Quantum Computing

The following notes have been written by Théo Saulus, based on Prof. Dr. Jean-Pierre Seifert lectures and slides. They are meant as a support for the students following the course, but should not be considered as a replacement for the professor's lectures and materials. This document has not been reviewed by the professor, and should therefore be used carefully.

Table of content

I. Kick-off session

I.A Organisation

Lecture (Summer)

- 2 SWS Lecture
- Thursday 14:15-15:45
- PC203

Exercise (with practical programming) (Summer)

- 2 SWS Exercise/Tutorial
- Day: Friday 10:15-11:45
- Room: HL001/zoom???

Lecturer: Jean-Pierre Seifert

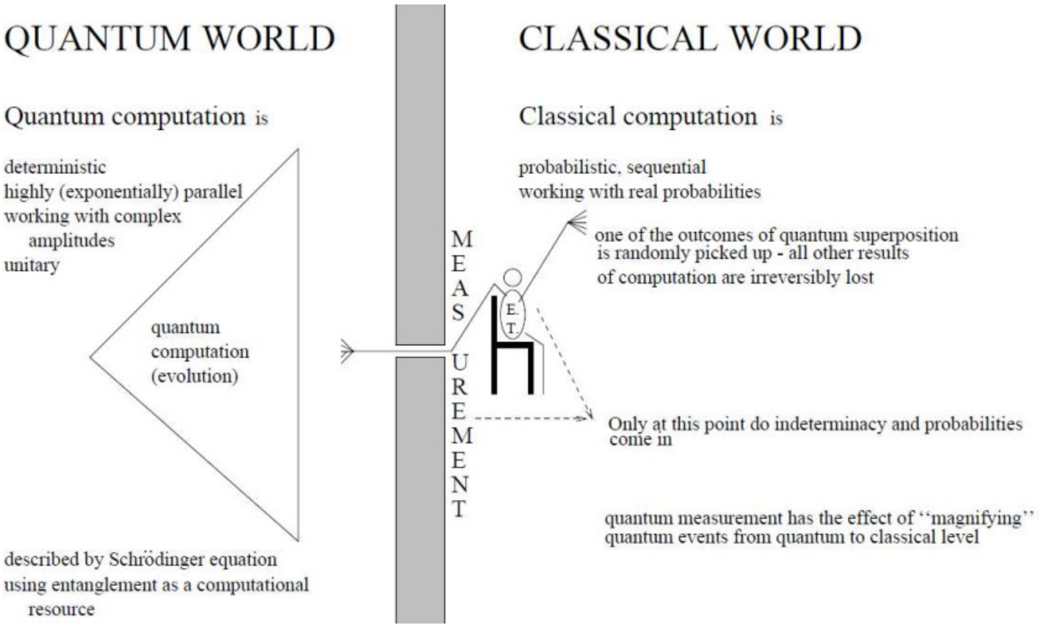
- Office: TEL 16
- E-Mail: Jean-Pierre.Seifert@external.telekom.de
- Consultation: pls. send email to Secretary

Tutor: Zarin Shakibaei/Niklas Pirnay

- Office: TEL 16
- E-Mail: zarin.shakibaei@tu-berlin.de; n.pirnay@tu-berlin.de
- Consultation: pls. send email to them

Secretary: Claudia Petzsch

- Office: TEL16
- E-Mail: Claudia.Petzsch@external.telekom.de


QUANTUM WORLD
Quantum computation is
deterministic
highly (exponentially) parallel
working with complex amplitudes
unitary
quantum computation (evolution)
described by Schrödinger equation
using entanglement as a computational resource
MEASUREMENT
E.T.
CLASSICAL WORLD
Classical computation is
probabilistic, sequential
working with real probabilities
one of the outcomes of quantum superposition is randomly picked up - all other results of computation are irreversibly lost
Only at this point do indeterminacy and probabilities come in
quantum measurement has the effect of ''magnifying'' quantum events from quantum to classical level

I.B Some useful on-line material

- Preskill lecture notes from: http://www.theory.caltech.edu/people/preskill/ph229
- A self-contained nice primer from Dorit Aharonov: Quantum Computation - A Review
- Feynmann lectures are really nice: http://www.feynmanlectures.info/
- Best QC book is from my point of view: http://twoqubits.wikidot.com/start
- The QC bible Quantum Computation and Quantum Information by "Mike and Ike“ is: https://en.wikipedia.org/wiki/Quantum_Computation_and_Quantum_Information

II. Introduction and Motivation

In this first lecture we mainly deal why we should be interested in **quantum information processing** and also with very basic experiments, principles and formalism of quantum mechanics. We deal also, in some details, with classical **reversible** computations, as a special case of quantum computation.

In quantum computing we witness an interaction between the two most important areas of science and technology of the 20th century, between quantum physics and computer science. This may have important consequences for 21st century.

II.A Introduction to quantum physics

II.A.1 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.

At the end of 19th century it was believed by most that the laws of Newton and Maxwell were correct and complete laws of physics. At the beginning of 20th century it got clear that these laws are not sufficient to explain all observed physical phenomena. As a result, a new mathematical framework for physics called quantum mechanics was formulated and new theories of physics, called quantum physics were developed.

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

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

II.A.2 Introduction to quantum physics

Quantum physics is an elegant and conceptually simple theory that describes with astonishing 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 super-fluids, functioning of laser, the substance of chemistry, the structure and function of DNA, the existence and behaviour of solid bodies, colour of stars,...

Quantum physics deals with **fundamental entities of physics**, particles like:

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

We call them **particles** although 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 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 have been invented by mathematicians in the 19th century without any input from experiments. It was not, but it could have been (Aaronson, 1997)

II.A.3 What quantum physics tells us?

Quantum physics tells us **what** happens, but it does not tell us **why** it happens, and does not tell us either **how** it happens, nor **how much** it costs.

“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*

II.A.4 Mathematics behind quantum mechanics

Quantum physics phenomena are difficult to understand since at attempts to understand quantum physics most of our everyday experiences are not applicable. Quantum mechanics is a theory in mathematical sense: it is governed by a set of axioms.

Concerning mathematics behind quantum mechanics, one should actually do not try to understand what this means, one should try to **learn to work with it**! Nobody saw superposition of quantum states - one can “see” only **basis states**.

It is well known that it is very hard to understand quantum physics. However, it is less known that understanding of quantum physics is child’s play comparing with understanding of child’s play.

II.B Introduction to quantum computing

II.B.1 Why is Quantum Information Processing and Computing so important?

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

1. QIPC is believed to lead to new **Quantum Information Processing Technologies** that could have deep and broad impacts.
2. Several areas of science and technology are approaching the point at which they badly need expertise with **isolation, manipulating and transmission of particles**.
3. It is increasingly believed that new, **quantum information processing** based, and understanding of (complex) quantum phenomena and systems can be developed.
4. **Quantum cryptography** seems to offer new level of security and is already feasible.
5. QIPC has been shown to be more **efficient** in interesting & important cases.
6. TCS and Information Theory got a **new dimension and fresh impulses**.

II.B.2 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 away from what would be required to make even rudimentary implementations of a QC. The concept of randomized algorithms was not known. No public key cryptography was known (and required).

II.B.3 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 Computer Science?

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 a new vision, namely that everything is information"

Quantum physics is an 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 the theory of quantum information processing.

II.B.4 Moore's law

There are no reasons why the increase of performance of processors should not follow **Moore's law** in the near future. A long term increase of performance of processors according to Moore's law seems to be possible only if, at the performance of computational processes, we get more and more to the atomic level. An extrapolation of the curve depicting the number of electrons needed to store a bit of information shows that around 2020 we will require only very few electrons to store one bit.

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, at 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 applications, 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

On the base of quantum mechanics one can determine that the "ultimate laptop" of mass 1 kg and size 1 liter **cannot perform more than $\mathbf{2.7 \times 1050}$ bit operations per second**.

Calculations (S. Lloyd, 1999) are based only on the amount of energy needed to switch from one state to another distinguishable state. It seems to be harder to determine the number of bits of such an "ultimate laptop". However, the bound 3.8×1016 has been determined for a computer compressed to form a black hole. It is quite clear that Moore's law cannot hold longer than for another 200 years.

II.B.5 Pre-history of computation

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 QKD 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.

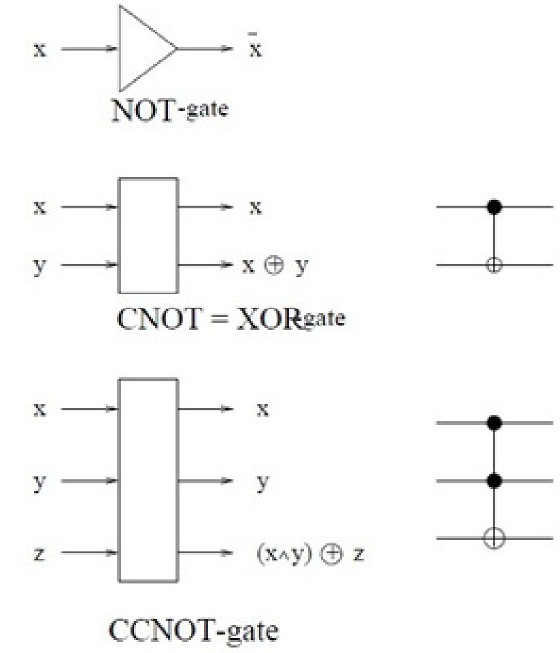
1996 The existence of quantum fault-tolerant computation was shown by Shor

II.B.6 Reversibility

Quantum processes are reversible. An operation is **reversible** if its outputs uniquely determine its inputs:

- $(a, b) \to a + b$ is a non-reversible operation
- $(a, b) \to (a + b, a - b)$ is a reversible operation
- If $a \to f(a)$ is a mapping (not necessarily reversible), then $(a, 0) \to \big(a, f(a)\big)$ is surely reversible

Three reversible classical gates: NOT, XOR (CNOT) and Toffoli (CCNOT)



A universal reversible gate for Boolean logic

Definition: A set $\mathcal{G}$ of gates is **universal** for classical computation if for any positive integers n, m and function $f: \{0,1\}^n \to \{0,1\}^m$, a circuit can be designed for computing f using only gates from $\mathcal{G}$.

The sets {NAND} and {Toffoli, FREDKIN} form a universal set of gates.

The set consisting of just the Toffoli gate is also universal for classical computing – provided we add the ability to add ancillary bits to the circuit that can be initiated to either 0 or 1 as required

II.B.7 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 in 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 $a \to \big(a, g(a), f(a)\big)$.

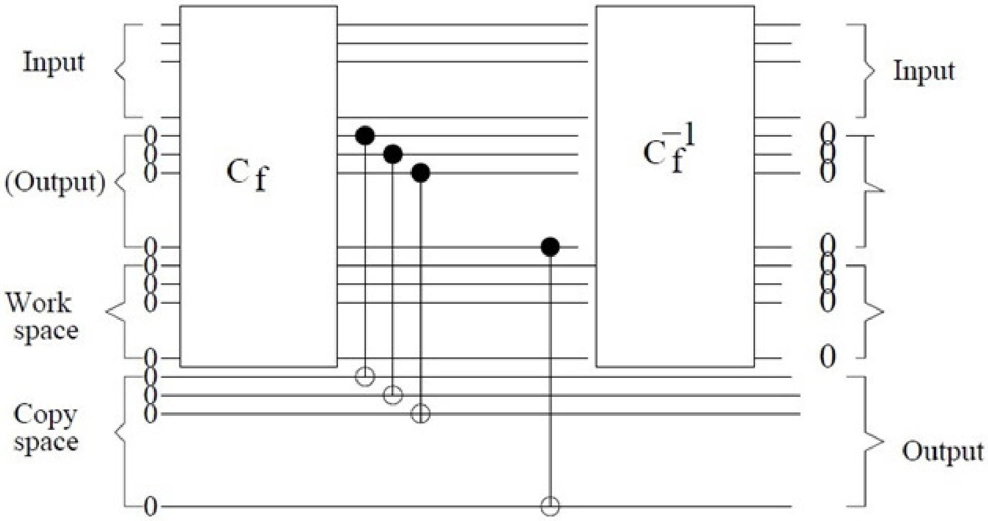
Bennett has also shown that there is an elegant reversible way how to remove garbage $g(a)$:

- Basic computation of $f: a \to \big(a, g(a), f(a)\big)$
- Fanout: $\big(a, g(a), f(a)\big) \to \big(a, g(a), f(a), f(a)\big)$
- Uncomputing of f : $\big(a, g(a), f(a), f(a)\big) \to \big(a, f(a)\big)$

Observe that CNOT gate with 0 as the initial value of the target bit is a copy gate (we will see later if it is an actual copy, or not…). Indeed,

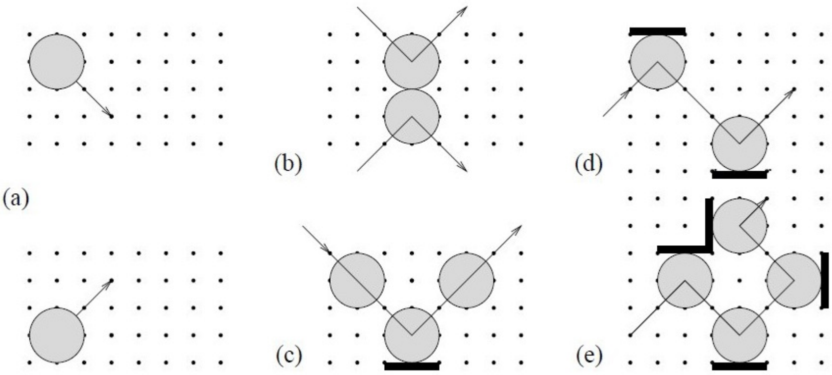
$$CNOT(x, 0) = (x, x)$$

A circuit version of the garbage removal has then the form:



C_f is made of reversible gates, therefore C_f^{-1} exists. We reset the work space and output space to 0, to save memory.

Billiard ball reversible computer (Fredkin and Tofolli):



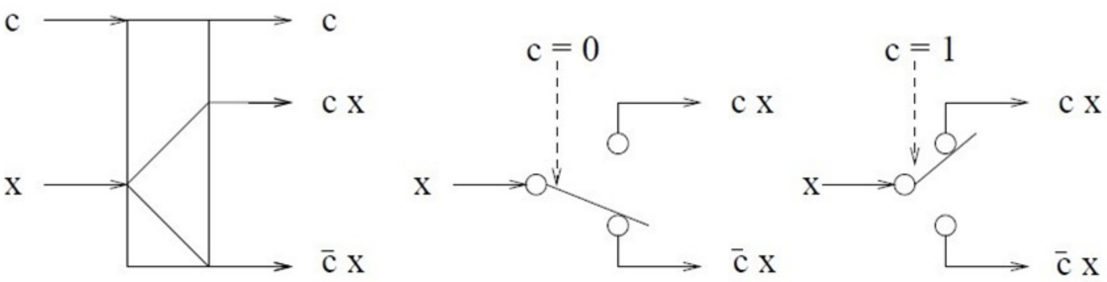


Figure 2: Switch gate

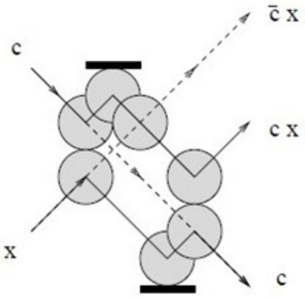
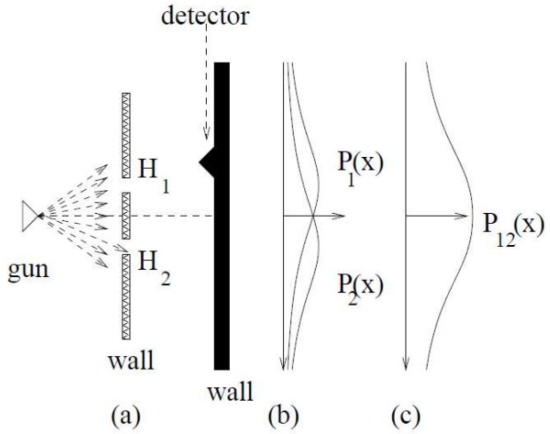


Figure 3: A billiard ball implementation of the switch gate

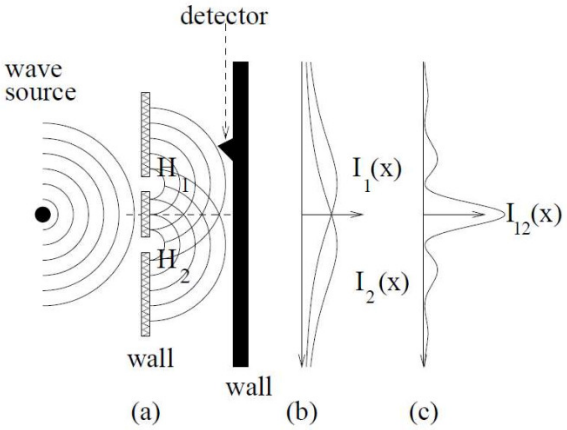
III. Mathematics of quantum mechanics

III.A Experiments

III.A.1 Classical experiments

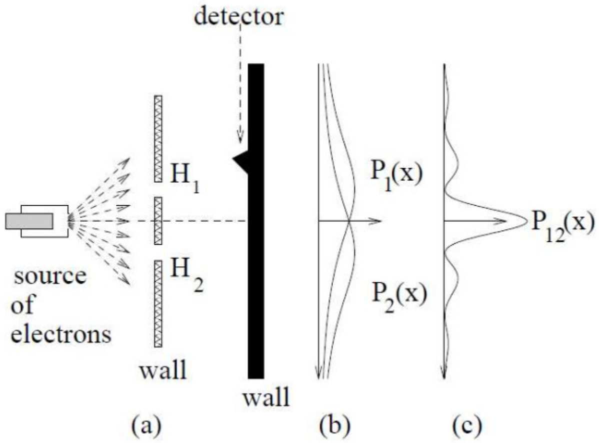


A gun firing bullets with only one hole open: if we measure where the bullet arrive, they will arrive around the open hole. The sum of the two curves $P_1(x)$ and $P_2(x)$ is $P_{12}(x)$. The same result is obtained if we open the two holes at the same time.

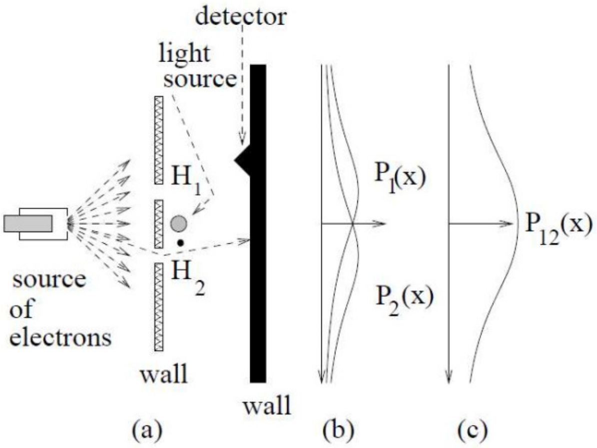


With waves, the result is different: when only one hole is open, we obtain the intensities $I_1(x)$ and $I_2(x)$. However, if both are open, we obtain $I_{12}(x)$, where we can see interferences, it is not the sum of the intensities.

III.A.2 Quantum experiments



Same experience as the bullets one, but with electrons. This time, we obtain a interferences like pattern.



Now, we have a light detector to know if electrons took one or the other hole. With both holes open, the probability curve does no longer show the interferences. As soon as we do a measurement, we completely change the quantum behaviour (electrons are quantum particles).

For more details, read the first pages of Feynman lectures.

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.

III.A.3 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 is equal exactly to its frequency times Planck's constant.)

III.B Quantum mechanics

III.B.1 Introduction to 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 required.
- For *quantum computational* purposes it is **sufficient** to have 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 whose elements are **norm-1 states** and are called (pure) **states** (object of the Hilbert space).

III.B.2 Bra-ket notation

P. Dirac introduced a very handy notation, the so called **bra-ket notation**, to deal with amplitudes, quantum states and linear mapping $f : H \to \mathbb{C}$, for some space H.

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

- $\langle\phi|\psi\rangle$ is a number: the **scalar product** between ϕ and ψ (or the amplitude of going from ψ to ϕ)
- $|\psi\rangle$ is a **ket-vector**: a column vector, an equivalent to ψ
- $\langle\phi|$ is a **bra-vector**: a row vector, the conjugate transpose of $|\phi\rangle$, i.e., linear functional on H such that $\langle\phi|\ (|\psi\rangle) = \langle\phi|\psi\rangle$

III.B.3 A quantum system is a Hilbert space

The Hilbert space $\mathcal{H}_n$ is an n-dimensional **complex** vector space with a scalar product

$$\langle\phi|\psi\rangle = \sum_{i=1}^{n} \phi_i^* \psi_i$$

Where $|\phi\rangle = \begin{pmatrix} \phi_1 \\ \dots \\ \phi_n \end{pmatrix}$ and $|\psi\rangle = \begin{pmatrix} \psi_1 \\ \dots \\ \psi_n \end{pmatrix}$

The **2-norm** for respective vectors is $\|\phi\| := \sqrt{|\langle\phi|\phi\rangle|}$, and the **metric** is $dist(\phi, \psi) = \|\phi - \psi\|$

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

Example:

If $\phi = (\phi_1, \dots, \phi_n)$ and $\psi = (\psi_1, \dots, \psi_n)$, then:

- $|\phi\rangle = \begin{pmatrix} \phi_1 \\ \dots \\ \phi_n \end{pmatrix}$ is a ket-vector
- $\langle\psi| = (\psi_1^*, \dots, \psi_n^*)$ is a bra-vector
- The **inner product** (scalar product) is $\langle\phi|\psi\rangle = \sum_{i=1}^{n} \phi_i^* \psi_i$
- The **outer product** is $|\phi\rangle\langle\psi| = \begin{pmatrix} \phi_1\psi_1^* & \cdots & \phi_1\psi_n^* \\ \vdots & \ddots & \vdots \\ \phi_n\psi_1^* & \cdots & \phi_n\psi_n^* \end{pmatrix}$

The meaning of the outer product is that of the mapping that maps any stat $|\gamma\rangle$ into the state

$$|\phi\rangle\langle\psi| \ \ (|\gamma\rangle) = |\phi\rangle\ (\langle\psi|\gamma\rangle) = \langle\psi|\gamma\rangle \ \ |\phi\rangle$$

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

A nice book about the current topics: *Quantum theory: concepts and methods*, Asher Peres

III.B.4 Orthogonality of pure states

Two quantum states $|\psi\rangle$ and $|\phi\rangle$ are called **orthogonal** iff their scalar product is zero, that is: $\langle\phi|\psi\rangle = 0$

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

In every Hilbert space, there are so-called **orthogonal bases**, which means that all states of it are mutually orthogonal

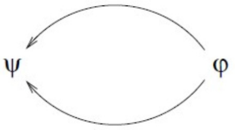
III.B.5 The three quantum principles

P1: To each transfer from a quantum state ϕ to a state ψ a complex number $\langle\phi|\psi\rangle$ is associated, which is called the **probability amplitude** of the transfer, such that $|\langle\phi|\psi\rangle|^2$ is the **probability** of the transfer. We take the absolute value before the square, to make sure the final value is actually positive and not complex.

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 of the transfer is the **product** of amplitudes of sub-transfers:

$$\langle\phi|\psi\rangle = \langle\phi|\phi'\rangle\langle\phi'|\psi\rangle$$

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



Then the resulting amplitude is the sum $\alpha + \beta$ of amplitudes of two sub-transfers. This is vastly different from classical operations, because the amplitudes can here be complex, thus attenuate each other, whereas classical probabilities (like in probabilistic Turing machines), can only add up.

IV. Beginnings of quantum computation

IV.A Qubits

A **single qubit** – a **two-level quantum system** – is a quantum state in $\mathcal{H}_2$

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

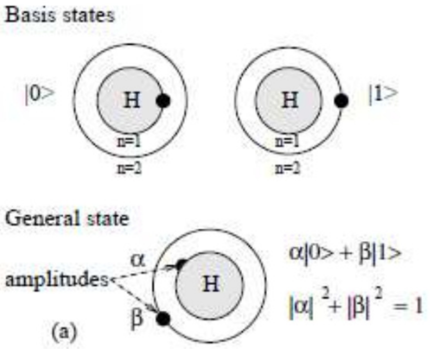
with $\alpha, \beta \in \mathbb{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$

and $\{\ |0\rangle\ \ ,|1\rangle\ \ \}$ some (standard) **basis** of $\mathcal{H}_2$, e.g. $|0\rangle = (1{,}0)$ and $|1\rangle = (0{,}1)$.

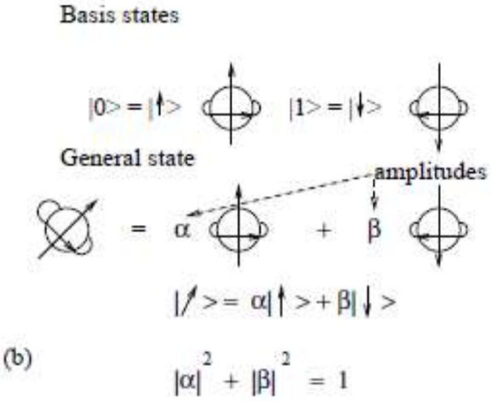
What does this constraint on the scalars mean for the length of the vector of ϕ? The norm of ϕ is also 1. It exists quantum systems that have a norm different than 1, but we will not work on them, and mostly focus on pure states, which are normalized.

Example: representation of qubits by:

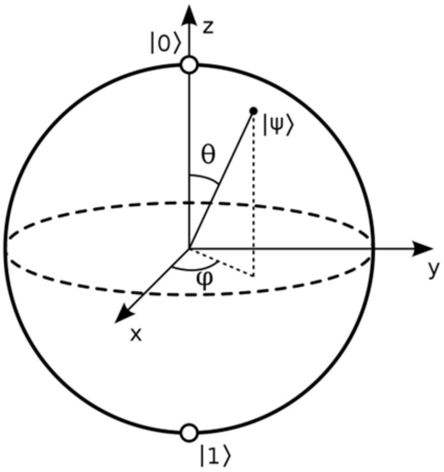
a) Electron in a hydrogen atom



b) A spin-1



Exercise *Show that any qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be expressed in the form $|\psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$ in the sense that $|\alpha|^2 = |\cos\theta|^2$ and $|\beta|^2 = |e^{i\phi}\sin\theta|^2$.*



Bloch sphere: nice 3D representation, which allows to see that $\|\psi\| = 1$, because $|\psi\rangle$ stays on the unity sphere. See animation https://javafxpert.github.io/grok-bloch/.

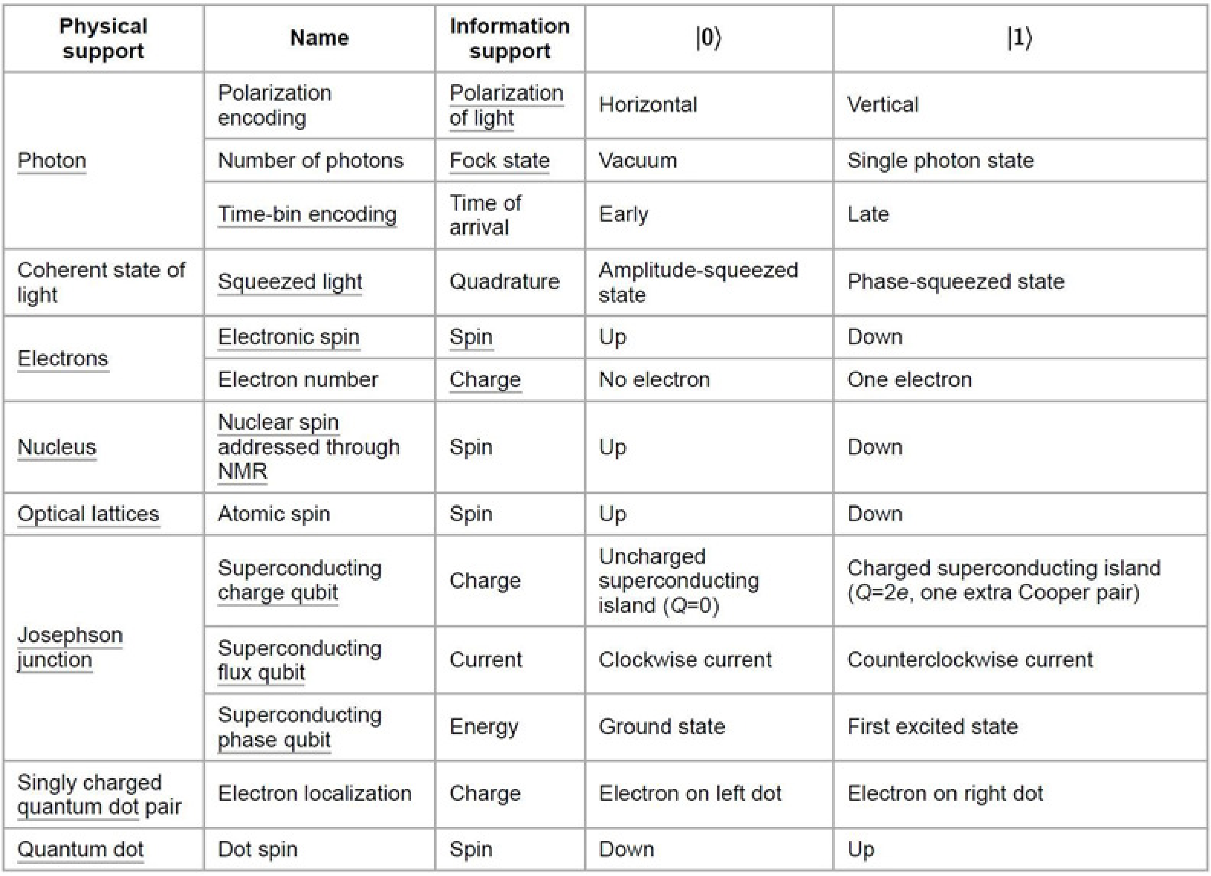
IV.A.1 Classical vs. Quantum computing

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 or 1**. [experts could say it is an approximation, but we do not care]

In quantum computers, information is represented on **microscopic level** using **qubits**, which can take for $|0\rangle, |1\rangle \in \mathcal{H}_2 = \mathbb{C}^2$ any value from uncountable many values $\alpha|0\rangle + \beta|1\rangle$, with $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$.

IV.A.2 Physical representations of a qubit



Physical support	Name	Information support	|0⟩	|1⟩
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state
Electrons	Electronic spin	Spin	Up	Down
	Electron number	Charge	No electron	One electron
Nucleus	Nuclear spin addressed through NMR	Spin	Up	Down
Optical lattices	Atomic spin	Spin	Up	Down
Josephson junction	Superconducting charge qubit	Charge	Uncharged superconducting island (*Q*=0)	Charged superconducting island (*Q*=2*e*, one extra Cooper pair)
	Superconducting flux qubit	Current	Clockwise current	Counterclockwise current
	Superconducting phase qubit	Energy	Ground state	First excited state
Singly charged quantum dot pair	Electron localization	Charge	Electron on left dot	Electron on right dot
Quantum dot	Dot spin	Spin	Down	Up

How is Moore's law forcing us to consider the quantum world when going under 4 nm? Because quantum effects...

Josephson junction has led to most of the currently large quantum computers (IBM, Google, ...), because it is the best understood.

Photon encoding has a major drawback compared to Josephson junction, silicon systems, and electrons, because it takes way too much space. A quantum computer makes only sense if it is scalable and not limited to a few qubits.

IV.B Mathematical framework

IV.B.1 (Two-dimensional) Hilbert space $\mathcal{H}_2$

Standard (computational) basis: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Dual basis (thanks to our friend Jacques Hadamard):

$$|0'\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} := |+\rangle, \qquad |1'\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} := |-\rangle$$

The **Hadamard matrix** (Hadamard operator in the standard basis) transforms the standard basis into the dual basis, and vice-versa:

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

With properties (it is **reversible**!):

$$\begin{aligned} H|0\rangle &= |0'\rangle \qquad & H|0'\rangle &= |0\rangle \\ H|1\rangle &= |1'\rangle \qquad & H|1'\rangle &= |1\rangle \end{aligned}$$

IV.B.2 Quantum evolution

Evolution in quantum system is ruled by **Schrödinger equation**, and is a computation in a Hilbert space.

Linear time-dependent Schrödinger equation:

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

$H(t)$ is a **Hermitian** operator representing the total energy of the system, from which it follows that $\psi(t) = e^{-\frac{1}{\hbar}H(t)}$ and therefore that a discretized evolution (**computation**) step of a quantum system is performed by a multiplication of the state vector by a **unitary operator**, i.e., a step of evolution is a multiplication by a **unitary matrix** A with a vector $|\psi\rangle$, i.e., $A|\psi\rangle$

IV.B.3 Hermitian operator

In mathematics, a **self-adjoint operator** on an infinite-dimensional complex vector space $\mathcal{V}$ with inner product $\langle\ |\ \rangle$ (respectively **Hermitian operator** on a finite-dimensional space) is a linear map A from $\mathcal{V}$ to itself that is its own adjoint, i.e.,

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

for all vectors ϕ and ψ.

If $\mathcal{V}$ is finite-dimensional with a given orthonormal basis, this is equivalent to the conclusion that the matrix A is a Hermitian matrix, i.e., equal to its **conjugate transpose** A^*

IV.B.4 Unitary Operator/Matrix

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

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

Once again this operation is reversible

A unitary mapping U is a linear mapping that preserves the inner product, that is $\langle U\phi|U\psi\rangle = \langle\phi|\psi\rangle$

IV.B.5 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 three former principles that tell us how to do so, i.e. the principles of quantum mechanics. Each quantum system is actually uniquely determined by a Hamiltonian.

We do not need to be bothered here with how to choose the Hamiltonian, only how to treat the system.

IV.B.6 Examples of unitary matrices

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

We can compute the square root of matrix, for example: $\sqrt{\sigma_x} = \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}$

Three other important unitary operations on qubits are rotation (by θ), phase shift (with respect to α), and scale (with respect to δ):

$$R(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \qquad PS(\alpha) = \begin{pmatrix} e^{i\frac{\alpha}{2}} & 0 \\ 0 & e^{-i\frac{\alpha}{2}} \end{pmatrix}, \qquad Scal(\delta) = \begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{pmatrix}$$

Theorem: *Each unitary matrix U of degree 2 can be written as follows:*

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

IV.B.7 Universal set of quantum gates

The main task of quantum computation is to express the **solution of a given problem $\boldsymbol{P}$ as a unitary matrix $\boldsymbol{U_P}$** and then to construct a circuit C_{U_P} with elementary quantum gates from universal sets of quantum gates to realize U. That is:

$$P \to U_P \to C_{U_P}$$

A simple universal set of quantum gates consists of gates:

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

Note: the $\sigma_z^{\frac{1}{4}}$ gate is difficult to build in practice

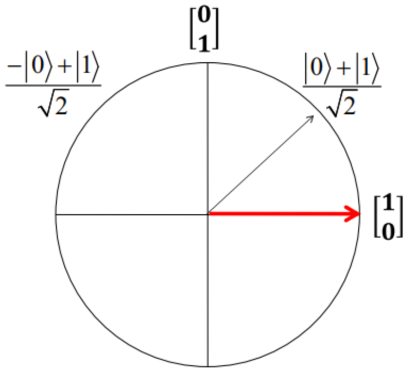
IV.B.8 Solving Schrödinger's equation

See slide 36 not covered

IV.B.9 Computation, and example of applications of gates

A quantum computation step multiplies the vector of amplitudes by a matrix, leading to a new state vector. Here for example, the Hadamard gate is applied:

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



$\begin{bmatrix} \mathbf{0} \\ \mathbf{1} \end{bmatrix}$
$\frac{-|0\rangle+|1\rangle}{\sqrt{2}}$
$\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
$\begin{bmatrix} \mathbf{1} \\ \mathbf{0} \end{bmatrix}$

Note also that:

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

Application of the CNOT gate:

$$CNOT = \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & 0 \\ & & 0 & 1 \\ & 0 & 1 & 0 \end{pmatrix} \text{ applied to } \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle : \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & 0 \\ & & 0 & 1 \\ & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Another example:

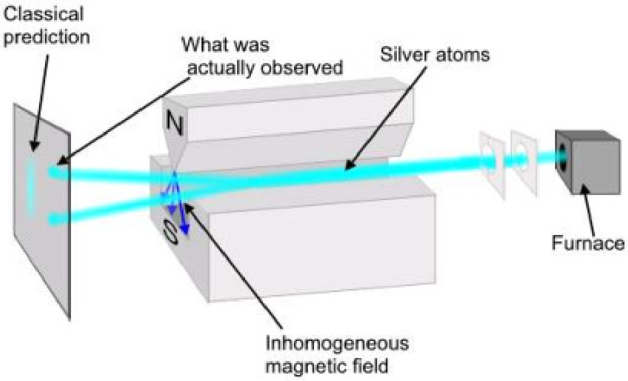
$$CNOT \text{ applied to } \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = |10\rangle : \begin{pmatrix}1 & 0 & & \\ 0 & 1 & & 0 \\ & 0 & 0 & 1 \\ & & 1 & 0\end{pmatrix} \cdot \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = |01\rangle$$

IV.C Measurement

IV.C.1 Stern-Gerlach measurement experiment

Let us consider, in a idealized form, one of the other famous experiments of quantum physics, which demonstrates that some quantum phenomena are not determined except when they are measured.

It was used to demonstrate that electrons and atoms have intrinsically quantum properties, and how **measurement** in quantum mechanics affects the system being measured.



Specifically, the experiment demonstrates the property of spin and its quantized nature.

Particles (silver atom in the original experiment) are sent through an inhomogeneous magnetic field to hit a screen. Spin causes the particles to have a magnetic moment, and the magnetic field deflects the particles from their straight path. The screen shows discrete points rather than a continuous distribution, owing to the quantum nature of spin.

The quantum theory explanation is the following one: Passing an atom through a magnetic field amounts to a **measurement** of its **magnetic alignment**, and until you make such a measurement there is no sense in sating what the atom's magnetic alignment might be. Only when you make a measurement you obtain **one of only two possible outcomes, with equal probability**, and those two possibilities are defined by the direction of the magnetic field that you use to make the measurement.

IV.C.2 Tensor product

A tensor product of **vectors** is:

$$(\phi_1, \dots, \phi_n) \otimes (\psi_1, \dots, \psi_m) = \begin{pmatrix}\phi_1\psi_1 & \cdots & \phi_1\psi_m \\ \vdots & \ddots & \vdots \\ \phi_n\psi_1 & \cdots & \phi_n\psi_m\end{pmatrix} \in \mathbb{C}^{n\times m}$$

A tensor product of **matrices** is:

$$A \otimes B = \begin{pmatrix}a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nn}B\end{pmatrix}$$

A tensor product of **Hilbert spaces** is: $\mathcal{H} \otimes \mathcal{H}'$, which is the complex vector space spanned by tensor products of vectors from $\mathcal{H}$ and $\mathcal{H}'$, that corresponds to the quantum system composed of the quantum systems corresponding to Hilbert spaces $\mathcal{H}$ and $\mathcal{H}'$.

IV.C.3 Entanglement

A very important difference between classical and quantum systems:

- A state of a composite classical system **can** always be composed from the states of its subsystems
- A state of a composite quantum system **cannot** always be composed from the states of its subsystems

IV.C.4 Quantum registers

Any ordered sequence of n quantum qubit systems create a so-called **quantum n-qubit register**. The Hilbert space corresponding to an n-qubit register is the n-fold tensor product of 2-dimensional Hilbert spaces:

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

Thus, n qubits allow for 2^n states.

Since the vectors $|0\rangle, |1\rangle$ form a basis of $\mathcal{H}_2$, one of the basis of $\mathcal{H}_{2^n}$, the so-called computational basis, consists of all possible n-fold tensor products where $b_i \in \{0,1\}$ for all i:

$$|b_1\rangle \otimes \ldots \otimes |b_n\rangle := |b_1, \ldots, b_n\rangle$$

Example: a 2-qubit register has as computational basis vectors

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

We do not want to use these 2^n unity vectors, we will rather make use of the tensor products! Quantum computers work on a 2^n dimensional space, it's huge.

IV.C.5 Quantum states and von Neuman measurements

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

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

Where $a_i = \langle \beta_i | \phi \rangle$ are called **probability amplitudes**, which can be complex numbers, and their squares $|a_i|^2 = \langle \phi | \beta_i \rangle \langle \beta_i | \phi \rangle$ provide **probabilities** that if the state $|\phi\rangle$ is measured with respect to the basis $\{\beta_i\}_i$, then the state $|\phi\rangle$ collapses into the state $|\beta_i\rangle$ with probability $|a_i|^2$.

The classical "outcome" of a (von Neuman) measurement of the state $|\phi\rangle$ with respect to the basis $\{\beta_i\}_i$ is the index i of that state $|\beta_i\rangle$ into which the state $|\phi\rangle$ collapses.

IV.C.6 Physical view of quantum measurement

In case of an orthonormal basis $\{\beta_i\}_i$ 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 $|\phi\rangle = \sum_{i=1}^{n} a_i |\beta_i\rangle$ with $\sum_{i=1}^{n} |a_i|^2 = 1$ with respect to $\{\beta_i\}_i$ 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 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.

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 abandoned.

"*A quantum state is a useful abstraction which frequently appears in the literature, but does not really exists in nature.*" A. Peres (1993)

IV.C.7 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 $|\phi\rangle$:

- Classical information into which subspace projection of $|\phi\rangle$ was made
- 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 and the representation of $|\phi\rangle$ at the basis states of the subspace.

Before quantum physics, it was take 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**.

IV.C.8 Probabilistic system vs. quantum system

Let's illustrate, on an example, a principal difference between a quantum evolution and a classical probabilistic evolution. If a qubit system develops under the evolution

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

Then, after one step of evolution, we observe both $|0\rangle$ and $|1\rangle$ with the probability $\frac{1}{2}$, but after *two* steps we get:

$$|0\rangle \to \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = |0\rangle$$

Therefore, any observation gives $|0\rangle$ with probability 1.

On the other hand, in case of the *classical probabilistic* evolution:

$$[0] \to \frac{1}{2}([0] + [1]), \qquad [1] \to \frac{1}{2}([0] + [1])$$

We have after one step of evolution both 0 and 1 with the same probability $\frac{1}{2}$ but after two septs, we have

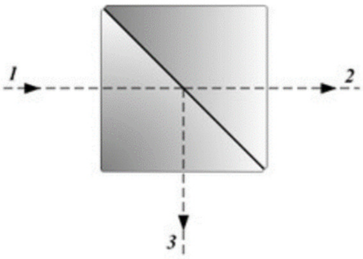
$$[0] \to \frac{1}{2}\left(\frac{1}{2}([0]+[1]) + \frac{1}{2}([0]+[1])\right) = \frac{1}{2}([0]+[1])$$

Therefore, after two steps of evolution, we have again both values 0 and 1 with the same probability $\frac{1}{2}$.

In the quantum case, during the second evolution step, amplitudes at $|1\rangle$ cancel each other and we have so-called **destructive interference**. At the same time, amplitudes at $|0\rangle$ amplify each other and we have so-called **constructive interference**.

IV.C.9 Loss of determinism

Example of a beam splitter: identical photons get transmitted or reflected randomly.

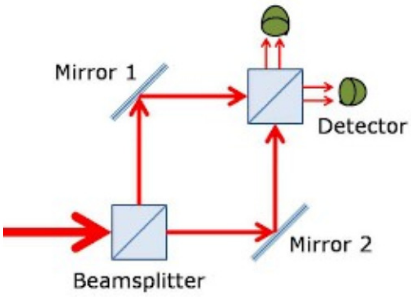


1: Incident light

2: 50% transmitted light

3: 50% reflected light

Mach-Zehnder interferometer: send single photos one by one.



There is interference happening in the second beam splitter: **each photon interferes with itself!** This appears as if each photon is on both beams at the same time

$$|0\rangle \to \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right) = |0\rangle$$

V. Quantum circuits

V.A One qubit

Two dimensional quantum systems are called qubits. A **single** qubit has a wave function which we write as $|v\rangle = v_0|0\rangle + v_1|1\rangle$. To be valid, the qubit wave function must verify $|v_0|^2 + |v_1|^2 = 1$.

V.A.1 Measuring qubits

A qubit, like a bit, is a quantum system with two possible states, 0 and 1. When we observe a qubit, we get the result 0 or the result 1.

If, before we observe the qubit the wave function of the qubit is $|v\rangle = v_0|0\rangle + v_1|1\rangle$, then:

- the probability that we observe 0 is $|v_0|^2$ and then **new wave** function for the qubit is $|0\rangle$
- the probability that we observe 1 is $|v_1|^2$ and then **new wave** function for the qubit is $|1\rangle$
- We thus say **measuring in the computational basis**.

Example: We are given a qubit with wave function $|v\rangle = \frac{1}{\sqrt{3}}|0\rangle + i\sqrt{\frac{2}{3}}|1\rangle$, which norm is $\||v\rangle\| = \sqrt{\left|\frac{1}{\sqrt{3}}\right|^2 + \left|i\sqrt{\frac{2}{3}}\right|^2} = 1$. If we observe the system in the computational basis, then we get outcome 0 with probability $\left|\frac{1}{\sqrt{3}}\right|^2 = \frac{1}{3}$ (and the new wave function is $|0\rangle$), and we get outcome 1 with probability $\left|i\sqrt{\frac{2}{3}}\right|^2 = \frac{2}{3}$

V.A.2 Unitary evolution for qubits

Unitary evolution will be described by a two dimensional unitary matrix $U = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix}$.

If initial qubit wave function is $|v\rangle = v_0|0\rangle + v_1|1\rangle = \begin{pmatrix} v_0 \\ v_1 \end{pmatrix}$, then this evolves to

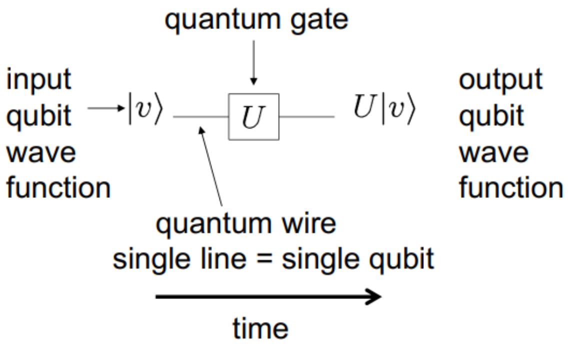
$$|v'\rangle = U|v\rangle = \begin{pmatrix} U_{00}v_0 & U_{01}v_1 \\ U_{10}v_0 & U_{11}v_1 \end{pmatrix}$$

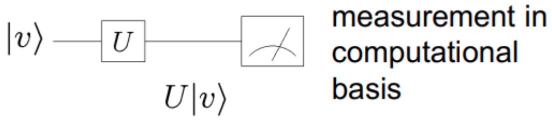
Example: For $U = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{i}{\sqrt{2}} & \frac{i}{\sqrt{2}} \end{pmatrix}$ and $|v\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle = \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}$, we have:

$$|v'\rangle = U|v\rangle = \begin{pmatrix} \dfrac{1+\sqrt{3}}{2\sqrt{2}} \\ i\dfrac{-1+\sqrt{3}}{2\sqrt{2}} \end{pmatrix} = \frac{1+\sqrt{3}}{2\sqrt{2}}|0\rangle + i\frac{-1+\sqrt{3}}{2\sqrt{2}}|1\rangle$$

V.A.3 Single qubit quantum circuits

Circuit diagrams for evolving qubits:


quantum gate
input qubit wave function
$|v\rangle$
U
$U|v\rangle$
output qubit wave function
quantum wire
single line = single qubit
time



V.B Two qubits

Two qubits, like bits, can be in one of four different states: 00, 01, 10, 11.

The wave function for two qubits thus has four components:

$$|v\rangle = \begin{pmatrix} v_{00} \\ v_{01} \\ v_{10} \\ v_{11} \end{pmatrix} = v_{00}|00\rangle + v_{01}|01\rangle + v_{10}|10\rangle + v_{11}|11\rangle$$

Examples:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}|00\rangle + \frac{i}{\sqrt{2}}|01\rangle, \qquad \begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|11\rangle, \qquad \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle$$

V.B.1 Separable qubits

Sometimes, we can write the wave function of two qubits as the **tensor product** of two one qubit wave function:

$$|v\rangle = |a\rangle \otimes |b\rangle$$

More explicitly, for $|a\rangle = a_0|0\rangle + a_1|1\rangle$ and $|b\rangle = b_0|0\rangle + b_1|1\rangle$:

$$\begin{aligned} |v\rangle &= (a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) \\ &= a_0b_0|0\rangle \otimes |0\rangle + a_0b_1|0\rangle \otimes |1\rangle + a_1b_0|1\rangle \otimes |0\rangle + a_1b_1|1\rangle \otimes |1\rangle \\ &= a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle \end{aligned}$$

Example: for $|a\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ and $|b\rangle = \frac{i}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$:

$$|v\rangle = \frac{i}{2\sqrt{5}}|00\rangle + \frac{1}{\sqrt{5}}|01\rangle + \frac{\sqrt{3}i}{2\sqrt{5}}|10\rangle + \sqrt{\frac{3}{5}}|11\rangle$$

V.B.2 Entangled qubits

If $|v\rangle$ is not a separable state, then it is **entangled**.

Example: $|v\rangle = \begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|11\rangle$. Assume that $|v\rangle = |a\rangle \otimes |b\rangle$.

Then, $|v\rangle = a_0 b_0|00\rangle + a_0 b_1|01\rangle + a_1 b_0|10\rangle + a_1 b_1|11\rangle$, which implies that $a_0 b_1 = 0$

Therefore, $\begin{cases} a_0 = 0 \text{ but this implies } a_0 b_0 = 0 \\ \text{or} \\ b_1 = 0 \text{ but this implies } a_1 b_1 = 0 \end{cases}$, which is contradictory. Thus $|v\rangle$ is entangled.

V.B.3 Measuring two qubits

If we measure both qubits in the computational basis, then we get one of four outcomes: 00, 01, 10, 11.

If the wave function for the two qubits is $|v\rangle = \begin{pmatrix} v_{00} \\ v_{01} \\ v_{10} \\ v_{11} \end{pmatrix} = v_{00}|00\rangle + v_{01}|01\rangle + v_{10}|10\rangle + v_{11}|11\rangle$

Then,

- Probability of 00 is $|v_{00}|^2$, and the new wave function is $|00\rangle$
- Probability of 01 is $|v_{01}|^2$, and the new wave function is $|01\rangle$
- Probability of 10 is $|v_{10}|^2$, and the new wave function is $|10\rangle$
- Probability of 11 is $|v_{11}|^2$, and the new wave function is $|11\rangle$

Example: for $|v\rangle = \frac{i}{2\sqrt{5}}|00\rangle + \frac{1}{\sqrt{5}}|01\rangle + \frac{\sqrt{3}i}{2\sqrt{5}}|10\rangle + \sqrt{\frac{3}{5}}|11\rangle$

- Probability of 00 is $\left|\frac{i}{2\sqrt{5}}\right|^2 = \frac{1}{20}$
- Probability of 00 is $\left|\frac{1}{\sqrt{5}}\right|^2 = \frac{1}{5}$
- Probability of 00 is $\left|\frac{\sqrt{3}i}{2\sqrt{5}}\right|^2 = \frac{3}{20}$
- Probability of 00 is $\left|\sqrt{\frac{3}{5}}\right|^2 = \frac{3}{5}$

V.B.4 Two qubits evolutions

The wave function of an N dimensional quantum system evolves in time according to a unitary matrix U. If the wave function is initially $|v\rangle$, then after the evolution U the new wave function is $|v'\rangle = U|v\rangle$

Example: if $U = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0 & 0 \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ and $|v\rangle = \begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|11\rangle$, then $|v'\rangle = U|v\rangle = \begin{pmatrix} \frac{1}{2\sqrt{2}} \\ \frac{i}{2\sqrt{2}} \\ \frac{\sqrt{3}}{2} \\ 0 \end{pmatrix}$

V.B.5 Manipulations of two qubits

We can apply unitary operations on only one of the qubits at a time, using tensor product. Let's consider $U = V \otimes I$, with $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$: this only modifies the first qubit. Conversely, $U = I \otimes V$ only acts on the second qubit.

Tensor product of matrices:

If $V = \begin{pmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{pmatrix}$ and $W = \begin{pmatrix} W_{00} & W_{01} \\ W_{10} & W_{11} \end{pmatrix}$, then $U = V \otimes W = \begin{pmatrix} V_{00}W_{00} & V_{00}W_{01} & V_{01}W_{00} & V_{01}W_{01} \\ V_{00}W_{10} & V_{00}W_{11} & V_{01}W_{10} & V_{01}W_{11} \\ V_{10}W_{00} & V_{10}W_{01} & V_{11}W_{00} & V_{11}W_{01} \\ V_{10}W_{10} & V_{10}W_{11} & V_{11}W_{10} & V_{11}W_{11} \end{pmatrix}$

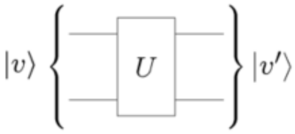
Example: for $V = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ and $W = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$, then $U = V \otimes W = \cdots$

Example: for $V = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, then $U = V \otimes I = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{i}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{i}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}$

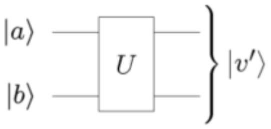
Example: for $V = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, then $U = I \otimes V = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0 & 0 \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ 0 & 0 & \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$

V.B.6 Two qubits quantum circuits

A two qubit unitary gate:

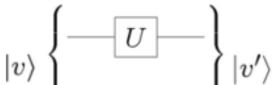


Sometimes our output is known to be separable:

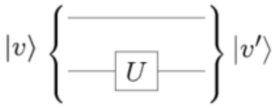


$$|v'\rangle = U(|a\rangle \otimes |b\rangle)$$

Sometimes we act only on one qubit:



$$|v'\rangle = (U \otimes I)|v\rangle$$



$$|v'\rangle = (I \otimes U)|v\rangle$$

V.B.7 Computational basis, unitary matrices and linearity

Let's consider $|v\rangle = v_{00}|00\rangle + v_{01}|01\rangle + v_{10}|10\rangle + v_{11}|11\rangle$

Then $|v'\rangle = U|v\rangle = v_{00}U|00\rangle + v_{01}U|01\rangle + v_{10}U|10\rangle + v_{11}U|11\rangle$

We can act on each computational basis state and then resume. This simplifies the calculations considerably. In particular, by examining the unitary evolution of all computational basis states, we can explicitly determine what is the unitary matrix.

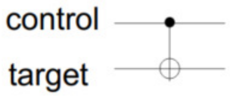
Example: for $U = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0 & 0 \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ and $|v\rangle = \begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|11\rangle$

$$\begin{aligned} |v'\rangle &= U|v\rangle \\ &= \frac{1}{2}U|00\rangle + \frac{\sqrt{3}}{2}U|11\rangle \\ &= \frac{1}{2}\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{i}{\sqrt{2}}|01\rangle\right) + \frac{\sqrt{3}}{2}|10\rangle \\ &= \frac{1}{2\sqrt{2}}|00\rangle + \frac{i}{2\sqrt{2}}|01\rangle + \frac{\sqrt{3}}{2}|10\rangle \end{aligned}$$

Example: for $U = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0 & 0 \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ and $|v\rangle = \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|01\rangle$

$$\begin{aligned} |v'\rangle &= U|v\rangle \\ &= \frac{1}{2}U|00\rangle + \frac{\sqrt{3}}{2}U|01\rangle \\ &= \frac{1}{2}\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{i}{\sqrt{2}}|01\rangle\right) + \frac{\sqrt{3}}{2}\left(\frac{i}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle\right) \\ &= \frac{1+i\sqrt{3}}{2\sqrt{2}}|00\rangle + \frac{i+\sqrt{3}}{2\sqrt{2}}|01\rangle \end{aligned}$$

V.B.8 Some two qubit gates

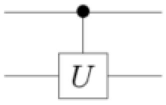


Controlled-NOT

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

If the control is 1, we apply XOR to the target.

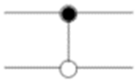
If the control is 0, nothing happens.



Controlled-U

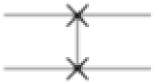
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{pmatrix}$$

Depending on the 1st qubit, we do or don't apply U to the second qubit.



Controlled-phase

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$



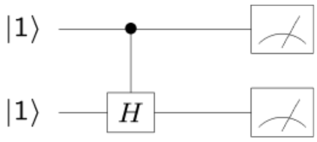
Swap

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

Example: controlled-H, $U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}$ and $|v\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$

$$|v'\rangle = U|v\rangle = \begin{pmatrix} 0 \\ 0 \\ \dfrac{1}{\sqrt{2}} \\ -\dfrac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)$$

Probability of 10 is $\frac{1}{2}$, probability of 11 is $\frac{1}{2}$ and probability of 00 and 01 is 0



V.C Measurement

V.C.1 Matrices, bras and kets

So far we have used bras and kets to describe row and column vectors. We can also use them to describe matrices, thanks to the outer product of two vectors:

$$|v\rangle\langle w| = \begin{pmatrix} v_1 w_1^* & v_1 w_2^* \\ v_2 w_1^* & v_2 w_2^* \end{pmatrix}$$

We can expand a matrix about all of the computational basis outer products

$$M = \sum_{i,j} M_{ij} |i\rangle\langle j| = \begin{pmatrix} M_{00} & \cdots & M_{0,N-1} \\ \vdots & \ddots & \vdots \\ M_{N-1,0} & \cdots & M_{N-1,N-1} \end{pmatrix}$$

Example: for $M = \begin{pmatrix} 1 & i \\ -1 & -i \end{pmatrix}$

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

Thus, $M = |0\rangle\langle 0| + i|0\rangle\langle 1| - 1|1\rangle\langle 0| - i|1\rangle\langle 1|$

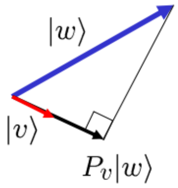
This notation makes it easy to operate on kets and bras:

$$M|v\rangle = \sum_{i,j} M_{ij} |i\rangle\langle j|v\rangle\,, \qquad \langle w|M = \sum_{i,j} M_{ij} \langle w|i\rangle\langle j|\,, \text{ where } \langle\cdot\,|\,\cdot\rangle \text{ are complex numbers}$$

Example: for $M = \begin{pmatrix} 1 & i \\ -1 & -i \end{pmatrix}$ and $|v\rangle = \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}$

$$\begin{aligned} M|v\rangle &= (|0\rangle\langle 0| + i|0\rangle\langle 1| - 1|1\rangle\langle 0| - i|1\rangle\langle 1|) \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \\ &= \frac{1 + i\sqrt{3}}{2}|0\rangle - \frac{1 + i\sqrt{3}}{2}|1\rangle \end{aligned}$$

V.C.2 Projectors



The projector onto a state $|v\rangle$ of unit norm is given by $P_v = |v\rangle\langle v|$.

Thus, $P_v|v\rangle = |v\rangle\langle v|v\rangle = |v\rangle$ and $P_v|w\rangle = |v\rangle\langle v|w\rangle = (\langle v|w\rangle)|v\rangle$.

Example: for $|v\rangle = |0\rangle$, and thus $P_v = |0\rangle\langle 0|$. Let's consider $|w\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$. The projection is therefore

$$P_v|w\rangle = |0\rangle\langle 0| \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) = \frac{1}{2}|0\rangle$$

V.C.3 Measurement rule

If we measure a quantum system whose wave function is $|v\rangle$ in the basis $|w_i\rangle$, then the **probability** of getting the outcome corresponding to $|w_i\rangle$ is given by

$$\mathbb{P}(|w_i\rangle) = |\langle w_i|v\rangle|^2 = \langle v|w_i\rangle\langle w_i|v\rangle = \langle v|P_{w_i}|v\rangle$$

The **new wave function** of the system after getting the measurement outcome corresponding to $|w_i\rangle$ is given by

$$|v'\rangle = \frac{P_{w_i}|v\rangle}{\sqrt{\mathbb{P}(|w_i\rangle)}}$$

For measuring in a complete basis, this reduces to our normal prescription for quantum measurement. However, suppose that we measure the first of two qubits in the computational basis. Then we can form the two projectors:

$$\begin{aligned} P_0 \otimes I &= |0\rangle\langle 0| \otimes I \\ P_1 \otimes I &= |1\rangle\langle 1| \otimes I \end{aligned} \qquad \text{where } I = |0\rangle\langle 0| + |1\rangle\langle 1|$$

If the two qubit wave function is $|v\rangle$ then the probabilities of these two outcomes are

$$\begin{aligned} \mathbb{P}(0) &= \langle v|P_0 \otimes I|v\rangle \\ \mathbb{P}(1) &= \langle v|P_1 \otimes I|v\rangle \end{aligned}$$

And the new state of the system is given by either

$$|v'\rangle = \frac{P_0 \otimes I|v\rangle}{\sqrt{\mathbb{P}(0)}} \text{ if the outcome was 0,} \qquad |v'\rangle = \frac{P_1 \otimes I|v\rangle}{\sqrt{\mathbb{P}(1)}} \text{ if the outcome was 1}$$

Example: for $|v\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$, we decide to measure the first qubit. What is the probability of 0?

$$\begin{aligned} P_0 \otimes I &= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| \end{aligned}$$

Thus,

$$\begin{aligned} \mathbb{P}(0) &= \langle v|P_0 \otimes I|v\rangle \\ &= \langle v| \left(\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle\right) \\ &= \frac{1}{2} \end{aligned}$$

We can thus obtain the new wave function supposing 0 is measured:

$$\begin{aligned} |v'\rangle &= \frac{P_0 \otimes I|v\rangle}{\sqrt{\mathbb{P}(0)}} \\ &= \frac{\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle}{\frac{1}{\sqrt{2}}} \\ &= |0\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \end{aligned}$$

Finally, and as we could have seen it from the beginning, $\mathbb{P}(0) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$

V.C.4 Instantaneous communication?

Suppose two distant parties each have a qubit and their joint quantum wave function is $|v\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. If one party now measures its qubit, then

$$\begin{aligned}\mathbb{P}(0) &= \frac{1}{2} \text{ and } |v'\rangle = |0\rangle \otimes |0\rangle\\ \mathbb{P}(1) &= \frac{1}{2} \text{ and } |v'\rangle = |1\rangle \otimes |1\rangle\end{aligned}$$

The other parties qubit is now either $|0\rangle$ or $|1\rangle$.

Is that instantaneous communication? No, because these two results happen with probabilities: correlation does not imply communication.

V.C.5 Important single qubit unitary matrices

Pauli matrices

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

Bit flip (classical not gate)

$$-\boxed{Y}- = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$-\boxed{Z}- = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Phase flip

$$\begin{aligned}\sigma_0 &= I\\ \sigma_1 &= X\\ \sigma_2 &= Y\\ \sigma_3 &= Z\end{aligned} \text{ and } \sigma_j^2 = I$$

Example:

$$-\boxed{X}-\boxed{Y}- = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} = -\boxed{-iZ}-$$

$$-\boxed{Y}-\boxed{X}- = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = -\boxed{iZ}-$$

Hadamard gate

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

$$H^2 = I$$

Example:

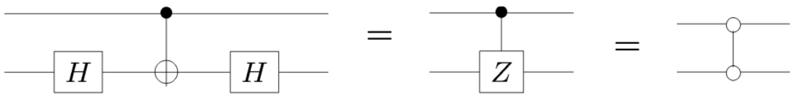
$$-\boxed{H}-\boxed{Z}-\boxed{H}- = \boxed{\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}}\boxed{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}\boxed{\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}}$$

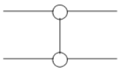
$$= \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = -\boxed{X}-$$

This allows us to compute easily HXH:

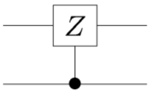
$$HXH = H(HZH)H = IZI = Z$$

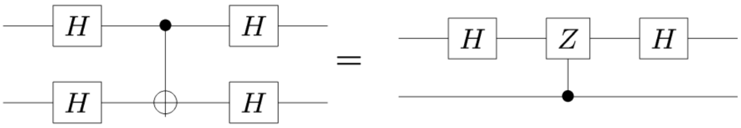
Example: Using the equality $HXH = Z$, we can prove an interesting circuit identity:

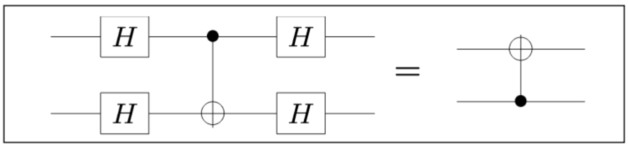




$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} =$$

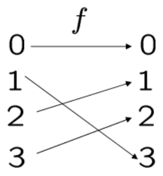






V.C.6 Reversible classical gates

A **reversible** classical gate on k bits is a one to one function on the 2^k values of these bits.



Example:

$$\begin{array}{l} 00 \to 00 \\ 01 \to 01 \\ 10 \to 11 \\ 11 \to 10 \end{array} \text{ is reversible, } \quad \begin{array}{l} 00 \to 00 \\ 01 \to 00 \\ 10 \to 10 \\ 11 \to 11 \end{array} \text{ is not reversible}$$

We can represent reversible classical gates by a permutation matrix. Permutation matrices are matrices in which every row and column contains at most one 1 and the rest of the elements are 0.

Example:

$$\begin{array}{l} 00 \to 00 \\ 01 \to 01 \\ 10 \to 11 \\ 11 \to 10 \end{array} \text{ is represented by: } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

V.C.7 Quantum versions of reversible classical gates

We can turn reversible classical gates into unitary quantum gates: use permutation matrix as unitary evolution matrix.

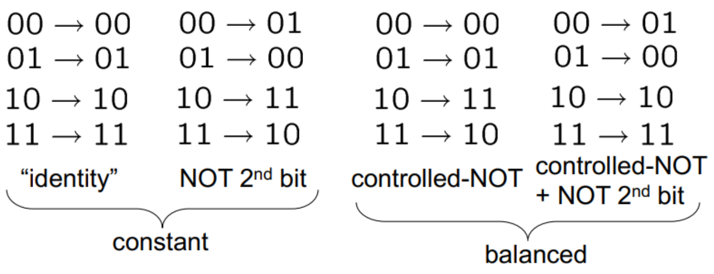
Example: the previous matrix is a controlled-NOT quantum gate.

V.D Deutsch's problem

"*Complexity theory has been mainly concerned with questions upon the computation of functions: which functions can be computed, how fast, and how much memory? With quantum computers, as with classical* *stochastic computers, one must also ask '**and with what probability?**' We have seen that the minimum computation time for certain tasks can be lower for quantum computers than for classical computers. Complexity theory for quantum computers deserved further investigation.*" David Deutsch, 1985

V.D.1 Classical Deutsch's problem

Suppose you are given a black box which computes one of the following four reversible gates:

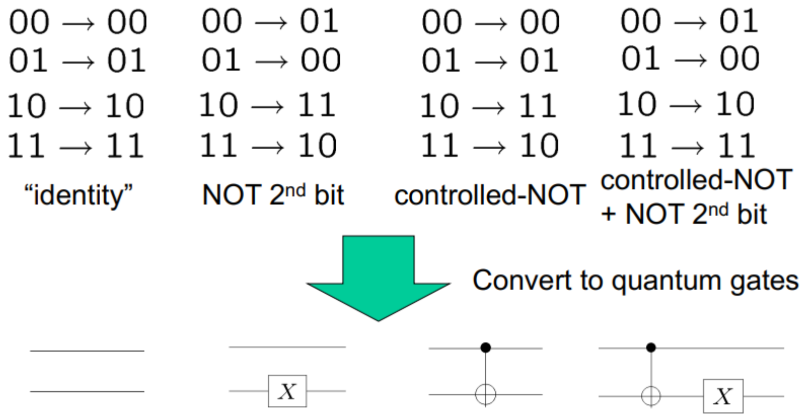


00 → 00	00 → 01	00 → 00	00 → 01
01 → 01	01 → 00	01 → 01	01 → 00
10 → 10	10 → 11	10 → 11	10 → 10
11 → 11	11 → 10	11 → 10	11 → 11
"identity"	NOT 2nd bit	controlled-NOT	controlled-NOT + NOT 2nd bit

Deutsch's (classical) problem: How many times do we have to use this black box to determine whether we are given the first two or the second two?

Notice that for every possible input, this des not separate the "constant" and "balanced" sets. This implies at least one use of the black box is needed. Querying the black box with 00 and 10 distinguishes between these two sets. Two uses of the black box are necessary and sufficient.

V.D.2 Quantum Deutsch's problem

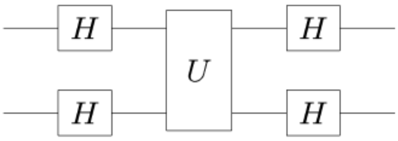


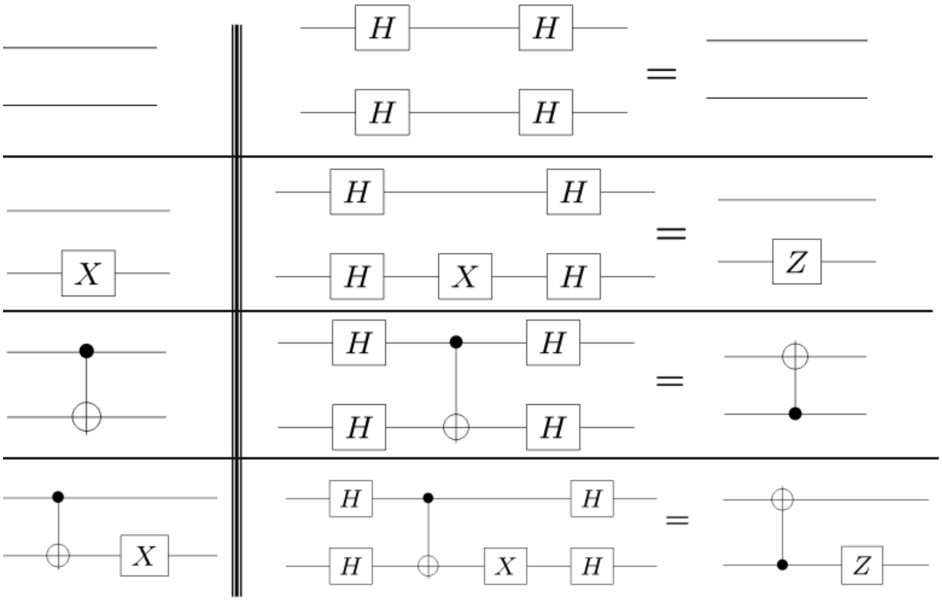
00 → 00	00 → 01	00 → 00	00 → 01
01 → 01	01 → 00	01 → 01	01 → 00
10 → 10	10 → 11	10 → 11	10 → 10
11 → 11	11 → 10	11 → 10	11 → 11
"identity"	NOT 2nd bit	controlled-NOT	controlled-NOT + NOT 2nd bit

Deutsch's (quantum) problem: How many times do we have to use these quantum gates to determine whether we are given the first two or the second two?

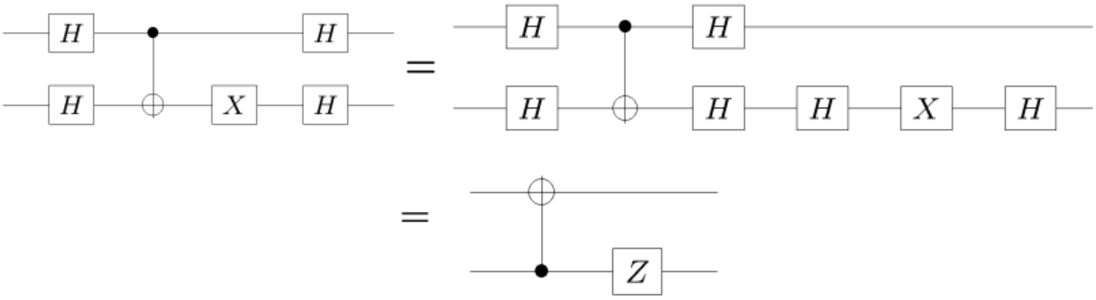
V.D.3 Make use of Hadamard gates

What if we perform Hadamard gates before and after the quantum gate?

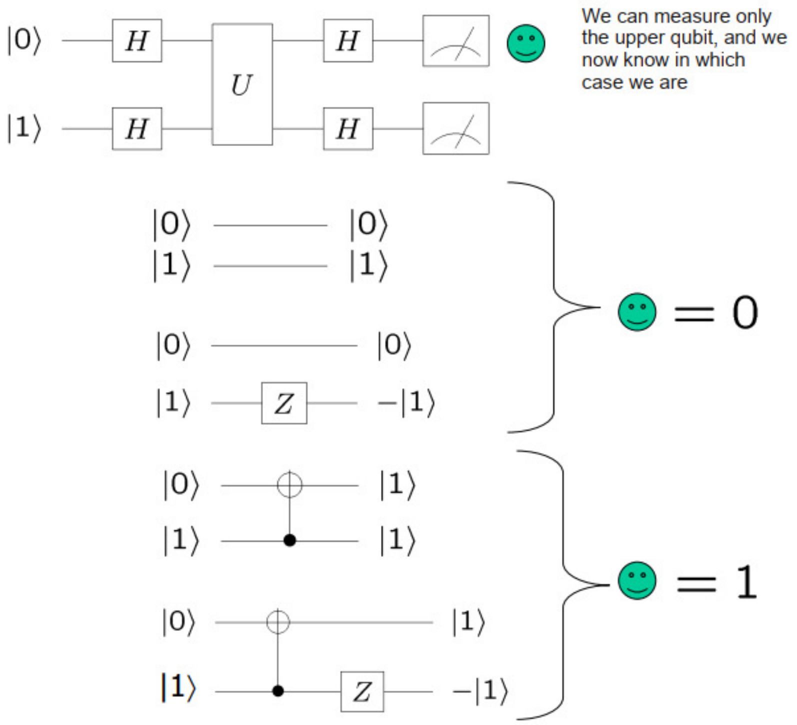




Explanations for the last gate:



Example: with some inputs



By querying with quantum states we are able to distinguish the first two (constant) from the second two (balanced) with **only one use of the quantum gate**! This is the first quantum speedup, in 1985.

VI. Simple quantum algorithms

Quantum algorithms that are more efficient than their classical counterparts: Deutsch, Deutsch-Jozsa and Simon. We will use the power of quantum parallelism, constructive and destructive interference and entanglement.

VI.A Quantum parallelism

Let

$$f : \{0, \dots , 2^n - 1\} \to \{0,1\}$$

$$f' : (x, b) \to \big(x, b \oplus f(x)\big)$$

where $x \in \{0, \dots , 2^n - 1\}$ and $b \in \{0,1\}$, with $\oplus$ being the addition modulo 2.

Then, f' is **one-to-one**, and therefore there is a unitary transformation U_f such that $U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$. Let's consider the following state

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|0\rangle\,, \quad \text{where } |i\rangle = |i_0\rangle \otimes \dots \otimes |i_{n-1}\rangle$$

Then, with a single application of the mapping U_f we will get

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

Thus, in a **single** computation step, 2^n values of f are computed.

VI.A.1 Interpretation of quantum parallelism

The last application of the unitary transformation U_f results in a state with 2^n values of function f. Such a massive parallelism is an important part of the magic quantum computation exhibits. However, the major part of such a magic is only apparent.

Actually, one cannot say that the result of such a computation is 2^n evaluations of f. All one can say is that such a unitary mapping results in a state that fully specifies all values of the function f. But there is, in general, no way to learn from the resulting state all the **values** of the function f. There is nonetheless often a way to get, using such quantum parallelism, important **relations** between values of the function f, usually at the price of being no longer able to get values of f, but instead to its arguments.

It is wrong, and deeply misleading to sat that after an application of the unitary matrix U_f the quantum computer has evaluated the function $f(x)$ for all $0 \leq x \leq 2^n$. Such assertion are based on the mistaken view that each quantum state encodes a property inherent in the qubits: as long as you have not measured, you know nothing! **The state encodes only the possibilities available for the extraction of information from those qubits**.

Due to that parallelism, quantum computing nevertheless permits quantum machines to perform *tricks* that no classical computer can accomplish.

VI.A.2 Measurement

If we measure the 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 $\{|z\rangle \mid z \in \{0{,}1\}^n\}$, 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 and $k = |\{x|f(x) = y\}|$

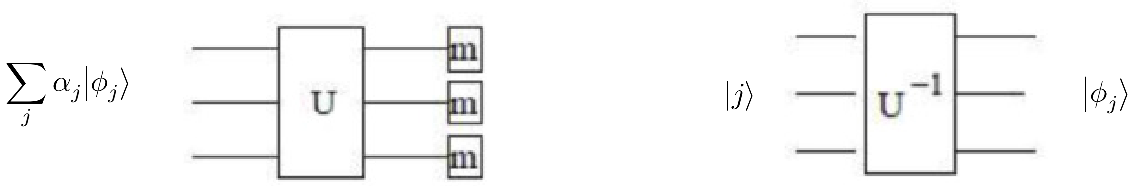
The collapse into the state $|\phi_y\rangle$ happens with the probability

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

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

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

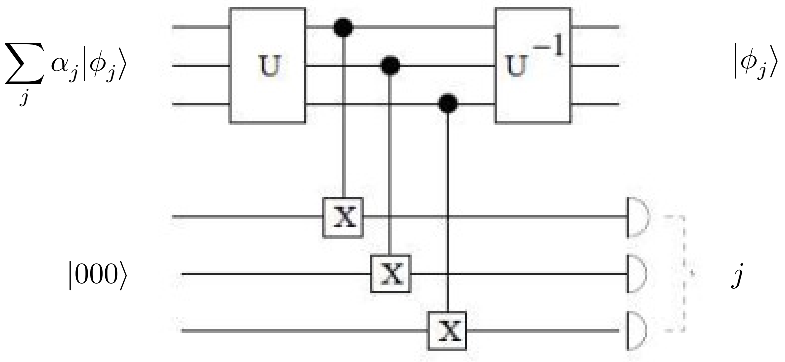
VI.A.3 Reduction of projective measurement to computational basis measurement



The above figure shows one way how to reduce the measurement with respect to any orthogonal basis $\{|\phi_j\rangle\}_{j=1,\ldots,2^n}$ to a measurement with respect to the computational basis $\{|j\rangle\}_{j=1,\ldots,2^n}$.

Through measurement the state $|j\rangle$ is obtained with probability $|\alpha_j|^2$. The state of the system after this measurement is $|j\rangle$. After inverse unitary U^{-1} is applied, the resulting state will be $|\phi_j\rangle$ of the standard basis.

At first, a unitary transformation U is applied, that transforms the basis $\{|\phi_j\rangle\}_j$ to the computational basis.



Another way to implement the von Neumann measurements is described in the schema above. First the outcome of the transformation U is mapped into ancillary registers to create the state $\sum_j \alpha_j |j\rangle|j\rangle$. The inverse basis change unitary U^{-1} leaves as result the state $\sum_j |\phi_j\rangle|j\rangle$. The following measurement of the ancillary register in the computational basis gives the outcome j with probability $|\alpha_j|^2$ and leaves the main register in the state $|\phi_j\rangle$.

VI.A.4 U_f and V_f operators

For the function $f : \{0, \dots, 2^n - 1\} \to \{0,1\}$, we can define the following operators

$$V_f : |x\rangle \to (-1)^{f(x)}|x\rangle$$

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

We can express V_f with U_f if we initialize the ancilla b to the state $b := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$ as follows

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

VI.B Deutsch's problem

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

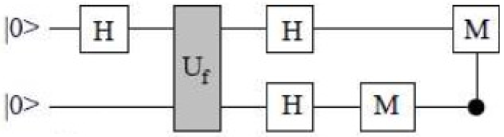
$$f(0) \oplus f(1) = 0 \text{ (constant)}$$

or

$$f(0) \oplus f(1) = 1 \text{ (balanced)}$$

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

VI.B.1 Randomized solution



Note that contrary to the solution we previously saw, there is no H gate in the bottom left.

The quantum algorithm as presented above solves the problem with **probability ½** in such a way that we know whether the answer is correct.

Let’s analyze the algorithm, step by step:

$$|00\rangle$$

$$\downarrow$$

$$(H \otimes I)|00\rangle = |+\rangle|0\rangle$$

$$\downarrow$$

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

$$\downarrow \qquad\qquad \downarrow$$

If f is constant

If f is balanced

$$U_f|+,0\rangle = \begin{cases} \dfrac{1}{\sqrt{2}}(|0,0\rangle + |1,0\rangle) \\ \text{or} \\ \dfrac{1}{\sqrt{2}}(|0,1\rangle + |1,1\rangle) \end{cases} \qquad U_f|+,0\rangle = \begin{cases} \dfrac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle) \\ \text{or} \\ \dfrac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle) \end{cases}$$

Entangled outputs

$$\downarrow \qquad\qquad \downarrow$$

$$HU_f|+,0\rangle = \begin{cases} \dfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ \text{or} \\ \dfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \end{cases} \qquad HU_f|+,0\rangle = \begin{cases} \dfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \\ \text{or} \\ \dfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle) \end{cases}$$

$$\downarrow \qquad\qquad \downarrow$$

In each case, notwithstanding we measure 0 or 1 on the second qubit, the first qubit will be in state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

If we measure the second qubit to 0, then the overall state is $|00\rangle + |10\rangle$

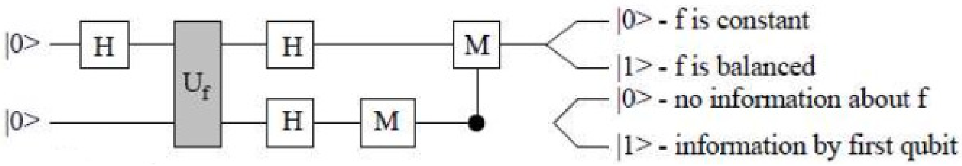
If we measure the second qubit to 1, then the overall state is $|01\rangle - |11\rangle$ or $-|01\rangle + |11\rangle$

Summing up our situation:

- Measure second qubit as 0, then the first qubit will be in state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $-\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Measure second qubit as 1,
  - then the first qubit will be in state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ if f is **constant**
  - then the first qubit will be in state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ if f is **balanced**

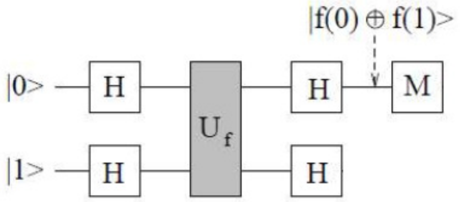
After the last Hadamard gate:

- Measure second qubit as 0, then the first qubit will be in state $|0\rangle$ or $-|0\rangle$
- Measure second qubit as 1,
  - then the first qubit will be in state $|0\rangle$ if f is **constant**
  - then the first qubit will be in state $|1\rangle$ if f is **balanced**


|0>
H
U_f
H
M
|0>
H
M
|0> - f is constant
|1> - f is balanced
|0> - no information about f
|1> - information by first qubit

If the measurement of the second qubit in the above provides 0, we have lost all information about f. Otherwise, the measurement of the first qubit yields the correct result.

VI.B.2 Deterministic solution



First, apply the Hadamard transform on both registers in the initial state $|0{,}1\rangle$ and then U_f:

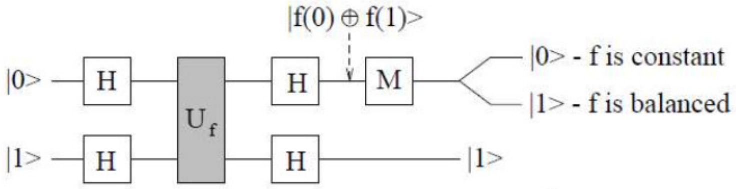
$$\begin{aligned}
|0{,}1\rangle &\overset{H_2}{\to} \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\
&= \frac{1}{2}\big(|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)\big) \\
&\overset{U_f}{\to} \frac{1}{2}\big(|0\rangle(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)\big) \\
&= \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)|1\rangle})(|0\rangle - |1\rangle)
\end{aligned}$$

Here are all the possibilities:

$$\text{if } f \text{ is constant } \begin{cases} \text{if } f(\{0{,}1\}) = 0, & \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = |0'\rangle|1'\rangle \\ \text{if } f(\{0{,}1\}) = 1, & \frac{1}{2}(|0\rangle + |1\rangle)(|1\rangle - |0\rangle) = -|0'\rangle|1'\rangle \end{cases}$$

$$\text{if } f \text{ is constant } \begin{cases} \text{if } f(0) = 0 \text{ and } f(1) = 1, & \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) = |1'\rangle|1'\rangle \\ \text{if } f(0) = 1 \text{ and } f(1) = 0, & \frac{1}{2}(|0\rangle - |1\rangle)(|1\rangle - |0\rangle) = -|1'\rangle|1'\rangle \end{cases}$$

By measuring the first bit, with respect to the dual basis, we can immediately see whether f is constant or balanced:



VI.C Deutsch-Jozsa problem

VI.C.1 Even-odd problem

A function $f : \{0{,}1\}^2 \to \{0{,}1\}$ is called **even** (resp. **odd**) if the range of f has an **even** (resp. **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.

One a quantum computer, one can do:

$$(H \otimes H)V_f(I \otimes H)V_f(H \otimes H)|00\rangle = \begin{cases} \frac{1}{\sqrt{2}}(\pm|00\rangle + |01\rangle) \text{ if } f \text{ is even} \\ \frac{1}{\sqrt{2}}(\pm|10\rangle + |01\rangle) \text{ if } f \text{ is odd} \end{cases}$$

Therefore, using only two quantum calls of 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.

VI.C.2 Deutsch-Jozsa promise problem

Given a function $f : \{0{,}1\}^n \to \{0{,}1\}$ as a black box, that is (promised to be) balanced or constant, decide which property f has.

Classical deterministic computers need, 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.

VI.C.3 First solution

Let us consider one quantum register with n qubits and apply the Hadamard transformation H_n to this register. This yields:

$$|0^n\rangle \overset{H_n}{\to} |\phi\rangle \overset{\text{def}}{=} \frac{1}{\sqrt{2}^n} \sum_{i=0}^{2^n-1} |i\rangle$$

By applying now the transformation V_f only on this register, we get:

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

Thanks to these operations, the values of f were transferred to their amplitudes. Let's make use of quantum superposition and a proper observable to now solve our initial problem.

Let us consider the observable $\mathcal{D} = \{E_a, E_b\}$, where E_a is the *one-dimensional subspace* spanned by the vector

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

and

$$E_b = E_a^{\perp}$$

The projection of $|\phi'\rangle$ onto $\mathcal{D}$ has the form:

$$|\phi'\rangle = \alpha|\psi_a\rangle + \beta|\psi_b\rangle$$

with $|\alpha|^2 + |\beta|^2 = 1$ and where $|\psi_b\rangle$ is a vector of E_b such that $|\psi_b\rangle \perp |\psi_a\rangle$. Thus, a measurement by $\mathcal{D}$ provides "the value a or b" with probability $|\alpha|^2$ or $|\beta|^2$. In particular,

$$\begin{aligned} \alpha &= \langle\psi_a|\phi'\rangle \\ &= \frac{1}{\sqrt{2}^n} \sum_{j=0}^{2^n-1} \langle j| \frac{1}{\sqrt{2}^n} \sum_{i=0}^{2^n-1} (-1)^{f(i)} |i\rangle \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2^n} \sum_{j=0}^{2^n-1} \sum_{i=0}^{2^n-1} (-1)^{f(i)} \langle j|i\rangle \\
&= \frac{1}{2^n} \sum_{i=0}^{2^n-1} (-1)^{f(i)} \text{ because } \langle j|i\rangle = 1 \text{ iff } j = i
\end{aligned}$$

Thus,

- If f is **balanced**, then the sum for α contains the same number of 1 and -1, and therefore $\alpha = 0$. A measurement of $|\phi'\rangle$ with respect to $\mathcal{D}$ provides, for sure, the outcome b.
- If f is **constant**, then either $\alpha = 1$ or $\alpha = -1$, and therefore the measurement with respect to $\mathcal{D}$ always gives the outcome a.

Therefore, a single measurement of $|\phi'\rangle$, with respect to $\mathcal{D}$ provides the solution to the problem with probability 1.

VI.C.4 Second solution

If the Hadamard transformation is applied to the state $|\phi'\rangle$, we get

$$\begin{aligned}
H_n|\phi'\rangle &= \frac{1}{\sqrt{2}^n} \sum_{i=0}^{2^n-1} (-1)^{f(i)} \frac{1}{\sqrt{2}^n} \sum_{j=0}^{2^n-1} (-1)^{j\cdot i} |j\rangle \\
&= \frac{1}{2^n} \sum_{j=0}^{2^n-1} \sum_{i=0}^{2^n-1} (-1)^{j\cdot i} (-1)^{f(i)} |j\rangle
\end{aligned}$$

Thus,

- If f is constant,

$$\sum_{i=0}^{2^n-1} (-1)^{j\cdot i} = \begin{cases} 0 \text{ if } u \neq 0 \\ 2^n \text{ if } j = 0 \end{cases}$$

- If f is balanced,

$$\sum_{i=0}^{2^n-1} (-1)^{j\cdot i} (-1)^{f(i)} = 0 \text{ iff } u = 0$$

One measurement therefore shows with probability 1 whether f is constant or balanced: $H_n|\phi'\rangle = |0\rangle$ with probability 1 iff f is constant.

VI.C.5 Randomized solution

It is easy to show that although deterministic algorithms to solve the Deutsch-Jozsa problem for $n = 2^k$ requires $2^{k-1} + 1$ queries in the worst case, there are probabilistic algorithms to solve this problem relatively fast, if we are willing to tolerate some error.

In particular, a randomized algorithm can solve the Deutsch-Jozsa problem with probability of error at most $\frac{1}{3}$ with only two queries. The probability of error can be reduced to less than $\frac{1}{2^k}$ with only $k+1$ queries.

Therefore, in spite of the fact that there is an exponential gap between deterministic classical and exact quantum query complexity, the gap between randomized classical complexity and quantum query complexity is in this case constant in the case of constant error: the advantage is vanishingly small.

VII. Simon's problem

Simon has discovered a simple problem with an expected quantum polynomial time algorithm, but having **no** polynomial time randomized algorithm.

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a function such that either:

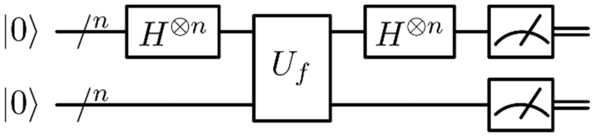
- f is one-to-one
- f is two-to-one, i.e., there exists a single $s \in \{0,1\}^n \neq \{0,\dots,0\}$ such that

$$\forall x \neq x', \qquad f(x) = f(x') \Leftrightarrow x' = x \oplus s$$

The task is to determine which of the above conditions holds for f, and in the second case, also determine s.

To solve the problem, **two** registers are used, both with $\boldsymbol{n}$ **qubits**. The initial states are $|0^n\rangle$ and the **Hadamard-twice scheme** is used for $\mathcal{O}(n)$ repetitions

VII.A Simon algorithm



First, apply the Hadamard transformation on the **first** register with the initial value $|0^n\rangle$, to produce the superposition

$$H_n|0^n\rangle \otimes |0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x, 0^n\rangle$$

Then, apply U_f to obtain the following

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x, f(x)\rangle$$

Finally, apply the Hadamard transformation on the **first** register again

$$|\psi'\rangle = \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{x\cdot y}|y, f(x)\rangle$$

After all these steps, observe the resulting state to get a pair $(y, f(x))$.

VII.A.1 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: $\frac{1}{2^n}$.

$n-1$ independent applications of the above 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 2^n possible pairs $(y, f(x))$.

VII.A.2 Case 2: f is two-to-one

In this case, there exists a single $s \in \{0,1\}^n \neq \{0,\dots,0\}$ such that

$$\forall x \neq x', \qquad f(x) = f(x') \Leftrightarrow x' = x \oplus s$$

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

$$\alpha(x, y) = \frac{1}{2^n}\left((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}\right)$$

If $y \cdot s \equiv 0 \ mod\ 2$ (even number), then

$$\begin{aligned} x \cdot y &\equiv (x \oplus s) \cdot y \ mod\ 2 \\ &\equiv (x \cdot y) \oplus (s \cdot y) \ mod\ 2 \end{aligned}$$

Therefore, $|\alpha(x, y)| = \frac{1}{2^{n-1}}$

Else, if $y \cdot s \equiv 1 \ mod\ 2$ (odd number), then $|\alpha(x, y)| = 0$, which means that this is never the case (zero probability)

$n - 1$ independent applications of the above scheme (Hadamard twice) therefore yields $n - 1$ independent pairs $(y_1, f(x_1)), \dots, (y_{n-1}, f(x_{n-1}))$, such that $\forall i \in \{1, \dots, n-1\}, y_i \cdot s \equiv 0 \ mod\ 2$.

VII.A.3 Summary

In both cases, after $n - 1$ repetitions of the Hadamard twice scheme, $n - 1$ vectors y_i are obtained. If these vectors are linearly independent, then the system of $n - 1$ linear equations $\forall i \in \{1, \dots, n-1\}, y_i \cdot s \equiv 0 \ mod\ 2$ over $\mathbb{Z}_2$ can be solved to obtain s in the case f is two-to-one. Note that in the case f is one-to-one, s obtained in such a way is a random string.

To distinguish these two cases, it is enough to compute $f(0^n)$ and $f(s)$: if $f(0^n) \neq f(s)$, then f is one-to-one. If the vectors obtained by this scheme are not linearly independent, then the whole process has to be repeated.

Executing this algorithm $k = \mathcal{O}(n)$ times yields random $y_1, \dots, y_k \in \{0,1\}^n$ such that $s \cdot y_1 = \dots = s \cdot y_k = 0$. This is a system of k linear equations:

$$\begin{pmatrix} y_{11} & \cdots & y_{1n} \\ \vdots & \ddots & \vdots \\ y_{k1} & \cdots & y_{kn} \end{pmatrix} \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \ mod\ 2$$

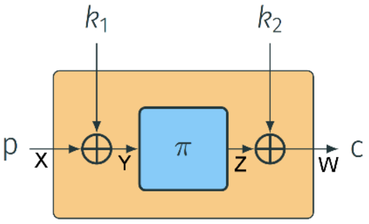
With high probability, there is a unique non-zero solution that is s (which can be efficiently found by linear algebra).

VII.A.4 Classical algorithm

Any classical algorithm needs to perform $\Omega(\sqrt{2^n})$ queries to solve Simon's problem.

VII.B Application to quantum crypto attacks

VII.B.1 The Even Mansour secret-key cipher



Two keys k_1 and k_2, one public permutation π (the latter is very expensive to store: a 64 to 64 bits permutation requires 2^{64} bits of storage).

From a classic point of view, the attacker is allowed to ask for D (stands for data) pairs of (X, W) values and to evaluate T (stands for time) pairs of (Y, Z) values.

It has been proved that the upper bound on attack success is $\mathcal{O}(\frac{DT}{2^n})$

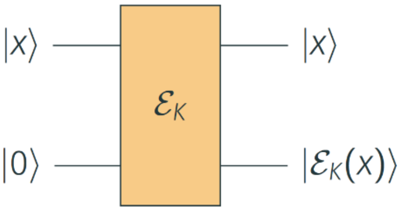
VII.B.2 Attacks on crypto algorithm

The attacker listens to communication over classical channel, he can also query the classic black box with secret key. Let's suppose that the attacker has a large quantum computer.

Other existing quantum algorithms:

- Recover key in $\mathcal{O}(2^{\frac{k}{2}})$ with Grover's algorithm
- Find hash function preimage in $\mathcal{O}(2^{\frac{n}{2}})$ with Grover's algorithm
- Find hash function collisions in $\mathcal{O}(2^{\frac{n}{3}})$ but needs a $\mathcal{O}(2^{\frac{n}{3}})$ hardware

Quantum oracle access to encryption algorithm: a very strong model for adversary



Let's denote the cipher as $\mathcal{E}_{k_1,k_2}$, such that

$$\mathcal{E}_{k_1,k_2}(x) = \pi(x \oplus k_1) \oplus k_2$$

We can then construct

$$\begin{aligned} f : \{0,1\}^n &\to \{0,1\}^n \\ x &\to \mathcal{E}_{k_1,k_2}(x) \oplus \pi(x) \end{aligned}$$

This function fulfills Simon's promise:

$$\begin{aligned} f(x) &= \pi(x \oplus k_1) \oplus k_2 \oplus \pi(x) \\ f(x \oplus k_1) &= \pi(x \oplus k_1 \oplus k_1) \oplus k_2 \oplus \pi(x \oplus k_1) \\ &= \pi(x) \oplus k_2 \oplus \pi(x \oplus k_1) \end{aligned}$$

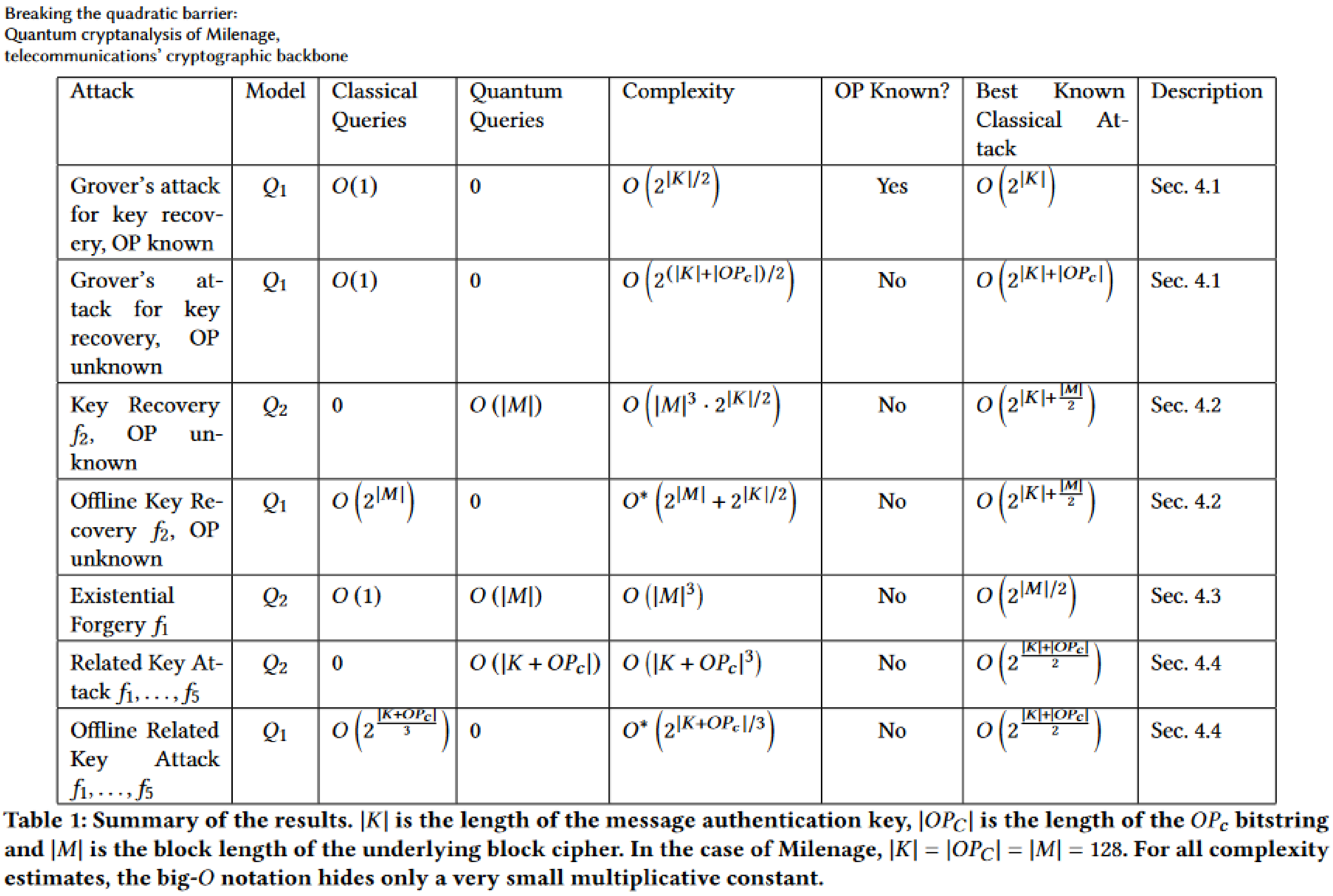
Therefore, we can recover k_1 with $\mathcal{O}(n)$ quantum queries.

Similar attacks apply to block cipher modes, MACs, authenticated encryption, improving slide attacks. The aim is always to construct f such that $f(x) = f(x \oplus s)$ for some secret s.

VII.B.3 Telecommunication crypto

The **entire** cryptography of contemporary cellular networks is centered around seven **secret-key** algorithms aggregated into a single "Authentication and Key Agreement" known as AKA algorithm set, denoted $f_1, \dots, f_5, f_1^*, f_5^*$.

We know that these seven algorithms are **provably secure** by all means in the classical world. But it is envisioned that 6G should not be broken even by quantum computers of arbitrary complexity.



Breaking the quadratic barrier:
Quantum cryptanalysis of Milenage,
telecommunications' cryptographic backbone

Attack	Model	Classical Queries	Quantum Queries	Complexity	OP Known?	Best Known Classical Attack	Description
Grover's attack for key recovery, OP known	Q_1	$O(1)$	0	$O\left(2^{\lvert K\rvert/2}\right)$	Yes	$O\left(2^{\lvert K\rvert}\right)$	Sec. 4.1
Grover's attack for key recovery, OP unknown	Q_1	$O(1)$	0	$O\left(2^{(\lvert K\rvert+\lvert OP_c\rvert)/2}\right)$	No	$O\left(2^{\lvert K\rvert+\lvert OP_c\rvert}\right)$	Sec. 4.1
Key Recovery f_2, OP unknown	Q_2	0	$O(\lvert M\rvert)$	$O\left(\lvert M\rvert^3 \cdot 2^{\lvert K\rvert/2}\right)$	No	$O\left(2^{\lvert K\rvert+\frac{\lvert M\rvert}{2}}\right)$	Sec. 4.2
Offline Key Recovery f_2, OP unknown	Q_1	$O\left(2^{\lvert M\rvert}\right)$	0	$O^*\left(2^{\lvert M\rvert}+2^{\lvert K\rvert/2}\right)$	No	$O\left(2^{\lvert K\rvert+\frac{\lvert M\rvert}{2}}\right)$	Sec. 4.2
Existential Forgery f_1	Q_2	$O(1)$	$O(\lvert M\rvert)$	$O(\lvert M\rvert^3)$	No	$O\left(2^{\lvert M\rvert/2}\right)$	Sec. 4.3
Related Key Attack $f_1,\dots,f_5$	Q_2	0	$O(\lvert K+OP_c\rvert)$	$O(\lvert K+OP_c\rvert^3)$	No	$O\left(2^{\frac{\lvert K\rvert+\lvert OP_c\rvert}{2}}\right)$	Sec. 4.4
Offline Related Key Attack $f_1,\dots,f_5$	Q_1	$O\left(2^{\frac{\lvert K+OP_c\rvert}{3}}\right)$	0	$O^*\left(2^{\lvert K+OP_c\rvert/3}\right)$	No	$O\left(2^{\frac{\lvert K\rvert+\lvert OP_c\rvert}{2}}\right)$	Sec. 4.4

Table 1: Summary of the results. $|K|$ is the length of the message authentication key, $|OP_C|$ is the length of the OP_c bitstring and $|M|$ is the block length of the underlying block cipher. In the case of Milenage, $|K| = |OP_C| = |M| = 128$. For all complexity estimates, the big-O notation hides only a very small multiplicative constant.

VII.C Computational power of entanglement

As illustrated in the following examples, in some cases there is a clever way to make use of quantum entanglement to compute efficiently some global properties of a function.

VII.C.1 An example problem

Let $f : \{1, \dots, n\} \to \{0,1\}$ be given as a black box. To determine f classically, n calls of f are needed, to get the string $w_f = f(1) \dots f(n)$

Quantumly, this can be done, with probability greater than 0.95 using $\frac{n}{2} + \sqrt{n}$ quantum calls of f. Indeed, we have

$$|w_f\rangle = H_n \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot w_f} |x\rangle$$

In order to compute $x \cdot w_f$ one needs $hw(x)$ calls of f, where $hw(x)$ is the Hamming weight of x.

VII.C.2 Entanglement trick

The trick is to compute the former identity but only for x such that $hw(x) \leq k$, for a suitable k.

If F_k is a function such that for $x \in \{0,1\}^n$,

$$F_k(x) = \begin{cases} x \cdot w_f \text{ if } hw(x) \leq k \\ \quad 0 \text{ otherwise} \end{cases}$$

Then,

$$V_{F_k}|x\rangle = \begin{cases} (-1)^{x \cdot w_f}|x\rangle \text{ if } hw(x) \leq k \\ |x\rangle \text{ otherwise} \end{cases}$$

We will apply V_{F_k} to the initial state $|\psi_k\rangle$ defined as

$$|\psi_k\rangle = \frac{1}{\sqrt{M_k}} \sum_{\substack{x \in \{0,1\}^n \\ hw(x) \leq k}} |x\rangle$$

where $M_k = \sum_{i=0}^{k} \binom{n}{i}$

Then,

$$|\psi'_k\rangle = V_{F_k}|\psi_k\rangle = \frac{1}{\sqrt{M_k}} \sum_{\substack{x \in \{0,1\}^n \\ hw(x) \leq k}} (-1)^{x \cdot w_f}|x\rangle$$

In order to compute $|\psi'_k\rangle$, at most k calls of f are needed. Let's now measure all n qubits of $|\psi''_k\rangle = H_n|\psi'_k\rangle$.

The probability of getting w_f is

$$\begin{aligned} \mathbb{P}(|\psi''_k\rangle \text{ yields at measurement } w_f) &= |\langle w_f|\psi''_k\rangle|^2 \\ &= \frac{M_k}{2^n} \\ &= \sum_{i=0}^{k} \frac{\binom{n}{i}}{2^n} \end{aligned}$$

This probability is greater than 0.95 if $k = \frac{n}{2} + \sqrt{n}$.

VII.C.3 Quantum Fourier Transform

The Quantum Fourier Transform (QFT) is a quantum variant of the Discrete Fourier Transform (DFT). It maps a discrete function to another discrete one with equally distant points as its domain.

For example, it maps a q-dimensional complex

$$\left(f(0), \ldots, f(q-1)\right) \text{ into } \left(\bar{f}(0), \ldots, \bar{f}(q-1)\right)$$

where

$$\forall c \in \{0, \ldots, q-1\}, \qquad \bar{f}(c) = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} e^{\frac{2\pi iac}{q}} f(a)$$

The quantum version of the DFT is the unitary transformation

$$\forall x \in \{0, \ldots, q-1\}, \qquad QFT_q : |x\rangle \to \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} e^{\frac{2\pi iax}{q}} |a\rangle$$

The unitary matrix is thus

$$F_q = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & \ldots & \omega^{q-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{2(q-1)} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{q-1} & \omega^{2(q-1)} & \ldots & \omega^{(q-1)^2} \end{pmatrix}$$

with $\omega = e^{\frac{2\pi i}{q}}$ the q^{th} root of unity.

If applied to a quantum superposition, QFT_q performs as:

$$\begin{aligned} QFT_q\left(\sum_{a=0}^{q-1} f(a)|a\rangle\right) &= \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1} e^{\frac{2\pi iac}{q}} f(a)|c\rangle \\ &= \sum_{c=0}^{q-1} \bar{f}(c)|c\rangle \end{aligned}$$

Note that

$$QFT_q(|0^n\rangle) = \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle$$

VIII. Grover's search algorithm

Until there, quantum attacks just meant that doubling the key size was enough to make the crypto algorithms secure again...

VIII.A Grover's search problem I

Grover's method applies to problems for which it is hard to find a solution, yet it is easy to recognize a solution. It is easy through a list of potential solutions to find the right one, but hard to find some special structure of the problem to speed-up search for a correct solution.

The problem can be formulated as follows: in an unsorted database of N items there is exactly one x_0 satisfying an easy to verify condition P. Find x_0.

A classical algorithms need on **average** $\frac{N}{2}$ checks, and a quantum algorithm needs $\mathcal{O}(\sqrt{N})$. Note: the speedup is substantial but we still cannot solve NP hard problems.

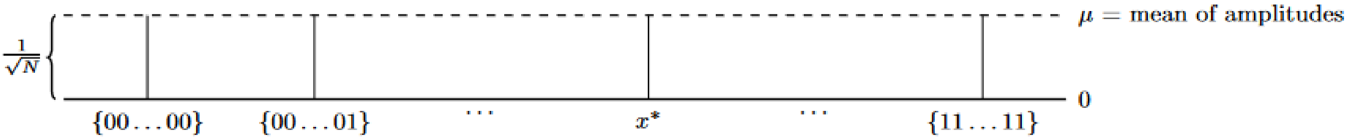
Here is the basic idea of the algorithm: "cooking" a solution.

VIII.A.1 Grover's search algorithm I

We will denote $N = 2^n$

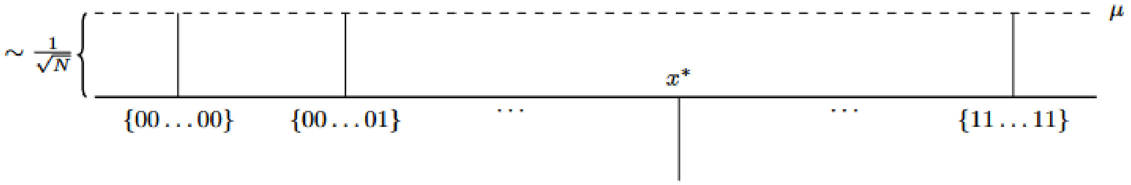
Starting state is the equally weighted superposition of all basis states, which can be obtained the following way:

$$|0^n\rangle \overset{H_n}{\to} \frac{1}{\sqrt{2}} \sum_{x\in\{0,1\}^n} |x\rangle$$

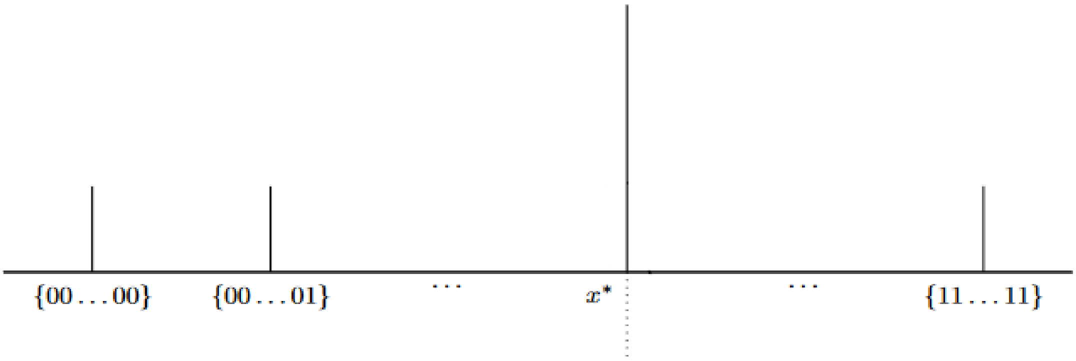


State $|x_0\rangle$ (x^* in the schema) is the one with $f(x_0) = 1$

Then, by applying V_f, we obtain -1 for the amplitude of the state $|x_0\rangle$. Now, the average of the overall amplitude is lower than $\frac{1}{\sqrt{2^n}}$ because there is a negative value among the amplitudes.



Next step, we apply an *inversion over the average*, which increases the amplitude of $|x_0\rangle$ and decreases all the other basis states. We do not have seen how to perform such an operation.



After that, we perform these operations a proper number of times, so much so that the amplitude at the state $|x_0\rangle$ is almost 1 and the amplitude of all other states are almost 0. A measurement in such a situation produces x_0 as the classical outcome.

VIII.B Grover's search problem II

Modified problem: given an easy to use black box U_f to compute a function

$$f : \{0,1\}^n \to \{0,1\}$$

find x_0 such that $f(x_0) = 1$, with t solutions, i.e. $t = |\{x|f(x) = 1\}|$

VIII.B.1 Inversion about the average

The inversion about the average is the unitary transformation

$$D_n : \sum_{i=0}^{2^n-1} a_i|\phi_i\rangle \to \sum_{i=0}^{2^n-1} (2E - a_i)|\phi_i\rangle$$

where E is the **average** of $\{a_i|0 \leq i < 2^n\}$

This operation can be performed by the matrix

$$-H_nV_0^nH_n = D_n = \begin{pmatrix} -1+\frac{1}{2^{n-1}} & \frac{1}{2^{n-1}} & \cdots & \frac{1}{2^{n-1}} \\ \frac{1}{2^{n-1}} & -1+\frac{1}{2^{n-1}} & \ddots & \frac{1}{2^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2^{n-1}} & \frac{1}{2^{n-1}} & \cdots & -1+\frac{1}{2^{n-1}} \end{pmatrix}$$

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 bellow (above) the average – which is precisely the inversion about the average. Note that this operation can be performed without knowing x_0.

The matrix D_n is clearly unitary and it can be shown to have the form $D_n = -H_nV_0^nH_n$, where

$$V_0^n[i,j] = \begin{cases} 0 \text{ if } i \neq j \\ -1 \text{ if } (i,j) = (1,1) \\ 1 \text{ if } i = j \text{ and } 1 < i \leq n \end{cases}$$

VIII.B.2 Presentation of Grover's search algorithm

We start with the state

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

Then, iterate $\lfloor 4\pi\sqrt{2^n} \rfloor$ times the transformation $D_n V_f$.

Finally, measure the resulting register to get x_0 and check whether $f(x_0) = 1$. If not, repeat the procedure. We will show later that the above algorithm is optimal for finding the solution with a **probability greater than $\frac{1}{2}$**.

NB: the fact that this the solution is true only *probably* comes from the fact that if we could do exactly $4\pi\sqrt{2^n}$ (i.e., a non-integer number of iterations), then the solution would be perfect. See later in this lesson.

In the case that there are t solutions, the above iteration should be repeated $\left\lfloor 4\pi\sqrt{\frac{2^n}{t}} \right\rfloor$ times.

VIII.B.3 Analysis of Grover's search algorithm

Denote $X_1 = \{x | f(x) = 1\}$ and $X_0 = \{x | f(x) = 0\}$, and let the state after the j^{th} iteration of Grover's iterate $D_n V_f$ be

$$|\phi_j\rangle = k_j \sum_{x \in X_1} |x\rangle + l_j \sum_{x \in X_0} |x\rangle \quad \text{with} \quad k_0 = l_0 = \frac{1}{\sqrt{2^n}}$$

We know that $|\phi_{j+1}\rangle = D_n V_f |\phi_j\rangle$, thus

$$\begin{aligned} k_{j+1} &= \frac{2^n - 2t}{2^n} k_j + 2 \cdot \frac{2^n - t}{2^n} l_j \\ l_{j+1} &= \frac{2^n - 2t}{2^n} l_j - \frac{2t}{2^n} k_j \end{aligned}$$

This yields to

$$\begin{cases} k_j = \dfrac{1}{\sqrt{t}} \sin\big((2j+1)\theta\big) \\ l_j = \dfrac{1}{\sqrt{2^n - t}} \cos\big((2j+1)\theta\big) \end{cases} \quad \text{with} \quad \frac{t}{2^n} = \sin^2\theta$$

The objective is now to find such a j which maximizes k_j and minimizes l_j. In our case, it means make k_j as close to 1 as possible, which is $k_j \simeq \frac{1}{\sqrt{t}}$.

Therefore, we chose j such that $\cos\big((2j+1)\theta\big) = 0$

$$\begin{aligned} \cos\big((2j+1)\theta\big) = 0 \ &\Rightarrow \ (2j+1)\theta = \frac{\pi}{2} + m\pi \quad \text{with} \quad m \in \mathbb{Z} \\ &\Rightarrow \ j = \frac{\pi}{4\theta} - \frac{1}{2} + \frac{m\pi}{2\theta} \quad \text{with} \quad m \in \mathbb{Z} \\ &\Rightarrow \ j = \left\lceil \frac{\pi}{4\theta} \right\rceil \end{aligned}$$

We have $\frac{t}{2^n} = \sin^2\theta$, so

$$0 \leq \sin\theta \leq \sqrt{\frac{t}{2^n}}$$

If t is small, then $\theta \simeq \sqrt{\frac{t}{2^n}}$, which yields finally to $j = \mathcal{O}\left(\sqrt{\frac{2^n}{t}}\right)$

VIII.B.4 Examples

1st example: take $N = 4$, with solution $x = 3$, and start with the state

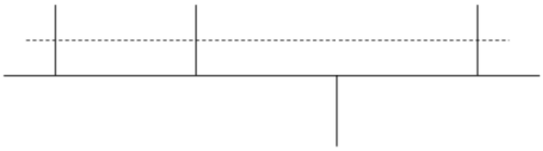
$$|s\rangle = \frac{1}{2}(|1\rangle + |2\rangle + |3\rangle + |4\rangle)$$

Therefore,

$$V_f|s\rangle = \frac{1}{2}(|1\rangle + |2\rangle - |3\rangle + |4\rangle)$$

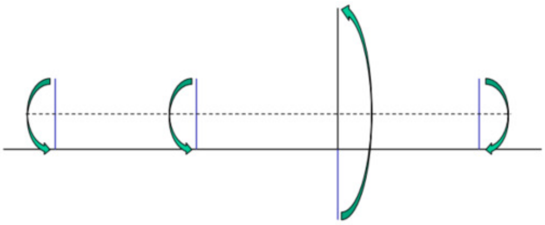
The mean is here

$$\bar{s} = \frac{1}{4}\left(\frac{1}{2} + \frac{1}{2} - \frac{1}{2} + \frac{1}{2}\right) = \frac{1}{4}$$



After applying the reflection operator D_2, we get

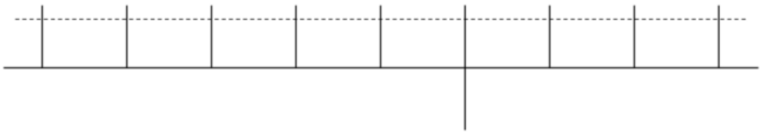
$$D_2V_f|s\rangle = \frac{1}{2}(|1\rangle + |2\rangle + |3\rangle + |4\rangle) - \frac{1}{2}(|1\rangle + |2\rangle - |3\rangle + |4\rangle) = |3\rangle$$



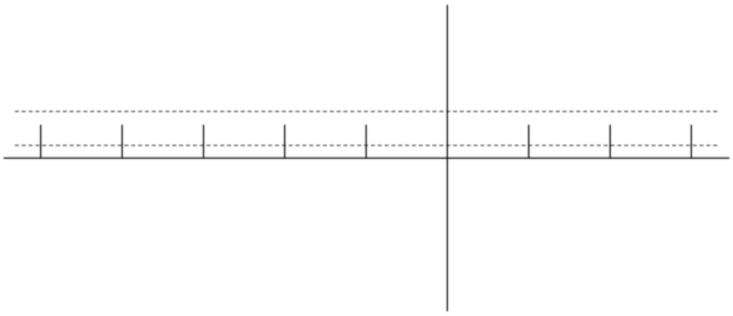
We learn from this example that if we have the perfect queuing of states, we can get the solution with probability 1 exactly. The number of iterations is an integer, that's why.

2nd example: take $N = 9$ with solution $x = 6$:

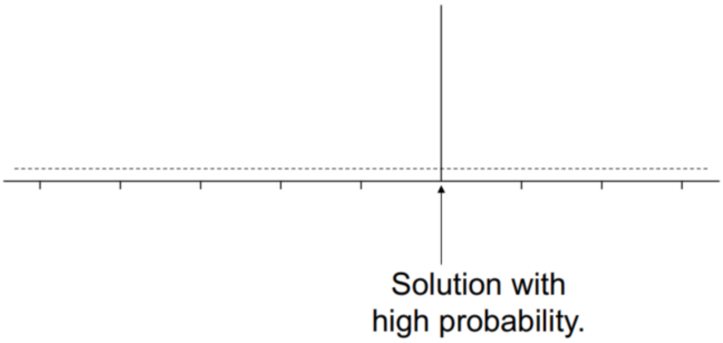
Reflecting target, the mean is $\frac{7}{27}$



Reflecting about the mean, reflecting target, the mean is now $\frac{17}{243}$



Reflecting about the mean



VIII.B.5 Refined analysis

Theorem:

Let $f : \{0,1\}^n \to \{0,1\}$ and let there be exactly t elements $x \in \{0,1\}^n$ such that $f(x) = 1$.

Assume that $0 < t < \frac{3}{4}2^n$ and let $\theta_0 \in [0, \frac{\pi}{3}]$ be chosen such that $\sin^2\theta_0 = \frac{t}{2^n} \leq \frac{3}{4}$.

After $\left\lfloor \frac{\pi}{4\theta_0} \right\rfloor$ iterations of the Grover iterates on the initial superposition $\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$, the probability of finding a solution is at least $\frac{1}{4}$.

Proof:

The probability of seeing a desired element is given by $\sin^2\big((2j+1)\theta_0\big)$ 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 $\left\lfloor \frac{\pi}{4\theta_0} \right\rfloor$.

Since $\left\lfloor \frac{\pi}{4\theta_0} \right\rfloor = -\frac{1}{2} + \frac{\pi}{4\theta_0} + \delta$ for some $|\delta| \leq \frac{1}{2}$, we have

$$\left(2\left\lfloor \frac{\pi}{4\theta_0} \right\rfloor + 1\right)\theta_0 = \frac{\pi}{2} + 2\delta\theta_0$$

And therefore, the distance of $\left(2\left\lfloor \frac{\pi}{4\theta_0} \right\rfloor + 1\right)\theta_0$ from $\frac{\pi}{2}$ is $|2\delta\theta_0| \leq \frac{\pi}{3}$. This implies that

$$\sin^2\left(\left(2\left\lfloor \frac{\pi}{4\theta_0} \right\rfloor + 1\right)\theta_0\right) \geq \sin^2\left(\frac{\pi}{2} - \frac{\pi}{3}\right) = \frac{1}{4}$$

VIII.B.6 Another view on Grover

Let $f : \{0,1\}^n \to \{0,1\}$ be a mapping such that $f(a) = 1$ for a single $a \in \{0,1\}^n$ and let V_f be our usual mapping such that for any $x \in \{0,1\}^n$, $V_f : |x\rangle \to (-1)^{f(x)}|x\rangle$.

Then, for any state $|\psi\rangle$, it holds that

$$V_f|\psi\rangle = |\psi\rangle - 2|a\rangle\langle a||\psi\rangle$$

Therefore,

$$V_f = Id - 2|a\rangle\langle a|$$

Thus, the operator V_f, when acting on any state, changes the sign of the amplitude of the basis state $|a\rangle$, while leaving amplitudes unchanged for the basis states orthogonal to $|a\rangle$

Let's define also our usual vector

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

and consider the new operator

$$W = 2|\phi\rangle\langle\phi| - Id$$

This operator W preserves the component of any state along $|\phi\rangle$, while changing the component orthogonal to $|\phi\rangle$.

The, the Grover algorithm can now be defined as an iterative application of the operator WV_f to the resulting states starting with the initial state $|\phi\rangle$.

Observe that

$$-W = Id - 2|\phi\rangle\langle\phi| = H_n(Id - 2|0^n\rangle\langle 0^n|)H_n$$

Both operators V_f and W when acting on a superposition of states $|a\rangle$ and $|\phi\rangle$ produce a superposition of the same states.

Indeed, since $\langle\phi|a\rangle = \frac{1}{\sqrt{2^n}}$ (there is a unique solution, the probability of measuring a is $\frac{1}{\sqrt{2^n}}$), it holds that

$$V_f|a\rangle = -|a\rangle, \qquad V_f|\phi\rangle = |\phi\rangle - \frac{2}{\sqrt{2^n}}|a\rangle$$

$$W|\phi\rangle = |\phi\rangle, \qquad W|a\rangle = \frac{2}{\sqrt{2^n}}|\phi\rangle - |a\rangle$$

As a consequence, a repeated application of the operator WV_f to the resulting states starting with the state $|\phi\rangle$ will always result in a state that will be a superposition of states $|a\rangle$ and $|\phi\rangle$. Graphically, it means that we are in a two-dimensional plane.

If we denote:

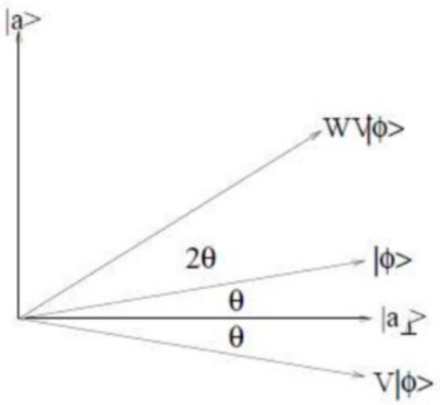
- $|a^{\perp}\rangle$ a state orthogonal to $|a\rangle$ in the subspace generated by $|a\rangle$ and $|\phi\rangle$
- θ and γ the angles such that $\sin\theta = \cos\gamma = \langle\phi|a^{\perp}\rangle = \frac{1}{\sqrt{2^n}}$

Then, for large n, we will have

$$\theta \simeq \frac{1}{\sqrt{2^n}}$$

The net effect of the operator W in two dimensional plane is to transform any vector by its **reflection** with respect to the mirror line through the origin along $|\phi\rangle$. Similarly, the net effect of the operator V_f on any vector is its reflection with respect to the vector $|a^{\perp}\rangle$.

Therefore, the net effect of the any application of the product WV_f of two operators that are two-dimensional reflections, is a rotation about the angle 2θ.



Since m iterations will result in the rotation by the angle $2m\theta$, with respect to the initial state $|\phi\rangle$, and θ is very close to $\frac{1}{\sqrt{2^n}}$, the number of iterations needed to come to the state orthogonal to $|a^\perp\rangle$, i.e., $|a\rangle$, should be approximately

$$\frac{\pi}{4}\sqrt{2^n}$$

This holds because for $m = \frac{\pi}{4}\sqrt{2^n}$, we have

$$2m\theta = \frac{\pi}{2}$$

This explains why the solution more probable than $\frac{1}{2}$, but not necessarily perfect: we may overshoot the perfect angle $\frac{\pi}{2}$ depending on the original angle. The error made in Grover is exponentially small.

VIII.B.7 Optimality of Grover's algorithm

Recall of the problem: given a function $f : \{0,1\}^n \to \{0,1\}$ mapping n bits to 1 bit, determine the value of x such that $f(x) = 1$.

Classically we need to evaluate $\mathcal{O}(N)$ values, where $N = 2^n$.

Grover's algorithm enables a search with $\mathcal{O}(\sqrt{N})$ queries. It has two crucial steps: calculate the function on all values simultaneously, then reflect about the equal superposition state. These steps are repeated $\mathcal{O}(\sqrt{N})$.

This algorithm is in fact **optimal**: it is not possible to perform any better.

NP is the class of problems that can be verified in polynomial time. That is, if given ω, you can verify that $f(\omega) = 1$ efficiently – but it is hard to find ω. If it were possible to achieve an **exponential** speedup for search, it would mean that a quantum computer can solve NP problems in polynomial time.

It was however proven that it is not possible to search on a quantum computer any faster than $\mathcal{O}(\sqrt{N})$, because NP problems are still fundamentally hard on quantum computers.