That is map that are *linear* (to preserve superpositions), *positive* and *trace preserving* (to map density operators to density operators) and actually completely positive.

A pragmatic approach says that superoperators are those operations that can be combined from unitary operations, adding ancillas, performing (non-selective) projective measurement and discarding subsystems (ancillas), by performing a tracing out operation.

A mathematical approach says that all basic quantum operations: adding and discarding quantum subsystems, unitary operations and non-selective projective measurements have **Kraus operator-sum representation**

$$\rho \longrightarrow \sum_{i=1}^{k} E_i \rho E_i^{\dagger},$$

where so called *Kraus operators* $E_i : \mathcal{H} \rightarrow \mathcal{H}$ are not necessarily Hermitian operators, but they should be positive and should form a “decomposition of the identity operator”, that is, $\Sigma_{i=1}^{k} E_i^{\dagger} E_i = I_{\mathcal{H}}$ – so called **completeness condition**.

It is a consequence of the completeness condition, and a property of the trace operation, that for any superoperator $\mathcal{E}$ holds

$$\mathit{Tr}(\mathcal{E}(\rho)) = \mathit{Tr}(\sum_i E_i \rho E_i^{\dagger}) = \mathit{Tr}(\sum_i E_i^{\dagger} E_i \rho) = \mathit{Tr}((\sum_i E_i^{\dagger} E_i)\rho) = \mathit{Tr}(\rho) = 1.$$

STINESPRING DILATION THEOREM

So called *Stinespring dilation theorem*, discussed below, says, that each superoperator can be realized in “one big three-stage-step” : adding an ancilla, performing a unitary operation on a composed quantum system and, finally, discarding the ancilla, see Figure 21, or other subsystems.

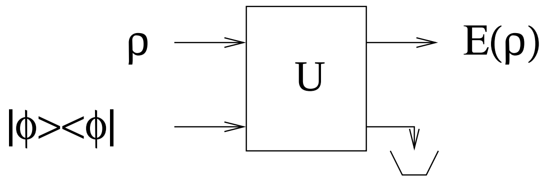


Figure 21: A Stinespring realization of a superoperator. In this view a superoperator $\mathcal{E}$ performs the mapping $\mathcal{E}(\rho) = Tr_a(U(\rho \times \rho_a)U^\dagger)$, where ρ_a is the “initial state”, for example $|\phi\rangle\langle\phi|$ of an ancilla subsystem, U is a unitary operation on composed system and, finally, a tracing out operation is performed.

NO-BROADCASTING THEOREM

- **Most general version of no-cloning theorem** For any pair of non-orthogonal pure states ρ_i, $i \in \{1, 2\}$, there is no trace-preserving completely positive map $\mathcal{E}$ such that $\forall i, \mathcal{E}(\rho_i) = \rho_i \otimes \rho_i$.
- A map $\mathcal{E}$ that takes states on $\mathcal{H}$ to states on $\mathcal{H}_A \otimes \mathcal{H}_B$ broadcasts a state ρ if $Tr_B(\mathcal{E}(\rho)) = Tr_A(\mathcal{E}(\rho)) = \rho$.
- **No-broadcasting theorem** A set of states is broadcastable if and only if they commute pairwise.
- **Generalised no-broadcasting theorem** No-broadcasting theorem holds in any non-classical finite-dimensional model satisfying a no-signaling criterion, including ones with ”super-quantum” correlations (quant-ph/0707.0620).

QUANTUM ERROR CORRECTION I

In the quantum case, information processing evolutions are far more under the negative impact of their environment, called in general *decoherence*, than in the classical computing.

The impact of decoherence is actually in all known technologies so strong, and grows exponentially in time, that till 1995 there have been strong doubts whether a powerful quantum information processing is possible at all.

A strong reason for pessimism was a belief (understanding) that in the quantum case one cannot use some quantum modification of so powerful classical error-correcting code approach.

There were several physical reasons for such a pessimism.

One of them was that in order to determine an error, we would need to measure the erroneous state, but that would irreversibly modify/destroy the erroneous state and we would have nothing to correct. Fortunately, it has turned out that there is a way out and quantum error correction can work well. The example presented in this section demonstrates the basic steps how such an error correction process can work, in principle.

QECC — EXAMPLE

Example of a qubit communication process through a noisy channel using a 3-qubit bit-error correction code.

Alice: encoding. Alice encodes the qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ by a network of two XOR gates and two additional qubits in the ancilla state $|00\rangle$ into the entangled state $\alpha|000\rangle + \beta|111\rangle$, see Figure.

Noisy channel. A bit error is assumed to occur with probability $p < \frac{1}{2}$ on any qubit and results in one of the states shown bellow:

resulting state	its probability
$\alpha|000\rangle + \beta|111\rangle$	$(1-p)^3$
$\alpha|100\rangle + \beta|011\rangle$	$p(1-p)^2$
$\alpha|010\rangle + \beta|101\rangle$	$p(1-p)^2$
$\alpha|001\rangle + \beta|110\rangle$	$p(1-p)^2$
$\alpha|110\rangle + \beta|001\rangle$	$p^2(1-p)$
$\alpha|101\rangle + \beta|010\rangle$	$p^2(1-p)$
$\alpha|011\rangle + \beta|100\rangle$	$p^2(1-p)$
$\alpha|111\rangle + \beta|000\rangle$	p^3

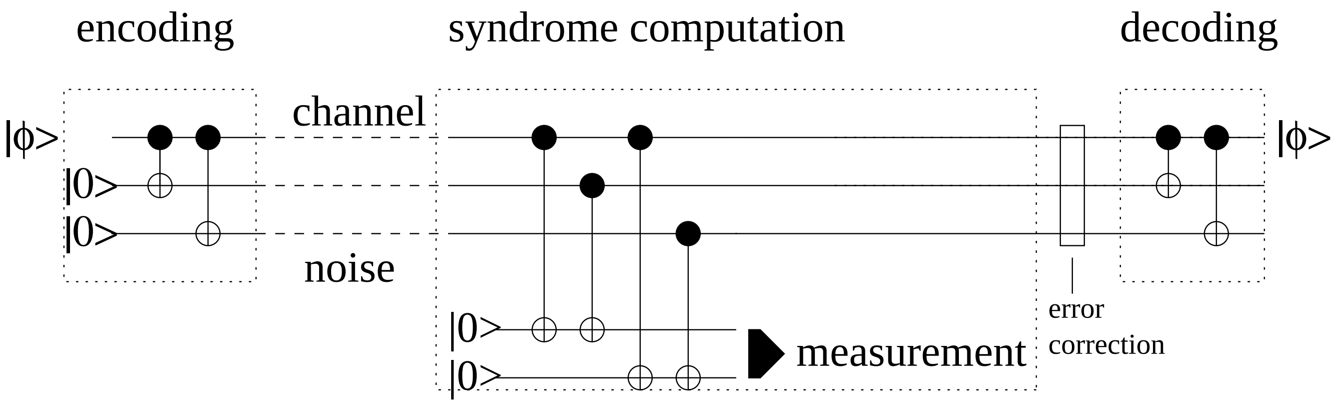
BOB: Syndrome computation process: By using two additional ancilla qubits in state $|00\rangle$ and four XOR operations syndromes of errors can be computed as shown in the following table

resulting state	its probability
$(\alpha\|000\rangle + \beta\|111\rangle)\|00\rangle$	$(1-p)^3$
$(\alpha\|100\rangle + \beta\|011\rangle)\|11\rangle$	$p(1-p)^2$
$(\alpha\|010\rangle + \beta\|101\rangle)\|10\rangle$	$p(1-p)^2$
$(\alpha\|001\rangle + \beta\|110\rangle)\|01\rangle$	$p(1-p)^2$
$(\alpha\|110\rangle + \beta\|001\rangle)\|01\rangle$	$p^2(1-p)$
$(\alpha\|101\rangle + \beta\|010\rangle)\|10\rangle$	$p^2(1-p)$
$(\alpha\|011\rangle + \beta\|100\rangle)\|11\rangle$	$p^2(1-p)$
$(\alpha\|111\rangle + \beta\|000\rangle)\|00\rangle$	p^3

Error correction. Bob does nothing if syndrome is 00 and performs σ_x operation

on third qubit if syndrome is 01
on second qubit if syndrome is 10
on first qubit if syndrome is 11

Resulting state is either $\alpha|000\rangle + \beta|111\rangle$ or $\beta|000\rangle + \alpha|111\rangle$.
Final decoding provides either the state $\alpha|0\rangle + \beta|1\rangle$ or the state $\beta|0\rangle + |1\rangle$.


encoding
syndrome computation
decoding
|φ>
|0>
|0>
channel
noise
|0>
|0>
measurement
error
correction
|φ>

BELL THEOREM

de Broglie (1927) and Bohm (1952) developed a hidden variable interpretation (theory)[2] of quantum mechanics. Einstein rejected it because it was inherently non-local.

Bell theorem, proved by Bell,says that each hidden variable theory of quantum mechanics has to be non-local.

Bell proved his theorem using a Gedanken experiment at which locally separated particles were measured and has shown that the average values of certain variables have then to satisfy certain inequalities, called in general *Bell inequalities*, provided a non-local theory of hidden variables holds and that these inequalities should be violated in case quantum mechanics with non-local effects hold.

As discussed later, various experiments confirmed violations of various Bell inequalities. This will be dealt with in more details in some of other chapters.

[2] Such a theory is often described as a theory in which individual quantum systems are described by classical parameters and they are responsible for randomness that appears in quantum experiments.

BELL THEOREM without BELL INEQUALITIES

there is a way to prove Bell theorem, one of the main outcome of quantum mechanics, also without Bell inequalities.

Let us assume that three photons are created in the state

$$\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$$

and photons move in three different directions where they are measured with respect to the standard ($\mathcal{B}$) or the dual basis ($\mathcal{D}$).

If we take results of the measurement as being 1 for $|0\rangle$ or $|0'\rangle$ and -1 for $|1\rangle$ or $|1'\rangle$ and $A(.,\lambda)$, $B(.,\lambda)$ and $C(.,\lambda)$ denotes the results of the measurement of the first, second and third photon in the appropriate basis submitted for the first parameter (with λ standing again for hidden variables), then it is easy to see that the product of the values of A,, B and C at different measurements have the following values

$$A(\mathcal{B},\lambda)B(\mathcal{B},\lambda)C(\mathcal{B},\lambda) = +1$$
$$A(\mathcal{B},\lambda)B(\mathcal{D},\lambda)C(\mathcal{D},\lambda) = -1$$
$$A(\mathcal{D},\lambda)B(\mathcal{B},\lambda)C(\mathcal{D},\lambda) = -1$$
$$A(\mathcal{D},\lambda)B(\mathcal{D},\lambda)C(\mathcal{B},\lambda) = -1$$

In the case there are no non-local influences the result of one measurement cannot influence the other two and therefore we can assume that values of variables A, B and C appearing in different equations for the same basis are the same. We can then multiply the left and the right sides of all four equalities. However, the product of the left sides gives the value 1 because each value appears there twice and the product of the right sides gives the value -1. A contradiction.

IS THE WORLD CLASSICAL?

The notion of the classical world includes mainly two ingredients: (a) realism; (b) determinism.

By realism we mean that any quantity that can be measured is well defined even if we do not measure it in practice.

By determinism we mean that that the result of a measurement is determined in a definite way by the state of the system and by the measurement setup.

Quantum world does not satisfy the above two requirements.

A particle in the state $|0'\rangle$ has no definite value with respect to measurement with respect to the standard basis - realism does not take place.

Measurement of a particle in state $0'\rangle$ with respect to the standard basis provides with the same probability results 0 and 1 - determinism does not take place.

CLASSICAL versus QUANTUM WORLDS

- The border between classical and quantum phenomena is just a question of money. (A. Zeilinger)
- The classical-quantum boundary is simply a matter of information control. (M. Aspelmeyer)
- There is no border between classical and quantum phenomena – you just have to look closer. (R. Bertlman)
- There is no classical world - there is only quantum world (D. Greenberger).
- There is no quantum world. There is only an abstract quantum physical description. It is wrong to think that the task of physics is to find out how Nature is. Physics concerns what we c an say about Nature. (N. Bohr)

CLASSICAL versus QUANTUM PHYSICS

I believe there is no classical world. There is only quantum world.

Classical physics is a collection of unrelated insights: Newton's laws. Hamilton's principle, etc. Only quantum theory brings out their connection.

An analogy is the Hawaiian Islands, which look like a bunch of island in the ocean. But if you could lower the water, you would see, that they are the peaks of a chain of mountains.

That is what quantum physics does to classical physics.

D. Greenberger

UNFINISHED REVOLUTION

- Some consider Einstein's revolution as unfinished because it does not provide a unified view of quantum world with space-time.
- Basic question: is quantum theory correct or it needs to be modified before it can be unified with our understanding of time and space.

UNSCRAMBLING of OMELET

Today we are beginning to realize how much of all physical science is really only *information, organized in a particular way*.

But we are far from unraveling the knotty question: *To what extent does this information reside in us, and to what extent is it a property of nature?*

Our present quantum mechanics formalism is a peculiar mixture describing in part laws of Nature, in part incomplete human information about Nature – all scrambled up together by Bohr into an omelet that nobody has seen how to unscramble,

Yet we think the unscrambling is a prerequisite for any further advances in basic physical theory. ..

Edwin T. Jaynes, 1990

KEY QUESTIONS and/or STEPS in the DEVELOPMENT of QIPC

Key steps in the development of QIPC were separations of four problems:

P1 Can we build powerful quantum computers?

P2 What could be achieved with powerful quantum computers?

P3 What are the laws and limitations of quantum information processing and communication?

P4 Can we develop a better understanding of the quantum world on the basis of the laws and limitations of QIPC?

This separation allowed complexity theory to make substantial contributions to the attempts to solve problems P2 and P3, especially P2, and to set as its new goal a contribution to the solution of the problem P4.

New recent goal and challenge of complexity theory is to help to deal with the problem P1.

WHAT IS QUANTUM INFORMATION?

The views on what is quantum information differ.

- There is no quantum information, there are only quantum carriers of classical information. (A. Zeilinger).
- Concept of quantum information is primary fundamental concept/ingredient of quantum physics that cannot be defined. However, the viewpoint it suggest is richly suggestive, leading to new interesting questions and interpretations of quantum processes. (J. Jozsa)

STARTING/CLOSING VIEWS

- Nothing exists except atoms and empty space; everything else is opinion. *Democritus of Abdera (ca. 400 BC)*.
- In science there is only Physics: all the rest is stamp collecting. Ernest Rutherford (1912)

CHANGING WORLD

Views on the role of physics in the understanding of the physical world keep developing.

- **Nothing exists except atoms and empty space; everything else is opinion.** ***Democritus of Abdera (ca. 400 BC)*.**
- **In Science there is only Physics: all the rest is stamps collecting.** ***Ernest Rutherford (1912)***
- **Physics is like sex; it produces sometimes practical results, but this is not reason why we do it. Feynman (19??)**
- **Physics is not the only science to get deep understanding of physical world. Informatics can and should help. Or, even, it should take an initiative?**

THERE IS A NEED TO CHANGE EMPHASES IN

QUANTUM INFORMATION PROCESSING

from

QUANTUM INFORMATION PRECESSING

to

CLASSICAL/QUANTUM INFORMATION PROCESSING

ANOTHER CLOSING MOTTO

Sorry, I am not young enough to know everything.

QUANTUM INFORMATION PROCESSING PRIMITIVES AND THEIR OPTIMAL USE

Jozef Gruska

Faculty of Informatics, Brno, Czech Republik

March 5, 2008

ABSTRACT

This talk deals with several concepts of universality in quantum information processing and with various (sometimes surprising) universal sets of (often surprising) quantum primitives.

In the talk we also deal with recent developments concerning an optimal use of some quantum primitives.

PART I - MOTIVATION

MOTTO I.

Progress in science is often done by pessimists.
Progress in technology is always done by optimists.

MOTTO II.

Progress in science is often done by pessimists.
Progress in technology is always done by knowledgeable and experienced optimists.

TWO STORIES TO REMEMBER

- The proposal to build Collosus, the first electronic computer for cryptanalysis purposes, was during 2WW rejected by a committee of prominent specialists as impossible to make, in spite of the fact that British cryptanalysts needed it badly to crack communication between Hitler and his generals.
- Collosus was then built by an ingenious optimist, Tommy Flowers, within 10 months in a Post office laboratory, and worked from the beginning successfully to break Lorenz cipher, starting January 1944.
- The key point was that Flowers realized that velvets were reliable provided they were never switched on and off. (Of course, nobody believed him.)
- The idea that 30m long ENIAC with 19000 vacuum tubes could work looked also crazy, for scientists, but it worked.

TRY TO BELIEVE IMPOSSIBLE

There's no use in trying, she said: one can't believe impossible things

I daresay you haven't had much practice said the Queen.

When I was your age, I always did it for half-an-hour a day.

Why sometimes I've believed as many as six impossible things before breakfast.

Lewis Carol: *Through the Looking-glass, 1872*

REALITY and PERSPECTIVES

- Factoring of the number 15 has been so far the most publicized outcome of experimental quantum computing (not to mention excellent cryptography, superposition, entanglement and teleportation experiments).
- DARPA set up as goal, in 2004 in the FoQuS program, to built a quantum processor to factorize 128 bit numbers in less than 30 seconds and with 99.99% accuracy.
- DARPA Quantum Cryptography Network operates in Cambridge, USA, connecting all campuses of Boston and Harvard University, and operates non-stop.
- Hundred qubits processors “are on the drawing table now (Steane (2005) has recently tried to justify that 300 qubit processors with laser controlled trap ion is feasible; Chuang et al. see possible to factorize 1024 numbers in 31 hours (classically it would require billion times longer than to factorize 512-bit numbers what required, in 2000, 8400 MIPS years).
- Emerging quantum technologies promise even larger scalability.

BASIC OBSERVATIONS – I

- Nature offers many ways – let us call them technologies – various quantum information processing primitives can be exhibited, realized and utilized.
- Since it appears to be very difficult to exploit potential of nature for QIP, it is of large importance to explore which quantum primitives form universal sets of primitives, and are (quite) easy to implement.
- Also from the point of view of understanding of the laws and limitations of QIP and also of quantum mechanics itself, the problems of finding rudimentary and universal QIP primitives , as well as methods for their optimal use, are of large experimental and fundamental importance.
- Search for quantum computation universal primitives, and their optimal use, is actually one of the major tasks of the current QIP research (both theoretical and experimental) that starts to attack the task of building quantum processors seriously.
- The search for sets of elementary, or even very rudimentary, but powerful, quantum computational primitives and for their optimal use, has brought a variety of deep and surprising results that seem to be also much encouraging for experimentalists.

BASIC OBSERVATIONS – II

Observation: An apparently small observation of a scientists or an experience of an engineer can turn a field upside down and “create a superstar from a sleeping beauty”.

Conclusion: It is very, very important to search for primitives and for new and new primitives - even in the areas one can hardly expect them.

BASIC QUESTIONS

- How to decide which primitives are of importance?
- Where to find “precedence” for such a decision?

TWO NATURAL QUESTIONS?

- What are the main reason that classical computing has been so successful?
- What can quantum computing learn from the classical computing success story?

WHY HAS BEEN CLASSICAL COMPUTING SO SUCCESSFUL?

Because perfect SEPARATION has been developed between

- Computing theory (models) - interface RAM
- Software design – interfaces RAM and RISC/PRAM
- Component design
- Hardware design – interface RISC/PRAM
- Network design – interface protocols

and each area could develop separately and still fully relevantly for other areas.

In each area several sets of primitives has been (slowly) identified and their optimal use has been investigated.

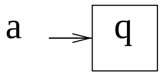
AN OBSERVATION

We need to find proper sets of primitives for quantum information processing.

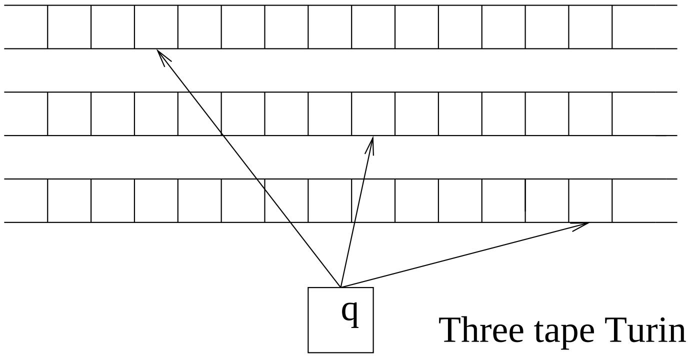
MODELS of UNIVERSAL COMPUTERS

- Classical models: circuits, Turing machines, cellular automata, RAM a PRAM
- Quantum models
  - (Unitary operations based) Quantum Turing Machines
  - (Unitary operations based) Quantum Circuits
  - Quantum cellular automata ????
  - Measurements based quantum circuits
  - Measurements based quantum Turing machines

MAIN MODELS of AUTOMATA

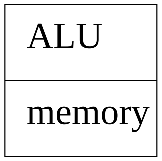


Finite automaton

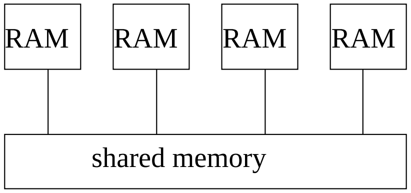


Three tape Turing machine

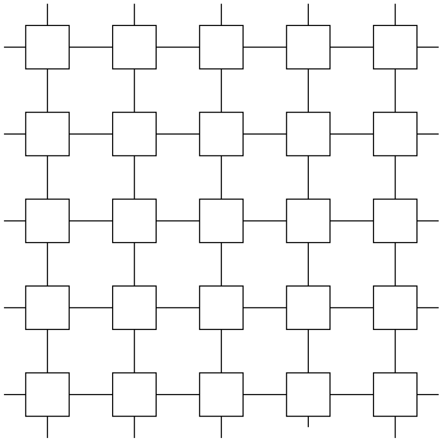
RAM



Operations: Load, Store
Add, Subtract
Jump, Jump−if



PRAM



Two−dimensional cellular automaton

INSIGHTS into QIPC

- BASIC TASKS of QUANTUM COMPUTER DESIGN
  - To find ways to set up initial state
  - To find ways to implement a universal sets of quantum gates
  - To realize ways to implement quantum circuits
  - To find ways to perform quantum measurements
- BASIC TASKS of (UNITARY-BASED) QUANTUM COMPUTATIONS
  - To set up an initial state
  - To make quantum system to implement unitary gates of a quantum circuit.
  - To perform measurements to get outcome
- NEW (MEASUREMENT-BASED) VIEW of QUANTUM COMPUTATIONS

  Measurement is the basic way to force closed quantum systems to do what we want it to do (to perform unitaries) in order to solve (classical) computation problems.

KEY STEPS in DEVELOPMENT of QIPC

Key steps in the development of QIPC were separations of four problems:

P1 Can we build (and how) powerful quantum computers?

P2 What could be achieved with powerful quantum computers?

P3 What are the laws and limitations of quantum information processing and communication?

P4 Can we develop a better understanding of the quantum world on the basis of the laws and limitations of QIPC?

This separation allowed complexity theory to make substantial contributions to the attempts to solve problems P2 and P3, especially P2, and to set as its new goal a contribution to the solution of the problem P4.

New recent goal and challenge of complexity theory is to help to answer the problem P1.

SETS of UNIVERSAL PRIMITIVES in CLASSICAL COMPUTING

- In *classical computing*, the most often used universal sets of gates are
  - AND-, OR- and NOT-gates,
  - AND- and NOT-gates,
  - NOR- (NAND-) or [AOI]-gate (that require few CMOS transistors)
- The optimization problem for classical circuits with such sets of gates has been solved quite satisfactorily.
- In case of *classical reversible computing*, universal are both the Toffoli gate

$$T(x, y, z) = (x, y, (x \wedge y) \oplus z)$$

and the Fredkin gate

$$F(x, y, z) = (x, \bar{x}y + xz, \bar{x}z + xy),$$

if constant inputs are allowed, as well as “wires” with the identity gates.

WHY REVERSIBLE CLASSICAL CIRCUITS?

Reversible classical circuits started to be of increased importance recently for several reasons:

- They are of importance in some applications, as signal processing, communication, cryptography, where circuits should be information lossless;
- Reversibility is of importance for some technologies where the loss of information due to irreversibility implies energy losses.
- Reversibility is of importance for some nanotechnologies, where switching devises with gain are not easy to construct;
- Reversible classical circuits are special cases of quantum circuits.

UNIVERSALITY of SETS of CLASSICAL REVERSIBLE GATES

Definition 0.1 *A set of reversible gates $\mathcal{G}$ is universal if for every n there exists a constant c_n such that for any permutation $\pi \in S_{2^n}$ there exists a $\mathcal{G}$-circuit which computes π using c_n ancilla wires.*

- Toffoli (1980) has shown that $a_n = n - 3$ in case the set of gates

  $$\text{CNT} = \{\text{CNOT, NOT, TOFFOLI}\}$$

  is used.

- Shende et al. (2002) have shown for circuits implementing even (odd) permutations that $c_n = 0$ ($c_n = 1$) in case of the set CNT.

OPTIMIZATION METHODS

Optimization of reversible circuits concerns the following characteristics: number of ancillas, number of gates and depth of the circuit.

- Optimization problem (concerning number of gates) for an important class of CNOT-circuits has been solved by K. N. Patel et al. (2002).
- The basic observation is that each circuit consisting of CNOT-gates realizes a so called xor-linear gate and vice verse.
- An n qubit gate U is called xor-linear if $U(x \oplus y) = U(x) \oplus U(y)$ holds for every $x, y \in \{0, 1\}^n$.
- They provide an algorithm that implements any xor-linear n qubit gate using $\mathcal{O}(n^2/lgn)$ CNOT-gates and they also showed that this result is asymptotically optimal.
- Optimization of $\{CNOT, NOT\}$ circuits has been solved by Iwama and Yamashita (2003). They found a complete set of transformation rules that can transform any $\{CNOT, NOT\}$-circuit to an optimal one. However, time complexity of optimization is exponential.

MINIMIZATION of the NUMBER of TOFFOLI GATES

Toffoli gates are, in a sense, strongest classical reversible gates. Of importance and interest is therefore the following problem.

Given a reversible function $f(\bar{x})$, what is the minimum number of Toffoli gates needed to construct a circuit that will evaluate $f(\bar{x})$ for every $\bar{x}$.

By Popescu et al. (04070350) there are reversible functions for which number of Toffoli gates grows exponentially.

Popescu et al. (0407035) have shown that given a classical reversible function f, one can construct a unitary transformation U_f such that if U_f is “non-local”, then f cannot be realized by a reversible circuit with two-bit gates only and the amount of non-locality of U_f provides a lower bound on the number of Toffoli gates needed.

The amount of non-locality of a gate U, denoted E_U, is defined as the minimum amount of entanglement, in ebits, which allows to implement U using LOCC.

LOWER BOUNDS on the number of TOFFOLI GATES

It holds

$$T_U \geq \frac{E_U}{E_{Tof}}$$

where T_U is number of Toffoli gates to implement U.

Popescu et al (0407035) have shown methods how to determine lower bound E_U and determined E_{Tof}.

This has been again an example that inherently quantum tools have been used to solve a classical problem.

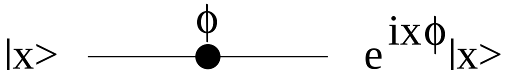
QUANTUM PRIMITIVES

UNIVERSAL SET of ONE-QUBIT GATES

Hadamard gate and the following phase shift gate

$$\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

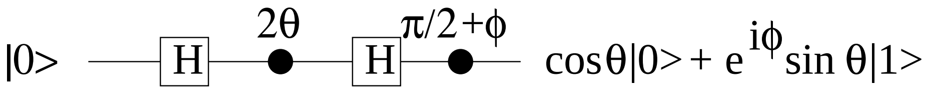
with notation



$|x\rangle \quad \phi \quad e^{ix\phi}|x\rangle$

form a universal set of gates for one-qubit gates.

Two Hadamard gates and two phase shift gates can generate the most general pure state of a single qubit



$|0\rangle \quad H \quad 2\theta \quad H \quad \pi/2+\phi \quad \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$

General form of a unitary matrix of degree 2

$$U = e^{i\gamma} \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{pmatrix}$$

BASIC CONCEPTS I

- Let $\mathcal{G}$ be a set of quantum gates. A $\mathcal{G}$-circuit is a quantum circuit with all gates from $\mathcal{G}$.
- Two n-qubit gates G_1 and G_2 are called locally equivalent if there are n one-qubit gates $U_1, \ldots, U_n$ and $V_1, \ldots, V_n$ such that

$$G_1 = (\bigotimes_{i=1}^{n} U_i) \otimes G_2 \otimes (\bigotimes_{i=1}^{n} V_i).$$

- A set of gates $\mathcal{G}_1$ is said to be adequate for a set of gates $\mathcal{G}_2$ if every gate form $\mathcal{G}_2$ can be implemented by a $\mathcal{G}_1$-circuit.
- Sets of gates $\mathcal{G}_1$ and $\mathcal{G}_2$ are called *equivalent* if $\mathcal{G}_1$ is adequate for $\mathcal{G}_2$ and vice verse.

BASIC CONCEPTS – APPROXIMABILITY

Definition An operator

$$U : \mathcal{H}_{2^r} \rightarrow \mathcal{H}_{2^r}$$

is ε-approximated, for an $\varepsilon > 0$, by an operator

$$\bar{U} : \mathcal{H}_{2^n} \rightarrow \mathcal{H}_{2^n},$$

where $n \geq r$, using an ancilla state $|\alpha\rangle \in \mathcal{H}_{2^{n-r}}$, if for any state $|\phi\rangle \in \mathcal{H}_{2^r}$,

$$||\bar{U}(|\phi\rangle \otimes |\alpha\rangle) - U(|\phi\rangle) \otimes |\alpha\rangle|| \leq \varepsilon.$$

TYPES of UNIVERSALITIES

Definition A set of gates $\mathcal{G}$ is called fully universal (f-universal) if every gate can be realized, up to a global phase factor, by a $\mathcal{G}$-circuit.

Definition A set of gates $\mathcal{G}$ is called universal if there is an integer n_0 such that any n-qubit unitary gate with $n \geq n_0$, can be, for any $\varepsilon > 0$, ε-approximated by a $\mathcal{G}$-circuit.

Definition A set of gates $\mathcal{G}$ is called densely universal (d-universal) if there exists an integer n_0 such that for any $n \geq n_0$, the subgroup generated by $\mathcal{G}$ is dense in $SU(2^n)$.

Definition A set of real gates $\mathcal{G}$ is called computationally universal (c-universal) if there is an integer n_0 such that any n-qubit real unitary gate with $n \geq n_0$, can be, for any $\varepsilon > 0$, ε-approximated by a $\mathcal{G}$-circuit.

BASIC GATES

Gates that will play an important role in the following:

$$\sigma_x = X, \sigma_y = Y, \sigma_z = Z, K = \sigma_z^{\frac{1}{2}}, T = \sigma_z^{\frac{1}{4}}.$$

where σ_x, σ_y and σ_z are Pauli operators;

$$CNOT = \Lambda_1(\sigma_x), \text{DCNOT}, \ \text{TOFFOLI} = \text{TOF} = \Lambda_2(\sigma_x),$$

where DCNOT$(x, y) = (y, x \oplus y)$ and for any one-qubit unitary U,

$$\Lambda_1(U) = \begin{pmatrix} 1_2 & 0_2 \\ 0_2 & U \end{pmatrix}, \quad \Lambda_2(U) = \begin{pmatrix} I_4 & 0_4 \\ 0_4 & \Lambda_1(U) \end{pmatrix}$$

are conditional operators and

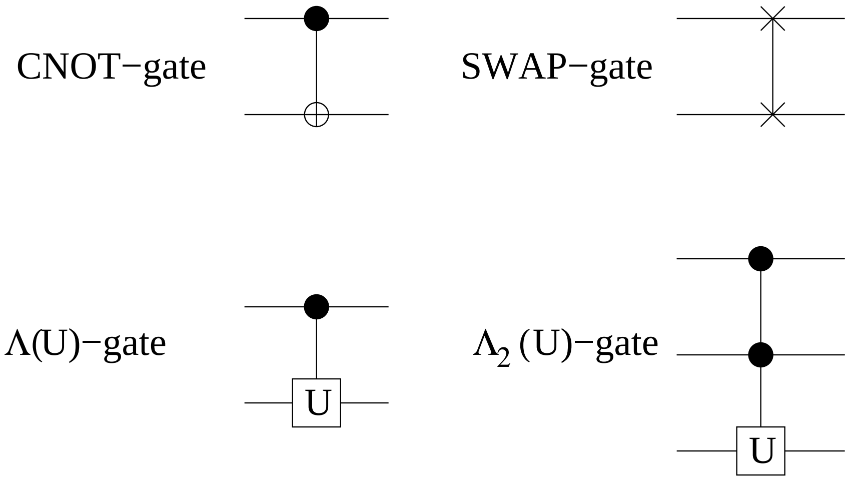
$$\text{HADAMARD} = H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z), \ \text{SWAP} \ \text{ and } \sqrt{\text{SWAP}},$$

where two-qubit unitary SWAP just exchanges inputs.

Observe that $\Lambda_1(\sigma_x) = (H \otimes I)\Lambda_1(\sigma_z)(H \otimes I)$ and therefore gates $\Lambda_1(\sigma_x)$ and $\Lambda_1(\sigma_z)$ are locally equivalent. Observe also that for any real α,

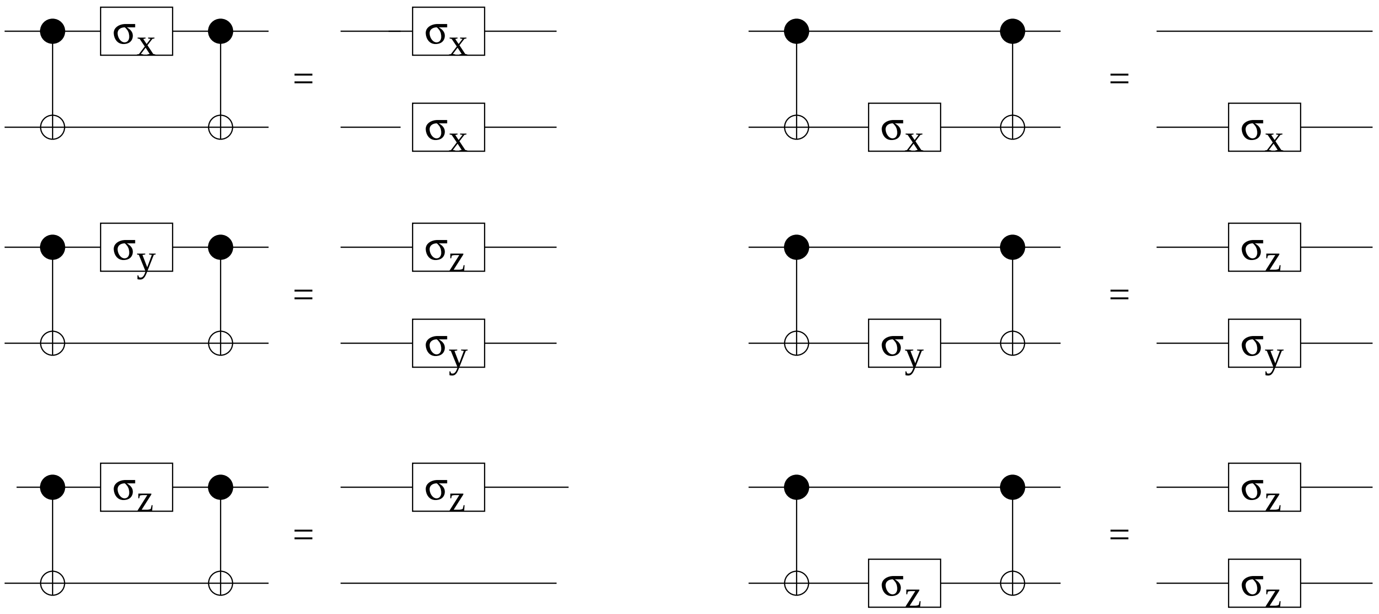
$$\sigma_z^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi\alpha} \end{pmatrix} = \Lambda_0(e^{i\pi\alpha}).$$

GRAPHICAL REPRESENTATION of some BASIC GATES

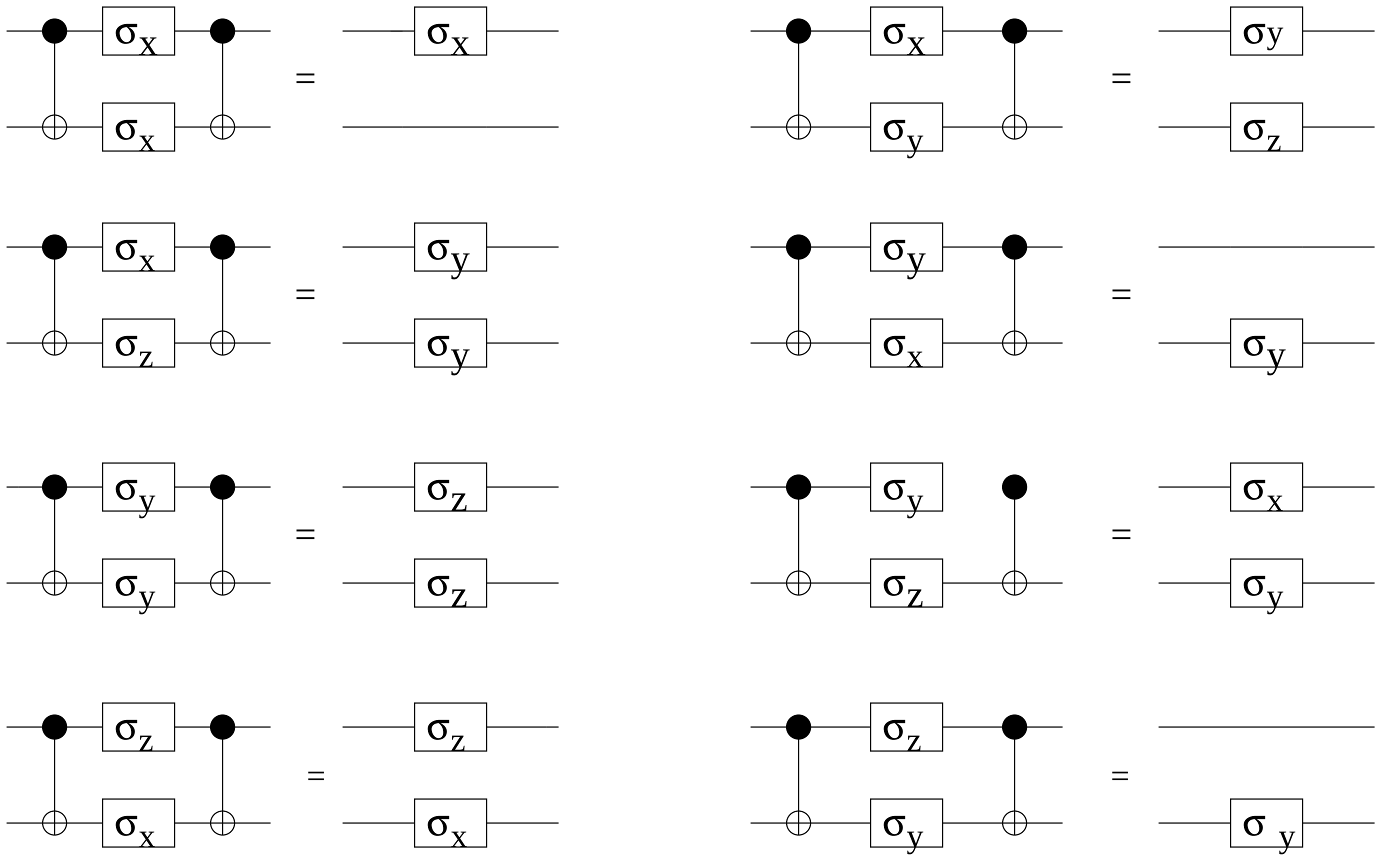


SOME USEFUL IDENTITIES

Several simple identities between elementary gates are surprisingly useful.


σ_x = σ_x σ_x
σ_x = σ_x
σ_y = σ_z σ_y
σ_y = σ_z σ_y
σ_z = σ_z
σ_z = σ_z σ_z

ANOTHER USEFUL IDENTITIES



BASIC ROTATION GATES

Rotations around axes:

$$R_x(\theta) = e^{-i\theta\sigma_x/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\sigma_x = \begin{pmatrix} \cos\tfrac{\theta}{2} & -i\sin\tfrac{\theta}{2} \\ -i\sin\tfrac{theta}{2} & \cos\tfrac{\theta}{2} \end{pmatrix}$$

$$R_y(\theta) = e^{-i\theta\sigma_y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\sigma_y = \begin{pmatrix} \cos\tfrac{\theta}{2} & -\sin\tfrac{\theta}{2} \\ \sin\tfrac{theta}{2} & \cos\tfrac{\theta}{2} \end{pmatrix}$$

$$R_z(\theta) = e^{-i\theta\sigma_z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\sigma_z = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{[}2} \end{pmatrix}$$

As a generalization we have a rotation around an arbitrary real unit vector $\bar{n} = (n_x, n_y, n_z)$ defined by

$$R_{\bar{n}}(\theta) = e^{-i\theta\bar{n}\cdot\bar{\sigma}/2} = \cos\frac{\theta}{2}(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z).$$

ONE-QUBIT GATES DECOMPOSITIONS

Let U be a one-qubit gate.

- $U = e^{i\alpha}R_{\bar{n}}(\beta)$ for some $\alpha, \beta, \bar{n}$.
- Let $\bar{m}$ and $\bar{n}$ be unit real orthogonal vectors, then

$$U = e^{i\alpha}R_{\bar{m}}(\beta)R_{\bar{n}}(\gamma)R_{\bar{m}}(\delta)$$

  for some $\alpha, \beta, \gamma \in R$
- $U = e^{i\alpha}A\sigma_xB\sigma_xC$, where $ABC = I$.

FIRST UNIVERSAL GATES

The first universal gate was discovered by Deutsch (1989). It is the 3-qubit gate

$$U_D = \left(\begin{array}{cc} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i\cos\theta & \sin\theta \\ 0 & 0 & \sin\theta & i\cos\theta \end{array} \end{array}\right),$$

where θ is an irrational multiple of π.

Deutsch's result has been improved to construct two-qubit universal gates. For example, Barenco (1995) showed universality of the following two-qubit gate

$$U_B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha}\cos\theta & -ie^{i(\alpha-\phi)}\sin\theta \\ 0 & 0 & -ie^{i(\alpha+\phi)}\sin\theta & e^{i\alpha}\cos\theta \end{pmatrix},$$

where α, θ, ϕ are irrational multiples of π.

Shortly afterwards, Barenco et al. (1995), Deutsch et al. (1995) and Lloyd (1995) showed that all randomly chosen 2-qubit gate, but a set of measure zero, form, with their reverse, universal sets of gates.

A SIMPLE UNIVERSAL GATE

It is well known that any rotation on Bloch sphere can be composed out of rotations

$$R_y(\phi) = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \qquad R_z(\phi) = \begin{pmatrix} e^{-i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

and these gates can be also used to construct a universal 2-qubit gate (Tamir, 2004)

$$\begin{pmatrix} R_y(\alpha) & 0 \\ 0 & R_z(\beta) \end{pmatrix},$$

where α, β and π are linearly independent over rationals.

FUNDAMENTAL RESULTS

The first really satisfactory results, concerning universality of gates, have been due to Barenco et al. (1995)

Theorem 0.2 *CNOT gate and all one-qubit gates form a universal set of gates.*

The proof is in principle a simple modification of the RQ-decomposition from linear algebra. Theorem 0.2 can be easily improved:

Theorem 0.3 *CNOT gate and* elementary rotation gates

$$R_\alpha(\theta) = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2}\sigma_\alpha, \quad \text{for} \quad \alpha \in \{x, y, z\}.$$

form a universal set of gates.

An important generalization has been due to Brylinskis (2001)

Theorem 0.4 *Any entangling two-qubit gate and all one-qubit gates (or all elementary gates) form an evolutionary universal set of gates.*

ENTANGLING GATES

- A two-qubit gate is called a entangling gate, or entangler, if it can map an unentangled state into an entangled one.
- Entangling is any two qubit gate that is not product of two one-qubit gates and it is not locally equivalent to the SWAP gate.
- An entangling gate is called a perfect entangler if it can map a product state into a maximally entangled state.
- CNOT and $\sqrt{\text{SWAP}}$ gates are perfect entanglers.

COMMENTS

- CNOT gate is an important primitive in the optics-based quantum information processing.
- In case of superconductor- and spin-based quantum computing more basic role play the gate $\sqrt{\text{SWAP}}$. This gate is, similarly as the CNOT gate, a maximally entangling gate.
- In general, for different technologies different two qubit gates or sets of gates e^{iHt}, for different t, generated by a Hamiltonian H, are considered as elementary and the circuit design task is then to decompose unitaries in terms of these elementary gates and one-qubit gates.

UNITARY OPERATIONS versus HAMILTONIANS

Unitary operations characterize discrete steps of quantum evolution.

In some sense, a more basic view of quantum evolution is to see it as a continuous process at which a quantum state evolves in time by a continuous rotation called a Hamiltonian.

A Hamiltonian H is a Hermitian matrix. The unitary operation $U(t)$ that is effected by “leaving H on for time t” is

$$U(t) = e^{-iHt}.$$

Example Hamiltonian for exchange computation (interaction0 has the form:

$$H = \frac{1}{2}(\sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z + I_2 \otimes I_2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

HAMILTONIAN for CNOT

For the Hamiltonian

$$H = \frac{\pi\hbar}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix} = \frac{\pi\hbar}{2}V$$

the Schödinger equation

$$i\hbar\frac{\partial U(t)}{\partial t} = HU(t)$$

has the solution

$$U(t) = e^{-\frac{i}{\hbar}Ht} = \sum_{k=1}^{\infty}\frac{(-\frac{i\pi}{2})^k V^k t^k}{k!} = I + \frac{1}{2}\sum_{k=0}^{\infty}\frac{(-\pi i t)^k}{k!}V$$

and therefore for $t = 1$,

$$e^{-\frac{i\pi}{2}V} = I + \frac{1}{2}(e^{-i\pi} - 1)V = I - V = XOR.$$

A RELATION TO TOPOLOGY

Let us call a two-qubit gate U locally universal (l-universal) if this gate and all one-qubit gates form a universal set of gates. Clearly any gate locally equivalent to an entangling gate is locally universal.

An interesting example of a locally universal gate is the gate

$$R = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

that transforms the standard basis into the Bell basis. This gate is also a solution of so called Yang-Baxter equation

$$(R \otimes I_2)(I_2 \otimes R)(R \otimes I_2) = (I_2 \otimes R)(R \otimes I_2)(I_2 \otimes R),$$

see Kauffman and Lomonoco (2004), which is a natural structure to think about topology of braids, knots and links[1], and therefore relates quantum topology and quantum computing.

[1] K not is an embedding of a circle, taken up to topological equivalence. Link is an embedding of a collection of circles.

MAJOR FINITE UNIVERSAL SETS OF GATES

The following are finite, interesting and important d-universal sets of gates:

- SHOR=$\{$TOF$, H, \sigma_z^{\frac{1}{2}}\}$, see Shor (1996).
- KLZ1 = $\{CNOT, \Lambda_1(\sigma_z^{\frac{1}{2}}), \sigma_z^{\frac{1}{2}}\}$, see Knill et al. (1998?).
- KITAEV = $\{\Lambda_1(\sigma_z^{\frac{1}{2}}), H\}$, see Kitaev (1997).
- BMPRV=$\{CNOT, H, \sigma_z^{\frac{1}{4}}\}$, see Boykin et al. (1999).

Kitaev (1997) has shown universality of the set KITAEV. Since sets KITAEV and SHOR are equivalent and gates in SHOR can be simulated by KLZ1-circuits. Universality of the set KLZ1 follows from that.

A THIN BORDER between UNIVERSALITY and NON-UNIVERSALITY

It is well known, as Gottesman-Knill theorem, that quantum circuits with operators in so called

Clifford set = $\{CNOT, H, K = \sigma_z^{\frac{1}{2}}\}$

can be simulated on classical computers in polynomial time. However, if the set of Clifford operators is “slightly enlarged”, by one of the special (mixed) states

1. $|H\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$;
2. $|G\rangle = \cos\beta|0\rangle + e^{i\frac{\pi}{4}}\sin\beta|1\rangle$, where $\cos(2\beta) = \frac{1}{\sqrt{3}}$;
3. By a one qubit mixed state ρ that is close, with respect to fidelity, to H-type or G-type states – states that can be obtained from the state $|H\rangle$ or $|G\rangle$ by a unitary transformation of the Clifford group,

we get already a universal set of quantum primitives (Bravyi and Kitaev, 2004).

WHY STATES $|H\rangle$ and $|G\rangle$?

The states $|H\rangle$ and $|G\rangle$ are not “fallen from the heavens”.

- $|H\rangle$ is eigenvector of the operator H.
- $|G\rangle$ is eigenvector of the operator $G = e^{\frac{i\pi}{4}}KH$.

G is again a “nice operator”. Indeed

$$G\sigma_x G^\dagger = \sigma_z, G\sigma_z G^\dagger = \sigma_y \text{ and } G\sigma_y G^\dagger = \sigma_x.$$

A SKETCH of the PROOF

We will deal with the case the state $|H\rangle$ is added.

It is easy to verify that $HK|H\rangle = e^{\frac{i\pi}{8}}|A_{-\pi/4}\rangle$, where

$$|A_\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\psi}|1\rangle.$$

Claim If we have sufficiently many copies of the state

$$|A_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle,$$

then we can implement, using Clifford set operation and Pauli operator eigenvalue measurements, the operator $\Lambda_0(e^{i\theta})$.

The operator $\Lambda_0(e^{i\theta})$ can be applied on a qubit $|\psi\rangle$ by a circuit shown in Figure 1.

The circuit applies randomly one of the operators $\Lambda_0(e^{\pm i\theta})$ and we know, due to classical outcomes of measurement, which one. By repeating the process several times we get, sooner or later, that the operator $\Lambda_0(e^{i\theta})$ is applied.

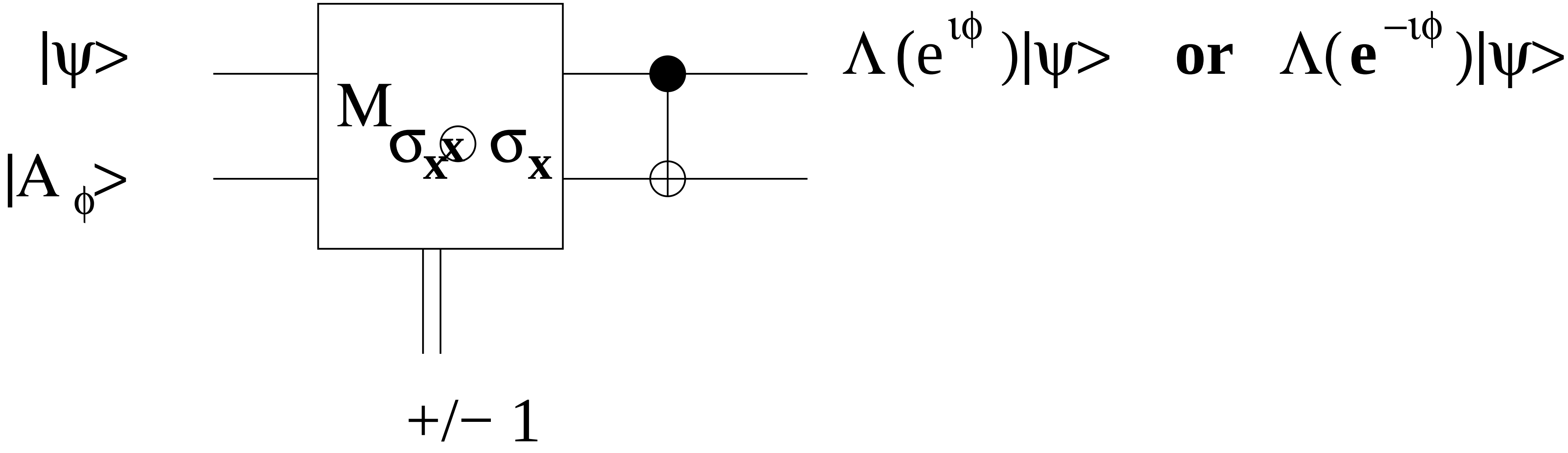


Figure 1: Implementation of the operator $\Lambda_0(e^{\pm i\theta})$

For $\theta = \frac{\pi}{4}$ we get an application of the operator $T = \sigma^{\frac{1}{4}}$, that is of the operator that is needed to enlarge the Clifford set of operations to a universal set of gates.

COMPUTATIONALLY UNIVERSAL SETS OF GATES

- Bernstein and Vazirani (1993) have shown that for having universal quantum computation it is sufficient to work with real amplitudes.
- Adleman et al. (1997) have shown that the set of amplitudes that is really needed is very small, for example

$$A = \{0, \pm 3/5, \pm 4/5, \pm 1\}, \text{ or } B = \{0, \pm 1/\sqrt{2}, \pm 1\},$$

  or $C = \{0, \pm\cos\theta, \pm\sin\theta, \pm 1\}$, for various θ.
- Rudolph and Grover (2002) have shown, surprisingly, that a simple two-qubit real gate

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\phi & -\sin\phi \\ 0 & 0 & \sin\phi & \cos\phi \end{pmatrix},$$

  with ϕ being an irrational multiple of π, is computationally universal.

SHI’s RESULTS

Surprising results have been obtained by Shi (2003)

Theorem 0.5

- *Toffoli gate and any one-qubit gate changing the computational basis form a computationally universal set of gates.*
- *CNOT gate and any one-qubit gate such that its square does not preserve computational basis form a universal set of g ates.*

As a consequence

- Toffoli and Hadamard gates form a computationally universal set of gates.

Since Toffoli gate is universal for classical reversible computing, Shi’s result means that full power of quantum computation is obtained by adding just the Hadamard gate.

PROOF of C-UNIVERSALITY of $\{H,T\}$

Lemma Any complex unitary gate U on n qubits can be replaced, from computational point of view, by a real gate U_r operating on $n+1$ qubits and defined by:

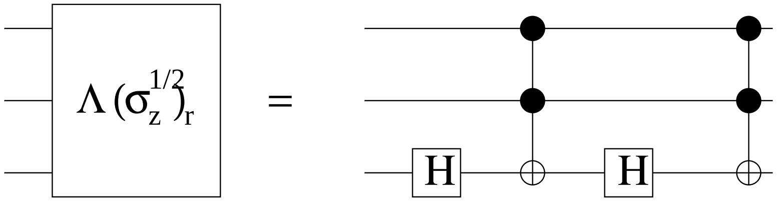
$$U_r|\phi\rangle|0\rangle = [Re(U)|\phi\rangle||0\rangle + [Im(U)|\phi\rangle]|1\rangle$$

$$U_r|\phi\rangle|1\rangle = -[Im(U)|\phi\rangle]|0\rangle + [re(U)|\phi\rangle]|1\rangle$$

where $[\phi\rangle$ is n-qubit state the gate U acts on.

For example the real version of the gate $\Lambda(\sigma_z^{\frac{1}{2}})$ is the gate $\Lambda_2(\sigma_x\sigma_z)$.

Since the set of gates $\{\Lambda(\sigma_z^{\frac{1}{2}}),H\}$ is universal, to show c-universality of the set $\{H,T\}$ it is enough to show a $\{H,T\}$ circuit implementing the gate $\Lambda(\sigma_z^{\frac{1}{2}})$. Since $\sigma_x\sigma_z = \sigma_x H\sigma_x H$, we have that as follows



POWER of the HADAMARD GATE

There are several ways to see what kind of power the Hadamard gate represents.

- On one side, Hadamard gate is a simple case of the Fourier transform and so one can say that, in some sense, quantum Fourier transform is what distinguishes classical and quantum computing.
- On the other hand, Hadamard gate can be seen as performing a random coin tossing and so one can say that it is just quantum random bit tossing what needs to be added to get quantum out of the classical computation.

FAULT-TOLERANTLY UNIVERSAL SETS of GATES

- Informally, a fault-tolerantly universal set of gates is a universal set of gates such that all gates of the set can operate in a noisy environment.
- More formal requirement is that there exists a quantum error correcting code such that all gates of the set can be performed on logical qubits without a need to decode them first and in such a way that propagation of single-qubit errors to other qubits in the same codeword is excluded.

The following sets of gates have been shown to be fault-tolerantly universal:

1. SHOR= $\{T, H, \sigma_z^{\frac{1}{2}}\}$, due to Shor (1996).
2. KITAEV =$\{\Lambda_1(\sigma_z^{\frac{1}{2}}), H\}$, due to Kitaev (1997).
3. BMPRV =$\{CNOT, H, \sigma_z^{\frac{1}{4}}\}$, due to Boykin et al. (1999).

ENCODED UNIVERSALITY of EXCHANGE INTERACTIONS

- *Encoded universality* refers to the capability to generate, or to approximate, all unitary matrices on a subspace of a Hilbert space created by some logical qubits.
- Heisenberg physical nearest neighbor exchange interaction is not universal for quantum computation in general, but, surprisingly, it can be universal on properly encoded logical qubits.

EXAMPLE

At the following encoding of the standard basis states of qubits by a row of 8 qubits, with the first and second four qubits for two basis states, see Hieh et al. (2003),

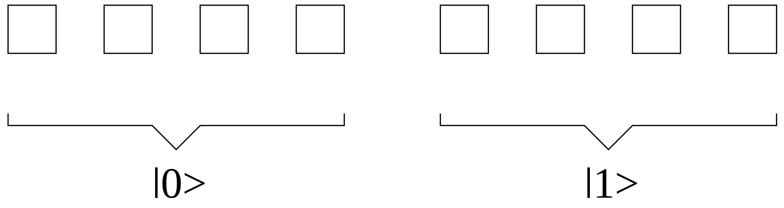


Figure 2: Encoding of two basis states

$$|0_L\rangle = \frac{1}{2}(|01\rangle - |10\rangle) \otimes (|01\rangle - |10\rangle)$$

$$|1_L\rangle = \frac{1}{\sqrt{3}}(|11\rangle \otimes |00\rangle - (\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \otimes (\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)) + |00\rangle \otimes |11\rangle).$$

the exchange of the first two (or the last two) qubits of each logical qubit realizes the operation $|0_L\rangle \rightarrow -|0_L\rangle$ and $|1_L\rangle \rightarrow |1_L\rangle$ and therefore, up to a phase factor, it actually realizes the σ_z operation on logical qubits.

One can then show that the Hamiltonian for $\sigma_z^{1/4}$ operation, realized by the nearing neighbors interactions is

$$e^{i\frac{\pi}{8}E_{1,2}},$$

where

$$E_{i,i+1}=\frac{1}{2}(\sigma_{x,i}\otimes\sigma_{x,i+1}+\sigma_{y,i}\otimes\sigma_{y,i+1}+\sigma_{z,i}\otimes\sigma_{z,i+1}+I\otimes I)$$

is the interaction between ith and $(i+1)$th qubit. With this notation an exact encoded Hadamard gate can be obtained as

$$H=e^{it_1E_{1,2}}e^{it_2E_{2,3}}e^{it_1E_{1,2}},\text{ where } t_1=\frac{1}{2}\arcsin\sqrt{\frac{2}{3}}\text{ and } t_2=\arccos\sqrt{\frac{1}{3}}.$$

To obtained an encoded realization of the CNOT gate, numerical methods have been used (with 27 parallel nearest neighbor exchange interactions or 50 serial gates).

As a consequence a single two qubit exchange interaction form a universal set (and therefore no one-qubit operations are needed) with respect to the encoded universality.

UNIVERSAL HAMILTONIANS

- An n-qubit Hamiltonian is called (dynamically) universal, if it is able to simulate any other n-qubit Hamiltonian using local unitaries.
- An n-qubit Hamiltonian is called entangling if every qubit is coupled to any other qubit, directly or via intermediate qubits.
- Bremner et al. (2003) have shown that an entangling Hamiltonian is universal iff it contains at least one coupling term involving an even number of interacting qubits.
- They have shown that there are only two fundamentally different types of entangling Hamiltonians on n qubits.

PART II - OPTIMIZATION

EFFICIENCY of UNIVERSAL SETS of QUANTUM PRIMITIVES

- It is a natural and important question to ask how good are, from the efficiency point of view, different universal sets of quantum primitives.
- Lloyd (1995) have shown that number of base gates needed grows exponentially in $\lg 1/\varepsilon$ to achieve precision ε.
- So called Solovay-Kitaev theorem implies that for evolutionary and computational universality, it is not costly to replace one universal basis by another one – it requires only poly-logarithmic overhead in $\lg 1/\varepsilon$ and that that number of base gates are needed.
- Solovay-Kitaev result implies that any gate from one finite universal set can be approximated with precision ε using polylog$(\frac{1}{\varepsilon})$ gates from other finite universal set of gates. More exactly, Solovay and Kitaev showed that there exist polynomial time algorithm (in $\lg 1/\varepsilon$ that creates a circuit with $\mathcal{O}(\lg^c(1/\varepsilon))$ gates, where $c \in [3,4]$.)
- Harrow et al. (2002) have shown that for some sets of universal gates number of gates required grows linearly in $\lg 1/\varepsilon$ (this is within a constant factor of the lower bound established by a counting argument).
- Of course, the above results are asymptotic and as such they have their limits.

DECOMPOSITION of UNITARIES into ONE- and TWO-QUBIT GATES

Two very basic questions concerning decomposition of n-qubit unitaries into one-and two-qubit gates are the following ones

- What is the total number of one-and two-qubits gates needed to decompose an arbitrary n qubit unitary operation – for different n?
- What is the total number of CNOT gates (or of some other entangling two qubit gates) needed to decompose an arbitrary n qubit unitary – for different n?

GENERAL RESULTS

- Barenco et al. (1995) have shown that any n qubit gate can be realized by $\mathcal{O}(n^3 4^n)$ CNOT and one-qubit gates.
- The above result has been improved, step by step, to $\mathcal{O}(n^2 4^n)$, $\mathcal{O}(n 4^n)$ and, finally, by Vartiainen et al. (2003) to $\mathcal{O}(4^n)$ – asymptotically tight.
- Concerning the CNOT gates only:
  - The best known upper bound is $\mathcal{O}(4^n)$ due to Vartiainen et al. (2003).
  - The best lower bound, due to Shende et al. (2003), is $\lceil (4^n - 3n - 1)/4 \rceil$.

DECOMPOSITION STEPS

- The basic idea of decomposition is borrowed from the QR-decomposition in linear algebra using so called Given's rotation matrices $G_{i,j,k}$ that are so called "two-level matrices" which operate non-trivially only on j-th and k-th basis vector and nullify elements on the i-th column and k-th row.
- The overall decomposition of a unitary ma trix U into a unit matrix has then the form

$$\left(\prod_{i=2^n-1}^{1} \prod_{j=i+1}^{2^n} G_{i,j,j-1} \right) U = I.$$

- Each two-level matrix can then be implemented using $C_{n-1}V$ and C_{n-1}NOT matrices, where V is a unitary 2×2 matrix and C_kV denotes a matrix with k control bits that control performance of the matrix V.
- A $C_{n-1}V$ matrix can be implemented with $\mathcal{O}(n^2)$ one- and two-qubit gates. Moreover, $\mathcal{O}(n)$ C_{n-1}NOT gates are needed between each two $C_{n-1}V$ gates and this leads to the total $\mathcal{O}(n^3 4^n)$ gates.

- An improvement to $\mathcal{O}(4^n)$ has been achieved when Gray-code ordering of the basis states has been used.
- An optimization method for quantum circuits, which is based on the existence of the above decomposition, and which concentrates on an optimization of the C_{n-1}NOT-gates is due to Aho and Svore (2003).

RECURSIVE DECOMPOSITION METHOD

An important general and recursive method of decomposition of any unitary matrix into one- and two-qubit unitary matrices, based on the Cartan decomposition of the Lie group $su(2^n)$, is due to Khaneja and Glaser (2000).

This methods has been used to obtain results presented below.

OPTIMAL REALIZATION of TWO-QUBIT GATES

Main problems with optimal realization of two-qubit circuits can be formulated as follows.

- Given a fixed entangling two-qubit gate G, what is the smallest number of gates G and of one-qubit (elementary) gates of a $\mathcal{G}$-circuit for implementation of an arbitrary given two-qubit gate U?
- Given a fixed entangling gate G, what is the minimal number of gates G needed, together with one-qubit gates, to realize an arbitrary two-qubit gate U?
- Given a fixed entangling gate G, find, as small as possible (with respect to the number of gates G and one-qubit (elementary) gates), a universal circuit scheme for implementation of any two-qubit unitary?
- To solve the above problems for special classes of entangling gates, or for specific entangling gates, as CNOT, or double CNOT (DCNOT), or $\sqrt{\text{SWAP}}$.

- If G is an entangling two-qubit gate and n_G is the minimal number of gates G needed to realize (with one-qubit gates) any two-qubit gate, then for any $1 \leq k \leq n_G$ it is of interest to determine necessary and sufficient conditions for a two-qubit gate to have implementation by a circuit with k gates G and some one-qubit gates.

CONTROLLED U-GATE CASE

Consider first the case that a two qubit Controlled-U gate G is given for a one-qubit gate U.

Since

$$U = e^{i(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)}$$

the controlled-U operation U_c can be written as

$$U_c = (I \otimes e^{\frac{-i\gamma}{2}\sigma_z}U_1^\dagger)e^{\frac{i\gamma}{2}\sigma_z\otimes\sigma_z}(I \otimes U_1)$$

for some one-qubit unitary U_1 and $\gamma = \sqrt{n_x^2 + n_y^2 + n_z^2}$.

Without the loss of generality we can therefore see, for our problem, any Controlled-U gate as having the form $U_c = e^{\frac{i\gamma}{2}\sigma_z\otimes\sigma_z}$.

It has been shown by Zhang et al. (2003) that having such a gate U_c the upper bound for a number of such controlled gates is $\lceil\frac{3\pi}{2\gamma}\rceil$ and they provide a procedure to design near optimal circuit for any two-qubit gate with U_c being the single two-qubit gate used.

KEY PROBLEMS

- The key problem is how many CNOT and one-qubit gates are necessary and sufficient to implement any two-qubit gate.
- Since each one-qubit gate can be expressed as a composition of any two of the elementary rotation gates R_x, R_y and R_z, it is of interest, and actually of large practical importance, to determine what is the minimal number of (elementary) gates R_x, R_y, R_z and $CNOT$ needed to implement an arbitrary two-qubit gate.

MAIN OUTCOMES

We discuss here only the best outcomes, so far, mainly due to Vidal and Dawson (2003), Shende et al. (2003) and Vatan and Williams (2003).

- 3 CNOT gates and 10 one-qubit and CNOT gates in total are sufficient to realize any two qubit gate.
- 3 CNOT gates and 9 gates in total are necessary.
- Each two-qubit gate can be realized using 3 CNOT gates and in total with 18 gates from the set containing the CNOT gate and any two of the three gates from the set $\{R_x, R_y, R_z\}$. (The above result is optimal for the case temporary storage is not allowed (because of being expensive).
- For gates from $SO(4)$ only 12 gates R_y, R_z are needed.

UNIVERSAL CIRCUIT SCHEMES

The universal two-qubit circuit scheme with three CNOT gates and 10 basic gates, or 18 gates from the set $\{CNOT, R_y, R_z\}$ is in Fig ure 5.

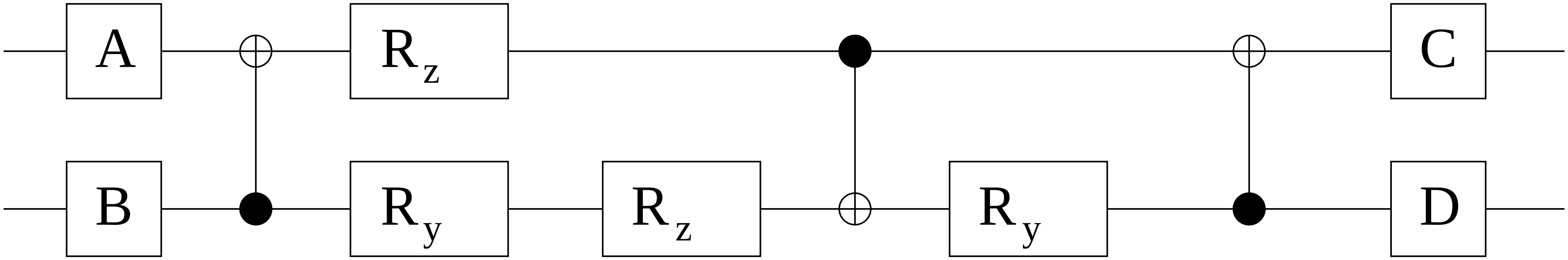


Figure 3: A universal 2-qubit circuit

USEFUL DECOMPOSITIONS

- Any two-qubit unitary matrix U has a unique decomposition

$$U = (A_1 \otimes B_1)e^{i(\theta_x X\otimes X+\theta_y Y\otimes Y+\theta_z Z\otimes Z)}(A_2 \otimes B_2),$$

  where $\frac{\pi}{4} \geq \theta_x \geq \theta_y \geq |\theta_z|$.

- Every real orthogonal $U \in SO(4)$ is in magic basis an element of $SU(2) \otimes SU(2)$.

GATES WITH SIMPLER DECOMPOSITIONS

The following criterion, due to Shende et al. (2003), allows to determine the number of CNOT gates needed to realize a two-qubit gate with the help of single qubit operations.

Theorem 0.6 *Let*

$$E = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

and for any matrix $U \in SU(4)$ let $\gamma(U) = UEUE$. Then it holds:

1. *U can be realized by a circuit with no CNOT gate if and only if $\gamma(U) = I$.*
2. *U can be realized by a circuit with one CNOT gate if and only if* Tr$(\gamma(U)) = 0$ *and* $\gamma(U)^2 = -I$.
3. *U can be simulated using two CNOT gates if and only if* Tr$(U))$ *is real.*

OPEN PROBLEMS

- Are there two two-qubit gates G_1 and G_2 such that any two-qubit gate can be implemented by a circuit with one-qubit gates and at most two of the gates G_1 and G_2?
- Design an algorithm which constructs, for any two-qubit entangling gate U, a minimal universal circuit scheme, with respect to the number of U gates, that uses U-gates as the only two qubit gates.

B-GATE STORY

Search for the best implementation of two qubit gates using a fixed two-qubit gate and one-qubit gates brought also a discovery of a new gate, so called **B-gate**. It is the gate realized by the following circuit:

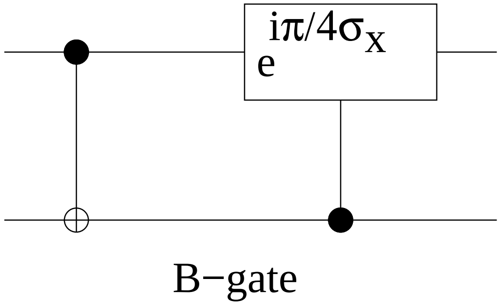


Figure 4: B-gate circuit

This gate is “better” than CNOT gate in the following sense.

Theorem Each two-qubit gate can be realized by a circuit with at most two B-gates and one-qubit gates.

GOING A STEP DOWN

PROBLEM: What is the minimal time to realize a two-qubit unitary using a fixed two-qubit entangling Hamiltonian and (fast) one-qubit unitaries?

SOLUTION (Khaneja et al. (2000), Vidal et al. (2001), Childs et al. (2003) If $U = e^{iH_1}$ is a two qubit unitary and H a two-qubit entangling Hamiltonian, then the minimal time required to simulate U using H and fast one-qubit unitaries is minimal t such that there exists a vector $\bar{m}$ of integers satisfying

$$\lambda(H_1) + \pi\bar{m} \prec \frac{\lambda(H + \tilde{H})}{2}t,$$

where $\lambda(A)$ denotes the vector of eigenvalues of a Hermitian matrix A and $\tilde{H} = (Y \otimes Y)H^T(Y \otimes Y)$.

3-QUBIT GATES CASE

- The case of an optimal realization of 3 qubits gates using a fixed two-qubit gate and one-qubit gates seems to be much more complex, but at the same time much more important.
- A universal circuit scheme with 40 CNOT gates and 98 one-qubit elementary gates, R_y and R_z, due to Vatan and Williams (2004), is, so far, the most efficient general way of implementation of 3 qubit gates.
- The above mentioned universal 3-qubit circuit has been also obtained using the general, already mentioned. decomposition method of Khaneja and Glaser (2001) and therefore it is likely that a more efficient universal circuit can be found.

HOW MANY CNOT Are NEEDED TO GENERATE 3-QUBIT STATES?

- For two qubits one CNOT is enough to go from any pure state to any other.
- For three qubits three CNOT are enough to go from $|000\rangle$ to any other pure state.
- For three qubits two CNOT are enough to go from GHZ state to any other pure state.
- As a corollary, four CNOT are enough to go from any 3-qubit state to any 3-qubit state.
- Open problem: can the previous result be improved?

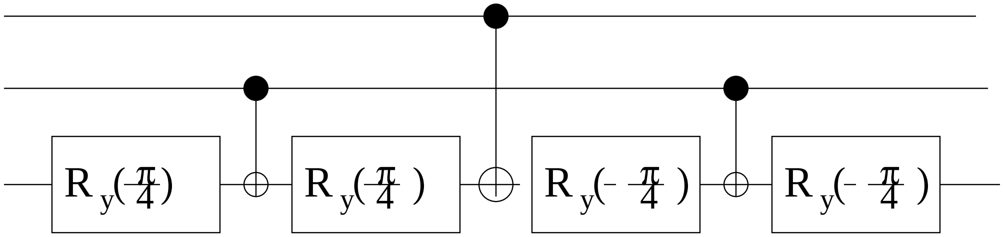
SPECIAL PROBLEMS CONCERNING OPTIMIZATION of QUANTUM CIRCUITS

At the circuit optimization it is of interest to consider the following three concepts of equivalence of states:

- Two states $|\phi\rangle$ and $|\psi\rangle$ are called identical if $|\phi\rangle = |\psi\rangle$;
- Two states $|\phi\rangle$, $|\psi\rangle$ are equivalent up to a global phase if $|\phi\rangle = e^{i\theta}|\psi\rangle$, where $\theta \in \mathbf{R}$.
- Two states $|\phi\rangle$, $|\psi\rangle$ are equivalent up to a relative phase if $|\phi\rangle$ can be mapped into $|\psi\rangle$ by a unitary diagonal matrix with diagonal $(e^{i\theta_0}, e^{i\theta_1} \ldots, e^{i\theta_k})$.

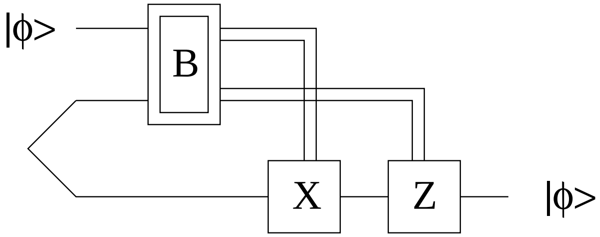
Toffoli gate can be exactly implemented by a circuit with 6 CNOT gates and 8 one-qubit gates.

On the other hand the following circuit is equivalent up to relative phase to Toffoli circuit.


$R_y(\frac{\pi}{4})$
$R_y(\frac{\pi}{4})$
$R_y(-\frac{\pi}{4})$
$R_y(-\frac{\pi}{4})$

UNIVERSALITY of ONE-QUBIT GATES, BELL MEASUREMENT and GHZ

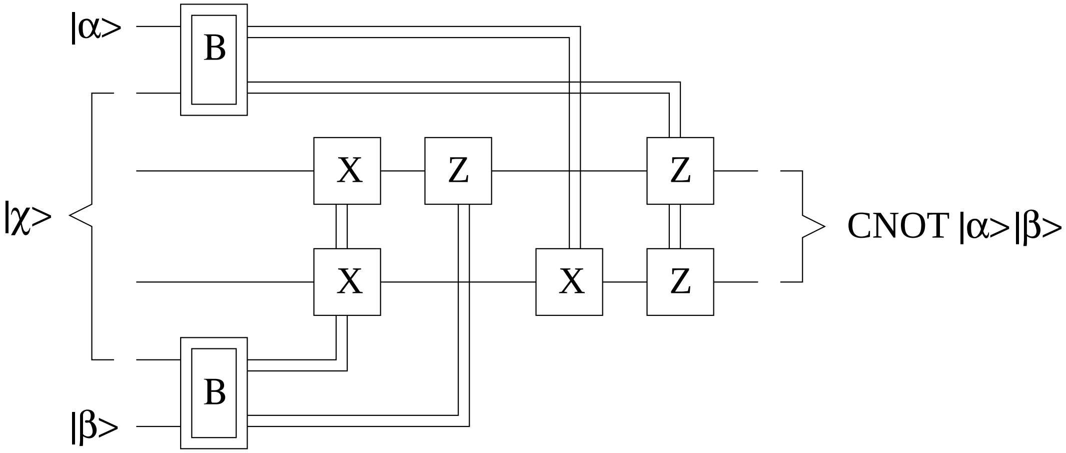
Another view of quantum teleportation:



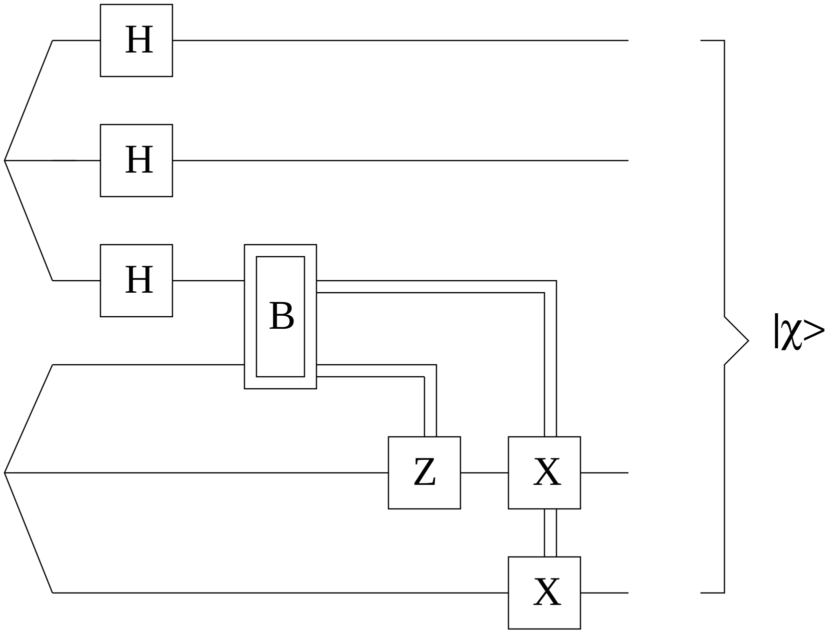
Using a special state

$$|\chi\rangle = \frac{(|00\rangle + |11\rangle)|00\rangle + (|01\rangle + |10\rangle)|11\rangle}{\sqrt{2}}$$

one can implement (Gottesmana and Chuang) CNOT as follows



$|\chi\rangle$ state can be realized, using two GHZ states as follows



STORY of PROJECTIVE MEASUREMENT PRIMITIVES

- Raussendorf and Briegel (2001) have shown that one-qubit projective measurements and a special fixed *cluster state*, that can be replaced by circuits dependent states that can be generated by 4 qubit measurements, form a universal set of quantum primitives.
- Nielsen (2001) has shown that 4 qubit measurements are sufficient to simulate all unitary operations.
- Leung has shown that almost any maximally entangling 4 qubit measurement is universal.
- Leung has improved various results concerning the power of projective measurements and showed that 2-qubit measurements are sufficient to simulate all 2 qubit operations.
- Leung (2003) has shown that there is a finite set of four 2-qubit measurements that can realize all 2-qubit unitary operations, if four ancilla qubits are available.
- Perdrix (2004) has shown that a simple set of *Pauli measurements* consisting of one two-qubit and three one-qubit measurements forms a universal set of quantum measurements if one-qubit ancilla as an additional resource is available. (These resources are minimal.)

BASIC IDEAS - VARIATIONS on TELEPORTATION

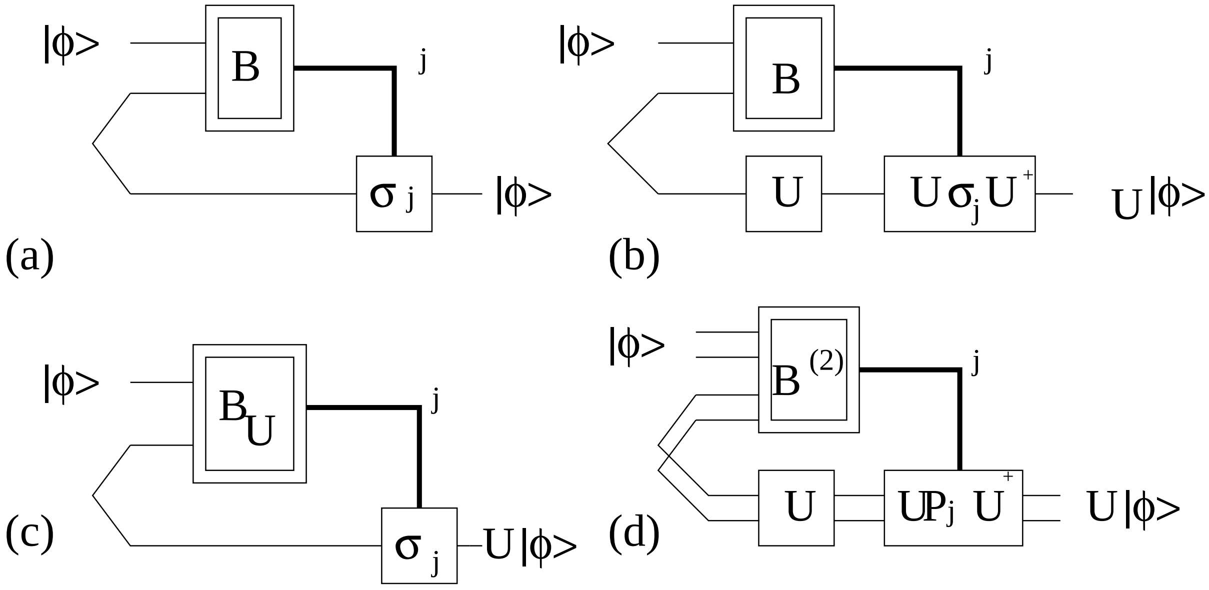
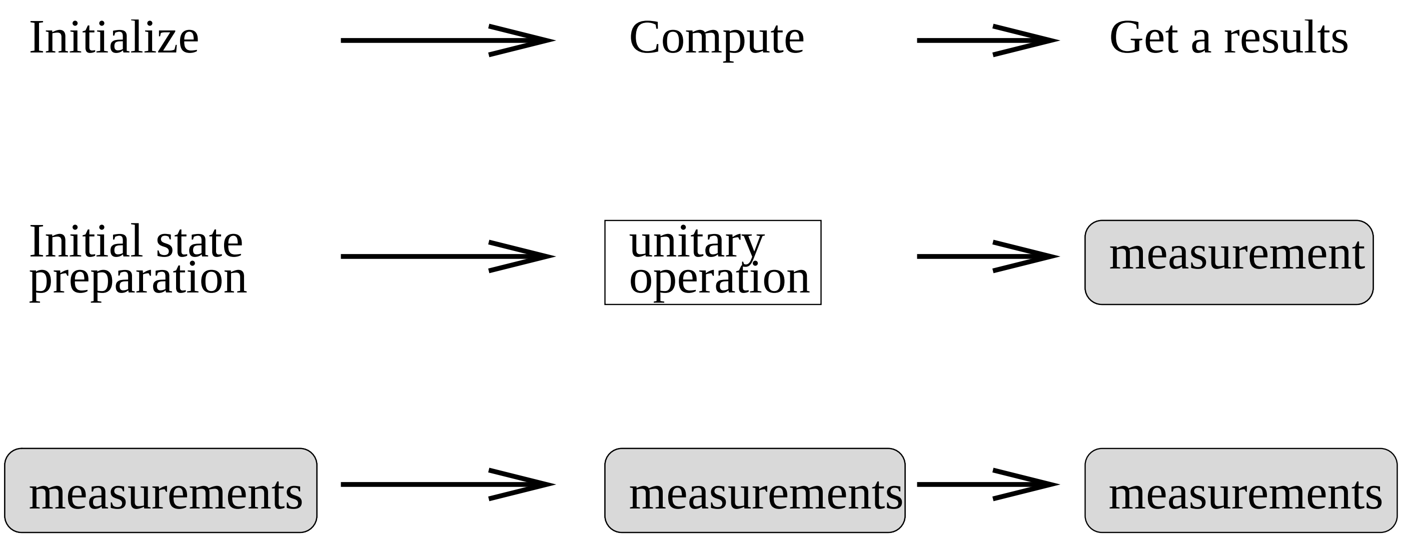


Figure 5: Teleportation of quantum operations

(a) Teleportation scheme; (b) Teleportation of an operation; (c) Teleportation of an operation by a measurement; (d) Teleportation of two-qubit operations.

TWO COMPUTATION MODES



Initialize → Compute → Get a results

Initial state preparation → unitary operation → measurement

measurements → measurements → measurements

Measurement = projective measurement.

MINIMAL RESOURCES for UNIVERSAL MEASUREMENTS

Perdrix (2004) has shown that one-qubit ancilla, one two-qubit Pauli measurement and three one-qubit Pauli measurements are sufficient to simulate any unitary operation.

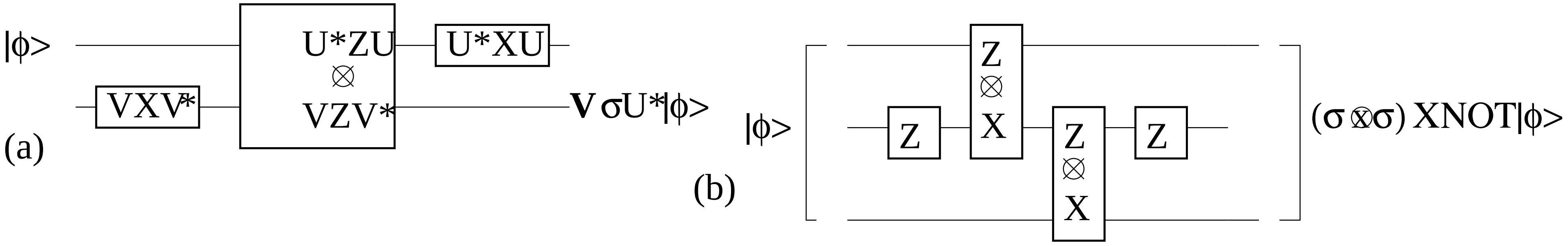


Figure 6: Two schemes for providing universal state transfer

- In the cases $U = H$ and $V = I$, the output has the form $\sigma H|\phi\rangle$.
- In the case $U = T = \sigma_z^{\frac{1}{4}}$ and $V = H$ the output has the form $\sigma HT|\phi\rangle$.
- In the above two cases only the measurements with observables X, Z, $\frac{1}{\sqrt{2}}(X+Y)$ and $X \otimes Z$ are used.

EXACT UNIVERSALITY of MEASUREMENTS

Perdrix and Jorrand have shown that the family of observables

$$\{Z \otimes X, Z, \cos(\theta)X - \sin(\theta)Y\}, \theta \in [0, 2\pi]$$

is universal, in the sense that any unitary can be realized, up to a Pauli operation only, using circuits consisting of such measurements.

OBSERVATIONS

- From strictly theoretical point of view closed quantum systems cannot be controlled, because if one tries to control them, they necessarily become open.
- Therefore, quantum measurement seem to be, in a sense, a unique tool to perform quantum computation.

MEASUREMENT BASED QUANTUM TURING MACHINES

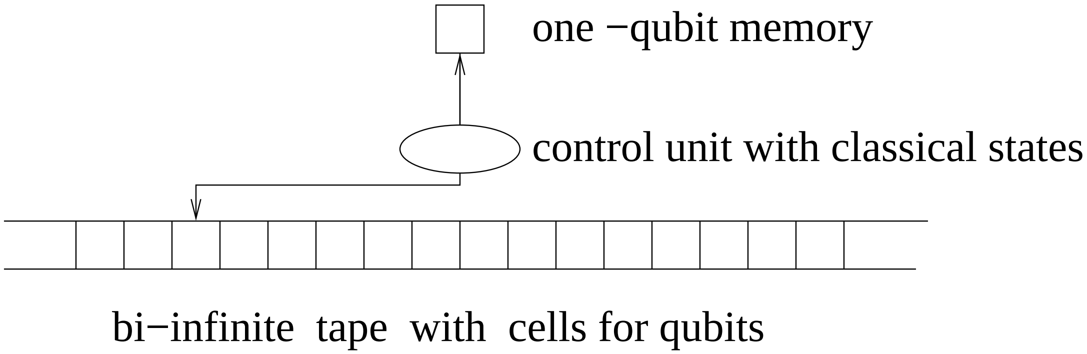

one −qubit memory
control unit with classical states
bi−infinite tape with cells for qubits

Figure 7: Universal QTM (Perdrix and Jorrand (2003)

Universal is the measurement based quantum Turing machine composed of (a) control unit; (b) one-qubit memory; (c) bi-infinite qubit tape with a transition function

States × Measurement outcomes → States × Observables × Head moves

and with the set of observables

$$\{X \otimes X, Z \otimes Z, X \otimes Z, X \otimes Z, X \otimes I, Z \otimes I, I \otimes X, I \otimes Z, \frac{1}{\sqrt{2}}(X \otimes X + X \otimes Y)\}.$$

OPTICAL QUANTUM COMPUTATION PRIMITIVES

Knill, Laflamme and Milburn (2001) demonstrated that all-optical quantum computation in principle needs only

- beamsplitters;
- phase shifters;
- single photon sources;
- photodetectors with feedforward.

They suggested to realize entangling gate

- probabilistically using single photon detectors, linear optics and photodetectors;
- to improve probability of the gate performance using teleportation, to gate gate working with probability $n^2/(n+1)^2$;
- to use farther error correction to improve probability of correct outcome.

Nielsen (2004) showed how to avoid last step using the idea of cluster states of Raussendorf and Briegel.

CLOSING OBSERVATION II

When a distinguished but elderly scientist states that something is possible, he is almost certainly right.

When he states that something is impossible,
he is almost certainly wrong,

Arthur C. Clarke

WISDOM

There is no quantum world. There is only an abstract quantum physical description. It is wrong to think that the task of physics is to find out how Nature is. Physics concerns what we can say about Nature.

Niels Bohr

CLOSING MOTTO

Progress in science is often done by pessimists.
Progress in technology is always done by optimists.

QUANTUM ALGORITHMS

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

March 6, 2008

3. QUANTUM ALGORITHMS

In the last two talks very basic techniques of designing quantum algorithms that are more efficient than their classical counterparts will be presented.

At first quantum algorithms for the Deutsch, Deutsch-Jozsa and Simon problems are presented and analyzed.

Secondly, main Shor's algorithms are analysed and their generalisation is discussed.

Finally, Grover algorithm and generalisations and modifications are presented and nalysed.

WHAT IS QUANTUM INFORMATION?

The views on what is quantum information differ.

- There is no quantum information, there are only quantum carriers of classical information. (A. Zeilinger).
- Concept of quantum information is primary fundamental concept/ingredient of quantum physics that cannot be defined. However, the viewpoint it suggest is richly suggestive, leading to new interesting questions and interpretations of quantum processes. (J. Jozsa)

CLOSING OBSERVATION I

When a distinguished but elderly scientist states that something is possible, he is almost certainly right.

When he states that something is impossible,
he is almost certainly wrong,

Arthur C. Clarke

BASICS of QUANTUM ALGORITHMS and SIMPLE QUANTUM ALGORITHMS

QUANTUM PARALLELISM

If

$$f : \{0, 1, \ldots, 2^n - 1\} \Longrightarrow \{0, 1, \ldots, 2^n - 1\}$$

then the mapping

$$f' : (x, b) \Longrightarrow (x, b \oplus f(x)),$$

where $x, b \in \{0, 1, \ldots, 2^n - 1\}$ is one-to-one and therefore there is a unitary transformation U_f such that.

$$U_f(|x\rangle|0\rangle) \Longrightarrow |x\rangle|f(x)\rangle$$

Let

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|0\rangle$$

With a **single application** of the mapping U_f we get

$$U_f|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle$$

IN A SINGLE COMPUTATIONAL STEP 2^n VALUES OF f ARE COMPUTED - in a sense!

MEASUREMENT — EXAMPLE

If we "measure" second register of the state

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle$$

with respect to the standard basis $\{|z\rangle \,|\, z \in \{0,1\}^n\}$, then the state $|\phi\rangle$ collapses into one of the states

$$|\phi_y\rangle = \frac{1}{\sqrt{k}} \sum_{\{x \,|\, f(x)=y\}} |x\rangle|y\rangle,$$

where

- y is in the range of the values of the function f.
- $k = |\{x \,|\, f(x) = y\}|$.

The collapse into the state $|\phi_y\rangle$ happens with the probability

$$\frac{k}{2^n}$$

and into the classical world one gets information which of y in the range of f, in the second register, has been (randomly) chosen.

This fact we usually interpret that y is the (classical) result of the measurement of the second register of the state$|\phi\rangle$, with respect to the standard basis.

U_f OPERATOR versus V_f OPERATOR

Another useful operator related to functions

$$f : \{0, 1, \ldots, 2^n - 1\} \rightarrow \{0, 1\}$$

is the operator

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

where $x \in \{0, 1, 2, \ldots, 2^n - 1\}$, which can be expressed using the operator

$$U_f : |x, b\rangle \rightarrow |x, b \oplus f(x)\rangle$$

and one additional qubit, called again **ancilla**, in the state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ as follows

$$\begin{aligned} U_f|x, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\rangle &= \frac{1}{\sqrt{2}}(x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle \\ &= (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

Warmup: Show how the operator V_f can be used to implement U_f.

EXAMPLE

Mapping $V_f : \{0,1\}^2 \leftrightarrow \{0,1\}$ is realized by the unitary matrix

$$V_f = \begin{pmatrix} (-1)^{f(00)} & 0 & 0 & 0 \\ 0 & (-1)^{f(01)} & 0 & 0 \\ 0 & 0 & (-1)^{f(10)} & 0 \\ 0 & 0 & 0 & (-1)^{f(11)} \end{pmatrix}.$$

DEUTSCH PROBLEM – RANDOMIZED SOLUTION

Given a function $f : \{0,1\} \rightarrow \{0,1\}$, as a black box, the task is to determine whether f is constant or balanced.

In classical computing 2 calls of f are needed.
In quantum computing 1 call of f is sufficient.

Quantum algorithm presented below solves the problem with probability $\frac{1}{2}$ in such a way that we know whether the answer is correct. Since

$$U_f : (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle) \rightarrow \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle),$$

the result can be written, in the standard and dual basis, as follows:

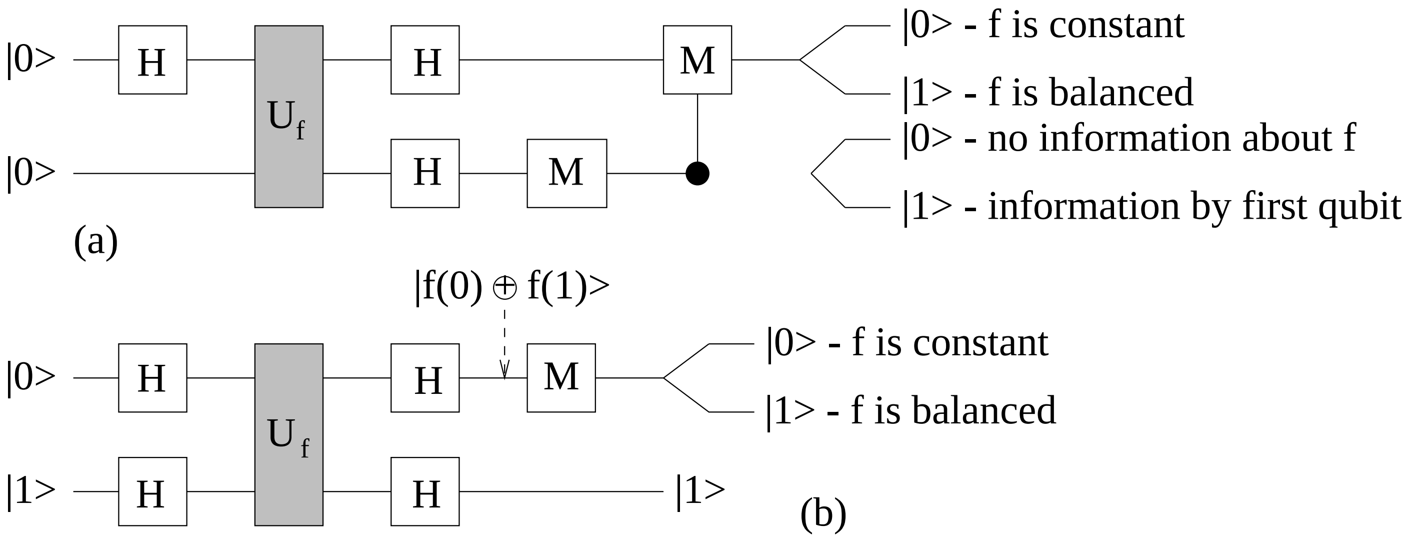
if f is constant:

$$\frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle) = \frac{1}{\sqrt{2}}(|0', 0'\rangle + (-1)^{f(0)}|0', 1'\rangle)$$

and if f is balanced:

$$\frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle) = \frac{1}{\sqrt{2}}(|0', 0'\rangle + (-1)^{f(0)}|1', 1'\rangle).$$

If the measurement of the second qubit in the dual bases provides 0 we have lost all information about f. Otherwise the measurement of the first qubit yields the correct result.
The corresponding circuit is shown in the following Figure.


|0>
|0>
H
U_f
H
H
M
M
|0> - f is constant
|1> - f is balanced
|0> - no information about f
|1> - information by first qubit
(a)
|f(0) ⊕ f(1)>
|0>
|1>
H
H
U_f
H
H
M
|0> - f is constant
|1> - f is balanced
|1>
(b)

DEUTSCH PROBLEM – DETERMINISTIC SOLUTION

Apply first the Hadamard transform on both registers in the initial state $|0,1\rangle$ and then U_f to get

$$\begin{aligned}
|0\rangle|1\rangle &\overset{H_2}{\rightarrow} \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\
&= \frac{1}{2}(|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)) \\
&\overset{U_f}{\rightarrow} \frac{1}{2}(|0\rangle(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)) \\
&= \frac{1}{2}(\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle)(|0\rangle - |1\rangle) \\
&= \frac{1}{2}(-1)^{f(0)}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle)(|0\rangle - |1\rangle). \qquad (1)
\end{aligned}$$

Hence

$$|0\rangle|1\rangle \overset{H_2}{\rightarrow} \tfrac{1}{2}(-1)^{f(0)}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle)(|0\rangle - |1\rangle) \tag{2}$$

From the right side in (2), the two possibilities for f to be constant lead to the left sides in (3) and (4) and two possibilities for f to be balanced lead to the left sides in (5) and (6):

$$\begin{aligned}
\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) &= \ \ |0'\rangle|1'\rangle \textbf{ if } f(0) = 0; & (3)\\
\frac{1}{2}(|0\rangle + |1\rangle)(|1\rangle - |0\rangle) &= -|0'\rangle|1'\rangle \textbf{ if } f(0) = 1; & (4)\\
\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) &= \ \ |1'\rangle|1'\rangle \textbf{ if } f(0) = 0; & (5)\\
\frac{1}{2}(|0\rangle - |1\rangle)(|1\rangle - |0\rangle) &= -|1'\rangle|1'\rangle \textbf{ if } f(0) = 1. & (6)
\end{aligned}$$

By measuring the first bit, with respect to the dual basis, we can immediately see whether f is constant or balanced.

SOMETIMES USEFUL WISDOM

If you are able to show that something

is impossssible

then, as the next step, it is often useful to try to show that

it is actually possible

from some other, useful, or at least interesting, point of view.

DE-QUANTUMIZATION in CASE of DEUTSCH PROBLEM

Surprisingly, quantum algorithms for Deutsch problem can be de-quantised as follows:

For a given $f : \{0,1\} \rightarrow \{0,1\}$ we define an oraculum mapping

$$C_f(a+bi) = (-1)^{0\oplus f(0)}a + (-1)^{1\oplus f(1)}bi$$

For the four possible functions f we get the following four functions C_f:

$$\begin{array}{lll} C_{00}(x) = x^* & \textbf{if} & f(0)=0, f(1)=0 \\ C_{01}(x) = x & \textbf{if} & f(0)=0, f(1)=1 \\ C_{10}(x) = -x & \textbf{if} & f(0)=1, f(1)=0 \\ C_{11}(x) = -x^* & \textbf{if} & f(0)=1, f(1)=1 \end{array}$$

The Deutsch problem can now be formulated as follows: A function is chosen secretly from the set of functions $\{C_{00}, C_{01}, C_{10}, C_{11}\}$ and the task is to determine, with a single query, which type of the function it is - balanced or constant.

Algorithm Given f, calculate $(i-1)f(1+i)$. If the outcome is real, then the function chosen is balanced; otherwise it is constant.

Correctness:

$$\begin{aligned}(i-1)C_{00}(1+i) &= (i-1)(1-i) = 2i\\ (i-1)C_{01}(1+i) &= (i-1)(1+i) = -2\\ (i-1)C_{10}(1+i) &= (i-1)(-1-i) = 2\\ (i-1)C_{11}(1+i) &= (i-1)(1-i) = -2i\end{aligned}$$

EVEN-ODD PROBLEM

A function $f : \{0,1\}^2 \leftrightarrow \{0,1\}$ is called even (odd) if the range of f has even (odd) number of ones.

Classically, given such a function f as an oracle, one needs 4 calls of f to determine whether f is even or odd.

Quantumly, it holds

$$(H \otimes H)V_f(I \otimes H)V_f(H \otimes H)|00\rangle = \begin{cases} \frac{1}{\sqrt{2}}(\pm|00\rangle + |01\rangle) & \text{if f is even} \\ \frac{1}{\sqrt{2}}(\pm|10\rangle + |01\rangle) & \text{if f is odd} \end{cases}$$

and therefore using only two quantum calls of f (of V_f), the problem is transformed into the problem to distinguish two non-orthogonal quantum states.

Unfortunately, there is no projection measurement that can faithfully distinguish such non-orthogonal states. However, as discussed already, there is a POVM measurement that either tells us whether a given function f is even or odd or the algorithm tells us “I don't know”.

DEUTSCH-JOZSA PROMISE PROBLEM

Given a function $f : \{0,1\}^n \rightarrow \{0,1\}$, as a black box, that is (promised to be) balanced or constant. Decide which property f has.

Classical deterministic computers needs, in the worst case, exponential time to solve the problem. Surprisingly, there is a quantum algorithm to solve the problem by applying f only once.

Let us consider one quantum register with n qubits and apply the Hadamard transformation H_n to the first register. This yields

$$|0^{(n)}\rangle \xrightarrow{H_n} |\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle.$$

By applying the transformation V_f on the first register we get

$$V_f|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)}|i\rangle = |\phi_1\rangle.$$

What has been achieved by these operations? The values of f were transferred to the amplitudes.

This can be utilized, through the power of quantum superposition and a proper observable, as follows.

Let us consider the observable $\mathcal{D} = \{E_a, E_b\}$, where E_a is the one-dimensional subspace spanned by the vector

$$|\psi_a\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle,$$

and $E_b = (E_a)^\perp$. The projection of $|\phi_1\rangle$ into E_a and E_b has the form

$$|\phi_1\rangle = \alpha|\psi_a\rangle + \beta|\psi_b\rangle \quad \textbf{with} \quad |\alpha|^2 + |\beta|^2 = 1,$$

where $|\psi_b\rangle$ is a vector in E_b such that $|\psi_a\rangle \perp |\psi_b\rangle$. A measurement by $\mathcal{D}$ provides "the value a or b" with probability $|\alpha|^2$ or $|\beta|^2$.
It is easy to determine α in

$$|\phi_1\rangle = \alpha|\psi_a\rangle + \beta|\psi_b\rangle \quad \textbf{with} \quad |\alpha|^2 + |\beta|^2 = 1,$$

using the projection of $|\phi_1\rangle$ onto E_a by the computation

$$\alpha = \langle\psi_a|\phi_1\rangle.$$

Indeed

$$\begin{aligned}\alpha &= \langle\psi_a|\phi_1\rangle = \left(\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}\langle i|\right)\left(\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}(-1)^{f(j)}|j\rangle\right) \\ &= \frac{1}{2^n}\sum_{i=0}^{2^n-1}\sum_{j=0}^{2^n-1}(-1)^{f(j)}\langle i|j\rangle = \frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^{f(i)},\end{aligned}$$

because $\langle i|j\rangle = 1$ if and only if $i = j$ and 0 otherwise.

If f is balanced, then the sum for α contains the same number of 1s and -1s and therefore $\alpha = 0$. A measurement of $|\phi_1\rangle$, with respect to $\mathcal{D}$ therefore provides, for sure, the outcome b.

If f is constant, then either $\alpha = 1$ or $\alpha = -1$ and therefore the measurement of $|\phi_1\rangle$ with respect to $\mathcal{D}$ always gives the outcome a.

A single measurement of $|\phi_1\rangle$, with respect to $\mathcal{D}$, therefore provides the solution of the problem with probability 1.

SECOND SOLUTION

If the Hadamard transformation is applied to the state $|\phi_1\rangle$ we get the state

$$|\phi_2\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}(-1)^{f(i)}\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{u\cdot i}|u\rangle = \frac{1}{2^n}\sum_{u=0}^{2^n-1}(\sum_{i=0}^{2^n-1}(-1)^{u\cdot i}(-1)^{f(i)})|u\rangle.$$

Case 1 f is constant. Then

$$\sum_{i=0}^{2^n-1}(-1)^{u\cdot i} = \begin{cases} 0 & \textbf{if } u \neq 0 \\ 2^n & \textbf{if } u = 0 \end{cases}$$

One measurement of the register therefore provides $u = 0$ with probability 1.

Case 2 f is balanced. In such a case

$$\sum_{i=0}^{2^n-1}(-1)^{u\cdot i}(-1)^{f(i)} = 0 \textbf{ if and only if } u = 0.$$

One measurement therefore shows whether f is balanced or not.

SIMON's PROBLEM

Simon has discovered a simple problem with expected polynomial time quantum algorithm, but with no polynomial time randomized algorithm.

Let $f : \{0,1\}^n \rightarrow \{0,1\}^n$ be a function such that either f is one-to-one or f is two-to-one and there exists a single $0 \neq s \in \{0,1\}^n$ such that

$$\forall x \neq x'(f(x) = f(x') \Leftrightarrow x' = x \oplus s).$$

The task is to determine which of the above conditions holds for f and, in the second case, to determine also s.

To solve the problem two registers are used, both with n qubits, and the initial states $|0^{(n)}\rangle$, and (expected) $\mathcal{O}(n)$ repetitions of the following version of the so-called Hadamard-twice scheme:

1. **Apply the Hadamard transformation on the first register, with the initial value $|0^{(n)}\rangle$, to produce the superposition $\frac{1}{\sqrt{2^n}}\Sigma_{x\in\{0,1\}^n}|x,0^{(n)}\rangle$.**
2. **Apply U_f to compute $|\psi\rangle = \frac{1}{\sqrt{2^n}}\Sigma_{x\in\{0,1\}^n}|x,f(x)\rangle$.**
3. **Apply Hadamard transformation on the first register to get**
$$\frac{1}{2^n}\sum_{x,y\in\{0,1\}^n}(-1)^{x\cdot y}|y,f(x)\rangle.$$
4. **Observe the resulting state to get a pair $(y,f(x))$.**

Case 1: f is one-to-one. After performing the first three steps of the above procedure all possible states $|y,f(x)\rangle$ in the superposition are distinct and the absolute value of their amplitudes is the same, namely 2^{-n}.

$n-1$ independent applications of the scheme *Hadamard-twice* therefore produce $n-1$ pairs $(y_1,f(x_1)),\dots,(y_{n-1},f(x_{n-1}))$, distributed uniformly and independently over all pairs $(y,f(x))$.

Case 2: There is some $s \neq 0^{(n)}$ such that

$$\forall x \neq x'((f(x) = f(x') \Leftrightarrow x' = x \oplus s).$$

In such a case for each y and x the states $|y, f(x)\rangle$ and $|y, f(x \oplus s)\rangle$ are identical. Their total amplitude $\alpha(x, y)$ has the value

$$\alpha(x, y) = 2^{-n}((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}).$$

If $y \cdot s \equiv 0 \bmod 2$, then $x \cdot y \equiv (x \oplus s) \cdot y \bmod 2$ and therefore $|\alpha(x, y)| = 2^{-n+1}$; otherwise $\alpha(x, y) = 0$. n independent applications of the scheme ***Hadamard-twice*** therefore yield $n - 1$ independent pairs

$$(y_1, f(x_1)), \ldots, (y_{n-1}, f(x_{n-1})) \text{ such that } y_i \cdot s \equiv 0 \pmod 2,$$

for all $1 \leq i \leq n - 1$.

In both cases, after $n - 1$ repetitions of the scheme ***Hadamard-twice***, $n - 1$ vectors $y_i, 1 \leq i \leq n - 1$, are obtained.

In both cases, after $n - 1$ repetitions of the scheme ***Hadamard-twice***, $n - 1$ vectors $y_i, 1 \leq i \leq n - 1$, are obtained.

If these vectors are linearly independent, then the system of $n-1$ linear equations in $\mathbf{Z}_2$,

$$y_i \cdot s \equiv 0 \pmod n$$

can be solved to obtain s.

In Case 2, if f is two-to-one, s obtained in such a way is the one to be found.

In Case 1, s obtained in such a way is a random string.

To distinguish these two cases, it is enough to compute $f(0)$ and $f(s)$.

If $f(0) \neq f(s)$, then f is one-to-one.

If the vectors obtained by the scheme *Hadamard-twice* are not linearly independent, then the whole process has to be repeated.

LOWER BOUND

One can show that each classical algorithm needs to perform $\Omega(\sqrt{2^n})$ queries to solve Simon's problem.

Indeed, let us assume that f is a randomly chosen function satisfying requirements of the Simon's problem. If k f-queries are performed then the number of potential s is decreased at most by $\frac{k(k-1)}{2}$ possibilities.

In total there are 2^n potential s.

Hence at least in half of the cases any classical algorithm needs to perform $\Omega(\sqrt{2^n})$ f-queries.

QUANTUM FOURIER TRANSFORM and SHOR's ALGORITHMS

Perhaps the most significant success of quantum computing so far has been Shor's polynomial time algorithm for factorization to be presented in this section. This is a highly nontrivial algorithm that uses a new technique, that of Quantum Fourier Transform, that will also be illustrated in this chapter.

The fastest classical algorithm to factor m bit numbers requires time $\mathcal{O}(e^{cm^{1/3}(\lg m)^{2/3}})$.

Shor's factorization algorithm requires $\mathcal{O}(m^2 \lg^2 m \lg \lg m)$ time on a quantum computer and polynomial time on a classical computer.

Of interest and importance is also another Shor's polynomial time algorithm for discrete logarithm to be also presented in this chapter.

Correctness and efficiency of Shor's algorithm is based on several simple results from number theory to be presented first.

BASICS

- Modulo operation: Given two integers $n > m$, then

$$n \bmod m$$

is the remmainder we get when n is divided by m.

Example: $24 \bmod 8 = 0$; $24 \bmod 7 = 3$; $24 \bmod 6 = 0$; $24 \bmod 5 = 4$.

Useful facts

$$a \cdot b \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$$

$$a^b \bmod n = ((a \bmod n)^b) \bmod n$$

Class work: Compute $3^{123456789} \bmod 26 = ???$

- For three integers a, b and n we define
$$a \equiv b(\mathrm{mod} n)$$
if
$$(a-b) \bmod n = 0$$
Examples $4 \equiv 11(\mathrm{mod} 15)$.
- Greatest common divisor Given integers n, m we denote by
$$\textit{gcd}(n,m)$$
the gretaest common divisor of m and n.

Examples; $\textit{gcd}(21,91)=7$; $\textit{gcd}(51,204)=$??

Useful fact 1 Already Euklid new a simple algorithm to compute greatest common divisor of arbitrary two integers.

Useful fact 2 For any integers n, a, b there are integers x, y such that
$$ax + by = \textit{gcd}(a,b) \bmod n$$

FIRST REDUCTION

Lemma 0.1 *If there is a polynomial time deterministic (randomized) [quantum] algorithm to find a nontrivial solution of the modular quadratic equations*

$$a^2 \equiv 1 \pmod{n},$$

then there is a polynomial time deterministic (randomized) [quantum] algorithm to factorize integers.

Proof. Let $a \neq \pm 1$ be such that $a^2 \equiv 1 \pmod{n}$. Since

$$a^2 - 1 = (a+1)(a-1),$$

if n is not prime, then a prime factor of n has to be a prime factor of either $a+1$ or $a-1$.

By using Euclid's algorithm to compute

$$gcd(a+1,n) \;\text{ and }\; gcd(a-1,n)$$

we can find, in $\mathcal{O}(\lg n)$ steps, a prime factor of n.

SECOND REDUCTION

The second key concept is that of **period** of the functions

$$f_{n,x}(k) = x^k \bmod n.$$

It is the smallest integer r such that

$$f_{n,x}(k+r) = f_{n,x}(k)$$

for any k, i.e. the smallest r such that

$$x^r \equiv 1 \pmod n.$$

AN ALGORITHM TO SOLVE EQUATION $x^2 \equiv 1 \pmod n$.

1. Choose randomly $1 < a < n$.
2. Compute $gcd(a,n)$. If $gcd(a,n) \neq 1$ we have a factor.
3. Find period r of function $a^k \bmod n$.
4. If r is odd or $a^{r/2} \equiv \pm 1 \pmod n$,then go to step 1; otherwise stop.

If this algorithm stops, then $a^{r/2}$ is a non-trivial solution of the equation

$$x^2 \equiv 1 \pmod n.$$

EXAMPLE

Let $n = 15$. Select $a < 15$ such that $gcd(a, 15) = 1$.
{The set of such a is $\{2, 4, 7, 8, 11, 13, 14\}$}

Choose $a = 11$. Values of $11^x \bmod 15$ are then

$$11, 1, 11, 1, 11, 1$$

what gives $r = 2$.

Hence $a^{r/2} = 11 \pmod{15}$. Therefore

$$gcd(15, 12) = 3, \qquad gcd(15, 10) = 5$$

For $a = 14$ we get again $r = 2$, but in this case

$$14^{2/2} \equiv -1 \pmod{15}$$

and the following algorithm fails.

1. Choose randomly $1 < a < n$.
2. Compute $gcd(a, n)$. If $gcd(a, n) \neq 1$ we have a factor.
3. Find period r of function $a^k \bmod n$.
4. If r is odd or $a^{r/2} \equiv \pm 1 \pmod{n}$,then go to step 1; otherwise stop.

EFFICIENCY of REDUCTION

Lemma 0.2 *If $1 < a < n$ satisfying $gcd(n, a) = 1$ is selected in the above algorithm randomly and n is not a power of prime, then*

$$Pr\{r \textit{ is even and } a^{r/2} \not\equiv \pm 1\} \geq \frac{9}{16}.$$

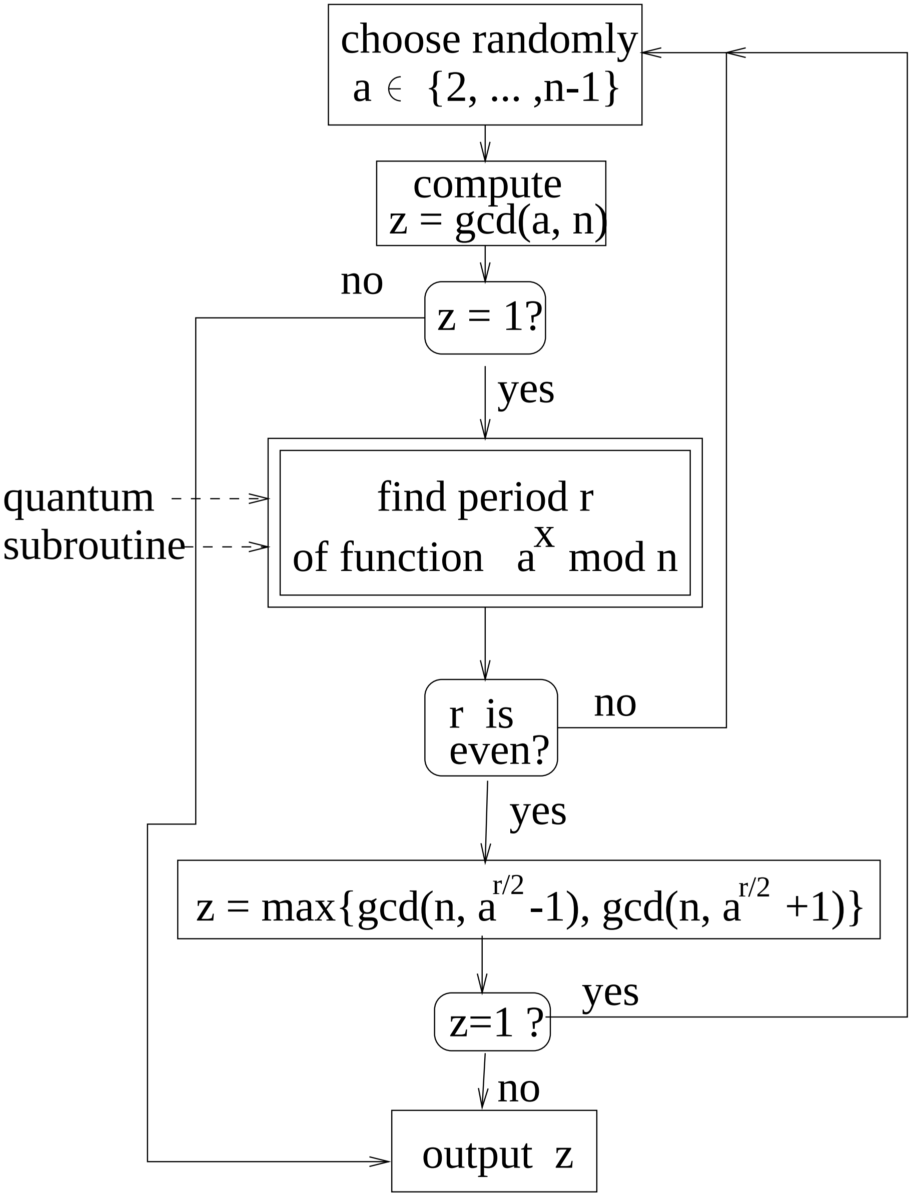
1. Choose randomly $1 < a < n$.
2. Compute $gcd(a, n)$. If $gcd(a, n) \neq 1$ we have a factor.
3. Find period r of function $a^k \bmod n$.
4. If r is odd or $a^{r/2} \equiv \pm 1 \pmod n$,then go to step 1; otherwise stop.

Corollary 0.3 *If there is a polynomial time randomized [quantum] algorithm to compute the period of the function*

$$f_{n,a}(k) = a^k \bmod n,$$

then there is a polynomial time randomized [quantum] algorithm to find non-trivial solution of the equation $a^2 \equiv 1 \pmod n$ (and therefore also to factorize integers).

A GENERAL SCHEME FOR SHOR'S ALGORITHM


choose randomly
a ∈ {2, ... ,n-1}
compute
z = gcd(a, n)
no
z = 1?
yes
quantum
subroutine
find period r
of function a^x mod n
r is even?
no
yes
z = max{gcd(n, $a^{r/2}$-1), gcd(n, $a^{r/2}$ +1)}
z=1 ?
yes
no
output z

SHOR's ALGORITHM

1. For given $n, q = 2^d, a$ create states
$$\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|n,a,q,x,\mathbf{0}\rangle \text{ and } \frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|n,a,q,x,a^x \bmod n\rangle$$
2. By measuring the last register the state collapses into the state
$$\frac{1}{\sqrt{A+1}}\sum_{j=0}^{A}|n,a,q,jr+l,y\rangle \text{ or, shortly } \frac{1}{\sqrt{A+1}}\sum_{j=0}^{A}|jr+l\rangle,$$
where A is the largest integer such that $l + Ar \leq q$, r is the period of $a^x \bmod n$ and l is the offset.
3. In case $A = \frac{q}{r} - 1$, the resulting state has the form.
$$\sqrt{\frac{r}{q}}\sum_{j=0}^{\frac{q}{r}-1}|jr+l\rangle$$
4. By applying quantum Fourier transformation we get then the state
$$\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}e^{2\pi ilj/r}|j\frac{q}{r}\rangle.$$
5. By measuring the resulting state we get $c = \frac{jq}{r}$ and if $gcd(j,r) = 1$, what happens with sufficient large probability, then from c and q we can determine the period r.

PERIOD COMPUTATION for $f_{n,a}(x) = a^x \bmod n, q = 2^d$

Hadamard transform applied to the state $|0^{(d)}, 0^{(d)}\rangle$ yields

$$|\phi\rangle = \frac{1}{\sqrt{2^d}} \sum_{x=0}^{q-1} |x, 0^{(d))}\rangle$$

and an application of the unitary transformation

$$U_{f_{n,a}} : |x, 0^{(d)}\rangle \rightarrow |x, a^x \bmod n\rangle$$

provides the state

$$|\phi_1\rangle = U_{f_{n,a}}|\phi\rangle = \frac{1}{\sqrt{2^d}} \sum_{x=0}^{q-1} |x, f_{n,a}(x)\rangle$$

Note 1: All possible values of the function $f_{n,a}$ are encoded in the second register in the state $|\phi_1\rangle$.

Note 2: We are interested in the period of the function $f_{n,a}$ and not in particular values of $f_{n,a}$.

Could we get period by measuring, several times, at first the second register and then the first one?

EXAMPLE

For $n = 15, a = 7$, $f_{n,a}(x) = 7^x \bmod 15$, $q = 16$, the state

$$U_{f_{n,a}}|\phi\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x, f_{n,a}(x)\rangle$$

has the form

$$\frac{1}{4}(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + \ldots + |14\rangle|4\rangle + |15\rangle|13\rangle).$$

If we measure at this point the second register, then we get as the outcome one of the numbers $1, 4, 7$ or 13, and the following table shows the corresponding post-measurement states in the second column.

result	post-measurement state	offset
1	$\frac{1}{2}(\|0\rangle + \|4\rangle + \|8\rangle + \|12\rangle)\|1\rangle$	0
4	$\frac{1}{2}(\|2\rangle + \|6\rangle + \|10\rangle + \|14\rangle)\|4\rangle$	2
7	$\frac{1}{2}(\|1\rangle + \|5\rangle + \|9\rangle + \|13\rangle)\|7\rangle$	1
13	$\frac{1}{2}(\|3\rangle + \|7\rangle + \|11\rangle + \|15\rangle)\|13\rangle$	3

The corresponding sequences of values of the first register are periodic with period 4 but they have different offsets (pre-periods) listed in column 3 of the table.

GRAPHICAL REPRESENTATION of STEPS

FOR SHOR's ALGORITHM

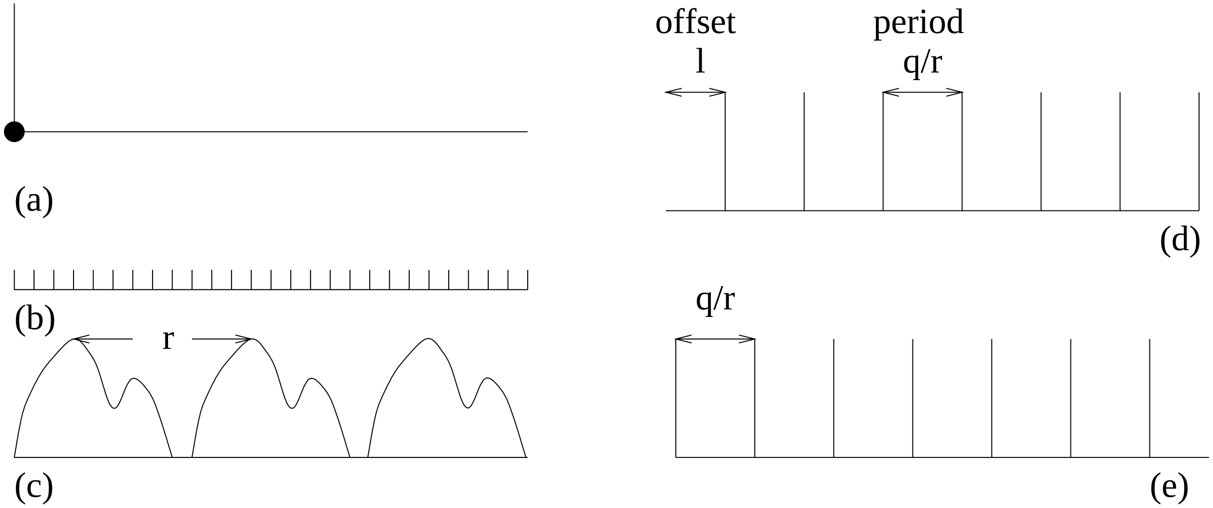


Figure 1: Graphical representation of steps of Shor's algorithm

DISCRETE FOURIER TRANSFORM

Discrete Fourier Transform maps a vector $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})^T$ into the vector $DFT(\mathbf{a}) = A_n\mathbf{a}$, where A_n is an $n \times n$ matrix such that $A_n[i,j] = \frac{1}{\sqrt{n}}\omega^{ij}$ for $0 \leq i, j < n$ and $\omega = e^{2\pi i/q}$ is the q**th root of unity**.

The matrix A_n has therefore the form

$$A_n = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & \ldots & \omega^{(n-1)} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{(n-1)} & \omega^{2(n-1)} & \ldots & \omega^{(n-1)^2} \end{pmatrix}.$$

The Inverse Discrete Fourier Transform is the mapping

$$DFT^{-1}(\mathbf{a}) = A_n^{-1}\mathbf{a},$$

where

$$A_n^{-1}[i,j] = \frac{1}{\sqrt{n}}\omega^{-ij}.$$

INSIDES into DFT

There is a close relation between Discrete Fourier Transform and polynomial evaluation and interpolation. Let us consider a polynomial

$$p(x) = \sum_{i=0}^{n-1} a_i x^i.$$

Such a polynomial can be uniquely represented in two ways: either by a list of its coefficients $a_0, a_1, \ldots, a_{n-1}$, or by a list of its values at n distinct points $x_0, x_1, \ldots, x_{n-1}$.

The process of finding the coefficient representation of the polynomial given its values at points $x_0, x_1, \ldots, x_{n-1}$ is called interpolation.

Computing the Discrete Fourier Transform of a vector $(a_0, a_1, \ldots, a_{n-1})$ is equivalent to converting the coefficient representation of the polynomial $\Sigma_{i=0}^{n-1} a_i x^i$ to its value representation at the points $\omega^0, \omega^1, \ldots, \omega^{n-1}$.

Likewise, the Inverse Discrete Fourier Transform is equivalent to interpolating a polynomial given its values at the n-th roots of unity.

QUANTUM FOURIER TRANSFORM

The Quantum Fourier Transform is a quantum variant of the Discrete Fourier Transform (DFT). DFT maps a discrete function to another discrete one with equally distant points as its domain. For example it maps a q-dimensional complex vector

$$\{f(0), f(1), \ldots, f(q-1)\} \ \ \textbf{into} \ \ \{\bar{f}(0), \bar{f}(1), \ldots, \bar{f}(q-1)\},$$

where for $c \in \{0, \ldots, q-1\}$

$$\bar{f}(c) = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} e^{2\pi iac/q} f(a), \tag{7}$$

for $c \in \{0, \ldots, q-1\}$.

The quantum version of DFT (QFT) is the unitary transformation

$$\mathbf{QFT}_q : |a\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi iac/q} |c\rangle \tag{8}$$

The quantum version of DFT (QFT) is the unitary transformation

$$\mathbf{QFT}_q : |a\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a c/q} |c\rangle \tag{9}$$

for $0 \leq a < q$, with the unitary matrix

$$F_q = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{(q-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(q-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{(q-1)} & \omega^{2(q-1)} & \dots & \omega^{(q-1)^2} \end{pmatrix},$$

where $\omega = e^{2\pi i/q}$ is the qth root of unity.
If applied to a quantum superposition, $\mathbf{QFT}_q$ performs as follows;

$$\mathbf{QFT}_q : \sum_{a=0}^{q-1} f(a)|a\rangle \rightarrow \sum_{c=0}^{q-1} \bar{f}(c)|c\rangle,$$

where $\bar{f}(c)$ is defined by (7).
Observe that

$$QFT_q : |\mathbf{0}\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{i=0}^{q-1} |i\rangle,$$

SHOR's ALGORITHM — PHASE 1

Design of states whose amplitudes have the same period as $f_{n,a}$

Given an m bit integer n we choose a $n^2 \leq q \leq 2n^2$ and start with five registers in states $|n, a, q, \mathbf{0}, \mathbf{0}\rangle$, where the last two registers have $m = \lceil \lg n \rceil$ qubits.
An application of the Hadamard transformation to the fourth register yields the state

$$\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |n, a, q, x, \mathbf{0}\rangle.$$

and using quantum parallelism we compute $a^x \bmod n$ for all x in one step, to get

$$\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |n, a, q, x, a^x \bmod n\rangle.$$

As the next step we perform a measurement on the last register. Let y be the value obtained, i.e. $y = a^l \bmod n$ for the smallest l_y with this property. If r is the period of $f_{n,a}$, then $a^{l_y} \equiv a^{jr+l_y} \pmod n$ for all j. Therefore, the measurement actually selects the sequence of x's values (in the fourth register), $l_y, l_y + r, l_y + 2r, \ldots, l_y + Ar$, where A is the largest integer such that $l_y + Ar \leq q - 1$. Clearly, $A \approx \frac{q}{r}$. The post-measurement state is then

$$|\phi_l\rangle = \frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |n, a, q, jr + l_y, y\rangle = \frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |jr + l_y\rangle. \qquad (10)$$

after omitting some registers being fixed from now on.

SHOR's ALGORITHM — PHASE 2.

Amplitude amplification by QFT

From now on we consider in detail only a special case. Namely that r divides q. In such a case $A = \frac{q}{r} - 1$. In such a case the last state can be written in the form

$$|\phi_l\rangle = \sqrt{\frac{r}{q}} \sum_{j=0}^{\frac{q}{r}-1} |jr + l_y\rangle$$

and after QFT$_q$ is applied on $|\phi_l\rangle$ we get:

$$\mathrm{QFT}_q|\phi_l\rangle = \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \sqrt{\frac{r}{q}} \sum_{j=0}^{\frac{q}{r}-1} e^{2\pi ic(jr+l_y)/q}|c\rangle = \frac{\sqrt{r}}{q} \sum_{c=0}^{q-1} e^{2\pi ilc/q} \left(\sum_{j=0}^{\frac{q}{r}-1} e^{2\pi ijcr/q} \right) |c\rangle = \sum_{c=0}^{q-1} \alpha_c|c\rangle \qquad (1)$$

If c is a multiple of $\frac{q}{r}$, then $e^{2\pi ijcr/q} = 1$ and if c is not a multiple of $\frac{q}{r}$, then

$$\sum_{j=0}^{\frac{q}{r}-1} e^{2\pi ijcr/q} = 0,$$

because the above sum is over a set of $\frac{q}{r}$ roots of unity equally spaced around the unit circle. Thus

$$\alpha_c = \begin{cases} \frac{1}{\sqrt{r}} e^{2\pi ilc/q}, \text{ if } c \text{ is a multiple of } \frac{q}{r}; \\ 0, \text{ otherwise}; \end{cases}$$

and therefore

$$|\phi_{out}\rangle = \mathsf{QFT}_q|\phi_l\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{2\pi i l_y j/r}|j\frac{q}{r}\rangle.$$

The key point is that the trouble-making offset l_y appears now in the phase factor $e^{2\pi i l_y j/r}$ and has no influence either on the probabilities or on the values in the register.

SHOR's ALGORITHM — PHASE 3

Period extraction

Each measurement of the state $|\phi_{out}\rangle$ therefore yields one of the multiples $c = \lambda\frac{q}{r}$, $\lambda \in \{0, 1, \ldots r-1\}$, where each λ is chosen with the same probability $\frac{1}{r}$.

Observe also that in this case the QFT transforms a function with the period r (and an offset l) to a function with the period $\frac{q}{r}$ and offset 0. After each measurement we therefore know c and q and

$$\frac{c}{q} = \frac{\lambda}{r},$$

where λ is randomly chosen.

If $gcd(\lambda, r) = 1$, then from q we can determine r by dividing q with $gcd(c, q)$. Since λ is chosen randomly, the probability that $gcd(\lambda, r) = 1$ is greater than $\Omega(\frac{1}{\lg\lg r})$. If the above computation is repeated $\mathcal{O}(\lg\lg r)$ times, then the success probability can be as close to 1 as desired and therefore r can be determined efficiently.[1]

In the general case, i.e., if $A \neq \frac{q}{r} - 1$, there is only a more sophisticated computation of the resulting probabilities and a more sophisticated way to determine r (using a continuous fraction method to extract the period from its approximation).

[1] As observed by Shor (1994) and shown by Cleve et al. (1998), the expected number of trials can be put down to a constant.

GENERAL CASE

Let us now sketch Shor's algorithm to compute the period of a function $f(x) = a^x \bmod n$ for the general case.

QFT$_q$ is applied to the first register of the state $\frac{1}{\sqrt{q}}\Sigma_{x=0}^{q-1}|x\rangle|f(x)\rangle$ and afterwords the measurement is performed on the first register to provide an $y_0 \in [0,\ldots,q-1]$.

To get the period r the following algorithm is realized where $\xi = \frac{y_0}{q}$, $a_0 = \lfloor\xi\rfloor$, $\xi_0 = \xi - a_0$, $p_0 = a_0, q_0 = 1$, $p_1 = a_1a_0 + 1, q_1 = a_1$

for $j = 1$ **until** $\xi_j = 0$ **do**

- compute p_j and q_j using the recursion (for the case $\xi_j \neq 0$);

$$a_j = \left\lfloor\frac{1}{\xi_{j-1}}\right\rfloor, \xi_j = \frac{1}{\xi_{j-1}} - a_j,$$

$$p_j = a_jp_{j-1} + p_{j-2}, \qquad q_j = a_jq_{j-1} + q_{j-2}$$

- Test whether $q_j = r$ by computing first $m^{q_j} = \Pi_i(m^{2^i})^{q_{j,i}} \bmod n$, where $q_j = \Sigma_i\, q_{j,i}2^i$ is the binary expansion of q_n.

  If $a^{q_j} = 1 \bmod n$, then exit with $r = q_j$; if not continue the loop.

The non-easy task is to show, what has been done, that the above algorithm provides the period r with sufficient probability ($> \frac{0.232}{\lg\lg n}(1-\frac{1}{n})^2$).

COMMENTS on SHOR's FACTORIZATION ALGORITHM

- **Efficient implementations of QFT$_q$, concerning the number of gates, are known for the the case $q = 2^d$ or q is smooth (that is if factors of q are smaller than $\mathcal{O}(\lg q)$).**
- **Efficient implementation of modular operations (including exponentiation) are known.**
- **An estimation says that $300 \lg n$ gates are needed to factor n.**
- **An estimation says that to factor 130 digit integers would require two weeks on an ideal quantum computer with switching frequency 1 MHz. However to factor 260-digit number only 16 times larger time would be needed.**
- **It has been shown that there is polynomial time factorization even in the case only one pure qubit is available and the rest of quantumness available is in mixed states.**

CLASSICAL SIMULATION and OPTIMIZATION of SHOR's ALGORITHM

Two problems much bothered QIPC community. To distil crucial elements of Shor's algorithm which allow speed-up it exhibits as well to optimise its implementation.

- It can be easily seen that Shor's algorithm has two main components: Quantum Fourier Transform and modular exponentiation.
- Surprisingly, see [quant-ph/0611156, quant-ph/0611241] approximate QFT (sufficient for Shor's algorithm) can be efficiently classically simulated.
- The key problem therefore seems modular exponentiation.
- This may seem strange because it seems that this can be done by a classical circuit.
- Indeed, it has been shown [quant-ph/0706-0872] that "any classical algorithm that can efficiently simulate the circuit implementing modular exponentiation for general product input states and product state measurements on the output, allows for an efficient simulation of a whole Shor's algorithm on classical computers.

Concerning optimisation, the best current outcome is that it is sufficient to use $1.5n$ qubits to factor n bit integers.

The first estimates were that ???? qubits are needed.

SHOR's DISCRETE LOGARITHM ALGORITHM

Shor's quantum algorithm for discrete logarithm will be again presented only for a special case.

The task is to determine an r such that $g^r \equiv x \pmod p$ given a prime p, a generator g of the group $\mathbf{Z}_p^*$ and a $0 < x < p$. The special case we consider is that $p-1$ is smooth.

Using QFT$_{p-1}$ twice, on the third and fourth sub-register of the register $|x, g, \mathbf{0}, \mathbf{0}, \mathbf{0}\rangle$, we get

$$|\phi\rangle = \frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|x, g, a, b, \mathbf{0}\rangle,$$

a uniform distribution of all pairs (a,b), $0 \leq a, b \leq p-2$. By applying to $|\phi\rangle$ a unitary mapping

$$(x, g, a, b, \mathbf{0}) \rightarrow (x, g, a, b, g^a x^{-b} \bmod p)$$

we get

$$|\phi'\rangle = \frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|x, g, a, b, g^a x^{-b} \bmod p\rangle.$$

Since x, g will not be changed in the following computations we will not write them explicitly any longer.

As the next step we apply QFT$_{p-1}$ on $|\phi'\rangle$ twice, once to map $a \rightarrow c$ with amplitude $\frac{1}{\sqrt{p-1}}e^{2\pi iac/(p-1)}$ and once to map $b \rightarrow d$ with amplitude $\frac{1}{\sqrt{p-1}}e^{2\pi ibd/(p-1)}$. The resulting state is

$$|\phi_1\rangle = \frac{1}{(p-1)^2}\sum_{a,b,c,d=0}^{p-2} e^{\frac{2\pi i}{p-1}(ac+bd)}|c, d, g^a x^{-b} \bmod p\rangle.$$

$$|\phi_1\rangle = \frac{1}{(p-1)^2}\sum_{a,b,c,d=0}^{p-2} e^{\frac{2\pi i}{p-1}(ac+bd)}|c,d,g^a x^{-b} \bmod p\rangle.$$

Let us now measure last register and denote by y the value we get.

The state $|\phi_1\rangle$ then collapses into the state (before normalization)

$$|\phi_2\rangle = \sum_{c,d=0}^{p-1} \alpha(c,d)|c,d,y\rangle,$$

where

$$\alpha(c,d) = \frac{1}{(p-1)^2}\sum_{\{(a,b)\,|\,y=g^a x^{-b} \bmod p\}} e^{\frac{2\pi i}{p-1}(ac+bd)}.$$

We now claim that if $y = g^a x^{-b} \bmod p$, then $y = g^k$ for some k such that

$$a - rb \equiv k \pmod{p-1}.$$

Indeed,

$$y = g^a x^{-b} \equiv g^a (g^r)^{-b} = g^{a-rb}.$$

If $a - rb \equiv k \pmod{p-1}$, then

$$g^{a-br} \equiv g^k \pmod{p}$$

Therefore

$$\alpha(c,d) = \frac{1}{(p-1)^2} \sum_{\{(a,b)\,|\,a-rb\equiv k \pmod{p-1}\}} e^{\frac{2\pi i}{p-1}(ac+bd)}$$

For the probability *Pr* that, for fixed c and d we get by measurement of $|\phi_2\rangle$ a value y is therefore

$$\left|\frac{1}{(p-1)^2}\sum_{a,b=0}^{p-2}\{e^{\frac{2\pi i}{p-1}(ac+bd)}\,|a-rb\equiv k \pmod{p-1}\}\right|^2.$$

By substituting $a = k + rb + j_b(p-1)$ we get the probability

$$\mathit{Pr} = \left|\frac{1}{(p-1)^2}\sum_{b=0}^{p-2} e^{\frac{2\pi i}{p-1}(kc+cj_b(p-1)+b(d+rc))}\right|^2.$$

$$\left|\frac{1}{(p-1)^2}e^{\frac{2\pi iac}{p-1}}\sum_{b=0}^{p-2} e^{\frac{2\pi i}{p-1}(b(d+rc))}\right|^2$$

what equals

$$\left|\frac{1}{(p-1)^2}\sum_{b=0}^{p-2} e^{\frac{2\pi i}{p-1}(b(d+rc))}\right|^2$$

The above probability Pr is therefore 0 if

$$d + rc \not\equiv 0 \bmod (p-1)$$

because, as in the previous algorithm, in such a case the sum in the above expression is over a set of $(p-1)$st roots of unity equally spaced around the unit circle.

On the other hand, if

$$d \equiv -rc \pmod{p-1},$$

then the above sum does not depend on b and it is equal to

$$(p-1)^{-1}e^{(2\pi ikc/(p-1))}.$$

The square of its absolute value, the probability, is therefore $\frac{1}{(p-1)^2}$.

Consequence: the measurements on the first and second register provide a (random) $c < p-1$ and a d such that

$$d \equiv -rc \pmod{p-1}.$$

If $gcd(c, p-1) = 1$, r can now be obtained as a unique solution of the above congruence equation.

Therefore, the number of computations needed to perform in order to get the probability close to 1 for finding r is polynomial in $\lg\lg p$.

COMMENTS on SHOR's ALGORITHMS

- **To factor an integer n shor's algorithm uses $\mathcal{O}(\lg^3 n)$ steps and success probability is guarantd to be at least $\Omega(\frac{1}{\lg\lg n})$.**
- **An analysis of Shor's algorithm therefore shows that by running the alsgorithm $\mathcal{O}(\lg\lg n)$ times, therefore in total in $\mathcal{O}(\lg^3 n \lg\lg n)$ timnes we have very high success probability.**
- **Shor's algorithms make some of the important current cryptosystems, as RSA, ElGamal and so on vulnerable to attacks using quantum computers.**
- **Shor's result have been generalized to show that a large range of cryptosystems, including elliptic curve cryptosystems, would be vulnerable to attacks using quantum computers.**

EXTRAS

COSETS

Given am additive group G and its subgroup G_0, then a

left coset of G, with respect to G_0

is any set

$$a + G_0,$$

where $a \in G$.

Useful fact Two cosets are either identical or disjoint.

Useful fact: Each coset has $|G_0|$ elements.

HIDDEN SUBGROUP PROBLEM

Given: An (efficiently computable) function $f : G \rightarrow R$, where G group and R a finite set.

Promise: There exists a subgroup $G_0 \leq G$ such that f is constant and distinct on the cossets of G_0.

Task: Find a generating set for G_0 (in polynomial time (in $\lg |G|$) number of calls to the oracle for f and in the overall polynomial time).[2]

[2] A way to solve the problem is to show that in polynomial number of oracle calls (or time) the states corresponding to different candidate subgroups have exponentially small inner product and are therefore distinguishable.

SPECAIL HIDDEN SUBGROUP PROBLEMS

Deutsch's problem, $G = \mathbf{Z}_2$, $f : \{0,1\} \rightarrow \{0,1\}$,
$x - y \in G_0 \Leftrightarrow f(x) = f(y)$. Decide whether $G_0 = \{0\}$ (and f is balanced) or $G_0 = \{0,1\}$ (and f is constant).

Simon's problem, $G = \mathbf{Z}_2^n$, $f : G \rightarrow R$. $x - y \in G_0 \Leftrightarrow f(x) = f(y)$,
$G_0 = \{0^{(n)}, s\}$, $s \in \mathbf{Z}_2^n$. Decide whether $G_0 = \{0^{(n)}\}$ or
$G_0 = \{0^{(n)}, s\}$, with an $s \neq 0^{(n)}$ (and in the second case find s).

Order-finding problem, $G = \mathbf{Z}$, $a \in \mathbf{N}$, $f(x) = a^x$,
$x - y \in G_0 \Leftrightarrow f(x) = f(y)$, $G_0 = \{rk \,|\, k \in \mathbf{Z}$ for the smallest r such that $a^r = 1.\}$ Find r.

Discrete logarithm problem, $G = \mathbf{Z}_r \times \mathbf{Z}_r$, $a^r = 1$, $b = a^m$,
$a, b \in \mathbf{N}$, $f(x,y) = a^x b^y$,
$f(x_1, y_1) = f(x_2, y_2) \Leftrightarrow (x_1, y_1) - (x_2, y_2) \in G_0$.
$G_0 = \{(-km, m) \,|\, k \in \mathbf{Z}_r\}$. Find G_0 (or m).

IMPORTANT FACTS

- Hidden subgroup problem can be solved in quantum polynomial time if the underlying group is Abelian.
- It is an open problem whether the Hiden subgroup problem can be solved in quantum polynomial time also for any non-Abelian group.
- Would the Hideen subgroup problem be always solvable in quantum polynomial time, this would imply that the Graph isomorphism problem can be solved in quantum polynomial time.

IMPLEMENTATION Of THE QUANTUM FOURIER TRANSFORM in $\mathbf{Z}_{2^m}$

The clue to the design of a quantum circuit to implement the QFT

$$|x\rangle \rightarrow \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i x y}{2^m}} |y\rangle$$

for $|x\rangle = |x_{m-1}\rangle|x_{m-2}\rangle \ldots |x_0\rangle$ is the decomposition

$$\sum_{y=0}^{2^m-1} e^{\frac{2\pi i x y}{2^m}} |y\rangle = (|0\rangle + e^{\frac{\pi i x}{2^0}}|1\rangle)(|0\rangle + e^{\frac{\pi i x}{2^1}}|1\rangle)\ldots(|0\rangle + e^{\frac{\pi i x}{2^{m-1}}}|1\rangle)$$

The exponent in th l-th factor of the above decomposition can be written as follows

$$\exp(\frac{\pi i(2^{m-1}x_{m-1} + 2^{m-2}x_{m-2} + \ldots + 2x_1 + x_0)}{2^{l-1}})$$

$$= \exp(\frac{\pi i(2^{l-1}x_{l-1} + 2^{l-2}x_{l-2} + \ldots + 2x_1 + x_0)}{2^{l-1}})$$

$$= (-1)^{x_{l-1}} exp(\frac{\pi i x_{l-2}}{2}) \ldots exp(\frac{\pi i x_1}{2^{l-2}}) exp(\frac{\pi i x_0}{2^{l-1}})$$

DESIGN of CIRCUIT

Starting, for convenience, with the reverse representation of x as $x_0x_1\ldots x_{m-1}$ we show how to implement

$$(|0\rangle + e^{\frac{\pi ix}{2^0}}|1\rangle)(|0\rangle + e^{\frac{\pi ix}{2^1}}|1\rangle)\ldots(|0\rangle + e^{\frac{\pi ix}{2^{m-1}}}|1\rangle)$$

for qubits $m-1, m-2, \ldots, 0$, step by step, starting with $(m-1)$-th qubit.

Using Hadamard transform on the $m-1$-th qubit we get

$$\frac{1}{\sqrt{2}}|x_0\rangle|x_1\rangle\ldots|x_{m-2}\rangle(|0\rangle + (-1)^{x_{m-1}}|1\rangle)$$

and then we can complete the phase $(-1)^{x_{m-1}}$ to

$$(-1)^{x_{m-1}}exp(\frac{\pi ix_{m-2}}{2^1})\ldots exp(\frac{\pi ix_1}{2^{m-2}})exp(\frac{\pi ix_0}{2^{m-1}})$$

by using conditionally phase rotations

$$exp(\frac{\pi i}{2^1}),\ldots,exp(\frac{\pi i}{2^{m-2}})exp(\frac{\pi i}{2^{m-1}})$$

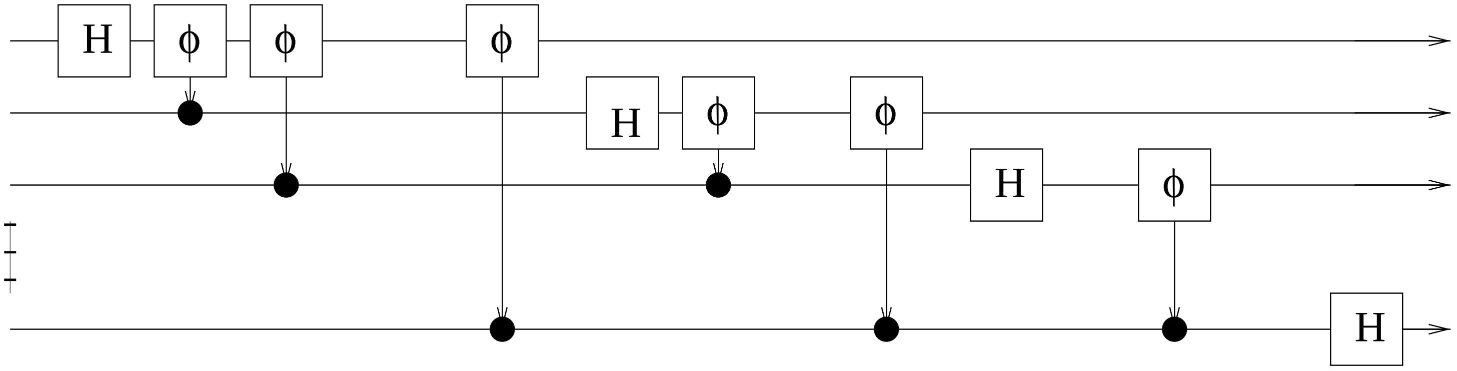
This means that for each $l \in \{1, 2, \ldots, m-1\}$ a phase factor $exp(\frac{\pi i}{2^{m-l}})$ is introduced to the m-th bit if and only if mth and lth qubits are both 1. This will provide the state

$$\frac{1}{\sqrt{2}}|x_0\rangle|x_1\rangle\ldots|x_{m-2}\rangle(|0\rangle + e^{\frac{2\pi i x}{2^{m-1}}}|1\rangle)$$

This process can be repeated with other qubits. Each time we use once the Hadamard transform and then the unitary

$$\phi_{kl} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{\pi i}{2^{l-k}}} \end{pmatrix}$$

which acts on the lth and kth qubit. The resulting circuit has then the following form:


H
ϕ
ϕ
ϕ
H
ϕ
ϕ
H
ϕ
H

COMPLEXITY of FOURIER TRANSFORM

- The naive algorithm to compute all elements of classical Fourier transform, element by element using basic definition, requires $\mathcal{O}(2^{2m})$ steps.
- A special recursive method, called **Fast Fourier Transform**, that recursively reduces computation of DFT in $\mathbf{Z}_{2^m}$ to computation of two DFT in $\mathbf{Z}_{2^{m-1}}$, requires $\mathcal{O}(m2^m)$ steps - a significant improvement.
- Quantum Fourier Transform in $\mathbf{Z}_{2^m}$ can be done in $\mathcal{O}(m^2)$ quantum steps.

Moreover, in the classical case, physical representation of

$$(f(0), f(1), \ldots, f(2^m - 1))$$

requires $\Omega(2^m)$ bits,

but in the quantum case representation of

$$c_0|0\rangle + c_1|1\rangle + \ldots + c_{2^m-1}|2^m - 1\rangle$$

requires only m qubits.

FOURIER TRANSFORM on FINITE ABELIAN GROUPS

We show now basics how the concept of Fourier Transform is defined on any finite Abelian group.

CHARACTERS of ABELIAN GROUPS

Let G be an Abelian group written additively, and $|G| = n$. A character χ of G is any morphism $\chi : G \rightarrow \mathbf{C}/0$. That is, it holds, for any $g_1, g_2 \in G$:

$$\chi(g_1 + g_2) = \chi(g_1)\chi(g_2).$$

This implies that $\chi(0) = 1$ and $1 = \chi(ng) = \chi(g)^n$ for any $g \in G$. Therefore, all values of χ are nth roots of unity.

If we define multiplication of characters χ_1 and χ_2 by $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$, then characters form a so-called dual group Ĝ. Groups G and Ĝ are isomorphic for all Abelian groups G.

Example 1 Any cyclic group of n elements is isomorphic to the group $\mathbf{Z}_n$ and all its characters have the form, for $y \in \mathbf{Z}_n$:

$$\chi_y(x) = e^{\frac{2\pi i x y}{n}}.$$

Example 2 In the additive group $\mathbf{F_2}^m$, of all binary strings of length m, all characters have the form, for binary m-bit strings x and y:

$$\chi_y(x) = (-1)^{x \cdot y},$$

where $x \cdot y = \Sigma_{i=1}^m x_i y_1 \bmod 2$

ORTHOGONALITY of CHARACTERS

Any function $f : G \rightarrow \mathbf{C}$ on an Abelian group $G = \{g_1, \ldots, g_n\}$ can be specified by the vector $(f(g_1), \ldots, f(g_n))$, and if the scalar product of two functions is defined in the standard way as

$$\langle f|g\rangle = \sum_{i=1}^{n} f^*(g_i)h(g_i),$$

then for any characters χ_1 and χ_2 on G it holds

$$\langle \chi_i|\chi_j\rangle = \begin{cases} 0, & \text{if } i \neq j \\ n, & \text{if } i = j \end{cases}$$

Therefore, the functions $\{B_i = \frac{1}{\sqrt{n}}\chi_i\}$ form an orthonormal basis on the set of all functions $f : G \rightarrow \mathbf{C}$.

FOURIER TRANSFORM

Since any $F : G \rightarrow \mathbf{C}$ has a unique representation with respect to the basis $\{B_i = \frac{1}{\sqrt{n}}\chi_i\}_{i=1}^{n}$,

$$f = \hat{\mathsf{f}}_1 B_1 + \ldots + \hat{\mathsf{f}}_n B_n$$

the function $\hat{\mathsf{f}}$: $G \rightarrow \mathbf{C}$ defined by

$$\hat{\mathsf{f}}(g_i) = \hat{\mathsf{f}}_i$$

is called the Fourier transform of f.

Since $\hat{\mathsf{f}}_i = \langle B_i | f \rangle$, we get

$$\hat{\mathsf{f}}(g_i) = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \chi_i^*(g_k) f(g_k),$$

and therefore in $\mathbf{Z}_n$ the Fourier transform has the form

$$\hat{\mathsf{f}}(x) = \frac{1}{\sqrt{n}} \sum_{y \in \mathbf{Z}_n} e^{-\frac{2\pi i x y}{n}} f(y)$$

and in $\mathbf{F}_2^m$ the Fourier transform has the form

$$\hat{\mathsf{f}}(x) = \frac{1}{\sqrt{2^m}} \sum_{y \in \mathbf{F}_2^m} (-1)^{x \cdot y} f(y).$$

GROVER's SEARCH PROBLEM

Grover's method applies to problems for which it is hard to find a solution, but it is easy to check a to-be-solution.

> **Problem:** In an unsorted database of N items there is one, x_0, satisfying an easy to verify condition P. Find x_0.

Classical algorithms need in average $\frac{N}{2}$ checks.
Quantum algorithm exists that needs $\mathcal{O}(\sqrt{N})$ steps.

Modified problem: Given an easy to compute black-box function

$$f : \{0,1\}^n \rightarrow \{0,1\}$$

find an x_0 such that $f(x_0) = 1$ (let there is single such x_0). Basic idea of the algorithm:

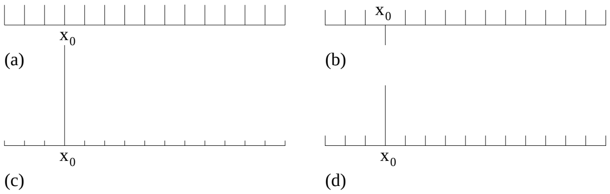


Figure 2: "Cooking" the solution with Grover's algorithm

We shall deal also with a more general problem. Namely that there is more than one solution, especially the case that the following number is known

$$t = |\{x \mid f(x) = 1\}|$$

INVERSION ABOUT THE AVERAGE

Example 0.4 (Inversion about the average) *The unitary transformation*

$$D_n : \sum_{i=0}^{2^n-1} a_i|\phi_i\rangle \rightarrow \sum_{i=0}^{2^n-1}(2E - a_i)|\phi_i\rangle,$$

where E is the average of $\{a_i \,|\, 0 \leq i < 2^n\}$, can be performed by the matrix

$$-H_nV_0^nH_n = D_n = \begin{pmatrix} -1+\frac{2}{2^n} & \frac{2}{2^n} & \dots & \frac{2}{2^n} \\ \frac{2}{2^n} & -1+\frac{2}{2^n} & \ddots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \dots & -1+\frac{2}{2^n} \end{pmatrix}.$$

The name of the operation comes from the fact that $2E - x = E + E - x$ and therefore the new value is as much above (below) the average as it was initially below (above) the average—which is precisely the inversion about the average.

The matrix D_n is clearly unitary and it can be shown to have the form $D_n = -H_nV_0^nH_n$, where

$$V_0^n[i,j] = 0 \textit{ if } i \neq j, V_0^n[1,1] = -1 \textit{ and } V_0^n[i,i] = 1 \textit{ if } 1 < i \leq n.$$

Let us consider again the unitary transformation

$$D_n : \sum_{i=0}^{2^n-1} a_i|\phi_i\rangle \rightarrow \sum_{i=0}^{2^n-1} (2E - a_i)|\phi_i\rangle,$$

and the following example:

Example: Let $a_i = a$ if $i \neq x_0$ and $a_{x_0} = -a$. Then

$$E = a - \frac{2}{2^n}a$$

$$2E - a_i = \begin{cases} a - \frac{4}{2^n}a \text{ if } i \neq x_0 \\ 2E - a_{x_0} = 3a - \frac{4}{2^n}a; \text{ otherwise} \end{cases}$$

GROVER's SEARCH ALGORITHM

Start in the state

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

and iterate $\lfloor \frac{\pi}{4}\sqrt{2^n} \rfloor$ times the transformation

$$-\underbrace{H_n V_0^n H_n V_f}_{\text{Grover's iterate}} |\phi\rangle \rightarrow |\phi\rangle.$$

Finally, measure the register to get x_0 and check whether $f(x_0) = 1$. If not, repeat the procedure.

It has been shown that the above algorithm is optimal for finding the solution with probability $> \frac{1}{2}$.

In the case that there are t solutions, repeat the above iteration

$$\left\lfloor \frac{\pi}{4}\sqrt{\frac{2^n}{t}} \right\rfloor \quad \text{times}$$

ANALYSIS of GROVER's ALGORITHM

Denote

$$X_1 = \{x \mid f(x) = 1\} \qquad X_0 = \{x \mid f(x) = 0\}$$

and denote the state after jth iteration of Grover's iterate $-H_nV_0^nH_nV_f$ as

$$|\phi_j\rangle = k_j \sum_{x\in X_1} |x\rangle + l_j \sum_{x\in X_0} |x\rangle$$

with

$$k_0 = \frac{1}{\sqrt{2^n}} = l_0.$$

Since

$$|\phi_{j+1}\rangle = -H_nV_0^nH_nV_f|\phi_j\rangle,$$

it holds

$$k_{j+1} = \frac{2^n-2t}{2^n}k_j + \frac{2(2^n-t)}{2^n}l_j, \quad l_{j+1} = \frac{2^n-2t}{2^n}l_j - \frac{2t}{2^n}k_j$$

what yields

$$k_j = \frac{1}{\sqrt{t}}\sin((2j+1)\theta)$$

$$l_j = \frac{1}{\sqrt{2^n-t}}\cos((2j+1)\theta)$$

where

$$\sin^2\theta = \frac{t}{2^n}.$$

Recurrence relations therefore provide

$$k_j = \frac{1}{\sqrt{t}} \sin((2j+1)\theta), \quad l_j = \frac{1}{\sqrt{2^n - t}} \cos((2j+1)\theta)$$

where

$$\sin^2 \theta = \frac{t}{2^n}.$$

The aim now is to find such an j which maximizes k_j and minimizes l_j. Take j such that $\cos((2j+1)\theta) = 0$, that is $(2j+1)\theta = (2m+1)\frac{\pi}{2}$.

Hence

$$j = \frac{\pi}{4\theta} - \frac{1}{2} + \frac{m\pi}{2\theta}$$

what yields

$$j_0 = \lceil \frac{\pi}{4\theta} \rceil,$$

and because

$$\sin^2 \theta = \frac{t}{2^n}$$

we have

$$0 \leq \sin \theta \leq \sqrt{\frac{t}{2^n}}$$

and therefore

$$j_0 = \mathcal{O}\left(\sqrt{\frac{2^n}{t}}\right).$$

A MORE DETAILED ANALYSIS

Theorem Let $f \in \mathbf{F_2^n} \rightarrow \{0,1\}$ and let there be exactly t elements $x \in \mathbf{F}_2^n$ such that $f(x) = 1$. Assume that $0 < t < \frac{3}{4}2^n$, and let $\theta_0 \in [0, \pi/3]$ be chosen such that $\sin^2 \theta_0 = \frac{t}{2^n} \leq \frac{3}{4}$. After $\lfloor \frac{\pi}{4\theta_0} \rceil$ iterations of the Grover iterates on the initial superposition $\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{F}_2^n} |x\rangle$ the probability of finding a solution is at least $\frac{1}{4}$.

Proof The probability of seeing a desired element is given by $\sin^2((2j+1)\theta_0)$ and therefore $j = -\frac{1}{2} + \frac{\pi}{4\theta_0}$ would give a probability 1.

Therefore we need only to estimate the error when $-\frac{1}{2} + \frac{\pi}{4\theta_0}$ is replaced by $\lfloor \frac{\pi}{4\theta_0} \rfloor$. Since

$$\lfloor \frac{\pi}{4\theta_0} \rfloor = -\frac{1}{2} + \frac{\pi}{4\theta_0} + \delta$$

for some $|\delta| \leq \frac{1}{2}$, we have

$$(2\lfloor \frac{\pi}{4\theta_0} \rfloor + 1)\theta_0 = \frac{\pi}{2} + 2\delta\theta_0,$$

and therefore the distance of $(2\lfloor \frac{\pi}{4\theta_0} \rfloor + 1)\theta_0$ from $\frac{\pi}{2}$ is $|2\delta\theta_0| \leq \frac{\pi}{3}$. This implies

$$\sin^2((2\lfloor \frac{\pi}{4\theta_0} \rfloor + 1)\theta_0) \geq \sin^2(\frac{\pi}{2} - \frac{\pi}{3}) = \frac{1}{4}.$$

A VARIATION on GROVER's ALGORITHM

Input A black box function $f : \mathbf{F}_2^n \rightarrow \{0,1\}$ and $k = |\{x \,|\, f(x) = 1\}| > 0$

Output: an y such that $f(y) = 1$

Algorithm:

1. If $t > \frac{3}{4}2^n$, then choose randomly an $y \in \mathbf{F}_2^n$ and stop.
2. Otherwise compute $r = \lfloor \frac{\pi}{4\theta_0} \rfloor$, where $\theta_0 \in [0, \pi/3]$ and $\sin^2\theta_0 = \frac{t}{2^n}$ and apply Grover's iterate G_n r times starting with the state
$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{F}_2^n} |x\rangle$$
and measure the resulting state to get some y.

If the first step is apply we get correct outcome with probability $\frac{3}{4}$ and if second step is applied then with probability at least $\frac{1}{4}$.

Very special case is $t = \frac{1}{4}2^n$. On such a case $\sin^2\theta_0 = \frac{1}{4}$ and therefore $\theta_0 = \frac{\pi}{6}$. The probability to get the correct result after one step is then

$$\sin^2((2 \cdot 1 + 1)\theta_0) = \sin^2(\frac{\pi}{2}) = 1.$$

THE CASE of UNKNOWN NUMBER of SOLUTIONS

To deal with the general case – that number of elements we search for is not known – we will need the following technical lemma:

Lemma For any real α and any positive integer m

$$\sum_{r=0}^{m-1} \cos((2r+1)\alpha) = \frac{\sin(2m\alpha)}{2\sin\alpha}.$$

MAIN LEMMA

Lemma Let $f : \mathbf{F}_2^n \rightarrow \{0,1\}$ be a blackbox function with $t \leq \frac{3}{4}2^n$ solutions and $\theta_0 \in [0, \frac{\pi}{3}]$ be defined by $\sin^2 \theta_0 = \frac{t}{2^n}$. Let $m > 0$ be any integer and $r \in_r [0, m-1]$. If Grover's iterate is applied to the initial state

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{F}_2^n} |x\rangle$$

r times, then the probability of seeing a solution is

$$P_r = \frac{1}{2} - \frac{\sin(4m\theta_0)}{4m \sin(2\theta_0)}$$

and if $m > \frac{1}{\sin(2\theta_0)}$, then $P_r \geq \frac{1}{4}$.

Proof We know that the probability of seeing solution after r iteration of Grover's iterate is $\sin^2((2r+1)\theta_0)$.

Therefore if $r \in_r [0, m-1]$, then the probability of seeing a solution is

$$\begin{aligned} P_m &= \frac{1}{m}\sum_{r=0}^{m-1}\sin^2((2r+1)\theta_0) && (12)\\ &= \frac{1}{2m}\sum_{r=0}^{m-1}(1-\cos((2r+1)2\theta_0)) && (13)\\ &= \frac{1}{2}-\frac{\sin(4m\theta_0)}{4m\sin(2\theta_0)}. && (14)\end{aligned}$$

Moreover, if $m \geq \frac{1}{\sin(2\theta_0)}$, then

$$\sin(4m\theta_0) \leq 1 = \frac{1}{\sin(2\theta_0)}\sin(2\theta_0) \leq m\sin(2\theta_0$$

and therefore $\frac{\sin(4m\theta_0)}{4m\sin(2\theta_0)} \leq \frac{1}{4}$ what implies that $P_m \geq \frac{1}{4}$

ALGORITHM

Input A blackbox function $f : \mathbf{F}_2^n \rightarrow \{0,1\}$.

Output An $y \in \mathbf{F}_2^n$ such that $f(y) = 1$.

Algorithm

1. Choose an $x \in_r \mathbf{F}_2^n$ and if $f(x) = 1$ then output x and stop.
2. Choose $r \in_r [0, m-1]$, where $m = \sqrt{2^n} + 1$ and apply Grover's iterate G_n r times to
$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{F}_2^n} |x\rangle.$$
Observe the outcome to get some y.

Algorithm works. Indeed, if $t > \frac{3}{4}2^n$, then algorithm will output a solution after the first step with probability at least $\frac{3}{4}$, Otherwise

$$m \geq \sqrt{\frac{2^n}{t}} \geq \frac{1}{\sin(2\theta_0)}$$

and the fact that we get a proper outcome with probability at least $\frac{1}{4}$ follows from previous lemma.

ANOTHER DERIVATION of GROVER's ALGORITHM

Given is an $f : \{0, 1, 2, \ldots, 2^n - 1\} \longrightarrow \{0, 1\}$, for which there is a single y such that $f(x) = \delta_{xy}$. Given is also an oracle $\mathcal{O}$ that can identify y if y comes as an input for $\mathcal{O}$. Namely, $\mathcal{O}$ provides for $x \in \{0, 1, 2, \ldots, 2^n - 1\}$

$$\mathcal{O}|x\rangle = (-1)^{f(x)}|x\rangle.$$

We can say that oracle marks the solution by shifting the phase.
The crucial ingridient is the following Grover operator, defined as the one performing the following sequence of actions:

1. apply the oracle $\mathcal{O}$;
2. apply the Hadamard transform H_n;
3. apply the conditional phase shift $F_c|0\rangle = |0\rangle$ and $F_c|x\rangle = -|x\rangle$ for $x > 0$;
4. aply H_n again.

Observe that $F_c = 2|0\rangle\langle 0| - I$ and therefore the Grover operator G has the form

$$G = H_n F_c H_n \mathcal{O} = H_n(2|0\rangle\langle 0| - I)H_n\mathcal{O}$$

If we denote

$$|\psi_n\rangle = H_n|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$$

and take into consideration that $H_n^2 = I$, the Grover operator has the form

$$G = (2|\psi_n\rangle\langle\psi_n| - I)\mathcal{O}.$$

We show now that G can be seen as a two-dimensional rotation. Indeed, denote

$$|\alpha\rangle = \frac{1}{\sqrt{2^n - 1}}\sum_{x \neq y}|x\rangle$$

and then

$$|\psi_n\rangle = \sqrt{1 - \frac{1}{2^n}}|\alpha\rangle + \sqrt{\frac{1}{2^n}}|y\rangle.$$

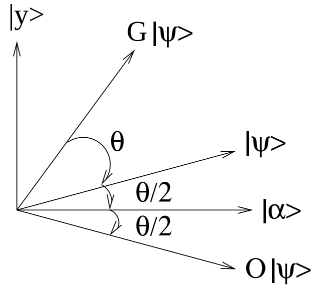
Observe now that the oracle $\mathcal{O}$ actually performs a reflection acros $|\alpha\rangle$ in the plane $\mathcal{P}$ spanned by $|\alpha\rangle$ and $|y\rangle$. Indeed, it holds

$$\mathcal{O}(a|\alpha\rangle + b|y\rangle) = a|\alpha\rangle - b|y\rangle.$$

Similarly, operator $2|\psi\rangle\langle\psi| - I$ performs a reflection in $\mathcal{P}$ acros $|\psi\rangle$. Indeed, if $|\psi_n^\perp\rangle$ is a unit vector orthogonal to $|\psi_n\rangle$ in $\mathcal{P}$, then

$$(2|\psi_n\rangle\langle\psi_n| - I)(a|\psi_n\rangle + b|\psi_n^\perp\rangle) = a|\psi_n\rangle - b|\psi_n^\perp\rangle$$

However, the product of two reflections, with respects to lines L_1 and L_2, is a rotation, by an angle that is twice the angle between these two lines. This also tells us that $G^k|\psi_n\rangle$ remains in $\mathcal{P}$ for all k



The rotation angle can be now obtained as follows: Let

$$\cos(\theta/2) = \sqrt{\frac{2^n - 1}{2^n}}$$

and then

$$|\psi_n = \psi =\rangle \cos(\frac{\theta}{2})|\alpha\rangle + \sin(\frac{\theta}{2})|y\rangle,$$

and therefore, see the figure above,

$$G|\psi_n\rangle = \cos(\frac{3\theta}{2})|\alpha\rangle + \sin(\frac{3\theta}{2})|y\rangle$$

and

$$G^k|\psi_n\rangle = \cos(\frac{2k-1}{2}\theta)|\alpha\rangle + \sin(\frac{2k-1}{2}\theta)|y\rangle$$

and the rest of reasoning is similar as in the first proof.

QUANTUM SEARCH in ORDERED LISTS

A related problem to that of a search in an unordered list is a search in an ordered list of n items.

- The best upper bound known today is $\frac{3}{4}\lg n$.
- The best lower bound known today is $\frac{1}{12}\lg n - \mathcal{O}(1)$.

EFFICIENCY of GROVER's SEARCH

There are at least four different proofs that Grover's search is asymptotically optimal.

Quite a bit is known about the relation between the error ε and the number T of queries when searching an unordered list of n elements.

- ε can be an arbitrary small constant if $\mathcal{O}(\sqrt{n})$ queries are used, but not when $o(\sqrt{n})$ queries are used.
- ε can be at most $\frac{1}{2^{n^{\alpha}}}$ using $\mathcal{O}(n^{0.5+\alpha})$ queries.
- To achieve no error ($\varepsilon = 0$), $\theta(n)$ queries are needed.

APPLICATIONS of GROVER's SEARCH

There is a variety of applications of Grover's search algorithm. Let us mention some of them.

- **Extremes of functions computation** (minimum, maximum).
- **Collision problem** Task is to find, for a given black-box function $f : X \rightarrow Y$, two different $x \neq y$ such that $f(x) = f(y)$, given a promise that such a pair exist.

  On a more general level an analogical problem deals with the so-called **r-to-one functions** every element of their image has exactly r pre-images. It has been shown that there is a quantum algorithm to solve collision problem for r-to-one functions in quantum time $\mathcal{O}((n/r)^{1/3})$. It has been shown in 2003 by Shi that the above upper bound cannot be asymptotically improved.
- **Verification of predicate calculus formulas.** Grover's search algorithm can be seen as a method to verify formulas

  $$\exists x P(x),$$

  where P is a black-box predicate.

  It has been shown that also more generalized formulas of the type

  $$\forall x_1 \exists y_1 \forall x_2 \exists y_2 \ldots \forall x_k \exists y_k P(x_1, y_1, x_2, y_2, \ldots, x_k, y_k)$$

  can be verified quantumly with the number of queries $\mathcal{O}(\sqrt{2^{(2k)}})$.

QUANTUM MINIMUM FINDING ALGORITHM

Problem: Let $s = s_1, s_2, \ldots, s_n$ be an unsorted sequence of distinct elements. Find an m such that s_m is minimal.

Classical search algorithm needs $\theta(n)$ comparisons.

QUANTUM SEARCH ALGORITHM

1. Choose as a first "threshold" a random $y \in \{1, \ldots, n\}$.
2. Repeat the following three steps until the total running time is more than $22.5\sqrt{n} + 1.4 \lg^2 n$.
    - 2.1. Initialize
    $$|\psi_0\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle|y\rangle$$
    and consider an index i as **marked** if $s_i < s_y$.
    - 2.2. Apply Grover search to the first register to find an marked element.
    - 2.3. Measure the first register. If y' is the outcome and $s_{y'} < s_y$, take as a new threshold the index y'.
3. Return as the output the last threshold y.

It is shown in my book that the above algorithm finds the minimum with probability at least $\frac{1}{2}$ if the measurement is done after a total number of $\theta(\sqrt{n})$ operations.