Lecture notes on quantum computation

Leonardo Castellani

Dipartimento di Scienze e Innovazione Tecnologica
Università del Piemonte Orientale, viale T. Michel 11, 15121 Alessandria, Italy

INFN, Sezione di Torino, via P. Giuria 1, 10125 Torino, Italy

Arnold-Regge Center, via P. Giuria 1, 10125 Torino, Italy

Abstract

These are lecture notes for the course "Introduction to quantum computation", offered at the Laurea Magistrale in Fisica dei sistemi complessi, UPO and Torino University.

December 2021

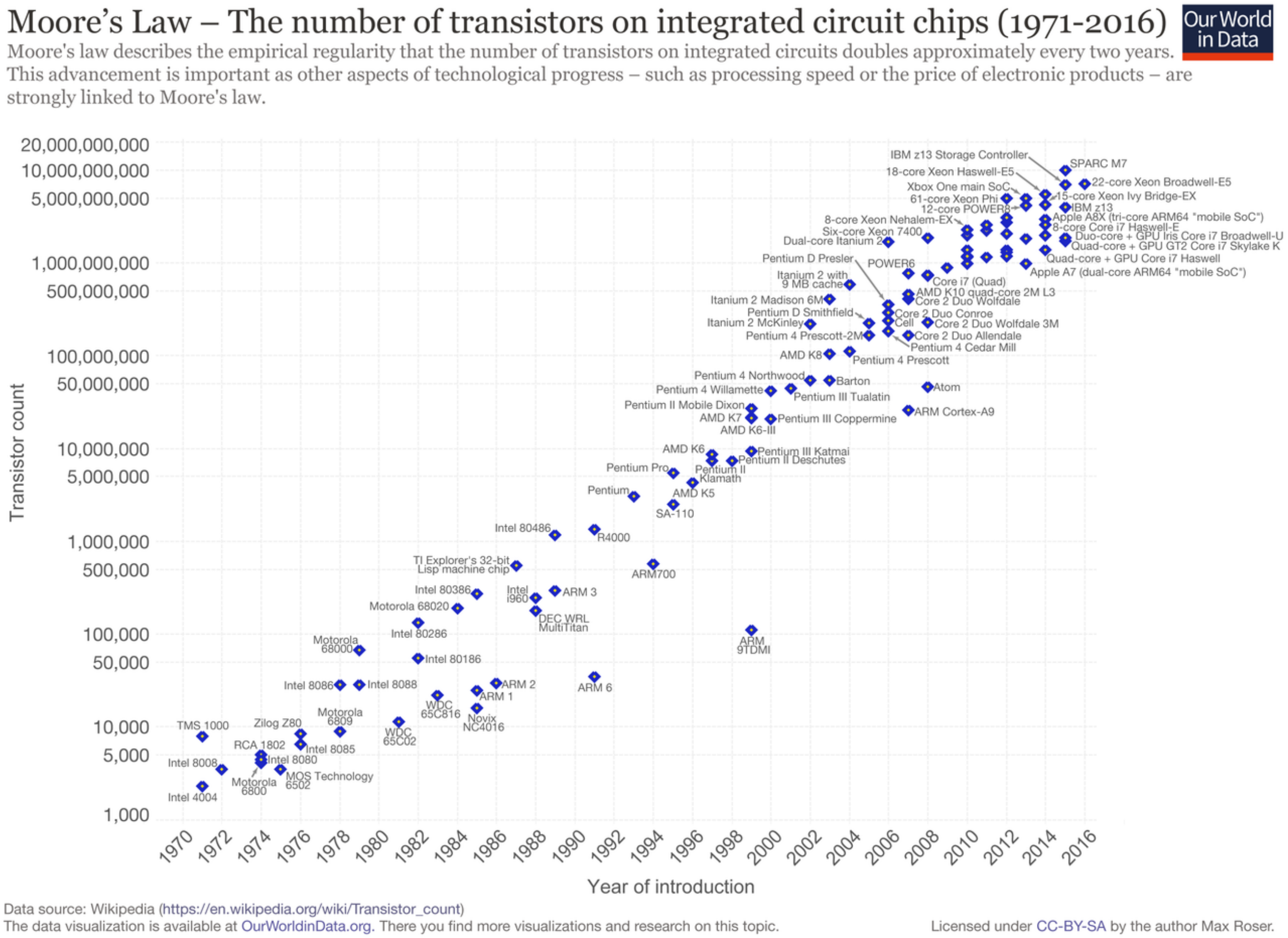
leonardo.castellani@uniupo.it

Contents

1 Lecture 1: Quantum bits (qubits)

1.1 Moore's law

• Gordon Moore's law: since 1950's computer speed doubles and chip dimensions are halved every 2 years approximately. From centimeters of vacuum tubes to micrometers. More precisely number of transistors on integrated circuits doubles approximately every two years. Single electron transistor ≈ 30 nm. Around year 2020 → atomic dimensions. The end of progress?



Moore's Law – The number of transistors on integrated circuit chips (1971-2016)

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are strongly linked to Moore's law.

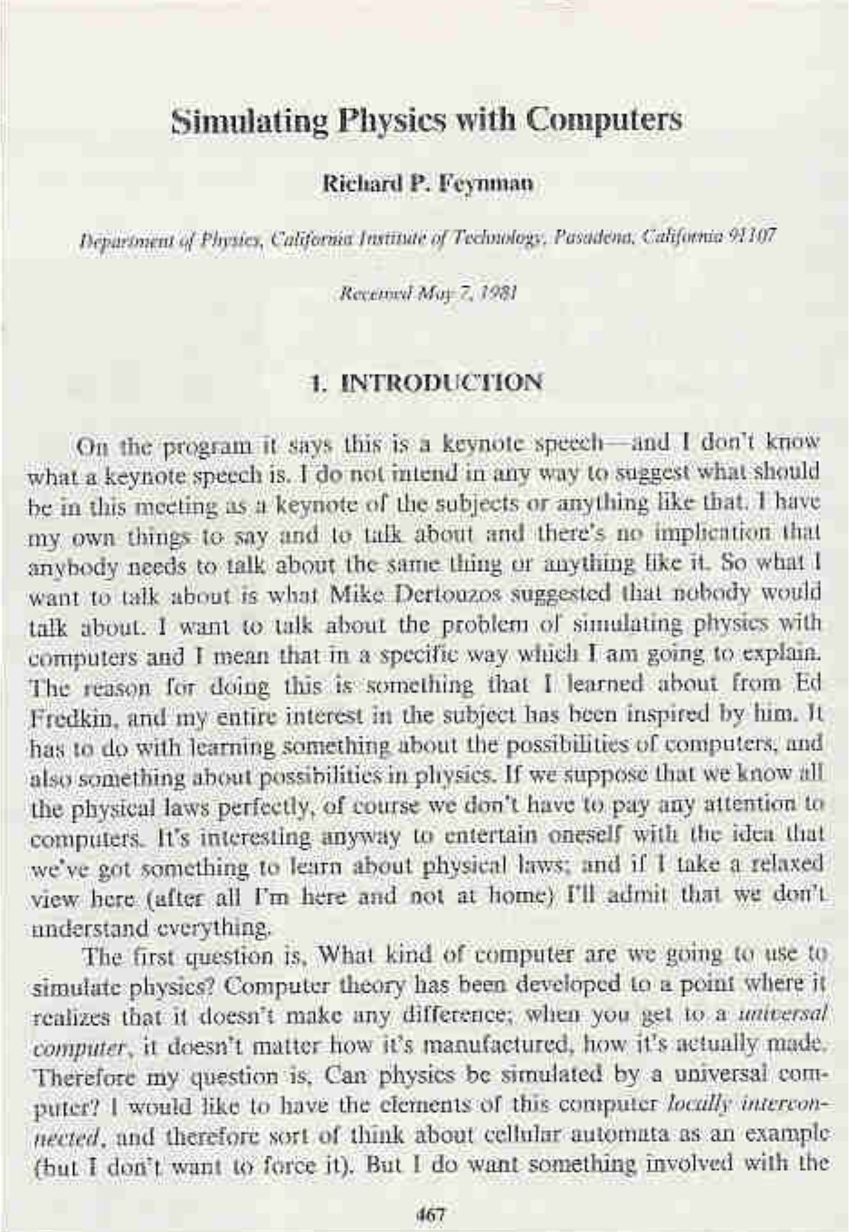
Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

Licensed under CC-BY-SA by the author Max Roser.

Fig. 1.1 Moore's law

1.2 Feynman's 1981 paper

• R. P. Feynman, "Simulating Physics with computers," Int. Jou. Theor. Phys. 21 (1982) 6.



Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain. The reason for doing this is something that I learned about from Ed Fredkin, and my entire interest in the subject has been inspired by him. It has to do with learning something about the possibilities of computers, and also something about possibilities in physics. If we suppose that we know all the physical laws perfectly, of course we don't have to pay any attention to computers. It's interesting anyway to entertain oneself with the idea that we've got something to learn about physical laws; and if I take a relaxed view here (after all I'm here and not at home) I'll admit that we don't understand everything.

The first question is, What kind of computer are we going to use to simulate physics? Computer theory has been developed to a point where it realizes that it doesn't make any difference; when you get to a *universal computer*, it doesn't matter how it's manufactured, how it's actually made. Therefore my question is, Can physics be simulated by a universal computer? I would like to have the elements of this computer *locally interconnected*, and therefore sort of think about cellular automata as an example (but I don't want to force it). But I do want something involved with the

467

Fig. 1.2 Feynman's paper 1981

Classical equations of motion (Newton's):

$$m_i \frac{d^2}{dt^2}\, x_i(t) = F_i(x_1, ...x_N, t) \tag{1.1}$$

require $\sim 2N$ operations at each time step for their numerical integration:

$$\frac{dx_i}{dt}(t + \Delta t) = \frac{dx_i}{dt}(t) + \frac{1}{m_i} F_i(x_1, ...x_N, t)\Delta t \tag{1.2}$$

$$x_i(t + \Delta t) = x_i(t) + \frac{dx_i}{dt}(t)\Delta t \tag{1.3}$$

Schrödinger equation:

$$i\hbar \frac{d}{dt}\psi(x_1, ...x_N, t) = H\psi(x_1, ...x_N, t) \tag{1.4}$$

requires instead $\sim P^N$ operations at each time step for its numerical integration, where each degree of freedom x_i $(i = 1, ...N)$ has been discretized in P points:

$$\psi(x_1, ...x_N, t + \Delta t) = \psi(x_1, ...x_N, t) + \frac{1}{i\hbar} H(x_i, -i\hbar \frac{\partial}{\partial x_i})\psi(x_1, ...x_N, t)\Delta t \tag{1.5}$$

Indeed the discretized support of the wave function ψ has P^N points, and it is necessary to compute ψ in each of these points.

1.3 Quantum bits (qubits)

• Quantum bits, or *qubits*, are quantum systems with a 2-dimensional vector space of physical states. Choosing an orthonormal basis $|0\rangle$, $|1\rangle$, the generic state of a qubit is:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.6}$$

The basis vectors $|0\rangle$ and $|1\rangle$ can be thought of as eigenvectors of some observable acting on qubits. According to the basic rules of quantum mechanics, a measurement of this observable yields the result "0" (i.e. the eigenvalue corresponding to the eigenvector $|0\rangle$) with probability $p(0) = |\alpha|^2$, and the result "1" with probability $p(1) = |\beta|^2$. The state after the measurement collapses into one of the basis states $|0\rangle$ or $|1\rangle$, depending on the result "0" or "1".

Qubits encode information in the complex constants α and β. Note however that we cannot extract this information by a *single* measurement on $|\psi\rangle$. For this purpose, it will be necessary to have many copies of the same qubit, or to manipulate and transform qubits so that results of measurements do depend on α, β.

• The basis vectors $|0\rangle$, $|1\rangle$ are orthonormal, i.e. their scalar products are given by $\langle 0|0\rangle = \langle 1|1\rangle = 1$, $\langle 0|1\rangle = 0$. This basis is called the *computational basis*. Infinitely many other orthonormal basis exist. For example

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.7}$$

1.4 The Bloch sphere

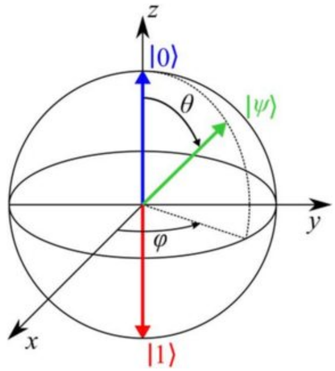


Fig. 1.3 Bloch sphere

- The Bloch sphere provides a geometrical representation of a qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1 \tag{1.8}$$

Writing the complex numbers α and β in the exponential form

$$\alpha = \rho_\alpha e^{i\varphi_\alpha}, \quad \beta = \rho_\beta e^{i\varphi_\beta} \tag{1.9}$$

we have

$$\rho_\alpha^2 + \rho_\beta^2 = 1, \quad \rho_\alpha \geq 0, \quad \rho_\beta \geq 0 \tag{1.10}$$

so that the moduli ρ_α and ρ_β can be parametrized by an angle χ:

$$\rho_\alpha = \cos\chi, \quad \rho_\beta = \sin\chi, \quad 0 \leq \chi \leq \frac{\pi}{2} \tag{1.11}$$

Then the qubit (1.8) takes the form

$$|\psi\rangle = \rho_\alpha e^{i\varphi_\alpha}|0\rangle + \rho_\beta e^{i\varphi_\beta}|1\rangle = e^{i\varphi_\alpha}(\cos\chi\ |0\rangle + e^{i(\varphi_\beta - \varphi_\alpha)} \sin\chi\ |1\rangle) \tag{1.12}$$

We can neglect the overall phase $e^{i\varphi_\alpha}$ (since quantum states are defined up to an overall phase), define $\varphi \equiv \varphi_\beta - \varphi_\alpha$ and $\theta \equiv 2\chi$ (so that θ varies from 0 to π). Then the qubit

$$|\psi\rangle = \cos\frac{\theta}{2}\ |0\rangle + e^{i\varphi} \sin\frac{\theta}{2}\ |1\rangle \tag{1.13}$$

can be represented faithfully on the Bloch sphere, in the sense that there is a 1-1 mapping between qubits and points on the surface of the sphere, labelled by their latitude θ and longitude φ.

1.5 Single qubit gates: $U(2)$

• To use classical or quantum bits for computation, we must be able to transform them. This we can do by acting with classical or quantum logical gates. For example the classical NOT gate negates the bit it acts on, transforming 0 into 1 and viceversa. It is representaed by the symbol

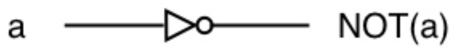


Fig. 1.4 Classical NOT gate

Thus $NOT(0) = 1$, $NOT(1) = 0$.

The quantum analogue is the (linear) operator X, defined by its action on the basis vectors:

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle \tag{1.14}$$

By linearity, its action on a generic superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is given by

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle \tag{1.15}$$

• Any quantum gate U must transform a physical state $|\psi\rangle$ in another physical state $|\psi'\rangle$. Thus the transformed qubit $|\psi'\rangle = U|\psi\rangle$ must have the same unit norm as the original $|\psi\rangle$:

$$\langle\psi'|\psi'\rangle = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle = 1 \tag{1.16}$$

and this requires

$$U^\dagger U = I \tag{1.17}$$

As we know from linear algebra (for a summary of linear algebra tools and notations see Lecture 6), this condition defines *unitary* operators. After choosing a basis, unitary operators acting on qubits can be represented by unitary 2×2 matrices.

• Examples of single qubit gates are the unitary operators X, Y, Z, H, represented (on the computational basis $|0\rangle, |1\rangle$) by the matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1.18}$$

Recalling that the adjoint of a matrix is its transpose complex-conjugated, it is immediate to verify that these matrices are indeed unitary.

• Unitary $N \times N$ matrices form a *group*, denoted by $U(N)$. A group is defined as a set satisfying three properties:

i) existence of a *composition law* $\circ$ that associates to two elements a, b of the set another element c of the set: $a \circ b = c$

ii) existence of an *identity element* I such that $a \circ I = I \circ a = a$ for any a.

iii) existence of an inverse a^{-1} for every element a, such that $a^{-1}a = aa^{-1} = I$

and it is straightforward to check that $U(N)$ is a group with composition law given by matrix multiplication. An important *subgroup* of $U(N)$ is $SU(N)$, the subset of $U(N)$ with determinant = 1, satisfying by itself the group properties (hence a subgroup).

• $U(2)$ matrices depend on 4 real parameters, since the unitarity condition $U^\dagger U = I$ eliminates 4 of the 8 independent real quantities of a 2×2 complex matrix. A convenient parametrization of $U(2)$ matrices is

$$U = e^{i\alpha} \begin{pmatrix} e^{-i\frac{\beta}{2}} & 0 \\ 0 & e^{i\frac{\beta}{2}} \end{pmatrix} \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix} \tag{1.19}$$

Exercise: find the $\alpha, \beta, \gamma, \delta$ parametrization of X, Y, Z, H.

2 Lecture 2: Multiple qubits

2.1 Tensor product

Composite systems are described by *tensor products* of states of the individual systems, when the individual systems are not interacting. We will denote by A and B the individual subsystems, and by AB the total system. Let us briefly justify the use of the tensor product.

Consider two qubits A and B, in the respective individual states

$$|\psi_A\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\psi_B\rangle = \gamma|0\rangle + \delta|1\rangle \tag{2.1}$$

What is the state of the total system ? It must be such that the rules of quantum mechanics correctly predict the outcomes of measurements on the system. Here the probability to obtain result 0 on the first qubit and result 0 on the second qubit is clearly the product of the probabilities $|\alpha|^2$ and $|\gamma|^2$, since the two qubits are not interacting. A similar reasoning holds for the probabilities of obtaining the results (0,1), (1,0) and (1,1), and therefore the state of the total system must be

$$|\Psi_{AB}\rangle = \alpha\gamma|0\rangle|0\rangle + \alpha\delta|0\rangle|1\rangle + \beta\gamma|1\rangle|0\rangle + \beta\delta|1\rangle|1\rangle \tag{2.2}$$

where $|0\rangle|0\rangle$ is the AB state when both qubits are in state $|0\rangle$, $|0\rangle|1\rangle$ is the AB state when qubit A is in state $|0\rangle$ and qubit B is in state $|1\rangle$ etc. Then the rules of QM give the correct probabilities for joint measurements on both qubits in the computational basis[1].

Note that the state (2.2) can be written as a *product* of two individual states:

$$|\Psi_{AB}\rangle = |\psi_A\rangle|\psi_B\rangle = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) \tag{2.3}$$

if this product satisfies the usual distributive properties with respect to the addition (or in other words if the product is linear in both factors). These are the properties of the *tensor product* of vectors, usually indicated by the symbol $\otimes$. The symbol will be often omitted between ket vectors (as in the above discussion) for simplicity of notations. In fact the notation $|0\rangle|0\rangle$ can be further simplified, by writing $|00\rangle$.

2.2 Basis for tensor spaces

A *basis* for the states of system AB is provided by all the tensor products of elements of the A basis with elements of the B basis:

$$|0\rangle|0\rangle, \quad |0\rangle|1\rangle, \quad |1\rangle|0\rangle, \quad |1\rangle|1\rangle \tag{2.4}$$

[1] in fact all terms in (2.2) could be multiplied by an arbitrary phase, and still the probabilities would come out the same. But this holds only for measurements in the computational basis, i.e. of observables with eigenvectors $|0\rangle$ and $|1\rangle$. Choosing another basis, for example the $|+\rangle$, $|-\rangle$ basis for both qubits, we obtain the correct probabilities only if the state is exactly the one in (2.2).

and in general a state of the AB system is expressible as a linear combination:

$$|\Psi\rangle = c_{00}|0\rangle|0\rangle + c_{01}|0\rangle|1\rangle + c_{10}|1\rangle|0\rangle + c_{11}|1\rangle|1\rangle \tag{2.5}$$

where c_{00},... are 4 complex numbers satisfying the condition

$$|c_{00}|^2 + |c_{01}|^2 + |c_{10}|^2 + |c_{11}|^2 = 1 \tag{2.6}$$

The discussion can be easily extended to N-qubit spaces: the state of a system of N qubits is specified by 2^N complex amplitudes subject to a normalization condition as in (2.6). We see here why qubits can potentially encode information in an exponentially more efficient way than classical bits. These latter can only take one precise binary value (or string of binary values for N bits), while N qubits can "contain" in the same state 2^N values.

In general, if V^A and V^B are the vector spaces for the subsystems A and B, the vector space for the composite system AB is called the tensor product of the vector spaces V^A and V^B, denoted by $V^A \otimes V^B$. A basis for $V^A \otimes V^B$ is given by the set $\{|u_i\rangle \otimes |v_j\rangle\}$, where $\{|u_i\rangle\}$ is a basis for V^A and $\{|v_j\rangle\}$ is a basis for V^B, and therefore

$$\dim(V^A \otimes V^B) = (\dim V^A)(\dim V^B) \tag{2.7}$$

2.3 Scalar product

The scalar product between elements of tensor spaces is defined as

$$(|\psi\rangle|\phi\rangle, |\xi\rangle|\chi\rangle) \equiv \langle\psi|\xi\rangle\langle\phi|\chi\rangle \tag{2.8}$$

and satisfies all the properties of a scalar product in complex vector spaces.

Exercise: verify this.

With this definition, the four states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ form an orthonormal basis for a 2-qubit system, and in general the tensor product of N computational bases yields an orthonormal basis for a system of N qubits.

2.4 Measurements by Alice and Bob

Consider the general two-qubit state (2.5), and suppose that Alice can make measurements on the first qubit and Bob on the second. What is the probability that in a joint measurement, Alice finds the result 0 and Bob finds the result 0 ? The answer is given by the standard Born rule:

$$p(0_A, 0_B) = \langle\Psi|P_{00}|\Psi\rangle = |c_{00}|^2, \quad P_{00} = |00\rangle\langle 00| \tag{2.9}$$

a similarly for the other three joint results 01, 10, 11. But suppose now that only Alice makes a measurement on her qubit. Then the probability for her to obtain 0 is:

$$p(0_A) = \langle\Psi|P_{0_A}|\Psi\rangle = |c_{00}|^2 + |c_{01}|^2, \quad P_{0_A} = |00\rangle\langle 00| + |01\rangle\langle 01| \tag{2.10}$$

where P_{0_A} is now the projector on the eigensubspace corresponding to the degenerate eigenvalue 0_A. Similarly the probability for Alice of obtaining 1 is

$$p(1_A) = \langle\Psi|P_{1_A}|\Psi\rangle = |c_{10}|^2 + |c_{11}|^2, \quad P_{1_A} = |10\rangle\langle 10| + |11\rangle\langle 11| \tag{2.11}$$

Analogous formulae hold for measurements performed by Bob.

The collapse after the measurement follows the usual rule, using the projector corresponding to the measurement outcome. For example, if Alice obtains 0, the two-qubit state (2.5) collapses into

$$|\Psi\rangle \;\longrightarrow\; \frac{P_{0_A}|\Psi\rangle}{\sqrt{\langle\Psi|P_{0_A}|\Psi\rangle}} = \frac{c_{00}|0\rangle|0\rangle + c_{01}|0\rangle|1\rangle}{\sqrt{|c_{00}|^2 + |c_{01}|^2}} \tag{2.12}$$

2.5 Entangled states and correlations

A state of a composite system is said to be a *separable* or *product state* if it can be written as a tensor product:

$$|\Psi\rangle = |\phi\rangle|\xi\rangle \tag{2.13}$$

A state of a composite system is *entangled* if it is not separable. For example

$$\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{2.14}$$

is separable, since it can be written as

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \tag{2.15}$$

On the other hand the state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.16}$$

is entangled, since it cannot be written as a product.

- **Exercise:** verify this. Hint: use (2.3).

Suppose that Alice and Bob measure their qubits when the composite system is in the state (2.14). If Alice makes the first measurement, she will find 0 or 1 with probability 1/2, and the global state collapses into $|00\rangle$ or $|10\rangle$ according to the result. In both cases a successive measurement by Bob will certainly yield the outcome 0, without further collapse. If Bob makes the first measurement, he will certainly obtain 0, the global state remains the same, and a successive measurement by Alice has 1/2 probabilities of obtaing 0 or 1. Thus the statistics for Alice and Bob are *uncorrelated*, i.e. they do not depend on the order of the measurements, or in other words the results of Alice do not depend on the results of Bob and viceversa.

The situation changes drastically if the initial state is entangled. Then the individual qubits are not in definite states: only the global state of the system is given. If Alice makes the first measurement on her qubit when the system is in the entangled state (2.16), she finds 0 or 1 with probability 1/2. But a successive measurement by Bob will have an outcome that depends on the result of Alice. Indeed, if Alice obtains 0, the global state collapses into $|00\rangle$, and a successive measurement by Bob yields 0. If Alice obtains 1, the global state collapses into $|11\rangle$, and a successive measurement by Bob yields 1. In this case the results of measurements by Alice and Bob are *correlated*. The same happens if Bob makes the first measurement.

The entangled qubits could be spatially separated, still remaining in an entangled global state. Could Alice send a message to a distant Bob exploiting the correlations and the collapse of the global state ? After all, if her measuring or not measuring could be detected by Bob instantaneously, Alice could communicate with superluminal velocity with Bob, contradicting a fundamental result of special relativity. Consider the entangled state (2.16): if Alice *does not measure* her qubit, the statistics for Bob measurements will be 1/2 probability to obtain 0 and 1/2 probability to obtain 1. On the other hand if Alice does measure her qubit, she will produce a collapse of the global state into $|00\rangle$ with probability 1/2, and to $|11\rangle$ with probability 1/2. Then if Bob measures his qubit, he will still find 0 with 1/2 probability and 1 with 1/2 probability, exactly the same statistics as before. Thus the act of measurement by Alice cannot be detected by Bob, and special relativity is safe.

Exercise:

i) if

$$|0\rangle = \alpha|a\rangle + \beta|b\rangle \tag{2.17}$$
$$|1\rangle = \gamma|a\rangle + \delta|b\rangle \tag{2.18}$$

prove that

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|aa\rangle + |bb\rangle}{\sqrt{2}} \tag{2.19}$$

when the matrix

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{2.20}$$

is orthogonal.

ii) prove that

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = \det(A)\frac{|ab\rangle - |ba\rangle}{\sqrt{2}} \tag{2.21}$$

when the matrix A is unitary.

As a consequence:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|++\rangle + |--\rangle}{\sqrt{2}} \tag{2.22}$$

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = -\frac{|+-\rangle - |-+\rangle}{\sqrt{2}} \tag{2.23}$$

3 Lecture 3: Quantum gates

3.1 Classical and quantum computation

Classical circuits are made out of wires and logical gates (AND, OR, NOT etc..), and are read from left to right:

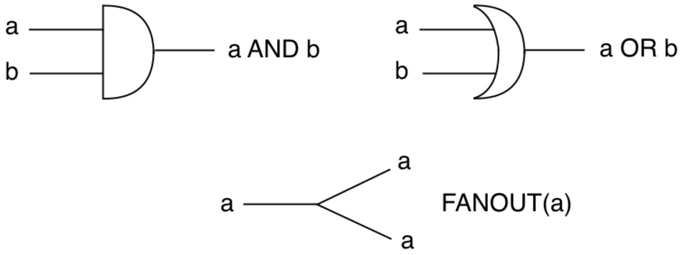


Fig. 3.1 Classical gates

The same conventions hold for quantum circuits, with classical gates replaced by quantum gates, effecting unitary operations on N-qubit states (and therefore represented by $2^N \times 2^N$ matrices). An important difference with respect to classical gates is their *reversibility*, since unitary operations are invertible. This implies that N-qubit gates transform N-qubit states into N-qubit states, whereas classical gates can transform N bits into M bits, with N not necessarily equal to M (for example the AND gate transforms 2 bits into 1 bit).

3.2 2-qubit gates: CNOT, Entangler, Exchanger

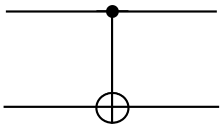


Fig. 3.2 CNOT gate

CNOT$|00\rangle = |00\rangle$, CNOT$|01\rangle = |01\rangle$, CNOT$|10\rangle = |11\rangle$, CNOT$|11\rangle = |10\rangle$.

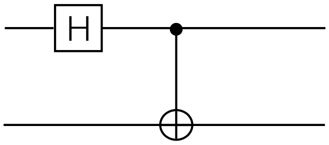


Fig. 3.3 Entangler gate, produces the Bell states

$$Entangler|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \equiv |\beta_{00}\rangle \tag{3.1}$$

$$Entangler|01\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \equiv |\beta_{01}\rangle \tag{3.2}$$

$$Entangler|10\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \equiv |\beta_{10}\rangle \tag{3.3}$$

$$Entangler|11\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \equiv |\beta_{11}\rangle \tag{3.4}$$

The states $|\beta_{ij}\rangle$ are entangled, and form an orthonormal basis (the *Bell basis*) for 2 qubit states.

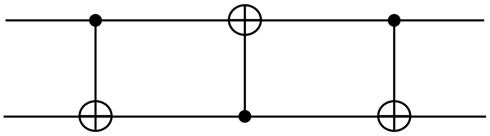


Fig. 3.4 Exchanger gate: exchanges the two qubits

• **Exercise**: show that

$$Exchanger|\psi\rangle|\chi\rangle = |\chi\rangle|\psi\rangle \tag{3.5}$$

for any two qubits $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\chi\rangle = \gamma|0\rangle + \delta|1\rangle$.

• **Exercise**: find the matrix representation of CNOT, Entangler and Exchanger.

3.3 No cloning theorem

The classical FANOUT gate yields two copies of the same bit. On the quantum side, however, no unitary operation can clone an unknown qubit. Indeed suppose a cloning machine U existed, transforming any qubit $|\psi\rangle$ tensored with a service qubit $|s\rangle$ into $|\psi\rangle|\psi\rangle$. The service qubit, a part of the cloning machine, is necessary since U is unitary, so that if the output is a 2-qubit state also the input must be a 2-qubit state. Then

$$U|\psi\rangle|s\rangle = |\psi\rangle|\psi\rangle \tag{3.6}$$

$$U|\phi\rangle|s\rangle = |\phi\rangle|\phi\rangle \tag{3.7}$$

for two different qubits $|\psi\rangle, |\phi\rangle$. The scalar product of the left hand sides:

$$(U|\psi\rangle|s\rangle, U|\phi\rangle|s\rangle) = (|\psi\rangle|s\rangle, |\phi\rangle|s\rangle) = \langle\psi|\phi\rangle\langle s|s\rangle = \langle\psi|\phi\rangle \tag{3.8}$$

must be equal to the scalar product of the right hand sides:

$$(|\psi\rangle|\psi\rangle, |\phi\rangle|\phi\rangle) = \langle\psi|\phi\rangle\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2 \tag{3.9}$$

Thus the machine U can clone qubits satisfying

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2 \tag{3.10}$$

with the only solution $\langle\psi|\phi\rangle = 0$, i.e. only for orthogonal qbits. (another solution would be $\langle\psi|\phi\rangle = 1$, excluded since $|\psi\rangle \neq |\phi\rangle$, cf. Schwarz inequality).

3.4 Non orthogonal states cannot be distinguished

If two quantum states are orthogonal, a measurement in the basis that includes these states will distinguish them. For example the 1-qubit states $|0\rangle$ and $|1\rangle$ can be distinguished by a measurement in the computational basis. On the contrary, if the quantum states are not orthogonal, it is impossible to distinguish them with any measurement: consider the non orthogonal qubit states

$$|0\rangle, \quad \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{3.11}$$

A measurement in the computational basis cannot distinguish them (the result 0 can be obtained for both states), and it is easy to prove that this holds in any basis.

• **Exercise:** prove that the existence of a cloning machine would allow to distinguish non-orthogonal states (and viceversa).

• **Exercise :** prove that a cloning machine (or equivalently a machine that distinguishes non orthogonal states) could be used for superluminal communication using the entangled 2-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{|++\rangle+|--\rangle}{\sqrt{2}}$.

3.5 Quantum money

This limitation can become a resource, and solve, at least in principle, the problem of printing banknotes that cannot be counterfeited. It is sufficient to "print" on every banknote a string of qubits in the states (3.11), each banknote having a different string, associated to a serial number appearing on the banknote. Since non-orthogonal states cannot be cloned, the banknote cannot be duplicated, and its authenticity can be checked by contacting the bank, where the list of correspondences (qubit string $\longleftrightarrow$ serial number) is kept secure. The bank then directs a sequence of measurements (depending on the serial number) in the appropriate computational or oblique basis, adapted to the sequence of states, so that all measurements must have results 0 or + only if the banknote is the original one. Failure to obtain the correct results, above a threshold due to experimental errors, signals that the banknote is false.

4 Lecture 4

4.1 Superdense coding (Bennet and Wiesner 1992)

Suppose that Alice and Bob share an entangled pair of qubits in the state (2.16). Then Alice can communicate 2 classical bits of information to Bob, by sending him just one qubit, the qubit in her possession. Before sending it to Bob, Alice performs on her qubit one of four operations:

nothing - if she wants to communicate the message 00
apply Z - if she wants to communicate the message 01
apply X - if she wants to communicate the message 10
apply iY - if she wants to communicate the message 11

By so doing, Alice is transforming the original entangled state $|\beta_{00}\rangle$ in one of the four Bell states $|\beta_{ij}\rangle$. When Bob receives the qubit of Alice, he can make measurements on the 2-qubit system in the (orthonormal) Bell basis, thus recognizing the particular Bell state that corresponds to the message of Alice.

This protocol is called *superdense coding*, and exemplifies the possibility of "squeezing" classical information into qubits, using less qubits than the bits necessary for the classical message.

4.2 Teleportation (Bennet et al. 1993)

The teleportation protocol allows Alice to "send" an unknown qubit $|\psi\rangle$ to Bob without using a quantum channel, i.e. without physically sending the qubit, but using only a classical channel, as for example a phone communication. To achieve this, Alice and Bob share a pair of qubits in the entangled state $|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Alice entangles her qubit with the unknown qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ she wants to teleport, using a CNOT gate. She then applies the Hadamard gate to the first qubit (the qubit that originally was in the state $|\psi\rangle$) and measures the two qubits. After this, Alice telephones the result of her meaurements to Bob. According to the result 00, 01, 10, 11 communicated by Alice, Bob effects one of four operations on his qubit , respectively I, Z, X, ZX, and by so doing transforms the state of his qubit exactly in the state $|\psi\rangle$ of the qubit originally owned by Alice.

The corresponding quantum circuit is

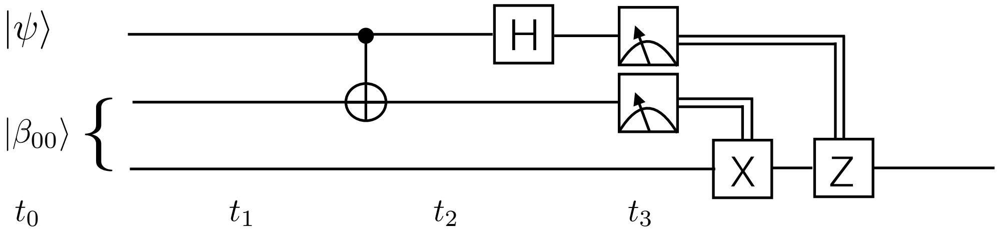


Fig. 4.1 Teleportation circuit

a 3-qubit circuit where the upper two qubits belong to Alice and the lower qubit belongs to Bob. By following the evolution of the initial 3-qubit state $(\alpha|0\rangle + \beta|1\rangle)\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ across the CNOT and H gates, one finds that the 3-qubit state before Alice measurements is

$$\frac{1}{2}\left[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle)+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle)\right] \tag{4.1}$$

A measurement by Alice produces a collapse into one of the four states contained in this superposition. For example if Alice measures 01 the state (4.1) collapses into

$$|01\rangle(\alpha|1\rangle+\beta|0\rangle) \tag{4.2}$$

This state is a product state, with Bob's qubit in the state

$$\alpha|1\rangle+\beta|0\rangle \tag{4.3}$$

Alice phones her result 01 to Bob, so that Bob learns that his qubit is in the state (4.3). He therefore applies to it the gate X and reconstructs the original $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ state.

• **Observations:**

i) the state $|\psi\rangle$ is teleported at a speed always $\leq c$, since it is limited by the speed of the classical communication.

ii) the original state $|\psi\rangle$ owned by Alice gets destroyed (by measurement), so that there is no violation of the no cloning theorem.

iii) teleportation is not vulnerable to noise, since it does not use a physical carrier. (The classical part of the protocol, i.e. communication of Alice' results to Bob, could be disturbed by classical causes).

5 Lecture 5

5.1 Quantum parallelism

Quantum gates implement linear operations, and therefore can operate in parallel on all the states contained in a superposition. Consider a Boolean function f, i.e. a function taking N bits into 1 bit. Thus the domain of f is the set of binary N-bit integers x and the image is $\{0,1\}$. By $|x\rangle$ we denote the N-qubit state specified by the string of 0's and 1's in x: thus for N=4 if $x = 0110$, then $|x\rangle = |0\rangle|1\rangle|1\rangle|0\rangle$. We define now a unitary N+1 qubit operator U_f that acts on the computational basis of N+1 qubits as follows:

$$U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle \tag{5.1}$$

where $\oplus$ denotes addition modulo 2. If the input N+1 qubit state is a "democratic" superposition of all the states of the computational basis, tensored with $|0\rangle$, we find

$$U_f(\frac{1}{\sqrt{2^N}}\sum_x |x\rangle|0\rangle) = \frac{1}{\sqrt{2^N}}\sum_x |x\rangle|f(x)\rangle \tag{5.2}$$

We see that applying U_f only once has produced a state containing *all the values* of the function f, an operation that classically would require 2^N evaluations of the function f, one for each value of the variable x. But extracting this information from the output state is not so easy. Measuring the N+1 qubit output state in the computational basis yields a particular value for x, giving the corresponding value for $f(x)$, and destroys all the rest of the information (all the other $x, f(x)$ values). We will see in next Section how interference may be used to recover more information.

The superposed state $\frac{1}{\sqrt{N}}\sum_x |x\rangle$ can be easily obtained by using N Hadamard gates on N qubits in the state $|0\rangle$:

$$(H \otimes H \otimes ... \otimes H)|0\rangle|0\rangle...|0\rangle = \frac{1}{\sqrt{2^N}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)...(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^N}}\sum_x |x\rangle \tag{5.3}$$

The combined action of the Hadamard gates and the U_f operator is represented by the following circuit:

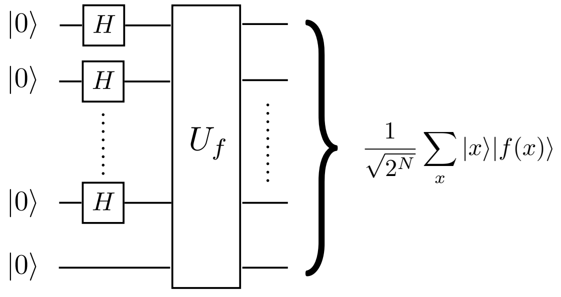


Fig. 5.1 Parallel evaluation of a Boolean function f

- **Exercise:** prove that U_f is unitary.

- **Exercise:** find the circuit that implements U_f when $N = 1$.

5.2 Deutsch algorithm

This algorithm allows to find whether a function f is constant or nonconstant, by combining parallelism and interference. Consider the circuit:

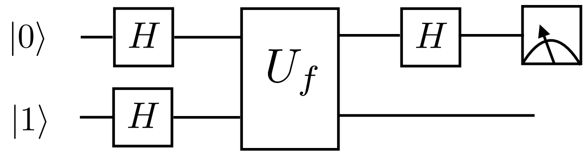


Fig. 5.2 Circuit for Deutsch's algorithm f

where U_f is defined in (5.1). Following the evolution of the initial 2-qubit state $|0\rangle|1\rangle$ through the unitary gates yields as final state:

$$\frac{|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle}{\sqrt{2}} = \pm\,|0\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \text{if } f(0) = f(1) \tag{5.4}$$

$$\frac{|1\rangle|f(0)\rangle - |1\rangle|f(1)\rangle}{\sqrt{2}} = \pm\,|1\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \text{if } f(0) \neq f(1) \tag{5.5}$$

or in a single formula:

$$\pm|f(0) \oplus f(1)\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{5.6}$$

Thus by measuring the first qubit we can determine whether the function f is constant (result 0) or nonconstant (result 1). Constancy of f is a global property, and classically two evaluations of f would be necessary to establish it, while a single application of Deutsch's quantum circuit is sufficient.

5.3 Deutsch-Jozsa algorithm

Combining together the two preceding Sections leads to a generalization of the Deutsch algorithm, due to Deutsch and Jozsa. The circuit is:

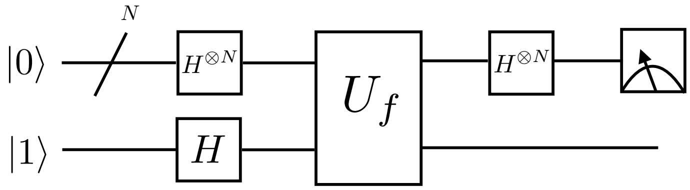


Fig. 5.3 Circuit for Deutsch-Jozsa algorithm f

where the slash in the first line indicates N qubits in the first register. The input state is a $N+1$ qubit state $|0...0\rangle|1\rangle$, with $|0...0\rangle$ = the state of N qubits all initialized to $|0\rangle$. The $N+1$ qubit state emerging from the first battery of H gates is

$$\frac{1}{\sqrt{2^N}}\sum_{x=0}^{2^N-1}|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{5.7}$$

which becomes, after applying U_f:

$$\frac{1}{\sqrt{2^N}}\sum_{x=0}^{2^N-1}|x\rangle\frac{|f(x)\rangle-|1\oplus f(x)\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2^N}}\sum_{x=0}^{2^N-1}(-1)^{f(x)}|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{5.8}$$

Observe now that the action of $H^{\otimes N}$ on $|x\rangle=|x_1\rangle|x_1\rangle...|x_N\rangle$:

$$H^{\otimes N}|x\rangle=\frac{1}{\sqrt{2^N}}(|0\rangle+(-1)^{x_1}|1\rangle)\;(|0\rangle+(-1)^{x_2}|1\rangle)\;...\;(|0\rangle+(-1)^{x_N}|1\rangle) \tag{5.9}$$

can also be written as

$$H^{\otimes N}|x\rangle=\frac{1}{\sqrt{2^N}}\sum_{y=0}^{2^N-1}(-1)^{x\cdot y}|y\rangle \tag{5.10}$$

with the definition

$$x\cdot y\equiv x_1y_1\oplus x_2y_2\oplus...\oplus x_Ny_N \tag{5.11}$$

Then the state of the first N-qubit register before the measurement is

$$\frac{1}{2^N}\sum_{y=0}^{2^N-1}\left[\sum_{x=0}^{2^N-1}(-1)^{f(x)}(-1)^{x\cdot y}\right]|y\rangle \tag{5.12}$$

Thus the probability of finding $0,0,...0$ in a measurement of the first register (N qubits) is

$$p(0,0,...0)=\left|\frac{1}{2^N}\sum_{x=0}^{2^N-1}(-1)^{f(x)}\right|^2 \tag{5.13}$$

This probability is 1 if $f(x)$ is *constant*, and is 0 if $f(x)$ is *balanced*, i.e. with an equal number of values 1 and 0. Then by measuring the first register (N measurements) we can find whether f is constant or not. The total number of operations grows linearly with N, even considering the H gates in the circuit 5.3, and only one "run" of U_f is necessary.

By contrast, to obtain this information classically would require 2^N evaluations of the function f, growing exponentially with N.

5.4 Qubit carriers: polarized photons, electrons

Many microscopic two-level systems can be considered qubits. Each has its own advantages and difficulties, due to conflicting requirements for their use in computation: on one hand physical qubits must be well protected from environmental disturbances, to prevent decoherence, on the other hand they must be accessible to controlled interaction, to implement the action of quantum gates.

Two examples of physical qubits are provided by photons and electrons, in their states of polarization and spin, respectively.

5.4.1 Polarized photons

The classical description of a plane wave of electromagnetic radiation is given by varying electric $\vec{E}$ and magnetic $\vec{B}$ fields, orthogonal to each other, in the plane perpendicular to the propagation of the wave. The direction of $\vec{E}$ defines the *polarization*. If $\vec{E}$ makes an angle θ with a conventional direction (for example the y direction) we say that the polarization is θ. The electric field, for linearly polarized radiation, can be written as

$$\vec{E} = \sin\theta \; Ee^{i(kz-\omega t)}\hat{x} + \cos\theta \; Ee^{i(kz-\omega t)}\hat{y} \tag{5.14}$$

where E is the modulus of $\vec{E}$, the exponential $\exp[i(kz-\omega t)]$ corresponds to a plane wave propagating in the z direction with frequency ω, and $\hat{x}$, $\hat{y}$ are unit vectors in the x and y directions, cf. Fig. 5.3. Note the complex notation for the electric field, a convenient technique that simplifies computations. The real electric field can be recovered by taking the real part of (5.14). The radiation described by (5.14) is linearly polarized since the direction of $\vec{E}$ does not change in time. The (real) components of $\vec{E}$ are given by:

$$E_x(t) = E\sin\theta\cos(\omega t), \qquad E_y(t) = E\cos\theta\cos(\omega t) \tag{5.15}$$

where we have taken the field in the origin $z = 0$. The two components oscillate in phase and the resultant field oscillates along the fixed direction θ.

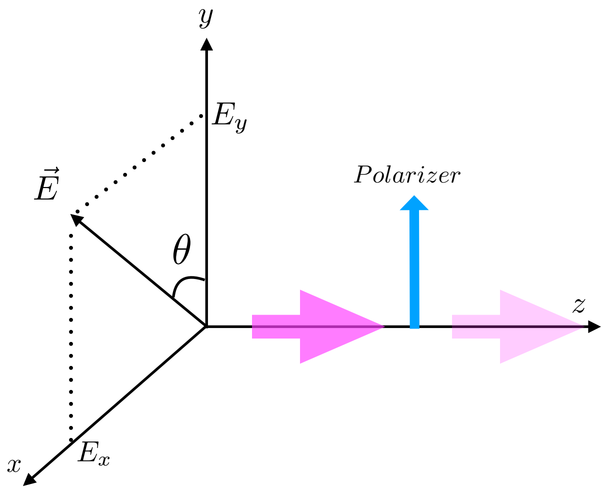


Fig. 5.4 Polarized radiation

The *intensity* of the radiation in (5.14) is proportional to $|\vec{E}|^2 = \vec{E}^* \cdot \vec{E} = E^2$. Suppose that a polarizer, oriented vertically, is placed in the path of the radiation. By definition, the vertical polarizer kills the horizontal x-component of the radiation in (5.14), and the emergent intensity is therefore reduced by a factor $\cos^2\theta$. This is the *Malus law* for linearly polarized radiation.

The electric field for a horizontally polarized radiation is $\vec{E} = Ee^{i(kz-\omega t)}\hat{x}$ and for a vertically polarized radiation is $\vec{E} = Ee^{i(kz-\omega t)}\hat{y}$. The superposition of these two functions, with weights $\sin\theta$ and $\cos\theta$ respectively, yields the total electric field.

Radiation in quantum mechanics is carried by *photons*: they are undivisible elementary quanta of the electromagnetic field. The probability of finding a photon in a given spacetime point x, y, z, t is proportional to the intensity of the classical radiation, which plays therefore the role of a square modulus of a wavefunction. This means that we can consider the electric field as the "wavefunction of the photon". We can then assign a ket vector $|0\rangle$ to the horizontally polarized photon with wavefunction $\psi_x = Ee^{i(kz-\omega t)}\hat{x}$ and a ket vector $|1\rangle$ to the vertically polarized photon with wavefunction $\psi_y = Ee^{i(kz-\omega t)}\hat{y}$. Then the photon linearly polarized in the θ direction has wavefunction $\psi = \sin\theta\psi_x + \cos\theta\psi_y$. Calling $|\theta\rangle$ the ket corresponding to ψ (photon θ-polarized) we have:

$$|\theta\rangle = \sin\theta|0\rangle + \cos\theta|1\rangle \tag{5.16}$$

Thus the polarization states of the photons are described quantum mechanically by kets living in a two dimensional space, with computational basis given by $|0\rangle$ (horizontal polarization) and $|1\rangle$ (vertical polarization). Photons are therefore good candidates to represent qubits.

Ket vectors can be assigned also to other types of polarization. The direction of the electric field can vary over time, describing for example a circle in the xy plane.

Consider the electric field:

$$\vec{E} = \frac{1}{\sqrt{2}}\ Ee^{i(kz-\omega t)}\hat{x} + \frac{i}{\sqrt{2}}\ Ee^{i(kz-\omega t)}\hat{y} \tag{5.17}$$

The $i = e^{\frac{i\pi}{2}}$ factor in front of the second term produces a phase shift in the y-component of $\vec{E}$, and we find:

$$E_x = \frac{E}{\sqrt{2}}\cos\omega t, \qquad E_y = \frac{E}{\sqrt{2}}\cos(\omega t - \frac{\pi}{2}) = \frac{E}{\sqrt{2}}\sin\omega t \tag{5.18}$$

describing an electric field rotating in the xy plane, clockwise (left rotation), with angular velocity ω. Similarly we obtain an anticlockwise (right) rotation when $-i$ multiplies the second term. Thus the two (orthonormal) vectors

$$|L\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle, \quad |R\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle \tag{5.19}$$

describe left and right circularly polarized photons.

Note: the electric fields $\vec{E}$ in (5.14) and (5.17) are both solutions of the Maxwell equations in vacuum.

5.4.2 Electrons

The electron is an elementary particle with spin 1/2, which implies that its spin states belong to a 2-dimensional vector space. Then also the spin states of the electron can play the role of qubit states. Conventionally the computational basis is taken to be the one of the eigenvectors of S_z, the spin along z. The spin observables are represented on this basis by the 2×2 matrices

$$S_x = \frac{\hbar}{2}X, \quad S_y = \frac{\hbar}{2}Y, \quad S_z = \frac{\hbar}{2}Z \tag{5.20}$$

where X, Y, Z are the 2×2 Pauli matrices already defined in (1.18).

6 Lecture 6: Topics in linear algebra

We give here a list, in logical order, of the basic notions in linear algebra that we need in Quantum Mechanics, and we assume to be well-known:

- Complex vector spaces, ket notation $|v\rangle$. Vector subspaces.

- Linear independence. Basis.

- Representation of vectors on a basis, components.

- Linear operators, their matrix representation on a basis.

- Scalar product

- Linear functionals. Bra vectors: $\langle v|$, their representation.

- Orthogonality, norm, orthonormal basis, Gram-Schmidt procedure.

- Scalar product in components.

- Definition of ket-bra operator $|v\rangle\langle w|$. Projectors.

- Completeness relation

- Schwarz inequality, triangular inequality.

- Adjoint operator

- Self-adjoint (hermitian) and unitary operators.

- Change of basis. Determinant and Trace of an operator.

- Eigenvalues and eigenvectors of a linear operator. Characteristic equation.

- Normal operators, spectral theorem, spectral representation.

- Positive operators (see below).

- Functions of operators (see below).

- Polar and singular decomposition of an arbitrary matrix (see below).

- Schmidt decomposition (will be discussed in Lecture 10)

6.1 Positive operators

Definition: an operator A is *positive* if $\langle v|A|v\rangle$ is a real number ≥ 0, $\forall\ |v\rangle$.

Theorem: a positive operator is hermitian.

Proof: any operator A can be written as a sum of hermitian and antihermitian parts $A = \frac{A+A^\dagger}{2} + \frac{A-A^\dagger}{2}$ or also $A = B + iC$ with B and C both hermitian. Thus if A is positive, for any $|v\rangle$ we have $\langle v|B|v\rangle + i\langle v|C|v\rangle =$ real number ≥ 0, but since both $\langle v|B|v\rangle$ and $\langle v|C|v\rangle$ are real numbers (because B and C are hermitian), C must be absent (otherwise $\langle v|A|v\rangle$ would not be real). Then A must contain only the hermitian part B, i.e. A is hermitian. □

Example: $A^\dagger A$ is a positive operator for any operator A (the proof is immediate).

6.2 Functions of operators

Given a function $f(x)$ of a real variable x, we can define the function of the operator A, $f(A)$, by using the spectral decomposition of A:

$$A = \sum_i a_i P_{a_i}, \qquad f(A) \equiv \sum_i f(a_i) P_{a_i} \tag{6.1}$$

where a_i are the eigenvalues of A, and P_{a_i} the projectors on the eigensubspaces corresponding to the eigenvalues a_i. This definition can be implemented only when A is normal (i.e. commutes with its adjoint), so that its eigenvectors form an orthonormal basis and A has a spectral representation. If this is not the case, a definition of $f(A)$ can be given in terms of a power series (when $f(x)$ can be expanded in a power series). For example if $f(x) = e^x$,

$$e^A = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + ... \tag{6.2}$$

a well-defined operator since A^n always exists.

6.3 Polar decomposition

Theorem: any matrix A admits the decomposition

$$A = UJ = KU \tag{6.3}$$

where U is a unitary matrix, and J, K are positive operators defined by

$$J = \sqrt{A^\dagger A}, \quad K = \sqrt{AA^\dagger} \tag{6.4}$$

Moreover, if A is invertible, U is unique. Note: $A^\dagger A$, $AA^\dagger$ being positive and therefore normal, their square root is well defined through the spectral decomposition, where positive square roots of the eigenvalues are used.

Proof: $J = \sqrt{A^\dagger A}$ has the spectral decomposition $J = \sum_i \lambda_i |i\rangle\langle i|$ with $\lambda_i \geq 0$. Defining $|\psi_i\rangle \equiv A|i\rangle$, we have $\langle\psi_i|\psi_i\rangle = \lambda_i^2$ and thus $A|i\rangle = 0$ when $\lambda_i = 0$. Consider the indices i for which $\lambda_i > 0$, and define $|e_i\rangle \equiv \frac{|\psi_i\rangle}{\lambda_i}$. Then $\langle e_i|e_j\rangle = \frac{\langle i|A^\dagger A|j\rangle}{\lambda_i\lambda_j} = \frac{\langle i|J^2|j\rangle}{\lambda_i\lambda_j} = \delta_{ij}$. Using the Gram-Schmidt procedure, we extend the set $\{|e_i\rangle\}$ to a complete orthonormal basis, again indicated by $\{|e_i\rangle\}$.

Consider now the unitary operator $U = \sum_i |e_i\rangle\langle i|$. When $\lambda_i \neq 0$ we find $UJ|i\rangle = \lambda_i|e_i\rangle = |\psi_i\rangle = A|i\rangle$. When $\lambda_i = 0$, we find $UJ|i\rangle = 0 = A|i\rangle$ (recall $A|i\rangle = 0$ when $\lambda_i = 0$). Thus A and UJ have the same action on the basis $|i\rangle$, and therefore coincide $\Rightarrow A = UJ$.

If A is invertible, so is J (since $A = UJ$ and U is invertible being unitary). Then U is unique and equal to AJ^{-1}.

Finally, $A = UJ = UJU^\dagger U = KU$, with $K = UJU^\dagger$, and since $AA^\dagger = KUU^\dagger K = K^2$ (K is positive, hence hermitian), we find $K = \sqrt{AA^\dagger}$. □

6.4 Singular decomposition

Theorem: for any square matrix A, there exist unitary matrices U and V, and a diagonal matrix D with elements ≥ 0 such that

$$A = UDV \tag{6.5}$$

The diagonal elements of D are called the *singular values* of A.

Proof: using the polar decomposition we find $A = SJ$ with S unitary and J positive. From the spectral theorem we have $J = TDT^\dagger$ with T unitary and D diagonal with elements ≥ 0. Setting $U = ST$, $V = T^\dagger$ the theorem is proved, since $A = SJ = STDT^\dagger$. □

7 Lecture 7: Measurement

7.1 The rules of Quantum Mechanics: summary

• State: represented by a ket vector $|\psi\rangle$, normalized $\langle\psi|\psi\rangle = 1$

• Physical quantities (observables): hermitian operators.

• Possible results of a measurement of the observable A: its eigenvalues a_i.

• Probability of obtaining a_i in measuring A on state $|\psi\rangle$:

$$p(a_i) = \langle\psi|P_{a_i}|\psi\rangle \tag{7.1}$$

with P_{a_i} = projector on eigensubspace corresponding to the eigenvalue a_i.

• State after measurement (collapse):

$$|\psi\rangle \longrightarrow \frac{P_{a_i}|\psi\rangle}{\sqrt{\langle\psi|P_{a_i}|\psi\rangle}} \tag{7.2}$$

• Schrödinger equation:

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle \tag{7.3}$$

with H = Hamiltonian.

Note 1: the expectation value of an observable A is given by

$$\langle A\rangle = \sum_{a_i} p(a_i)a_i = \sum_{a_i}\langle\psi|P_{a_i}|\psi\rangle a_i = \langle\psi|A|\psi\rangle \tag{7.4}$$

where we have used the spectral decomposition $A = \sum_{a_i} a_i P_{a_i}$.

Note 2: while the action of quantum gates (or of time evolution according to Schrödinger equation) is unitary, measurement on the contrary is not a unitary operation, but a projection. This clash has generated many of the discussions on the foundational issues of quantum mechanics.

7.2 Generalized measurements

A generalization of *projective measurements* described by projectors P_{a_i} (see 7.1), useful to describe the the statistics and effect of measurement on *subsystems*. Projectors are replaced by *measurement operators* M_m, where m refers to the result of the measurement. These operators are in 1-1 correspondence with the possible measurement outcomes.

The rules in 7.1 are generalized as follows:

• Quantum measurements are described by a set $\{M_m\}$ of *measurement operators*. If the state of the system is $|\psi\rangle$, the probability of obtaining the result m is

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{7.5}$$

The operators M_m satisfy the condition

$$\sum_m M_m^\dagger M_m = I \tag{7.6}$$

so that $\sum_m p(m) = 1$, as is required if $p(m)$ are probabilities.

• The state after the measurement is:

$$|\psi\rangle \longrightarrow \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \tag{7.7}$$

Note: the usual projective measurements are recovered by identifying the measurement operators with the projectors of 7.1. The M_m however are not, in general, projectors.

7.3 An example

Consider a qubit A in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, and a qubit B in the state $|0\rangle$ The state of the composite system AB is

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|00\rangle + \beta|10\rangle \tag{7.8}$$

Next we entangle system A with system B via a CNOT gate, and then perform projective measurements on B. The CNOT gate yields the state

$$|\Psi\rangle = CNOT(\alpha|00\rangle + \beta|10\rangle) = \alpha|00\rangle + \beta|11\rangle \tag{7.9}$$

We now measure qubit B in the $|+\rangle, |-\rangle$ basis. It is then convenient to re-express the 2-qubit state (7.9) as:

$$\begin{aligned}|\Psi\rangle &= \frac{1}{\sqrt{2}}[\alpha|0\rangle|+\rangle + \alpha|0\rangle|-\rangle + \beta|1\rangle|+\rangle - \beta|1\rangle|-\rangle] = \\ &= \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)|+\rangle + \frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle)|-\rangle = M_+|\psi\rangle|+\rangle + M_-|\psi\rangle|-\rangle\end{aligned} \tag{7.10}$$

with

$$M_+ \equiv \frac{1}{\sqrt{2}}I, \qquad M_- \equiv \frac{1}{\sqrt{2}}Z \tag{7.11}$$

Measuring the qubit B in the $|+\rangle, |-\rangle$ basis means to measure an observable that acts on system B and has eigenvectors $|+\rangle$ and $|-\rangle$. This measurement is described by the projectors

$$\mathbb{P}_+ = I \otimes |+\rangle\langle+|, \quad \mathbb{P}_- = I \otimes |-\rangle\langle-| \tag{7.12}$$

and the probability of obtaining the results + or - is:

$$p(+) = \langle\Psi|\mathbb{P}_+|\Psi\rangle = \langle\psi|M_+^\dagger M_+|\psi\rangle = \frac{1}{2}, \quad p(-) = \langle\Psi|\mathbb{P}_-|\Psi\rangle = \langle\psi|M_-^\dagger M_-|\psi\rangle = \frac{1}{2} \tag{7.13}$$

The state after the measurement with result m ($m = +, -$) is

$$|\Psi\rangle \longrightarrow \frac{\mathbb{P}_m|\Psi\rangle}{\sqrt{\langle\Psi|\mathbb{P}_m|\Psi\rangle}} = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}|m\rangle \tag{7.14}$$

Thus a measurement by Bob on his qubit, in the $|m\rangle$ basis, can be described by Alice by using the measurement operators M_m and the rules of Section 7.2. Note that in this way Alice can describe statistics and effect of a measurement by Bob in terms of quantities belonging only to her subsystem, i.e. the ket $|\psi\rangle$ and the measurement operators M_+, M_-.

7.4 POVM

If we are not interested in the state after the measurement, we can use the operators POVM (Positive Operator Valued Measurement) defined by

$$E_m \equiv M_m^\dagger M_m \tag{7.15}$$

Indeed only the product $M_m^\dagger M_m$ enters the formula for the probability $p(m)$. The POVM operators must satisfy

$$\sum_m E_m = I \tag{7.16}$$

due to (7.6). The name comes from the fact that they are positive operators ($A^\dagger A$ is positive for any operator A). In the next paragraph we provide an example that illustrates their use.

7.5 Example: projective measurements on $\mathbb{V}^3$ as POVM in $\mathbb{V}^2$

Consider the following orthonormal basis in a 3-dimensional vector space $\mathbb{V}^3$:

$$|\phi_1\rangle = \frac{|0\rangle + |2\rangle}{\sqrt{2}}, \quad |\phi_2\rangle = \frac{|0\rangle + |1\rangle - |2\rangle}{\sqrt{3}}, \quad |\phi_3\rangle = \frac{|0\rangle - 2|1\rangle - |2\rangle}{\sqrt{6}} \tag{7.17}$$

$|0\rangle, |1\rangle, |2\rangle$ being the computational basis. The vectors $|\phi_i\rangle$ can be eigenvectors of an observable Q, acting on $\mathbb{V}^3$. Suppose that the eigenvectors correspond to eigenvalues 1,2,3, respectively, and that we measure this observable on the two states $|\psi_1\rangle$ and $|\psi_2\rangle$

$$|\psi_1\rangle = |1\rangle, \quad |\psi_2\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{7.18}$$

According to the usual rule in (7.1), using the projectors $P_m = |\phi_m\rangle\langle\phi_m|$ we can compute the probabilities $p(m) = \langle\psi_i|P_m|\psi_i\rangle$ of obtaining m in a measurement on $|\psi_i\rangle$:

$$p(1) = 0, \quad p(2) = \frac{1}{3}, \quad p(3) = \frac{2}{3} \qquad \text{if the state is } |\psi_1\rangle \tag{7.19}$$

$$p(1) = \frac{1}{4}, \quad p(2) = 0, \quad p(3) = \frac{3}{4} \qquad \text{if the state is } |\psi_2\rangle \tag{7.20}$$

For example for a measurement on $|\psi_2\rangle$, $p(1) = \langle\psi_2|P_1|\psi_2\rangle = |\langle\psi_2|\phi_2\rangle|^2 = 1/4$.

If we obtain 1, we know with certainty that the state on which we have performed the measurement is $|\psi_2\rangle$, since $p(1) = 0$ for $|\psi_1\rangle$. Similarly, if we obtain 2, the state must be $|\psi_1\rangle$. Thus if we obtain either 1 or 2 we can distinguish the two non-orthogonal states . However if we obtain 3 (and this result has in fact higher probability) we cannot say on which state we have measured Q. The situation is nevertheless better than the one we have discussed in Section 3.4, where we can only perform measurements on the states (7.18) in the computational basis: then only $|\psi_2\rangle$ is recognizable with certainty (when the result is 0).

This example illustrates the usefulness of the POVM formalism. Indeed the same statistics as in (7.19), (7.20) can be reproduced by using operators POVM acting only on the subspace $\mathbb{V}^2$. The POVM can be obtained from the projectors $P_m = |\phi_m\rangle\langle\phi_m|$ by setting $|2\rangle = 0$:

$$E_1 = \frac{1}{2}|0\rangle\langle 0|, \quad E_2 = \frac{1}{3}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|), \quad E_3 = \frac{1}{6}(|0\rangle - 2|1\rangle)(\langle 0| - 2\langle 1|) \tag{7.21}$$

It is straightforward to check that $E_1 + E_2 + E_3 = I$, where I is the identity in $\mathbb{V}^2$. Indeed the sum of the three projectors, before deleting $|2\rangle$, is equal to $|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|$, the identity in $\mathbb{V}^3$. Deleting $|2\rangle$ reduces it to the identity in $\mathbb{V}^2$. Thus E_1, E_2, E_3 satisfy the properties required for POVM operators in $\mathbb{V}^2$: they are positive operators (proportional to projectors, which are positive) and sum to the identity.

Using these POVM it is a simple matter to check that the statistics in (7.19), (7.20) of measurements on $|\psi_i\rangle$ can be obtained as $p(m) = \langle\psi_i|E_m|\psi_i\rangle$, using only quantities defined in $\mathbb{V}^2$. This holds because the states to be measured do not contain a component along $|2\rangle$, and therefore the action of E_m on them is identical to the action of the projectors P_m.

8 Lecture 8: Density operator

Systems whose state is not completely known are described by a *density operator* ρ, associated to a statistical ensemble of states $\{|\psi_i\rangle, p_i\}$ as follows:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad Tr\rho = \sum_i p_i = 1 \tag{8.1}$$

the trace = 1 property must hold since p_i are probabilities.

The ρ operator contains all the physical information on the system. It allows to compute the probabilities for measurements, as we now discuss.

8.1 Probabilities

If the initial state of the system were $|\psi_i\rangle$, the probability of obtaining result m would be given by the usual rule of 7.1:

$$p(m|i) = \langle\psi_i|P_m|\psi_i\rangle \tag{8.2}$$

where now $p(m|i)$ is the *conditional probability* of obtaining m provided the state of the system is $|\psi_i\rangle$. Note that this probability can be rewritten in terms of a trace:

$$p(m|i) = Tr(P_m|\psi_i\rangle\langle\psi_i|) \tag{8.3}$$

Then the probability $p(m)$ of obtaining m in a statistical ensemble described by ρ is:

$$p(m) = \sum_i p(m|i)p_i = \sum_i p_i \; Tr(P_m|\psi_i\rangle\langle\psi_i|) = \sum_i Tr(P_m p_i|\psi_i\rangle\langle\psi_i|) = Tr(P_m\rho) \tag{8.4}$$

Also the expectation value of an observable A can be given in terms of ρ:

$$\langle A\rangle = \sum_m p(m)a_m = \sum_m a_m Tr(P_m\rho) = Tr(A\rho) \tag{8.5}$$

where a_m are the eigenvalues of A, and $A = \sum_m a_m P_m$ (spectral decomposition).

All the above formulas reduce to the ones in Section 7.1 when the statistical ensemble contains only one vector $|\psi\rangle$ with $p = 1$. In this case $\rho = |\psi\rangle\langle\psi|$ describes a *pure state*, as opposed to a *mixed state* occurring when more than one p_i is different from 0.

8.2 Collapse of ρ

How does ρ change after the result m has been obtained in the measurement ? If the initial state was $|\psi_i\rangle$, a measurement with result m would collapse it into the state:

$$|\psi_i^{(m)}\rangle = \frac{P_m|\psi_i\rangle}{\sqrt{\langle\psi_i|P_m|\psi_i\rangle}} \tag{8.6}$$

Then after obtaining m, we have an ensemble of states $|\psi_i^{(m)}\rangle$, each with probability $p(i|m)$ (this is the conditional probability that, having obtained m, the state has become $|\psi_i^{(m)}\rangle$). Therefore ρ becomes, after the measurement:

$$\rho \longrightarrow \rho_m = \sum_i p(i|m)\ |\psi_i^{(m)}\rangle\langle\psi_i^{(m)}| = \sum_i p(i|m)\ \frac{P_m|\psi_i\rangle\langle\psi_i|P_m}{\langle\psi_i|P_m|\psi_i\rangle} \tag{8.7}$$

We use now Bayes formula for conditional probabilities:

$$p(x,y) = p(y|x)p(x) = p(x|y)p(y) \Longrightarrow p(x|y) = p(y|x)\frac{p(x)}{p(y)} \tag{8.8}$$

and apply it to $p(i|m)$:

$$p(i|m) = p(m|i)\frac{p_i}{p(m)} = \langle\psi_i|P_m|\psi_i\rangle\frac{p_i}{p(m)} \tag{8.9}$$

and substituting into (8.7) yields

$$\rho_m = \sum_i p_i\ \frac{P_m|\psi_i\rangle\langle\psi_i|P_m}{Tr(P_m\rho)} = \frac{P_m\rho\ P_m}{Tr(P_m\rho)} \tag{8.10}$$

8.3 General properties of ρ

Theorem: Every density operator ρ satisfies the properties:

$$i)\quad Tr(\rho) = 1 \tag{8.11}$$

$$ii)\quad \rho \text{ positive operator} \tag{8.12}$$

Viceversa, if an operator satisfies these properties, it is the density operator of some statistical ensemble.

Proof: we have already observed that $Tr\rho = 1$ is just the requirement that p_i be interpretable as probabilities, i.e. $\sum_i p_i = 1$. The density operator is also a positive operator, since it is a weighted sum of projectors (with positive weights), and projectors are positive operators. Viceversa, suppose that an operator ρ satisfies both properties (8.11),(8.12). Being positive, it admits a spectral decomposition

$$\rho = \sum_i \lambda_i|i\rangle\langle i| \tag{8.13}$$

where $|i\rangle$ are its eigenvectors and λ_i the corresponding eigenvalues, which are real ≥ 0 since ρ is positive. Furthermore, the unit trace condition implies $\sum_i \lambda_i = 1$, so that λ_i can be interpreted as probabilities. Thus, ρ is the density operator for the ensemble $\{|i\rangle, \lambda_i\}$. □

8.4 Test of purity

The following Theorem provides a means to establish whether ρ describes a pure or a mixed state.

Theorem: $Tr\rho^2 \leq 1$, equality holding if and only if ρ describes a pure state.

Proof: if $\rho = |\psi\rangle\langle\psi|$, $\rho^2 = \rho$ and $Tr\rho^2 = Tr\rho = 1$. When $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ with at least two terms in the sum, we have:

$$\rho^2 = \sum_{i,j} p_i p_j \langle\psi_i|\psi_j\rangle \; |\psi_i\rangle\langle\psi_j| \Longrightarrow Tr\rho^2 = \sum_{i,j} p_i p_j \; |\langle\psi_i|\psi_j\rangle|^2 \tag{8.14}$$

Notice now that

$$\sum_{i,j} p_i p_j \; |\langle\psi_i|\psi_j\rangle|^2 = \sum_i p_i \sum_j p_j |\langle\psi_i|\psi_j\rangle|^2 \tag{8.15}$$

and since $\sum_j p_j |\langle\psi_i|\psi_j\rangle|^2 < 1$ because of Schwarz' inequality ($|\langle\psi_i|\psi_j\rangle|^2 < 1$ when $|\psi_i\rangle \neq |\psi_j\rangle$), then also $\sum_i p_i \sum_j p_j |\langle\psi_i|\psi_j\rangle|^2 < 1$. □

8.5 Different ensembles for the same ρ

The same ρ can correspond to different statistical ensembles: For example it is easy to verify that

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| \tag{8.16}$$

where $|+\rangle, |-\rangle$ is the oblique basis. Thus the same ρ describes both a system that is in the state $|0\rangle$ or $|1\rangle$ with equal probabilities, and a system in a state $|+\rangle$ or $|-\rangle$ with equal probabilities. Another example is given by

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b| \tag{8.17}$$

with

$$|a\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle, \quad |b\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle \tag{8.18}$$

Note that $|a\rangle$ and $|b\rangle$ are not orthogonal.

The next Theorem answers the question: when do two different ensembles $\{|\psi_i\rangle, p_i\}$, $\{|\phi_j\rangle, q_j\}$ give rise to the same ρ ? Define for convenience

$$|\tilde{\psi_i}\rangle \equiv \sqrt{p_i}|\psi_i\rangle, \quad |\tilde{\phi_j}\rangle \equiv \sqrt{q_j}|\phi_j\rangle \tag{8.19}$$

where the probabilities p_i and q_j of the two ensembles have been absorbed in the definition of the tilde vectors.

Theorem:

$$\rho = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_j |\tilde{\phi}_j\rangle\langle\tilde{\phi}_j| \tag{8.20}$$

if and only if

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij}|\tilde{\phi}_j\rangle \qquad \text{with } u_{ij} \text{ unitary} \tag{8.21}$$

Note that the range of the indices i and j does not need to be the same. When this is the case, one introduces null tilde vectors in the ensemble with lower cardinality (equivalent to introducing new vectors with 0 probability in the ensemble), so as to have ensembles with the same number of vectors.

Proof: the "if" part of the Theorem is easy to prove:

$$\sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_{i,j,k} u_{ij}u^*_{ik}\ |\tilde{\phi}_j\rangle\langle\tilde{\phi}_k| = \sum_{j,k}(\sum_i u^\dagger_{ki}u_{ij})\ |\tilde{\phi}_j\rangle\langle\tilde{\phi}_k| = \sum_j |\tilde{\phi}_j\rangle\langle\tilde{\phi}_j| \tag{8.22}$$

The "only if" part makes use of the spectral decomposition of $\rho = \sum_k \lambda_k|k\rangle\langle k|$. If $\sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_j |\tilde{\phi}_j\rangle\langle\tilde{\phi}_j| = \sum_k |\tilde{k}\rangle\langle\tilde{k}|$ (with $|\tilde{k}\rangle \equiv \sqrt{\lambda}|k\rangle$, then we can prove that both $|\tilde{\psi}_i\rangle$ and $|\tilde{\phi}_j\rangle$ can be expressed as a linear combination of the $|\tilde{k}\rangle$. Indeed a vector $|\chi\rangle$ orthogonal to the subspace spanned by the $|\tilde{k}\rangle$ satisfies $0 = \langle\chi|\rho|\chi\rangle = \sum_i\langle\chi|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|\chi\rangle = \sum_i |\langle\chi|\tilde{\psi}_i\rangle|^2$ so that $\langle\chi|\tilde{\psi}_i\rangle = 0, \forall i$, implying that $|\tilde{\psi}_i\rangle$ is in the same subspace spanned by the $|\tilde{k}\rangle$. Then $|\tilde{\psi}_i\rangle = \sum_k c_{ik}|\tilde{k}\rangle$ and

$$\rho = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_{k,l}\left(\sum_i c_{ik}c^*_{il}\right)|\tilde{k}\rangle\langle\tilde{l}| = \sum_k |\tilde{k}\rangle\langle\tilde{k}| \tag{8.23}$$

Since the $\sum_k |\tilde{k}\rangle\langle\tilde{l}|$ operators are linearly independent, the above equation implies $\sum c_{ik}c^*_{il} = \delta_{kl}$, and we can find a unitary matrix v_{ik} such that $|\tilde{\psi}_i\rangle = \sum_k v_{ik}|\tilde{k}\rangle$ after complementing, if necessary, the list of $|\tilde{k}\rangle$ vectors with null vectors so as to have the same range of i and k indices. The same reasoning can be repeated for $|\tilde{\phi}_j\rangle$, and therefore also $|\tilde{\phi}_j\rangle = \sum_k w_{jk}|\tilde{k}\rangle$ holds, with w_{jk} unitary. Putting these results together, we conclude that

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij}|\tilde{\phi}_j\rangle \tag{8.24}$$

with $u = vw^\dagger$ unitary. □

8.6 The rules of Quantum Mechanics in terms of ρ

I. To every (closed) physical system corresponds a complex vector space with scalar product, called the *state space*. The system is completely described by the density operator ρ, a positive operator with unit trace, acting on the state space.

II. Measurements are described by a collection of operators $\{M_m\}$, called *measure operators*, acting on the state space, and corresponding to the possible outcomes m. They satisfy the completeness relation

$$\sum_m M_m^\dagger M_m = I \tag{8.25}$$

Projective measurements of an observable A correspond to measure operators being projectors on eigensubspaces of A. If the state of the system before measurement is described by ρ (then we say that the system is in the state ρ), the probability to obtain m is:

$$p(m) = Tr(M_m^\dagger M_m \rho) \tag{8.26}$$

and the state after the measurement becomes

$$\rho \longrightarrow \rho_m = \frac{M_m \rho \ M_m^\dagger}{Tr(M_m^\dagger M_m \rho)} \tag{8.27}$$

III. The time evolution of a closed physical system is described by a unitary transformation

$$\rho(t) = U(t)\rho(0) \ U^\dagger(t) \tag{8.28}$$

where U is the time evolution operator. For conservative systems $U(t) = e^{-\frac{i}{\hbar}Ht}$.

IV. The state space of composite systems is the *tensor product* of the state spaces of the individual subsystems. If these subsystems are in the states $\rho_1, \rho_2, ...\rho_n$, the composite system is in the state

$$\rho = \rho_1 \otimes \rho_2 \otimes ... \otimes \rho_n \tag{8.29}$$

Note : if a quantum system is prepared in a state ρ_i with probability p_i, it is described by a density operator

$$\rho = \sum_i p_i \rho_i \tag{8.30}$$

Thus we have a statistical ensemble of density operators, rather than state vectors. It is in fact a generalization of the mixed states defined in 8.1, and when ρ_i are pure states (8.30) reproduces eq. (8.1). It is easy to verify that the rule (8.30) makes sense: if $\rho_i \equiv \sum_j p_{ij} |\psi_{ij}\rangle\langle\psi_{ij}|$, the probability of finding the system in state $|\psi_{ij}\rangle$ is $p_i p_{ij}$. Then the density operator for such a system is $\rho = \sum_{i,j} p_i p_{ij} |\psi_{ij}\rangle\langle\psi_{ij}| = \sum_i p_i \rho_i$.

Mixed states can occur for example when noise produces ignorance of the state, or when the result of a measurement gets lost. In this last case the system will be in the state ρ_m (the state after a measurement with result m) with probability $p(m) = Tr(M_m^\dagger M_m \rho)$. Then it is described by the density operator

$$\rho' = \sum_m p(m)\rho_m = \sum_m Tr(M_m^\dagger M_m \rho) \frac{M_m \rho \ M_m^\dagger}{Tr(M_m^\dagger M_m \rho)} = \sum_m M_m \rho \ M_m^\dagger \tag{8.31}$$

8.6.1 An example

Suppose we measure a qubit $|\psi = \alpha|0\rangle + \beta|1\rangle$ in the computational basis, and ignore the result. In which state is the qubit ? The answer is: it is in the state $|0\rangle$ with probability $|\alpha|^2$ and in the state $|1\rangle$ with probability $|\beta|^2$. This means that his state is a mixed state described by the density operator

$$\rho = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| \tag{8.32}$$

This is to be compared with the (pure) state $|\psi\rangle$ before the measurement, a quite different state. In the mixed state all information on the phases of α and β has been lost.

9 Lecture 9

9.1 Reduced density operator

Describes subsystems of composite systems. If two subsystems A and B form a system AB, with density operator ρ^{AB}, the *reduced density operator* for system A is defined by

$$\rho^A = Tr_B(\rho^{AB}) \tag{9.1}$$

where Tr_B is the *partial trace* on system B. The partial traces Tr_A and Tr_B are defined on tensor products of operators as

$$Tr_A(O_A \otimes O_B) \equiv Tr(O_A)O_B, \quad Tr_B(O_A \otimes O_B) \equiv O_A Tr(O_B) \tag{9.2}$$

Thus for example

$$Tr_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = (|a_1\rangle\langle a_2| Tr(|b_1\rangle\langle b_2|) = \langle b_2|b_1\rangle \; |a_1\rangle\langle a_2| \tag{9.3}$$

Note 1: any operator in AB can be written as a sum of tensor products $O_A \otimes O_B$. Indeed the ket-bra representation of an operator C on system AB is

$$C = \sum_{ir,js} c_{ir,js}|i\rangle|r\rangle\langle j|\langle s| \tag{9.4}$$

the vectors $|i\rangle|r\rangle$ forming a basis in AB. The constants $c_{ir,js}$ are the matrix elements of C on this basis. Notice now that $|i\rangle|r\rangle\langle j|\langle s| = |i\rangle\langle j| \otimes |r\rangle\langle s|$ (both sides act on the same way on the basis vectors) and therefore every C can be written as a sum of tensor products of operators. Then the definition of the partial trace can be extended by linearity to any C on AB.

Note 2: $Tr_{AB}(O_A \otimes O_B) = Tr_A[Tr_B(O_A \otimes O_B)]$ since $Tr_{AB}(O_A \otimes O_B) = Tr(O_A)Tr(O_B)$ as can be verified for ket-bra operators.

9.2 Probabilities

Suppose that in a bipartite system AB, Alice wants to compute the probability to obtain a result m by measuring an observable Q. To be measured by Alice, this observable must act on the vector space A. But this observable can also be measured by an observer having access to the whole AB. Thus it must be expressible also as an observable $\mathbb{Q}$ on the whole AB. There is only one way to extend Q to an observable $\mathbb{Q}$ acting on the whole AB, and having the same spectrum, i.e.

$$\mathbb{Q} = Q \otimes I \tag{9.5}$$

Indeed if the spectral expansion of Q is $Q = \sum_m mP_m$, we find

$$\mathbb{Q} = \sum_m m(P_m \otimes I) \tag{9.6}$$

and we see that $\mathbb{Q}$ has the same spectrum as Q, with corresponding projectors

$$\mathbb{P}_m = P_m \otimes I \tag{9.7}$$

We can then compute the probability that a measurement of $\mathbb{Q}$ yields the result m. According to the rule in (8.4), we find

$$p(m) = Tr_{AB}(\mathbb{P}_m \rho^{AB}) = Tr_{AB}[(P_m \otimes I)\rho^{AB}] = Tr_A\left(Tr_B[(P_m \otimes I)\rho^{AB}]\right) \tag{9.8}$$

Next we notice that

$$Tr_B[(P_m \otimes I)\rho^{AB}] = P_m Tr_B(\rho^{AB}) = P_m \rho^A \tag{9.9}$$

as can be easily checked by expanding ρ^{AB} in a sum of tensor products (cf. Note 1 in Section 9.1):

$$\rho^{AB} = \sum_i O^i_A \otimes O^i_B \tag{9.10}$$

Therefore

$$p(m) = Tr_{AB}(\mathbb{P}_m \rho^{AB}) = Tr_A(P_m \rho^A) \tag{9.11}$$

This formula shows that Alice can compute $p(m)$ using only quantities relating to the subsystem A, provided she uses $\rho^A \equiv Tr_B(\rho^{AB})$ as her density operator, describing her subsystem. This justifies the definition (9.1) as the effective density operator for Alice's subsystem.

9.3 Collapse of ρ^A

The collapsed density operator due to the measurement of $\mathbb{Q}$ (after having obtained m) is:

$$\rho^{AB}_m = \frac{\mathbb{P}_m \rho^{AB}\ \mathbb{P}_m}{Tr_{AB}(\mathbb{P}_m \rho^{AB})} \tag{9.12}$$

Using $\rho^{AB} = \sum_i O^i_A \otimes O^i_B$ and (9.11), it can be rewritten as follows :

$$\rho^{AB}_m = \frac{\sum_i P_m O^i_A P_m \otimes O^i_B}{Tr_A(P_m \rho^A)} \tag{9.13}$$

Taking now the partial trace over B produces the reduced density operator for Alice:

$$\rho^A_m = Tr_B(\rho^{AB}_m) = \frac{\sum_i P_m O^i_A P_m Tr(O^i_B)}{Tr_A(P_m \rho^A)} = \frac{P_m Tr_B(\rho^{AB}) P_m}{Tr_A(P_m \rho^A)} = \frac{P_m \rho^A P_m}{Tr_A(P_m \rho^A)} \tag{9.14}$$

The last equality shows that the collapse due to the measurement of $\mathbb{Q}$ can be described by Alice exclusively in terms of her reduced density operator ρ^A, using the rule (8.27).

Thus the reduced density operator *correctly encodes all the information on subsystem A, that Alice can use to predict probabilities and collapse.*

9.4 Examples

9.4.1 Product state

Suppose that the state of a bipartite system AB is

$$\rho^{AB} = \rho \otimes \sigma \tag{9.15}$$

It is said then to be in a product state (and generalizes the product state in case of pure states). The partial traces are

$$Tr_A(\rho^{AB}) = \rho^B = \sigma, \quad Tr_B(\rho^{AB}) = \rho^A = \sigma \tag{9.16}$$

and yield the density matrices of the individual subsystems, as expected.

9.4.2 Pure entangled state

Consider the entangled state of a 2-qubit system

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{9.17}$$

The corresponding density operator is

$$\rho^{AB} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \frac{\langle 00| + \langle 11|}{\sqrt{2}} = \frac{|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|}{2} \tag{9.18}$$

The reduced density operator for Alice (who owns qubit A) is:

$$\begin{aligned} \rho^A &= \frac{1}{2} Tr_B(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) = \\ &= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 1|0\rangle + |0\rangle\langle 1|\langle 0|1\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} = \\ &= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2} \end{aligned} \tag{9.19}$$

Since $Tr(\rho^A)^2 = 1/2 < 1$ this reduced density operator describes a *mixed state* for qubit A. The ensemble can equally well be considered $\{|0\rangle, |1\rangle\}$ with equal probabilities 1/2, or $\{|+\rangle, |-\rangle\}$ with equal probabilities 1/2, or any other ensemble related to these via a unitary trasformation (see Section 8.4).

9.4.3 Teleportation state

Consider the 3-qubit state (4.1) in the teleportation protocol of Section 4.2. After Alice's measurement, if we ignore the result obtained by Alice, the state is described by a statistical ensemble

$$\begin{aligned}
&|00\rangle(\alpha|0\rangle+\beta|1\rangle) \quad \text{with prob. } \frac{1}{4}\\
&|10\rangle(\alpha|1\rangle+\beta|0\rangle) \quad \text{with prob. } \frac{1}{4}\\
&|01\rangle(\alpha|0\rangle-\beta|1\rangle) \quad \text{with prob. } \frac{1}{4}\\
&|11\rangle(\alpha|1\rangle-\beta|0\rangle) \quad \text{with prob. } \frac{1}{4}
\end{aligned} \tag{9.20}$$

The density operator is therefore:

$$\begin{aligned}
\rho = \frac{1}{4}[&|00\rangle\langle 00| \otimes (\alpha|0\rangle+\beta|1\rangle)(\alpha^*\langle 0|\rangle+\beta^*\langle 1|)\\
&+|01\rangle\langle 01| \otimes (\alpha|1\rangle+\beta|0\rangle)(\alpha^*\langle 1|\rangle+\beta^*\langle 0|)\\
&+|10\rangle\langle 10| \otimes (\alpha|0\rangle-\beta|1\rangle)(\alpha^*\langle 0|\rangle-\beta^*\langle 1|)\\
&+|11\rangle\langle 11| \otimes (\alpha|1\rangle-\beta|0\rangle)(\alpha^*\langle 1|\rangle-\beta^*\langle 0|)]
\end{aligned} \tag{9.21}$$

Taking the partial trace with respect to A (the space of the first two qubits) yields the reduced density operator for Bob:

$$\begin{aligned}
\rho^B = \frac{1}{4}[&(\alpha|0\rangle+\beta|1\rangle)(\alpha^*\langle 0|\rangle+\beta^*\langle 1|)\\
&+(\alpha|1\rangle+\beta|0\rangle)(\alpha^*\langle 1|\rangle+\beta^*\langle 0|)\\
&+(\alpha|0\rangle-\beta|1\rangle)(\alpha^*\langle 0|\rangle-\beta^*\langle 1|)\\
&+(\alpha|1\rangle-\beta|0\rangle)(\alpha^*\langle 1|\rangle-\beta^*\langle 0|)] =\\
= \frac{2(|\alpha|^2+|\beta|^2)|0\rangle\langle 0|+2(|\alpha|^2+|\beta|^2)|1\rangle\langle 1|}{4} &= \frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2} = \frac{I}{2}
\end{aligned} \tag{9.22}$$

Thus the state of Bob's system, *after* Alice has performed the measurement on her qubits, but *before* Bob has learned the result, is $\rho^B = I/2$. This state carries no information on the state $|\psi\rangle$ to be teleported (no information on α and β) $\Longrightarrow$ no measurement by Bob can contain information on $|\psi\rangle$. This prevents Alice to use teleportation for superluminal communication, since only after a phone call (at speed $\leq c$) can Bob reconstruct $|\psi\rangle$ in his lab.

10 Lecture 10

10.1 Schmidt decomposition

A very useful Theorem provides a convenient decomposition for any vector of a composite space:

Theorem: if $|\psi\rangle$ is a pure state of a composite system AB, there exist orthonormal vectors $|i_A\rangle$ for system A and $|i_B\rangle$ for system B such that

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle \otimes |i_B\rangle \tag{10.1}$$

with $\lambda_i \geq 0$ and $\sum_i \lambda_i^2 = 1$. The λ_i are called *Schmidt coefficients*.

Note that this expansion is much more economical than the usual expansion in terms of tensor products of two bases in A and B: the Schmidt decomposition has at most n terms, where $n = \min(dimA, dimB)$, whereas the usual expansion on tensor products of the bases has $dimA \times dimB$ terms.

Proof: suppose at first that $dimA = dimB$, and that $|j\rangle$, $|k\rangle$ are orthonormal bases for A and B. Then $|\psi\rangle$ can be expanded as:

$$|\psi\rangle = \sum_{j,k} a_{jk} |j\rangle |k\rangle \tag{10.2}$$

From the singular decomposition (Section 6.4) we know that any matrix a can be written as $a = udv$, where u and v are unitary matrices, and d is a diagonal matrix with elements ≥ 0. Then

$$|\psi\rangle = \sum_{i,j,k} u_{ji} d_{ii} v_{ik} |j\rangle |k\rangle \tag{10.3}$$

and defining

$$|i_A\rangle \equiv \sum_j u_{ji} |j\rangle, \quad |i_B\rangle \equiv \sum_k v_{ik} |k\rangle, \quad \lambda_i \equiv d_{ii} \tag{10.4}$$

proves the Theorem. The $|i_A\rangle$ and $|i_B\rangle$ are orthonormal bases (the *Schmidt bases* for A and B) , since they are related to the orthonormal bases $|j\rangle$ and $|k\rangle$ by unitary transformations. Note that the Schmidt bases *depend* on the vector $|\psi\rangle$. Finally, the $\sum_i \lambda_i^2 = 1$ relation is due to $\langle\psi|\psi\rangle = 1$.

If $dimA > dimB$, we enlarge the smaller space B by adding extra basis vectors until the dimensions match. Call these vectors $|\tilde{k}\rangle$. Then we apply the above proof, and find $|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$.
Consider the tensor products $|i_A\rangle|k\rangle$, where the $|k\rangle$ include also the extra $|\tilde{k}\rangle$. These products are a complete basis on the enlarged AB space. We observe that $|\psi\rangle$ cannot have components along the basis elements $|i_A\rangle|\tilde{k}\rangle$, since it was defined as a

vector on the original (not enlarged) AB space. Therefore the $|i_B\rangle$ present in the decomposition of $|\psi\rangle$ cannot contain $|\tilde{k}\rangle$ either. We conclude that the decomposition

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle \tag{10.5}$$

holds, with the sum on i running on $dimB$ values, the vectors $|i_B\rangle$ being genuine orthonormal vectors of B. The $|i_A\rangle$ are an orthonormal set, but not necessarily a complete basis for A. □

The next Theorem illustrates the usefulness of the Schmidt decomposition.

Theorem: consider a pure state $|\psi\rangle$ for a composite system AB. Then

$$\rho^A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|, \qquad \rho^B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B| \tag{10.6}$$

Proof: immediate using the Schmidt decomposition for $|\psi\rangle$ and taking the partial traces of $\rho^{AB} = |\psi\rangle\langle\psi|$. □

Thus the eigenvalues of ρ^A and ρ^B are identical and equal to λ_i^2. Many properties of quantum systems depend on the eigenvalues of the reduced density operator. For a pure state of a composite AB system these properties will be the same for both subsystems. For example the pure state

$$|\psi\rangle = \frac{|00\rangle + |01\rangle + |11\rangle}{\sqrt{3}} \tag{10.7}$$

has no evident symmetries between A and B, but we find

$$Tr(\rho^A)^2 = Tr(\rho^B)^2 = \frac{7}{9} \tag{10.8}$$

• The number of nonvanishing λ_i in the Schmidt decomposition for a state $|\psi\rangle$ of a composite AB system is called the *Schmidt number* of $|\psi\rangle$, and denoted by $Sch(|\psi\rangle)$. It gives a *quantitative measure of the entanglement* between A and B, present in the vector $|\psi\rangle$. If $Sch(|\psi\rangle) = 1$ the state is separable, and when $Sch(|\psi\rangle) > 1$ the state is entangled.

• The Schmidt number is preserved by unitary transformations that act only on A or only on B. Indeed if $|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle$ is the Schmidt decomposition for $|\psi\rangle$, then $U_A|\psi\rangle = \sum_i \lambda_i U_A|i_A\rangle|i_B\rangle$, where U_A is a unitary operator acting only on A, and $U_A|i_A\rangle, |i_B\rangle$ are the Schmidt bases for $U_A|\psi\rangle$. The λ_i are unchanged: they are the same for the vectors $|\psi\rangle$ and $U_A|\psi\rangle$. Thus *local unitary transformations* (i.e. of the form $U_A \otimes U_B$) do not change the Schmidt number, and as a consequence *cannot increase the entanglement*.

Exercise : show that a state $|\psi\rangle$ of a composite system is a product state iff ρ^A (and therefore also ρ^B) describe pure states. Hint: use the Schmidt decomposition for $|\psi\rangle$. As a consequence, the reduced density operator for an entangled AB state is always a mixed state.

10.2 Purification

Theorem: Given a mixed state ρ^A of a system A, it is always possible to introduce another system R (a copy of the system A) and define a *pure state* $|AR\rangle$ for the system AR such that $\rho^A = Tr_R(|AR\rangle\langle AR|)$

This procedure, that permits to associate pure states to mixed states ρ^A, is called *purification*.

Proof: ρ^A, being a positive operator, has the spectral decomposition:

$$\rho^A = \sum_i p_i \; |i^A\rangle\langle i^A| \tag{10.9}$$

with $p_i \geq 0$, and $|i^A\rangle$ a complete set of orthonormal eigenvectors of ρ^A. Introducing a system R with the same states of A, with orthonormal basis $\{|i^R\rangle\}$, we can define the pure state for system AR:

$$|AR\rangle \equiv \sum_i \sqrt{p_i} \; |i^A\rangle|i^R\rangle \tag{10.10}$$

with corresponding density matrix $\rho^{AB} = |AR\rangle\langle AR|$. Computing now the reduced density matrix $Tr_R(\rho^{AB})$ we find

$$Tr_R(\rho^{AB}) = \sum_{i,j} \sqrt{p_i p_j} \; |i^A\rangle\langle j^A| Tr(|i^R\rangle\langle j^R|) = \sum_{i,j} \sqrt{p_i p_j} \; |i^A\rangle\langle j^A|\delta_{ij} = \sum_i p_i |i^A\rangle\langle i^A| \tag{10.11}$$

recovering the density matrix ρ^A of (10.9). □

11 Lecture 11: the full Bloch sphere

We can represent both pure and mixed states for single qubits on the full Bloch sphere, where pure states are points on the surface, and mixed states points in the interior.

11.1 Pure states

Consider first the points on the surface. They are described by a vector $\vec{r}$ in $\mathbb{R}^3$, of length 1:

$$\vec{r} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \sin\theta\cos\varphi \\ \sin\theta\sin\varphi \\ \cos\theta \end{pmatrix} \tag{11.1}$$

see Fig. 1.3. This vector is also called the *Bloch vector*, and corresponds to the 1-qubit state

$$|\vec{r}\rangle \equiv \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{11.2}$$

We have thus the correspondance $\vec{r} \longleftrightarrow |\vec{r}\rangle$ between a vector in $\mathbb{R}^3$ with unit length and a quantum 1-qubit state, living in a 2-dimensional Hilbert space.

Exercise: show that $(\vec{r}\cdot\vec{\sigma})^2 = I$, where $\sigma_x, \sigma_y, \sigma_z$ are the Pauli matrices, i.e. the matrices X, Y, Z defined as single qubit gates in Section 1.5. *Hint*: use the relation for products of Pauli matrices:

$$\sigma_i\sigma_j = \delta_{ij}I + i\sum_k \varepsilon_{ijk}\sigma_k \tag{11.3}$$

where ε_{ijk} is totally antisymmetric, and $\varepsilon_{123} = 1$.

This exercise proves that the eigenvalues of $\vec{r}\cdot\vec{\sigma}$ can take only the values +1, -1.

Theorem: $|\vec{r}\rangle$ is eigenvector of the operator $\vec{r}\cdot\vec{\sigma}$ with eigenvalue +1.

Proof:

$$\begin{aligned}
\vec{r}\cdot\vec{\sigma}\ |\vec{r}\rangle &= \begin{pmatrix} z & x-iy \\ x+iy & -z \end{pmatrix}\begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} \end{pmatrix} = \\
&= \begin{pmatrix} \cos\theta & \sin\theta\cos\phi - i\sin\theta\sin\phi \\ \sin\theta\cos\phi + i\sin\theta\sin\phi & -\cos\theta \end{pmatrix}\begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} \end{pmatrix} = \\
&= \begin{pmatrix} \cos\theta & \sin\theta e^{-i\varphi} \\ \sin\theta e^{i\varphi} & -\cos\theta \end{pmatrix}\begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} \cos\theta\cos\frac{\theta}{2} + \sin\theta\sin\frac{\theta}{2} \\ e^{i\varphi}(\sin\theta\cos\frac{\theta}{2} - \cos\theta\sin\frac{\theta}{2}) \end{pmatrix} = \\
&= \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} \end{pmatrix} = |\vec{r}\rangle
\end{aligned} \tag{11.4}$$

using elementary trigonometry (Euler formula, and sin and cos of sums of angles). □

It is easy to find the other eigenvector of $\vec{r} \cdot \vec{\sigma}$, with eigenvalue -1. Indeed $\vec{r} \cdot \vec{\sigma} \; |\vec{r}\rangle = |\vec{r}\rangle$ implies (taking $\vec{r}$ into $-\vec{r}$) also $-\vec{r} \cdot \vec{\sigma} \; |-\vec{r}\rangle = |-\vec{r}\rangle$, or

$$\vec{r} \cdot \vec{\sigma} \; |-\vec{r}\rangle = -|-\vec{r}\rangle \tag{11.5}$$

Thus the eigenvector of $\vec{r} \cdot \vec{\sigma}$ with eigenvalue -1 is represented by the antipodal point (with Bloch vector $-\vec{r}$) on the Bloch sphere.

Note: If θ, φ are the angular coordinates of the vector $\vec{r}$, the antipodal point corresponding to $-\vec{r}$ has angular coordinates $\theta' = \pi - \theta, \varphi' = \varphi + \pi$, and therefore

$$|-\vec{r}\rangle = \begin{pmatrix} \cos\frac{(\pi-\theta)}{2} \\ e^{i(\varphi+\pi)} \sin\frac{(\pi-\theta)}{2} \end{pmatrix} = \begin{pmatrix} -\sin\frac{\theta}{2} \\ e^{i\varphi} \cos\frac{\theta}{2} \end{pmatrix} \tag{11.6}$$

We can immediately verify that $\langle\vec{r}|-\vec{r}\rangle = 0$.

Theorem: the operator

$$\frac{I \pm \vec{r} \cdot \vec{\sigma}}{2} \tag{11.7}$$

is the projector on $|\pm\vec{r}\rangle$.

Proof: use the spectral decomposition for $\vec{r} \cdot \vec{\sigma}$, and the completeness of the basis $|\vec{r}\rangle, |-\vec{r}\rangle$:

$$\vec{r} \cdot \vec{\sigma} = |\vec{r}\rangle\langle\vec{r}| - |-\vec{r}\rangle\langle-\vec{r}| \tag{11.8}$$

$$I = |\vec{r}\rangle\langle\vec{r}| + |-\vec{r}\rangle\langle-\vec{r}| \tag{11.9}$$

Summing and subtracting both relations yields

$$\frac{I + \vec{r} \cdot \vec{\sigma}}{2} = |\vec{r}\rangle\langle\vec{r}|, \qquad \frac{I - \vec{r} \cdot \vec{\sigma}}{2} = |-\vec{r}\rangle\langle-\vec{r}| \tag{11.10}$$

proving the Theorem. □

11.2 Mixed states

By definition, an arbitrary mixed state can be described by a density operator

$$\rho = p_1\rho_1 + p_2\rho_2 + ... + p_n\rho_n \tag{11.11}$$

where the ρ_i are projectors on pure states, and $\sum_i p_i = 1$. The projectors ρ_i can be written as $\rho_i = |\vec{r}_i\rangle\langle\vec{r}_i|$, where $\vec{r}_i$ are the Bloch vectors of the pure states. Thus

$$\begin{aligned} \rho = p_1|\vec{r}_1\rangle\langle\vec{r}_1| + p_2|\vec{r}_2\rangle\langle\vec{r}_2| + ...p_n|\vec{r}_n\rangle\langle\vec{r}_n| = p_1\frac{I + \vec{r}_1 \cdot \vec{\sigma}}{2} + ... + p_n\frac{I + \vec{r}_n \cdot \vec{\sigma}}{2} \\ = \frac{I}{2}(p_1 + ... + p_n) + \frac{(p_1\vec{r}_1 + ... + p_n\vec{r}_n) \cdot \vec{\sigma}}{2} = \frac{I + (\sum_i p_i\vec{r}_i) \cdot \vec{\sigma}}{2} \end{aligned} \tag{11.12}$$

Observe now that the euclidean $\mathbb{R}^3$ vector $\vec{r} \equiv \sum_i p_i \vec{r}_i$ has length < 1, because of the triangular inequality (the length of the sum of two vectors is smaller than the sum of their lengths, if the vectors are not proportional). Therefore the density matrix of a mixed state has the form

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2} \tag{11.13}$$

where $|\vec{r}| < 1$. This provides a geometrical representation of mixed states in terms of a vector $\vec{r}$ that spans all the points *inside* the Bloch sphere. In fact there is a 1-1 correspondence between the interior points of the sphere and mixed states. The points on the surface correspond instead to pure states, with $|\vec{r}| = 1$. Thus the *full* Bloch sphere faithfully describes pure and mixed 1-qubit states, with a density operator given in all cases by (11.13).

Exercise: prove that $Tr(\rho^2) < 1$ when $\vec{r} \cdot \vec{r} < 1$, using (11.13).

12 Lecture 12: EPR and Bell inequality

12.1 EPR

In their celebrated 1935 paper (A. Einstein, B. Podolski and N. Rosen, "Can Quantum Mechanical Description of Physical Reality be considered complete ?", Phys. Rev 47 (10) 777, 1935) the authors consider two particles correlated in position and momentum, as depicted in Fig. 12.1.

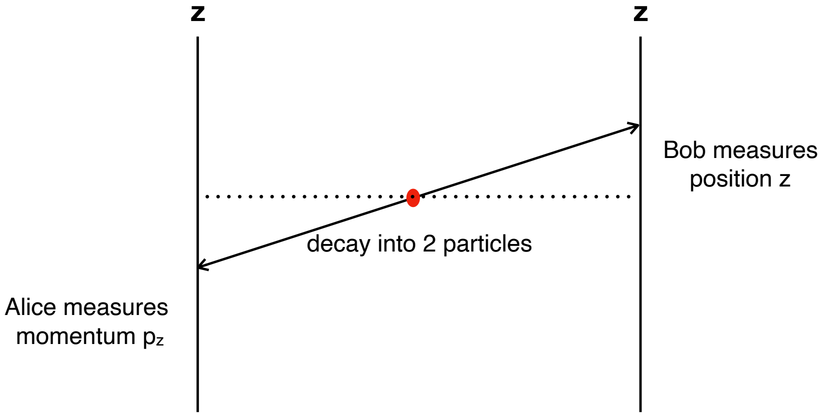


Fig. 12.1 EPR: conservation of momentum in the decay implies opposite p_z and opposite impact coordinates z for the two particles

Since momentum is conserved in the central decay (red dot), the two particles travel in opposite directions, with opposite momenta. They impact on two screens A (in Alice lab) and B (in Bob lab). Then if Alice measures on her particle a momentum p_z, Bob will measure on his particle a momentum $-p_z$. Likewise, if Bob measures a position of impact z, Alice will measure a position of impact $-z$. The two particles are correlated in position of impact and in momentum.

The two main assumptions of the EPR paper are:

i) a criterion for "*reality*": in the words of EPR, *"If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of reality corresponding to that quantity"*.

ii) the request of *locality*: no action taken on one particle can instantaneously affect the other, since this would involve information being transmitted faster than light, which is forbidden by the theory of relativity.

EPR then proceed with a thought experiment (Fig. 12.1). Alice measures the *momentum* of her particle, and finds a value p_z. This value becomes then an element of reality for Alice's particle. Bob measures the *position* of his particle, and finds a value z. Then, because positions are correlated, Alice's particle must have position $-z$. Note that, according to assumption ii), the measurement of Bob cannot influence in any way the state of Alice's particle, in particular cannot change the value of its momentum p_z. Thus for Alice's particle there are two elements of reality, the values of its position $-z$ and its momentum p_z.

However these two elements of reality cannot coexist in quantum theory, due to Heisenberg's principle. EPR conclude that quantum mechanics, in its Copenhagen formulation, is an *incomplete theory* since it does not contain all its elements of reality. One should look for a *realistic* theory (where for ex. values of position and momentum coexist on the same particle) satisying also *locality*.

The EPR reasoning, however, does not lead to a paradox. Indeed it is true that Bob cannot influence instantaneously Alice's particle state, however her measuring the momentum of her particle destroys the position correlation with Bob's particle. Then one cannot conclude that her particle has position $-z$. But this is not accepted by EPR: modifying long-range correlations seems to violate the assumption of locality, and their conclusion is that QM is incomplete.

Most physicists today accept the nonlocality of correlations (in modern terms the existence of entangled states). In fact, as we discuss in next Section, quantum mechanics explicitly violates at least one of the assumptions of reality and locality.

It is useful to reformulate the EPR argument with quantities that can have only discrete values, e.g. spin.

Alice and Bob can share a couple of qubits in the entangled state

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|++\rangle + |--\rangle}{\sqrt{2}} \tag{12.1}$$

Then results of measurements in the computational basis (for electrons: measurements of S_z) are correlated. But according to (12.1) also results of measurements in the oblique basis (measurements of S_x) are correlated.

Alice measures her qubit in the computational basis, and Bob in the oblique basis. The EPR argument would conclude that Alice's qubit has coexistent values for both S_z and S_x. Here we can examine the measurement sequence in detail: suppose that Alice obtains 0 for her measurement in the computational basis, and that Bob obtains + for his measurement in the oblique basis. The 2-qubit state undergoes the modifications

$$|\beta_{00}\rangle \longrightarrow |0\rangle|0\rangle \longrightarrow |0\rangle|+\rangle \tag{12.2}$$

The first measurement by Alice, producing the collapse into $|0\rangle|0\rangle$, has destroyed the correlations in S_x measurements.

Note that the final state does not depend on the order the measurements are made. In fact, if Alice and Bob are separated by a spacelike interval, the order of measurements depends on the system of reference, and is a relative concept depending on the observer. Thus the intermediate state $|0\rangle|0\rangle$ or $|+\rangle|+\rangle$ depends on the frame of reference. Only the state after *both* measurements is independent from the reference frame of the observer.

12.2 Bell's inequality

In 1964 John S. Bell published a paper with title "On the EPR paradox", in Physics 1 (3) 195 (1964), where he shows that any theory that agrees with the predictions of quantum mechanics must violate the assumptions of the EPR paper.

The first part concerns an inequality that must hold whenever we deal with properties (for example values of measurements) that can coexist on the same object. Suppose we have three properties A, B, C that can each have 2 values, respectively $(a, \bar{a})$, $(b, \bar{b})$, $(c, \bar{c})$. For example the property A could be the shade of hair, with two values: $a =$ light and $\bar{a} =$ dark, etc. Moreover consider a collection of objects for which these three properties can have definite values. Then the following inequality holds:

$$N(a, \bar{b}) + N(b, \bar{c}) \geq N(a, \bar{c}) \tag{12.3}$$

where $N(a, \bar{b})$ indicates the number of objects having property A with value a and property B with value $\bar{b}$, etc. This is proven by substituting

$$\begin{aligned} N(a, \bar{b}) &= N(a, \bar{b}, c) + N(a, \bar{b}, \bar{c}), \\ N(b, \bar{c}) &= N(a, b, \bar{c}) + N(\bar{a}, b, \bar{c}), \\ N(a, \bar{c}) &= N(a, b, \bar{c}) + N(a, \bar{b}, \bar{c}) \end{aligned} \tag{12.4}$$

in the inequality (12.3), which rephrases the inequality as

$$N(a, \bar{b}, c) + N(\bar{a}, b, \bar{c}) \geq 0 \tag{12.5}$$

always satisfied since all the numbers N are positive. The Bell inequality then relies on the hypothesis that all three properties can hold together on every object of the collection. This is the "realism" hypothesis: the values of these properties pre-exist the act of measurement, and co-exist on the same object. They can be simultaneously known for every object.

In quantum mechanics there are properties (called observables) whose values cannot be known simultaneously, for example position and momentum of a particle, or polarization of a photon in different directions (after a photon passes through a vertical polarizer, we cannot predict with certainty whether it will pass through a polarizer at $\theta \neq 0$). But following the suggestion of the EPR paper, we could envisage the existence of a theory, a completion of quantum mechanics, capable to assign precise values of position and momentum to the same particle, or precise values to polarization in different directions for the same photon. Measuring these quantities would simply *reveal* the values of properties that preexist the measurement (then observables would be objective quantities in a realistic world). This hypothetical theory is often referred to as *hidden variables theory*, in the sense that it contains extra variables that enable a description of physical states more complete than the one given by quantum mechanics.

For such a theory, the polarizations in three different directions of a collection of photons should satisfy the Bell inequality (12.3). To create hypothetical photons with definite values for two polarizations in different directions we could use correlations, following the EPR idea. Suppose that Charlie has a series of pairs of anticorrelated photons, and sends one photon of the pair to Alice and the other to Bob. Anticorrelation means that if Alice's photon passes a θ polarizer, Bob's photon is absorbed by a θ polarizer, which means that it passes a $\theta + \frac{\pi}{2}$ polarizer. Moreover Alice and Bob have each three polarizers oriented at 0 degrees (vertical polarizer), at θ degrees, and at φ degrees, and we call them for short 0-pol, θ-pol and φ-pol. On each pair Alice and Bob measure the polarization of their photon choosing for a first series of M pairs respectively the 0-pol (Alice) and the θ-pol (Bob), for a second series of M pairs the θ-pol and the φ-pol, and for a third series of M pairs the 0-pol and the φ-pol. At the end of the three series, Alice and Bob compare their results, and obtain the numbers $N(0, \theta)$ of photon pairs that have passed the 0-pol of Alice and the θ-pol of Bob, and similarly for $N(\theta, \varphi)$ and $N(0, \varphi)$. Notice that $N(0, \theta)$ is also the number $N_A(0, \theta + \frac{\pi}{2})$ of Alice's photons with "simultaneous" 0-polarization and $\theta + \frac{\pi}{2}$ polarization, since the other photon of the pair has been measured by Bob to have θ-polarization, and the pair is anticorrelated.

Bell's inequality applied to Alice's photons becomes in this case

$$N_A(0, \theta + \frac{\pi}{2}) + N_A(\theta, \varphi + \frac{\pi}{2}) \geq N_A(0, \varphi + \frac{\pi}{2}) \tag{12.6}$$

or equivalently

$$N(0, \theta) + N(\theta, \varphi) \geq N(0, \varphi) \tag{12.7}$$

This inequality can be rewritten in terms of probabilities

$$p(0, \theta) + p(\theta, \varphi) \geq p(0, \varphi) \tag{12.8}$$

where $p(0, \theta)$ is the probability that in a pair Alice's photon passes the 0-pol and Bob's photon passes the θ-pol, etc., obtained as $p(0, \theta) \approx N(0, \theta)/M$.

We can now prove that the above probabilities computed with the quantum mechanical rules violate the inequality.

In quantum mechanics linearly polarized photons in the θ, $\theta + \frac{\pi}{2}$ directions are described by the orthogonal states (cf. Section 5.3.1):

$$|\theta\rangle = \sin\theta \ |0\rangle + \cos\theta \ |1\rangle, \quad |\theta + \frac{\pi}{2}\rangle = \cos\theta \ |0\rangle - \sin\theta \ |1\rangle \tag{12.9}$$

and the following relation holds:

$$\frac{|1\rangle|0\rangle - |0\rangle|1\rangle}{\sqrt{2}} = \frac{|\theta\rangle|\theta + \frac{\pi}{2}\rangle - |\theta + \frac{\pi}{2}\rangle|\theta\rangle}{\sqrt{2}} \tag{12.10}$$

a special case of (2.21).

Consider now many pairs of photons in the entangled state (12.10). The pairs are sent to Alice and Bob, as discussed above. Alice and Bob make measurements on the photons they receive, with polarizers oriented in three different directions $0, \theta, \varphi$. Note that since the pairs are in the entangled state (12.10), the results of Alice and Bob on every pair will be (anti)correlated in measurements of θ-polarization for any value of θ, due to relation (12.10). We are then in the conditions in which the inequality (12.8) should hold. The probabilities in (12.8) can be computed with the rules of QM. In general we find

$$\begin{aligned} p(\theta,\phi) &= |\langle\theta|\langle\phi|\frac{|1\rangle|0\rangle-|0\rangle|1\rangle}{\sqrt{2}}|^2 = \\ &= |(\langle 0|\sin\theta+\langle 1|\cos\theta)(\langle 0|\sin\varphi+\langle 1|\cos\varphi)\frac{|1\rangle|0\rangle-|0\rangle|1\rangle}{\sqrt{2}}|^2 = \\ &= \frac{1}{2}(-\sin\theta\cos\varphi+\cos\theta\sin\varphi)^2 = \frac{1}{2}\sin^2(\varphi-\theta) \end{aligned} \tag{12.11}$$

for any θ, φ. Applying this formula in (12.8) yields

$$\frac{1}{2}\sin^2\theta + \frac{1}{2}\sin^2(\varphi-\theta) \geq \frac{1}{2}\sin^2\varphi \tag{12.12}$$

which is explicitly violated for example when $\theta = \pi/6, \varphi = \pi/3$ since $1/8 + 1/8 < 3/8$. This thought experiment can be also carried out in a real laboratory with polarized photons, polarizers, single photon counters, and birefringent crystals that create entangled photon couples: the results confirm the predictions of quantum mechanics, and violate Bell's inequality (12.3).

12.3 CHSH inequality

Clauser, Horne, Shimony and Holt proposed a refinement of Bell's inequality in 1969. Again they first consider a classical setting, with Charlie preparing pairs of particles and sending the members of the pair to Alice and Bob. Here Alice has two measuring devices, that measure the physical quantities Q and R, with possible results equal to the values $q = \pm 1, r = \pm 1$. The values q and r are objective properties of Alice's particle, simply revealed by her measurement. After Alice receives the particle, she randomly decides (for example tossing a coin) which quantity to measure. Analogously for Bob who has two measuring devices for quantities S and T, with possible results $s = \pm 1, t = \pm 1$.

Alice and Bob perform their measurements on each pair of particles simultaneously: therefore the measurements are causally disconnected, and Alice's measurement cannot influence the result obtined by Bob and viceversa.

Consider the quantity

$$QS + RS + RT - QT = (R+Q)S + (R-Q)T \tag{12.13}$$

Since R, Q can take only values ± 1, if $R+Q$ takes value ± 2 then $R-Q$ takes value 0 and viceversa. Then the quantity in (12.13) can only take the values ± 2.

Consider now the probability $p(q,r,s,t)$ that the 2-particle system be in the state $Q=q$, $R=r$, $S=s$, $T=t$, i.e. that measurements of Q,R,S,T yield the results q,r,s,t. These probabilities can depend on how Charlie prepares the system, or on transmission noise etc. Denoting by $E(..)$ the average of a statistical variable, we find

$$E(QS+RS+RT-QT) = \sum_{q,r,s,t} p(q,r,s,t)(qs+rs+rt-qt) \le \sum_{q,r,s,t} p(q,r,s,t)2 = 2 \tag{12.14}$$

since the sum on all probabilities is 1. Finally, the average of a sum is the sum of averages, and we have the CHSH inequality:

$$E(QS)+E(RS)+E(RT)-E(QT) \le 2 \tag{12.15}$$

Repeated measurements by Alice and Bob on the 2 particles (prepared always with the same $p(q,r,s,t)$ by Charlie) allow to determine the averages of QS, RS, RT, QT. Alice and Bob communicate after the sequence of measurements and compare results to determine for ex. $E(QS)$ in those measurements where Alice has measured Q and Bob has measured S, etc..

Suppose now that Charlie prepares a quantum state of 2 qubits in the state

$$|\Psi\rangle = \frac{|1\rangle|0\rangle - |0\rangle|1\rangle}{\sqrt{2}} \tag{12.16}$$

and Alice and Bob measure the observables

$$Q = Z \otimes I, \quad R = X \otimes I, \qquad S = I \otimes (-\frac{Z+X}{\sqrt{2}}), \quad T = I \otimes (\frac{Z-X}{\sqrt{2}}) \tag{12.17}$$

Computing the expectation values of the products QS, RS, RT, QT in the state (12.16) yields

$$\langle QS\rangle = \frac{1}{\sqrt{2}}, \quad \langle RS\rangle = \frac{1}{\sqrt{2}}, \quad \langle RT\rangle = \frac{1}{\sqrt{2}}, \quad \langle QT\rangle = -\frac{1}{\sqrt{2}} \tag{12.18}$$

so that

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2} \tag{12.19}$$

violating the CHSH inequality. This violation has been experimentally verified using polarized photons.

Exercise: verify (12.18).

As a consequence, one or more assumptions that underlie the derivation of the CHSH identity must be abandoned. The two main assumptions are:

1) the quantities Q, R, S, T have definite values independent from the observer's measurement. This is the "realism" hypothesis.

2) the measurement by Alice cannot influence the result of Bob's measurement. This is the locality assumption.

In conclusion, the theoretical (using thought experiments) and experimental violation of the Bell and CHSH inequalities show that *nature is not locally realistic*.

13 Lecture 13: Classical and Quantum Cryptography

13.1 Topics in classical cryptography

• Cesar's code: alphabetical substitutions. Symmetric key for coding and decoding

• Frequency analysis. Vernam: keys are random and as long as message, and one key for one message (one-time pad).

• Mechanical encrypting devices, Leonardo da Vinci, Leon Battista Alberti.

• Arthur Scherbius: Enigma (3 rotating disks). Reflector ⇒ symmetric coding. $26 \times 26 \times 26 = 17576$ initial positions of the rotors. Interchangeable rotors: number of possible keys increases by a factor 3!. Insertion of a plugboard (interchanges 6 couples of letters before entering the rotors. 100391791500 ways to do it, with 26 letters) In total $\sim 10^{16}$ key combinations. Weighs 12 kg, $34 \times 28 \times 15$ cm.

• Alan Turing, "On Computable Numbers" , 1937. Bletchley Park, the Bombe, Colossus.

• ENIAC, Electronic Numerical Integrator and Calculator, 1945.

• Data Encryption Standard (DES), 1976. All these systems need key transmission: same key necessary to encrypt and decrypt.

• Public key cryptography: the lock metaphor. Asymmetric key, using modular arithmetic and practical irreversibility of some mathematical functions. Whit Diffie and Martin Hellmann, "New Directions in Cryptography", 1976. Ron Rivest, Adi Shamir and Leonard Adleman, RSA algorithm based on the difficulty of inverting $pq = N$, with $p, q =$ large primes.

Bibliography

Marcus du Sautoy, "The music of the primes" (trad. italiana: "L' enigma dei numeri primi", Rizzoli 2004)

Simon Singh, "The Codebook", 1999

13.2 Modular arithmetic

13.2.1 Definition and properties

Systematically studied by Carl Friedrich Gauss (1801).

The notation

$$a \equiv b \ (mod \ n) \tag{13.1}$$

means that the relative integers a and b differ by integer multiples of n, i.e.:

$$a = b + nk \tag{13.2}$$

with k relative integer. For example $2 \equiv 38$ $(mod\ 12)$ and also $38 \equiv 2$ $(mod\ 12)$.

Modularity is compatible with addition and multiplication. If $a \equiv b$ $(mod\ n)$ and $c \equiv d$ $(mod\ n)$, then

$$a + c \equiv b + d\ (mod\ n), \qquad ac \equiv bd\ (mod\ n) \tag{13.3}$$

Cancellation law: if

$$ux \equiv uy\ (mod\ n) \tag{13.4}$$

then

$$x \equiv y\ (mod\ n) \tag{13.5}$$

only if u is coprime with n (no common factors). Indeed $ux \equiv uy$ $(mod\ n)$ means that n divides $u(x-y)$, and if n is coprime with u, it cannot divide it, and therefore must divide $x - y$, i.e. $x \equiv y$ $(mod\ n)$.

The smaller a satisfying $a \equiv b$ $(mod\ n)$ is simply the remainder of the division b/n. Conventionally we denote this remainder by b $(mod\ n)$. Thus the notation

$$a = b\ (mod\ n) \tag{13.6}$$

with $=$ sign means that a is the remainder of b/n. Note that in this case $a < n$. For example $2 = 38$ $(mod\ 12)$ but $26 \equiv 38$ $(mod\ 12)$. The following property holds:

$$ab\ (mod\ n) = [a\ (mod\ n)\ b\ (mod\ n)]\ (mod\ n) \tag{13.7}$$

13.2.2 Little Fermat Theorem

$$a^p \equiv a\ (mod\ p) \tag{13.8}$$

for any integer a and prime p.

Proof: by induction. It evidently holds for $a = 1$. Suppose that (13.8) holds for an arbitrary integer a, then prove that

$$(a + 1)^p \equiv a + 1\ (mod\ p) \tag{13.9}$$

Recall Newton's binomial expansion

$$(a + 1)^p = \sum_{n=0}^{p} \binom{p}{n} a^n = 1 + \binom{p}{1} a + \binom{p}{2} a^2 + ... \binom{p}{p-1} a^{p-1} + a^p \tag{13.10}$$

Notice now that, when $0 < n < p$:

$$\binom{p}{n} = \frac{p(p-1)...(p-n+1)}{n!} \tag{13.11}$$

is divisible by p if p is prime. Indeed binomial coefficients are integers, so that the denominator in the fraction must divide $(p-1)...(p-n+1)$ (it cannot divide the prime p), and therefore (13.11) for $0 < n < p$ is an integer multiple of p. Then all the terms in (13.10) between 1 and a^p are integer multiples of p, so that

$$(a+1)^p \equiv a^p + 1 \ (mod\ p) \equiv a + 1 \ (mod\ p) \tag{13.12}$$

after using the induction hypothesis $a^p \equiv a \ (mod\ p)$. □

Note: if p does not divide a (as for example when $a < p$) we can apply the cancellation law and Fermat's little theorem becomes

$$a^{p-1} \equiv 1 \ (mod\ p) \tag{13.13}$$

13.2.3 Euclid's algorithm

It is described in Euclid's books 7 and 10 of the *Elements* (circa 300 a.C.), and determines the *greatest common divisor* (GCD) of two integers a, b.

If $a > b$, the sequence

$$\begin{aligned}
&a = q_0 b + r_0 \\
&b = q_1 r_0 + r_1 \\
&r_0 = q_2 r_1 + r_2 \\
&\cdots \\
&r_{N-3} = q_{N-1} r_{N-2} + r_{N-1} \\
&r_{N-2} = q_N r_{N-1} + r_N
\end{aligned} \tag{13.14}$$

ends with $r_N = 0$ (a remainder is stricly smaller than the divisor, so that $r_k < r_{k-1}$ and the series of remainders must terminate with 0). Then the last nonvanishing remainder r_{N-1} is the greatest common divisor of a and b, denoted by GCD(a, b).

Proof: since $r_{N-2} = q_N r_{N-1}$, r_{N-1} divides r_{N-2}. Then $r_{N-3} = q_{N-1} r_{N-2} + r_{N-1} = (q_{N-1} q_N + 1) r_{N-1} \Longrightarrow r_{N-1}$ divides also r_{N-3}. Iterating, we prove that r_{N-1} divides all the remainders, and also a and b. Thus r_{N-1} is a divisor of a and b. Next we prove that it is the greatest divisor. Any divisor c must divide r_0, because $r_0 = a - q_0 b$. Analogously we show that c divides all the remainders, and therefore divides r_{N-1}, which implies $c \leq r_{N-1}$. Therefore r_{N-1} is the GCD of a and b. □

13.2.4 Extended Euclid's algorithm

An immediate consequence of Euclid's algorithm is that we can write the GCD of a and b as

$$GCD(a, b) = sa + tb \tag{13.15}$$

with s, t relative integers. Indeed starting from the bottom of the sequence in (13.14) we have GCD$(a, b) = r_{N-1} = r_{N-3} - q_{N-1} r_{N-2}$ and we obtain the GCD as a linear combination with integer coefficients of the remainders r_{N-2}, r_{N-3}. Similarly we can express r_{N-2} and r_{N-3} as linear combinations of preceding remainders, and so on $\Longrightarrow$ MCD(a, b) is expressed as in (13.15). □

13.2.5 Linear modular equations

The extended Euclid's algorithm allows to solve for x linear modular equations of the type:

$$ax \equiv c\ (mod\ b), \quad a, b, c, x\ integers \tag{13.16}$$

We want to find x such that $ax - c$ be an integer multiple of b, which is equivalent to find integers x, y such that

$$ax + by = c \tag{13.17}$$

Consider

$$sa + tb = g \tag{13.18}$$

where $g = \mathrm{GCD}(a, b)$, and s, t can be found with Euclid's extended algorithm. Since g divides a and b, g must divide also c, cf. (13.17). Thus c/g is an integer. A solution for x and y is then given by

$$x = s(c/g), \quad y = t(c/g) \tag{13.19}$$

Exercise: use the extended Euclid's algorithm to find x such that $7x \equiv 1\ (mod\, 160)$. Answer: $x = 23$.

13.3 RSA algorithm - public key cryptography

Rivest, Shamir and Adleman (RSA) algorithm is based on an asymmetric key. The key used to encode the message is public, and different from the secret key used to decrypt it.

Bob wants to send a message M to Alice. For example Alice is a bank and Bob is a client who wants to send his credit card number M to the bank. The protocol runs as follows.

Alice:

1) chooses two giant prime numbers, p and q. We assume that M is always less that the product pq. To illustrate the procedure, we take two small prime numbers $p = 17$, $q = 11$. The two primes are the *private key*, known only by Alice.

2) computes $N = pq$. Here $N = 187$.

3) chooses another number e, relatively prime with $(p - 1)(q - 1)$ and smaller than $(p - 1)(q - 1)$. For example $e = 7$ is relatively prime with 160 (i.e. their GCD is 1), and $<$ than 160.

4) publishes e and N. This couple of integers is the *public key*.

Bob:

1) encrypts his credit card number M into a coded message C with the formula:

$$C = M^e \ (mod\ N) \tag{13.20}$$

using the public key (N, e). For example, if $M = 88$, $C = 88^7\ (mod\ 187)$. This calculation is simplified if we use (13.7): $88^7\ (mod\ 187) = [88^4\ (mod\ 187) \times 88^2\ (mod\,187) \times 88\ (mod\,187)]\ (mod\,187) = 132 \times 77 \times 88\ (mod\,187) = 894432\ (mod\,187) = 11$. Thus $C = 11$ is the coded message.

2) sends C to Alice. A malicious interceptor, traditionally called Eve, will not be able to decode the message, if p and q are very large primes. Indeed to decrypt C, i.e. to invert formula (13.20), the knowledge of p and q is necessary. Eve can try to deduce p and q by factorizing the giant number N, but this is an arduous task with conventional computers: the number of necessary operations grows exponentially with N in all classical known algorithms.

Alice:

1) computes the *decryption key* d, defined by

$$ed = 1\ (mod\ (p-1)(q-1)) \tag{13.21}$$

In our example $7d = 1\ (mod\ 160)$ can be solved easily with Euclid's extended algorithm, to find $d = 23$.

2) using this key, which has required the knowledge of the secret couple (p,q), she can decrypt the coded message C by virtue of the inversion formula

$$M = C^d\ (mod\ N) \tag{13.22}$$

obtaining $M = 11^{23}\ (mod\ 187) = 88$, recovering the message M of Bob.

We now prove the inversion formula. Raising to the d-th power both members of the encryption formula yields

$$C^d \equiv M^{ed}\ (mod\ N) \tag{13.23}$$

The equation (13.21) defining d implies

$$ed = 1 + r(p-1)(q-1) = 1 + k(p-1) = 1 + h(q-1) \tag{13.24}$$

If M *is not a multiple* of p, then M and p are coprime, because p is prime. By Fermat's little theorem

$$M^{p-1} = 1\ (mod\ p) \tag{13.25}$$

and

$$M^{ed} = M^{1+k(p-1)} = (M^{p-1})^k M \equiv 1^k M \ (mod\ p) = M \ (mod\ p) \tag{13.26}$$

Thus

$$M^{ed} \equiv M(mod\ p) \tag{13.27}$$

If M *is a multiple* of p,

$$M^{ed} \equiv 0 \ (mod\ p) \equiv M \ (mod\ p) \tag{13.28}$$

We can conclude that p always divides $M^{ed} - M$. Similarly we prove that

$$M^{ed} \equiv M(mod\ q) \tag{13.29}$$

i.e. q divides $M^{ed} - M$. Since p and q are primes, also $N = pq$ divides $M^{ed} - M$:

$$M^{ed} \equiv M(mod\ N) \tag{13.30}$$

Thus, using (13.23)

$$C^d \equiv M^{ed} \ (mod\ N) \equiv M(mod\ N) \Longrightarrow M \equiv C^d \ (mod\ N) \tag{13.31}$$

Finally, since $M < N$ (N is very large), it is also the smallest M satisfying $M \equiv C^d \ (mod\ N)$, i.e.

$$M = C^d \ (mod\ N) \tag{13.32}$$

and the inversion formula is proved. □

13.4 Quantum cryptography

As discussed in Lecture 23, a quantum algorithm due to Peter Shor factorizes N in polynomial time. When quantum computers will be commercially available, the security of the RSA encryption protocol will vanish. Quantum mechanics however offers an intrinsecally secure solution: *quantum cryptography*.

13.4.1 BB84 protocol

Alice wants to send a message to Bob, in the form of a string of bits. Using polarized photons, Alice could send a sequence of them, with polarizations corresponding to the states $|0\rangle$ and $|1\rangle$, the sequence reproducing the message. Bob has a vertical polarizer, and can therefore distinguish the two orthogonal polarization states, and thus reconstruct the message of Alice.

However the photons can be intercepted by Eve, who can measure their polarization by using a vertical polarizer. She can read the message, and send the same sequence to Bob, who will not suspect Eve's intervention. So Eve's eavesdropping is undetected in this case, and the transmission between Alice and Bob is not secure.

However Alice can send photons in *two different bases*: the $|0\rangle, |1\rangle$ basis, corresponding to horizontal and vertical polarizations, and the $|+\rangle, |-\rangle$ basis, corresponding to 45° and 135° polarizations. Alice chooses the bases randomly, and so does Bob when he measures the photons sent by Alice, using vertical or 45° polarizers. The bit 0 is encoded in the $|0\rangle$ and $|+\rangle$ photons, while the bit 1 is encoded in the $|1\rangle$ and $|-\rangle$ photons. Exploiting the two bases, Alice and Bob can verify whether their communication is secure, free from interception. The BB84 protocol, proposed by Bennet and Brassard in 1984, runs as follows.

Alice sends a string of photons to check security, say 200 photons. She chooses the bases at random, and sends a string of 200 bits by coding the bits 0 and 1 as discussed above. Bob measures the photons sent by Alice using at random the polarizers corresponding to the two bases. When Bob uses the same basis chosen by Alice, the results of Alice and Bob will agree: if Alice sends the bit 0(1), Bob will measure the bit 0(1). When Alice and Bob use different bases, the measurement by Bob has a probability 1/2 to agree with the bit sent by Alice (for example a photon sent by Alice in the state $|-\rangle$ (bit 1) has a probability 1/2 to pass (bit 1) Bob's vertical polarizer). After the 200 photons have been sent by Alice, and measured by Bob, Alice calls Bob by phone, in a public channel, and compares with Bob the bases used for every photon. Alice and Bob can write down a list of the photons that have been sent and measured on the same bases (approximately one half of the 200 photons). The results on the other photons are just discarded. Then Alice and Bob check whether they agree on the bits encoded in the polarizations. If disagreements are above a certain threshold (depending for ex. on the noise of the optical fiber used or the transmission) they can deduce that Eve has tried to intercept.

Indeed, if Eve is intercepting, she measures the photons sent by Alice with two polarizers (let us suppose that she knows that Alice and Bob use vertical and 45° polarizers), but she cannot know which of the two bases has been used by Alice, since Alice phones Bob *after* the transmission of the 200 photons. Eve has a 50% chance to guess the correct basis, and use the correct polarizer to measure photons without disturbing them (recovering the bit and transmitting the same photon to Bob). In this case the bit sent by Alice will coincide with the bit received by Bob. However, in approximately the other half of the cases, Eve will not guess right, and use a polarizer not adapted to the basis chosen by Alice. In this case, the photon Eve transmits to Bob has a 50% chance to yield the correct bit (i.e. the same bit Alice sent) when it is measured by Bob. Thus, compounding these probabilities, Eve has a 75% chance of being undetected, for every photon she intercepts. With 100 photons, she has a $(3/4)^{100} \approx 3.2 \times 10^{-13}$ chance of being undetected, and Alice and Bob, checking the agreement between their bits, will know whether they have been intercepted.

After this security check, Alice and Bob can use the same channel (for ex. optical fiber) to send messages, or a secret key to encode future messages. This is why the BB84 algorithm is also called e quantum key distribution (QKD) algorithm. Note that the probabilistic character of measurement of photons using different bases in emission and reception can be used by Alice to produce genuinely random sequences of bits 0 and 1, and use them as secret keys if the channel is secure.

13.4.2 Ekert protocol

In this protocol, proposed by Artur Ekert in 1991, the photons are not prepared by Alice, but by a third party (Charlie) who produces pairs of entangled photons, for ex. in the Bell state $|\beta_{00}\rangle$, and sends one to Alice and the other to Bob. Alice and Bob measure the photons using again two different polarizing filters chosen at random. The remaining part of the protocol is identical to the BB84. If there are no interceptors, Alice and Bob receive correlated photons, and if they choose the same bases for the measurement their bits should be identical. If not, there is a detected intrusion by Eve.

14 Lecture 14: Turing machine

Models of classical computing:

- Turing machine
- Circuits.

14.1 Turing machine

Contains 4 elements:

1) program
2) finite state controller
3) tape
4) tape writer and reader

The INPUT is the initial content of the tape. The OUTPUT is the final content of the tape. The *finite state controller* operates on a finite set of internal states $q_1, ...q_m$, and is a sort of microprocessor, coordinating the machine operation. There are also two special internal states q_s, q_h, respectively the starting state and the halting state. The tape is written with 4 characters: 0, 1, $\triangleright$, b (blank).

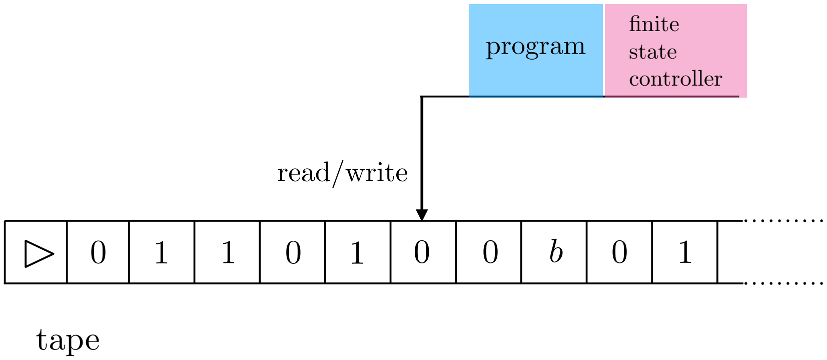


Fig. 14.1 Turing machine

The Turing machine (TM) starts in the internal state q_s, and with the tape writer/reader on the first square of the tape, containing the start symbol $\triangleright$. The computation proceeds serially according to the *program*. When the internal state becomes q_h, the machine halts and the result of the computation is the content of the tape.

A program is a finite list of instructions of the form (q, x, q', x', s) where

q: state
x: 0, 1, $\triangleright$, b
s: -1,0,+1

The controller examines the list of instructions (program), until it finds a program line (q, x, q', x', s) where q is the current state of the machine and x is the character under the tape reader/writer. In that case the controller executes the program line: it changes the internal state to q', overwrites the symbol x turning it into x', and moves the tape reader/writer one step left, right, or does not move it, according to $s = -1, +1, 0$. If no program line is found with q=internal state and x = character under the reader/writer, the state changes into q_h and the machine stops.

Exercise: consider the program

$(q_s, \triangleright, q_1, \triangleright, +1)$
$(q_1, 0, q_1, b, +1)$
$(q_1, 1, q_1, b, +1)$
$(q_1, b, q_2, b, -1)$
$(q_2, b, q_2, b, -1)$
$(q_2, \triangleright, q_3, \triangleright, +1)$
$(q_3, b, q_h, 1, 0)$

Show that it computes the function $f(z) = 1$, where z is a string of bits. *Hint:* verify it on a definite z, for example $z = 1001$, and show that if the initial tape configuration is $\triangleright, 1, 0, 0, 1, b, b, ...$, the output tape configuration is $\triangleright, 1, b, b, ...$

Every program executable on a modern computer can be translated in a program for TM and viceversa. This is *the Church-Turing thesis:* the class of functions computable with a TM coincides with the class of functions computable with an algorithm.

14.2 Turing number

To every TM we can assign an integer number T_M that identifies TM uniquely. The TM is characterized by its program: thus we assign a number T_M to every possible program. There are many ways to do it. For example, we can represent the ordered sequence of q_i in the program lines of the Exercise in previous Section by first establishing the dictionary $q_1 \to 1, q_2 \to 2, q_3 \to 3, q_s \to 4, q_h \to 0$, and then defining the integer in base 5 as

$$N_1 = 41111112222330 = 0 \cdot 5^0 + 3 \cdot 5^1 + 3 \cdot 5^2 + 2 \cdot 5^3 + \cdots \tag{14.1}$$

There is then a 1-1 correspondence between base 5 integers and arbitrary sequences of five possible internal states. If the internal states are m, the integer N_1 will be a base m integer. We need also to specify m, via the integer $N_0 = m$. Analogously we construct a base 4 integer N_2 describing the sequence of tape characters in the program lines, setting $0 \to 0, 1 \to 1, \triangleright\to 2, b \to 3$. For the program lines of the Exercise we find

$$N_2 = 22031333332231 \tag{14.2}$$

Finally for the sequence of s in the program lines we translate $0 \to 0, +1 \to 1, -1 \to 2$ and we find the base 3 integer

$$N_3 = 1112210 \tag{14.3}$$

The four integers N_0, N_1, N_2, N_3 contain the whole information on the program in the Exercise, and therefore uniquely determine the corresponding TM. However, we want to characterize a TM by a *single integer number* T_M. This is achieved by using for example a 1-1 correspondence between couples of integers (N_1, N_2) and integers N

$$(N_1, N_2) \longleftrightarrow N \tag{14.4}$$

and then using the same correspondence to assign an integer number N' to (N_0, N_3). Finally we assign

$$(N, N') \longleftrightarrow T_M \tag{14.5}$$

Then from the number T_M we can work out in reverse the couple (N, N'), and from N and N' the couples (N_1, N_2) and (N_0, N_3), and therefore the quadruple N_0, N_1, N_2, N_3 determining the TM.

One way to find a 1-1 correspondence between couples of integers and integers is illustrated below.

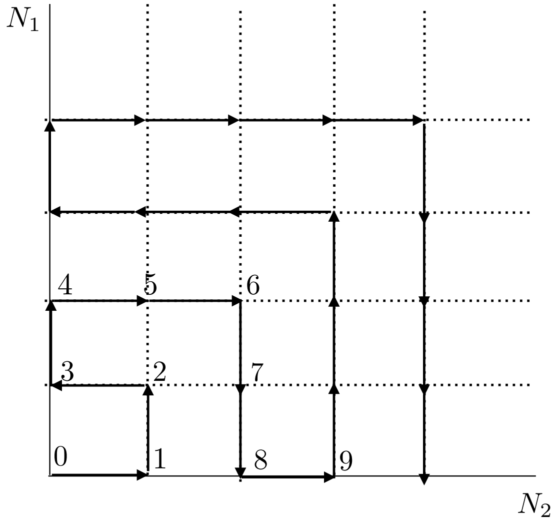


Fig. 14.2 A 1-1 correspondence between (N_1, N_2) and N: the numbers in the grid refer to N, and to every N corresponds a point with coordinates (N_1, N_2).

14.3 Universal Turing machine

Let M be a Turing machine with Turing number T_M.

The *universal Turing machine* (UTM) is defined as follows. If its input tape contains the binary representation of T_M, a blank, and a string of tape characters x, then UTM produces as output the same output M would produce with input x.

Thus UTM can simulate *any* Turing machine M. It is similar to a modern programmable computer. The program corresponding to T_M is written as input on the tape, and data to be processed by the program are written in a different part of the input tape. Then a fixed program (that defines the UTM) is used to execute the program T_M.

Exercise: discuss the case of an UTM input tape containing $T_M = T_{UTM}$.

14.4 Halting problem

Can all well-posed mathematical problems be solved by an algorithm ? The answer is no. There are easy problems, hard problems, and impossible problems (cf. Gödel).

An example of a problem with no algorithmic solution is the Halting problem. The following proposition

> "Does the program of a TM with Turing number x halt, if input is y ?"

is undecidable. In particular, no algorithm exists providing an answer to the proposition

> "Does the program of a TM with Turing number x halt, if input is x ?"

Proof: by contradiction. Define the *halting function*

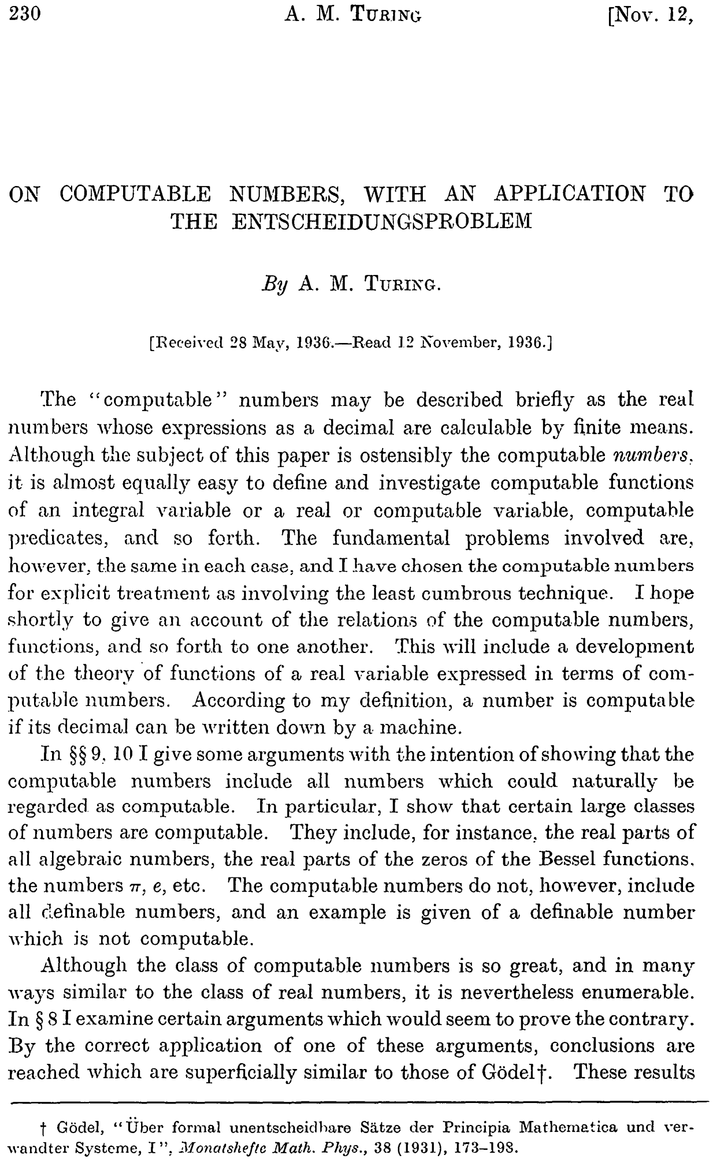
$$h(x) = \begin{cases} 0 & \text{if TM } x \text{ does not halt, with input } x \\ 1 & \text{if TM } x \text{ does halt, with input } x \end{cases}$$

Suppose an algorithm HALT(x) exists to evaluate $h(x)$. Then consider the following program:

```
TURING($x$)
$y$ = HALT($x$)
if $y = 0$ then
            halt
      else
            loop forever
end if                                    (14.6)
```

If HALT is a valid algorithm, TURING is a valid program with Turing number t. By definition of halting function, $h(t) = 1$ if and only if TURING halts with input

t. But examining TURING we see that it halts with input t if and only if $h(t) = 0$ $\Longrightarrow$ contradiction. Then the assumption that an algorithm exists for computing $h(x)$ is wrong: *no algorithm can be found for the halting problem.* □



230 A. M. Turing [Nov. 12,

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. Turing.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

In §§ 9, 10 I give some arguments with the intention of showing that the computable numbers include all numbers which could naturally be regarded as computable. In particular, I show that certain large classes of numbers are computable. They include, for instance, the real parts of all algebraic numbers, the real parts of the zeros of the Bessel functions, the numbers π, e, etc. The computable numbers do not, however, include all definable numbers, and an example is given of a definable number which is not computable.

Although the class of computable numbers is so great, and in many ways similar to the class of real numbers, it is nevertheless enumerable. In § 8 I examine certain arguments which would seem to prove the contrary. By the correct application of one of these arguments, conclusions are reached which are superficially similar to those of Gödel†. These results

† Gödel, "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I", *Monatshefte Math. Phys.*, 38 (1931), 173–198.

Fig. 14.3 First page of: Alan M.Turing, Proceedings of the London Mathematical Society, 2, 42 (1) 230-65 (1937)

15 Lecture 15: Classical circuits

Circuits, with wires and gates, are a model of computation equivalent to the Turing machine, and often more convenient and realistic.

15.1 Basic gates

A classical logical gate is a function $f : \{0,1\}^n \longrightarrow \{0,1\}^m$, taking n bits into m bits. When $m = 1$ the function is said to be *boolean*. For example, the NOT classical gate is a 1-bit to 1-bit function, the AND gate is a 2-bit to 1-bit function etc. Both implement boolean functions. Basic classical gates are given in Fig. 15.1.

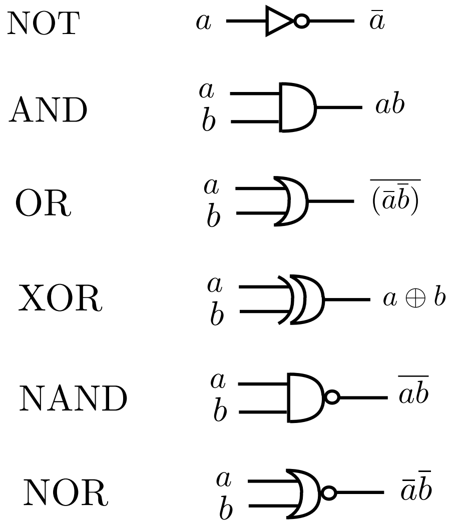


Fig. 15.1 Classical gates.

Example: a circuit that adds two 3-bit integers is shown in Fig. 15.2. It generalizes easily to n-bit integers.

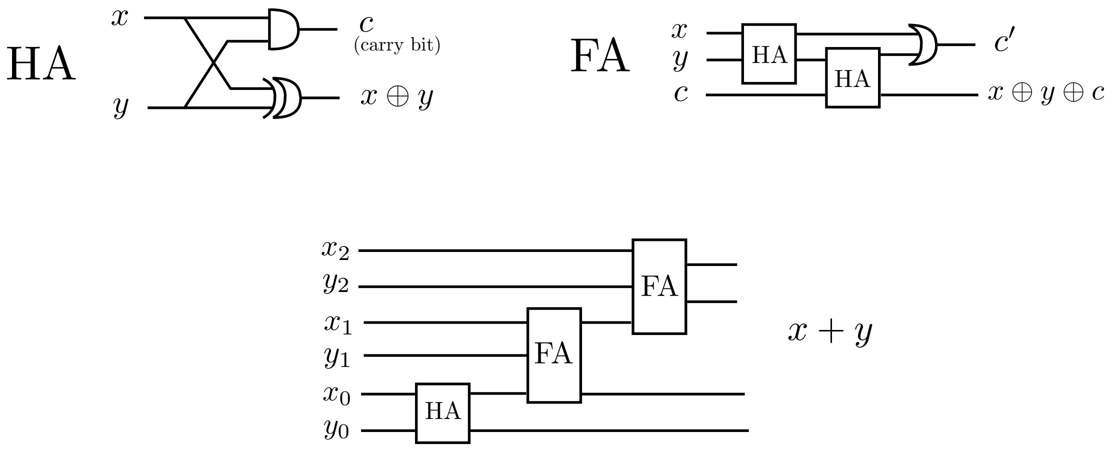


Fig. 15.2 Adds two binary integers $x = x_0x_1x_2$, $y = y_0y_1y_2$. The carry bit c in the half-adder HA is 1 if $x = y = 1$. The carry bit c' in the full-adder FA is 1 if at least two input bits are 1.

Observation: any function f of n bits into m bits:

$$f(x_1, ...x_n) = (f_1(x_1, ...x_n), f_2(x_1, ...x_n), ..., f_m(x_1, ...x_n)) \tag{15.1}$$

is equivalent to m functions $f_1, f_2, ..., f_n$ of n bits to 1 bit (the "components" of the function f).

15.2 Universal set: NAND and FANOUT

Theorem: the gates NAND and FANOUT are a *universal set*: using only these gates, every function $f : \{0, 1\}^n \longrightarrow \{0, 1\}^m$ can be implemented in a circuit.

In virtue of the above observation, we need to prove the Theorem only for boolean functions $f(x_1, ..., x_n)$.

We first give in Fig. 15.3 some examples of basic gates, realized with circuits that use only NAND and FANOUT.

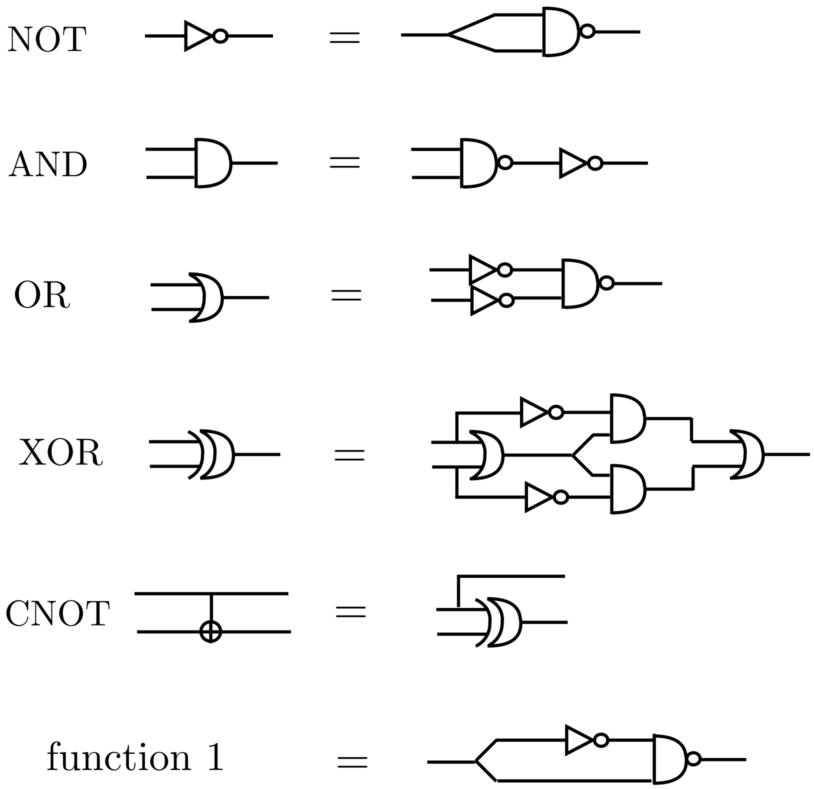


Fig. 15.3 Basic gates in terms of NAND and FANOUT

The proof of the Theorem proceeds by induction on n. For $n = 1$ there are 4 possible boolean functions: the identity (represented by a wire), the NOT gate, the 0 function and the 1 function. These functions are all implementable using only NAND and FANOUT, see Fig. 15.3 (the 0 function is obtained from the 1 function simply by adding the NOT gate to the circuit).

Next we suppose that the Theorem holds for n, and prove that it holds for $n+1$, i.e. for boolean functions $f(x_0, x_1, ..., x_n)$. To do so we define

$$f_0(x_1, ..., x_n) \equiv f(0, x_1, ..., x_n), \qquad f_1(x_1, ..., x_n) \equiv f(1, x_1, ..., x_n) \tag{15.2}$$

By the induction hypothesis, these two n-bit boolean functions are implemented by circuits with only NAND and FANOUT gates, represented in Fig. 15.4 with rectangular boxes. The same Figure proves the Theorem: indeed it realizes a circuit that computes $f(x_0, x_1, ..., x_n)$, using only NOT, AND, XOR and the rectangular boxes. All these circuit components can be realized with only NAND and FANOUT, cf. Fig. 15.3. □

To be precise, Fig. 15.4 contains also CROSSOVER components, since there are crossings between the wires. We recall that CROSSOVER can be realized with three CNOT gates, and CNOT is realizable with NAND and FANOUT, as in Fig. 15.3.

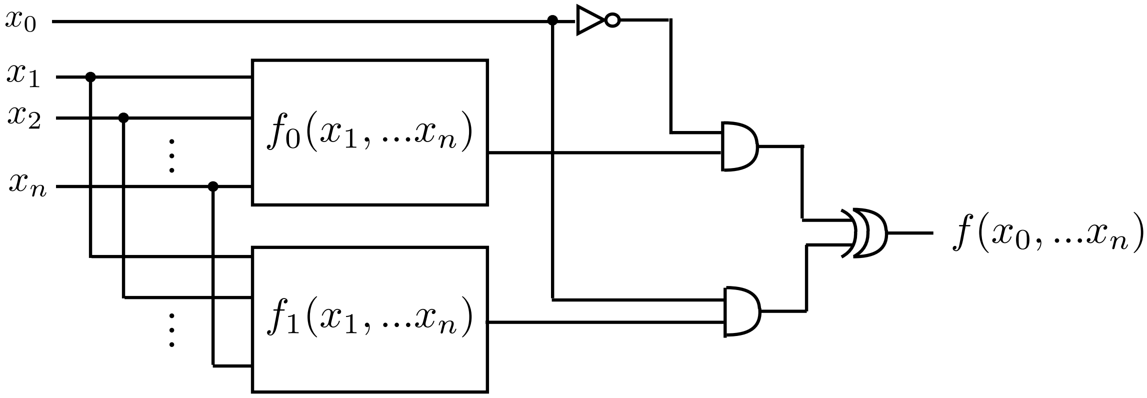


Fig. 15.4 Proof of universality of NAND and FANOUT

16 Lecture 16: Complexity

16.1 Asymptotic notation

A notation that captures the essential behaviour of a function for large values of its variable.

1) $f(n) = O(g(n))$ if there exists a n_0 such that for any $n > n_0$, $f(n) \leq c\, g(n)$ with $c =$ constant.

2) $f(n) = \Omega(g(n))$ if there exists a n_0 such that for any $n > n_0$, $f(n) \geq c\, g(n)$ with $c =$ constant.

3) $f(n) = \Theta(g(n))$ if $f(n)$ and $g(n)$ have the same asymptotic behaviour up to a constant factor. If $f(n) = O(g(n)) = \Omega(g(n))$ then $f(n) = \Theta(g(n))$.

Examples:

• $2n$ is $O(n^2)$, 2^n is $\Omega(n^3)$

• $7n^2 + \sqrt{n}\log n$ is $\Theta(n^2)$ since $7n^2 \leq 7n^2 + \sqrt{n}\log n \leq 8n^2$ for n sufficiently large.

• $f(n) = O(g(n)) \Leftrightarrow g(n) = \Omega(f(n))$, $f(n) = \Theta(g(n)) \Leftrightarrow g(n) = \Theta(f(n))$.

• if $g(n)$ is a polynomial of order k, $g(n) = O(n^l)$ for $k \leq l$.

• $\log n = O(n^k)$ for any $k > 0$.

• $n^{\log n}$ is superpolynomial: $n^k = O(n^{\log n})$ for any k, but $n^{\log n} \neq O(n^k)$.

• $n^{\log n}$ is subexponential: $c^n = \Omega(n^{\log n})$ for any $c > 1$, but $n^{\log n} \neq \Omega(c^n)$.

• if $e(n) = O(f(n))$ and $g(n) = O(h(n))$, then $e(n)g(n) = O(f(n)h(n))$.

Exercise: : show that ordering n names alphabetically is $\Omega(n \log n)$. Since algorithms are known, that are $O(n \log n)$, the ordering problem is $\Theta(n \log n)$.

16.2 Computational complexity

Easy problems: solution can be found in polynomial time, i.e. with a number of steps that is a polynomial function of the dimension n of the input. For example the addition of two n-bit integers scales as n.

Hard problems: superpolynomial in n. For example the factorization of an integer N requires a number of steps scaling as $\exp n$, if n is the number of digits of N.

The main *complexity classes* are:

P: problems that can be solved in polynomial time (easy problems).
NP: problems whose solution can be verified in polynomial time.
NP-complete: *any* NP problem can be reduced to a NP-complete problem.

Obviously NP includes P. No proof exists, but it is generally believed that **NP ≠ P**. If a polynomial-time resolution of a NP-complete problem was ever found, any NP problem could be solved in polynomial time, which would imply P = NP. The current consensus is that no polynomial time resolution of a NP-complete problem exists.

For example integer factorization is **NP**, since the solution can be checked (by multiplication) in polynomial time. However no polynomial time factorization algorithm is known within classical computation. The situation changes with quantum computation: the Shor algorithm, based on the quantum Fourier transform (see Lecture 23), factorizes in polynomial time. Unfortunatley the factorizing problem is not NP-complete, so that we cannot conclude P = NP within quantum computation.

16.3 Examples

• A *graph* is a finite collection of *vertices* $\{v_1, ...v_n\}$, connected by links (v_i, v_j). The graph is non-directional if the order of the vertices in the links is irrelevant. A *cycle* is a sequence of vertices $\{v_1, ...v_m\}$ such that every pair (v_j, v_{j+1}) is a link and (v_m, v_1) is a link. In words, a cycle is a closed path in the graph.

A cycle is *simple* if all its vertices appear only once.
A cycle is *Hamiltonian* if it is simple and includes all the vertices of the graph.
A cycle is *Eulerian* if every link of the graph is “visited” only once.

Given a graph, no polynomial algorithm is known to decide whether it admits a Hamiltonian cycle. Moreover the Hamiltonian cycle (HC) problem can be shown to be NP-complete.

Perhaps surprisingly, the Eulerian cycle (EC) problem is in class P. In fact, a graph admits an Eulerian cycle if it is connected and only an even number of lines originate from every vertex of the graph, a result due to Euler. Checking that it is connected requires $O(n^2)$ operations, and checking the number of incident lines for every vertex requires $O(n^3)$ operations (there are at most $n(n-1)/2$ lines in the graph with n vertices). Thus EC is in class P.

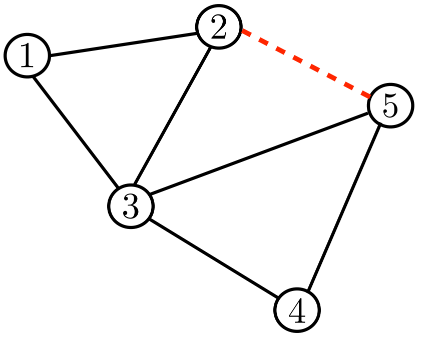


Fig. 16.1 Without the dashed line, this graph has no Hamiltonian cycle, but has a Eulerian cycle. With the dashed line, there is a Hamiltonian cycle, but no Eulerian cycle.

Both HC and EC are examples of *decisional problems*: an algorithm solving the problem anwers yes or no to the question of existence of particular cycles.

• The Traveling Salesman Problem (TSP) is another NP-complete decisional problem, and is formulated as follows:
"Given n towns and a distance d_{ij} between town i and town j, is there a closed path including all towns with total length $< d$? "

We now prove that HC reduces to TSP. It suffices to apply TSP with the following specifications: if the graph has n vertices, each vertex is considered a town, and the distance d_{ij} beween towns is assigned to be 1 if the corresponding vertices in the graph are connected by a link, and 2 otherwise. Then with TSP we can answer the question: does a closed path connecting all towns exist, with length $< n + 1$?. An algorithm solving TSP will provide the answer: if positive, it implies that such a path exists, and its length is n (it must be $< n + 1$ and, since the closed path connects n towns, it must be at least n). Then a Hamiltonian cycle exists in the graph, including all its vertices only once. □

Thus, given an algorithm that solves TSP, it can be converted to an algorithm that solves HC. Since HC is NP-complete, this implies that also TSP is NP-complete: if every NP problem reduces to HC, it also reduces to TSP.

• CSAT (circuit satisfybility) is the decisional problem: "Given a boolean circuit composed by AND, OR, NOT gates, does an input assignment exist that gives as output the bit 1 ? ". This problem can be shown (Cook-Levin proof) to be NP-complete, by use of the Turing machine paradigm, see for ex. Chuang and Nielsen, p.146. Thus if a problem is NP, and CSAT reduces to it, the problem is also NP-complete. In this way many other problems have been shown to be NP-complete.

• SUBSET SUM is another NP-complete problem, well suited to be attacked also by quantum computing protocols. It consists in finding whether a subset exists, in a list of integers $(n_1, ...n_N)$, having as sum a given integer S.

Note: no quantum protocol is known to solve in polynomial time NP-complete problems. It is widely believed that P $\neq$ NP also within quantum computation.

16.4 Energy and information

Energy requirements for computation are related to *reversibility*. In irreversible gates, as for example the classical NAND gate, there is loss of information. To cancel information, energy is required, as stated in Landauer's principle (1961):

To cancel 1 bit, an energy of at least $kT \log 2$ is required.

This principle can be justified by considering the encoding of 1 bit by using a gas in a box. The gas is very peculiar, consisting of only one molecule. The box is divided into two parts, with a mobile partition. As such, the box contains 1 bit of information, which has value 0 if the molecule is on left of the partition, and value 1 if on the right of the partition. Suppose we want to cancel this information: we remove the partition and compress the gas to the left with a piston, which slides halfway into the box. Now the molecule will be located with certainty in the left part of the box, and carries no information. A bit has been cancelled. But work was necessary to compress the gas. This work can be computed by considering the entropy of the system before and after compression. In the initial state, the box had entropy $S = k \log(\text{number of microstates}) = k \log 2$, since there are two possible microstates (molecule on the left, molecule on the right). After the compression, only 1 microstate survives, and the box has entropy = 0. Thus the box entropy has decreased by $\Delta S = k \log 2$, which corresponds to a work $W = T\Delta S = kT \log 2$.

16.5 Reversible classical computation: the TOFFOLI gate

The gates for a classical universal set, NAND and FANOUT , are non reversible. Information is lost: from the output we cannot reconstruct the input. Nevertheless, it is possible to simulate NAND and FANOUT with reversible gates. For example the Toffoli gate, a 3-bit to 3-bit gate, can be used as in Fig. 16.2 to act as NAND or FANOUT. Thus Toffoli by itself can be considered a universal set.

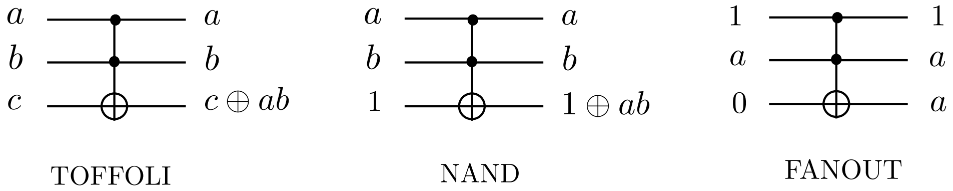


Fig. 16.2 The TOFFOLI gate, and its use to simulate NAND and FANOUT

This shows that classical computation can be made reversible, but at the cost of introducing service bits in input ("ancilla bits") , and producing extra bits in output (“garbage bits”). These extra bits must be cancelled at some stage, to reduce cluttering of the memory, and will require energy for their cancellation.

17 Lecture 17: Quantum circuits I

17.1 Rotation operators

We define the operators:

$$R_x(\theta) \equiv \exp(-i\frac{\theta}{2}X) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{17.1}$$

$$R_y(\theta) \equiv \exp(-i\frac{\theta}{2}Y) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{17.2}$$

$$R_z(\theta) \equiv \exp(-i\frac{\theta}{2}Z) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{pmatrix} \exp(-i\frac{\theta}{2}) & 0 \\ 0 & \exp(i\frac{\theta}{2}) \end{pmatrix} \tag{17.3}$$

These are unitary operators acting on 1-qubit states. They are called rotation operators because they rotate the qubits on the Bloch sphere, by an angle θ, respectively around the x, y, z axes. For example

$$R_x(\theta)|\vec{r}\rangle = |\vec{r}\,'\rangle, \qquad \vec{r}\,' = \mathcal{R}_x(\theta)\ \vec{r} \tag{17.4}$$

with $\mathcal{R}_x(\theta)$ acts on the 3-dimensional Bloch vector by rotating it around the axis x by an angle θ (counterclockwise). Thus we have a 1-1 correspondence between operators R on the qubit Hilbert space and geometric rotations $\mathcal{R}$ in the usual 3-dimensional euclidean space. We now prove eq. (17.4).

Proof: consider the density operator corresponding to a pure qubit state $|\vec{r}\rangle$:

$$\rho = |\vec{r}\rangle\langle\vec{r}| = \frac{I + \vec{r}\cdot\vec{\sigma}}{2} \tag{17.5}$$

cf. eq. (11.10). The density operator corresponding to the transformed state $|\vec{r}\,'\rangle$ is

$$\rho' = |\vec{r}\,'\rangle\langle\vec{r}\,'| = R_x(\theta)\ |\vec{r}\rangle\langle\vec{r}|\ R_x(\theta)^\dagger = R_x(\theta)\ \frac{I + \sum_i r_i\sigma_i}{2}\ R_x(\theta)^\dagger =$$
$$= \frac{I + \sum_i r_i\ R_x(\theta)\sigma_i R_x(\theta)^\dagger}{2} \tag{17.6}$$

On the other hand we also have

$$\rho' = \frac{I + \vec{r}\,'\cdot\vec{\sigma}}{2} \tag{17.7}$$

and comparing (17.6) and (17.7) we deduce r_i'. Computing $R_x(\theta)\sigma_i R_x(\theta)^\dagger$ we find

$$R_x(\theta)XR_x(\theta)^\dagger = X \tag{17.8}$$

$$R_x(\theta)YR_x(\theta)^\dagger = (\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X)\ Y\ (\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X) =$$
$$= \cos\theta\ Y + \sin\theta\ Z \tag{17.9}$$

$$R_x(\theta)ZR_x(\theta)^\dagger = (\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X)\ Z\ (\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X) =$$
$$= -\sin\theta\ Y + \cos\theta\ Z \tag{17.10}$$

using Pauli matrices identities $XYX = -Y$, $XY = iZ$ etc., and basic trigonometric identities $\cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} = \cos\theta$, $2\sin\frac{\theta}{2}\cos\frac{\theta}{2} = \sin\theta$. Thus

$$R_x(\theta)\sigma_i R_x(\theta)^\dagger = \sum_j a_{ij}(\theta)\sigma_j, \qquad a_{ij}(\theta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & \sin\theta \\ 0 & -\sin\theta & \cos\theta \end{pmatrix} \tag{17.11}$$

The matrix $a_{ij}(\theta)$ represents a geometric rotation around the x axis by an angle θ (clockwise). Substituting into (17.6) :

$$\rho' = \frac{I + \sum_i r_i\ R_x(\theta)\sigma_i R_x(\theta)^\dagger}{2} = \frac{I + \sum_i r_i\ \sum_j a_{ij}(\theta)\sigma_j}{2} = \frac{I + \sum_j(\sum_i a_{ij}(\theta) r_i)\sigma_j}{2} \tag{17.12}$$

so that

$$r'_j = \sum_i a_{ij}(\theta) r_i = \sum_i a_{ji}(-\theta) r_i \tag{17.13}$$

are the coordinates of the transformed $\vec{r}\,'$. We have therefore proved eq. (17.4): $\vec{r}\,'$ is obtained by a counterclockwise rotation of $\vec{r}$ around the x axis by an angle θ. □

In general, a counterclockwise rotation around an axis along the versor $\hat{n}$ of an angle θ corresponds to the operator:

$$R_{\hat{n}}(\theta) \equiv \exp(-i\frac{\theta}{2}\hat{n}\cdot\sigma) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2}\hat{n}\cdot\sigma \tag{17.14}$$

17.2 Decompositions of U with rotations

Theorem: any single qubit unitary U can be expressed as:

$$U = e^{i\alpha}\ R_{\hat{n}}(\theta) \tag{17.15}$$

Proof: geometrical, by observing that any point on the surface of the Bloch sphere can be reached from any other point with a rotation by an appropriate angle θ around an appropriate axis $\hat{n}$.

Exercise: verify that for the Hadamard gate H, formula (17.15) holds with $\alpha = \pi/2, \hat{n} = \frac{1}{\sqrt{2}}(1,0,1), \theta = \pi$.

Exercise: verify

$$XR_y(\theta)X = R_y(-\theta), \quad XR_z(\theta)X = R_z(-\theta) \tag{17.16}$$

Hint: use $XYX = -Y$ and $Xe^Y X = e^{XYX}$ (due to $X^2 = I$). Similar for $Y \to Z$.

Theorem: any single qubit unitary U can be expressed as:

$$U = e^{i\alpha}\ R_z(\beta)R_y(\gamma)R_z(\delta) \tag{17.17}$$

Proof: use the matrix expressions of the rotations, and eq. (1.19).

This Theorem can be generalized as:

$$U = e^{i\alpha}\ R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta) \tag{17.18}$$

with $\hat{n}$ and $\hat{m}$ not parallel.

Theorem: any single qubit unitary U can be expressed as:

$$U = e^{i\alpha}\ AXBXC \tag{17.19}$$

with A, B, C unitaries such that $ABC = I$.

Proof: set

$$A = R_z(\beta)R_y(\frac{\gamma}{2}), \quad B = R_y(-\frac{\gamma}{2})R_z(\frac{-\beta-\delta}{2}), \quad C = R_z(\frac{-\beta+\delta}{2}) \tag{17.20}$$

and use (17.16).

17.3 Controlled gates

Prototype of controlled gate: CNOT. More generally:

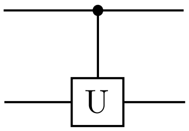


Fig. 17.1 Controlled U gate. For $U = X$ it becomes the CNOT gate.

Exercise: prove the following circuit equivalences :

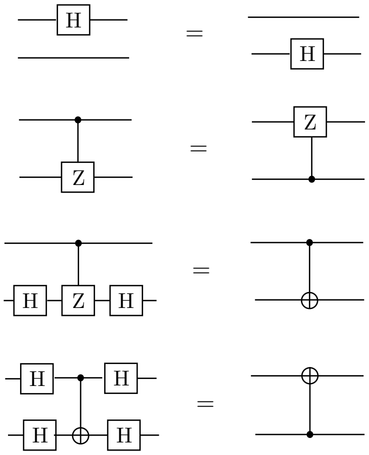


Fig. 17.2 Quantum circuit equivalences.

Problem: realize any controlled-U gate using only CNOT and single qubit gates.

Solution: use the $U = e^{i\alpha} AXBXC$ decomposition, see circuit equivalence in Fig. 17.3.

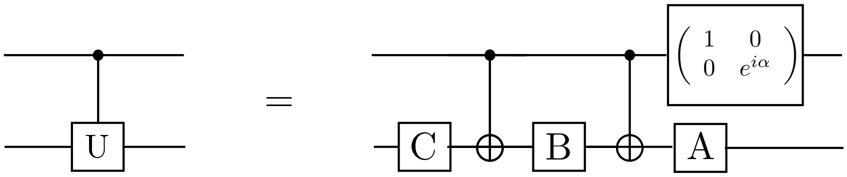


Fig. 17.3 Realization of controlled-U in terms of CNOT and single qubit gates.

Exercise: verify the equivalence in Fig 17.3.

Single qubit gates U controlled by n qubits are denoted by $C^n(U)$. Thus the CNOT gate is a $C^1(X)$ gate, the Toffoli gate a $C^2(X)$ gate etc.

Theorem: any $C^2(U)$ gate can be realized with CNOT and single qubit gates.

Proof: given by the equivalence in Fig. 17.4, where $C^2(U)$ is given in terms of CNOT gates and and controlled $C^1(V)$, $C^1(V^\dagger)$ gates, with $V^2 = U$. These controlled gates, in turn, can be realized in terms of CNOT and single qubit gates as in Fig. 17.3, and the Theorem is proved. □

This is a remarkable result: classically 1 and 2 bit reversible gates are not sufficient to realize the Toffoli gate, whereas 1 and 2 qubit gates are sufficient to realize the quantum Toffoli gate.

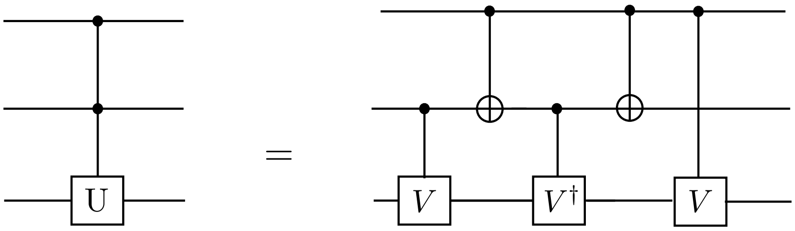


Fig. 17.4 Realization $C^2(U)$ in terms of CNOT and $C^1(V)$, $C^1(V^\dagger)$, with $V^2 = U$.

Exercise: verify the equivalence in Fig 17.4.

Note 1: in general a square root of a single qubit gate $U = e^{i\alpha}\ R_{\hat{n}}(\theta)$ can be found as the (unitary) gate $V = e^{i\alpha/2}\ R_{\hat{n}}(\theta/2)$.

Example: in the case $U = X$, we find that $V = (1 - i)(I + iX)/2$ satisfies $V^2 = X$. We can therefore express the Toffoli gate $C^2(X)$ in terms of CNOT and

$C^1(V), C^1(V^\dagger)$ gates. Resolving these C^1 gates in terms of CNOT and single qubit gates via the ABC procedure leads to the final result for the Toffoli gate:

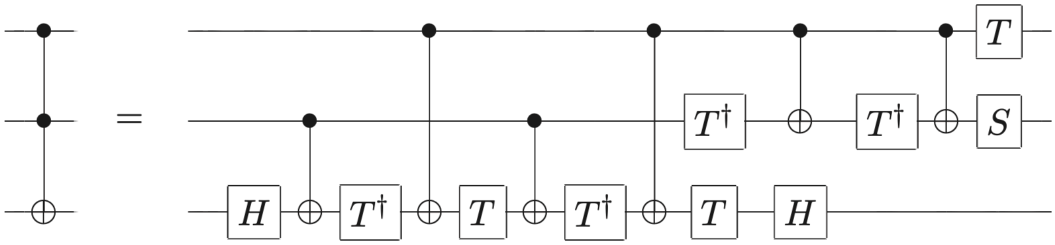


Fig. 17.5 Realization of the Toffoli gate in terms of CNOT and single qubit gates

where the T and S gates are given in (18.25) and (19.1).

Theorem: any $C^n(U)$ gate can be realized with CNOT and single qubit gates.

Proof: given by the equivalence in Fig. 17.5, where for definiteness we take $n = 5$. The Figure shows how to realize a controlled $C^5(U)$ gate using only Toffoli gates, and a $C^1(U)$ gate. Since Toffoli and $C^1(U)$ gates can be realized with CNOT and single qubit gates, the Theorem is proved. □

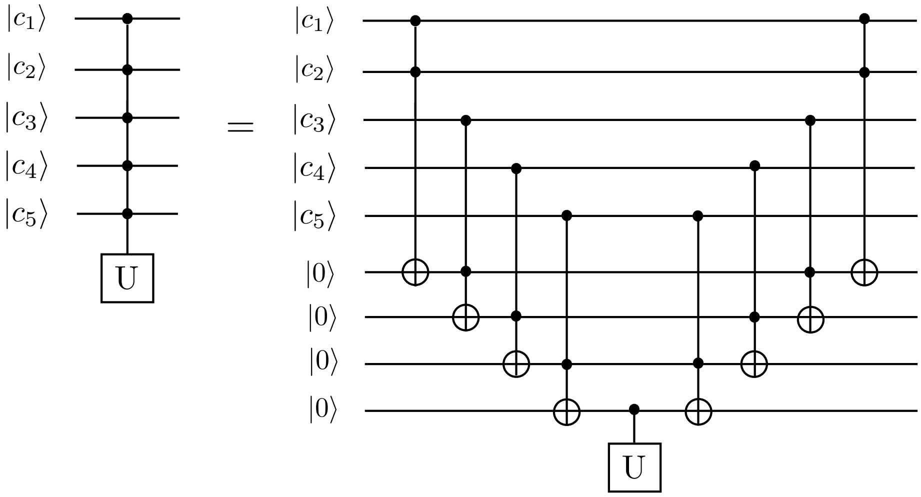


Fig. 17.5 Realization of $C^n(U)$ in terms of TOFFOLI and $C^1(U)$. The $|c_i\rangle$ are the control qubits, and there are $n-1$ input ancilla qubits set to $|0\rangle$.

Exercise: verify the equivalence in Fig 17.5.

Note 2: controlled gates can also be activated when the some of the control qubits are in the state $|0\rangle$. Then dots are replaced by circles to represent the controls. An example is given in Fig. 17.6:

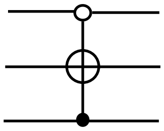


Fig. 17.6 A generalization of the Toffoli gate, where the unitary U is applied to the second qubit if the first and third control qubits are respectively in the state $|0\rangle$ and $|1\rangle$.

Note 3: Since the Toffoli gate is universal for classical computation (see Sect. 16.5), quantum circuits can compute all classical boolean functions (using the quantum Toffoli gate with qubits limited to $|0\rangle$ and $|1\rangle$).

18 Lecture 18: Universal set of quantum gates

Theorem 1: any unitary operation U on n qubits can be realized using only CNOT and single qubit gates.

Theorem 2: any single qubit gate can be approximated by products of the Hadamard gate H and the $\frac{\pi}{8}$ gate T defined in (18.25).

Thus CNOT, H, T are an universal set for quantum computation.

The proof involves three steps.

18.1 Step I: every unitary matrix U can be written as product of two-level unitary matrices.

A *two-level operator* (or matrix) is defined to act nontrivially only in a two-dimensional subspace spanned by two vectors of the computational basis. We proceed to prove Step 1 in the case of a 3×3 unitary matrix. The generalization to $n \times n$ matrices will be straightforward. Consider the unitary matrix

$$\begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix} \tag{18.1}$$

We now construct three unitary two-level matrices, U_1, U_2, U_3 such that

$$U_3 U_2 U_1 U = I \quad \Rightarrow \quad U = U_1^\dagger U_2^\dagger U_3^\dagger \tag{18.2}$$

Let us start with U_1. If $b = 0$, U_1 is taken equal to the identity matrix, otherwise

$$U_1 = \begin{pmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{18.3}$$

Then

$$U_1 U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix} \tag{18.4}$$

Note that $|a'|^2 + |c'|^2 = 1$ since $U_1 U$ is unitary. A similar procedure is used to find U_2. If $c' = 0$ then $U_2 = I$, otherwise

$$U_2 = \begin{pmatrix} \frac{a'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & -\frac{a'}{\sqrt{|a'|^2+|c'|^2}} \end{pmatrix} \tag{18.5}$$

so that

$$U_2U_1U = \begin{pmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix} \tag{18.6}$$

Because of unitarity of the matrix, the first row must have unit norm and therefore $d'' = g'' = 0$. Finally, choose U_3 as

$$U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{pmatrix} \tag{18.7}$$

so that $U_3U_2U_1U = I$. The procedure generalizes to any unitary $d \times d$ matrix U. With steps analogous to the ones described above, we can find two-level unitary matrices $U_1, \dots, U_{d-1}$ such that

$$U_{d-1}U_{d-2}\cdots U_1U = \begin{pmatrix} 1 & 0\cdot\cdot & 0 \\ 0 & & \\ : & U' & \\ 0 & & \end{pmatrix} \tag{18.8}$$

Next we iterate the procedure for the $(d-1) \times (d-1)$ submatrix U', and so on, until we arrive at

$$U_1U_2\cdots U_kU = I \tag{18.9}$$

with $U_1, \dots, U_k$ two-level unitary matrices. □

18.2 Step II: every two-level unitary operation can be implemented with CNOT and single qubit gates.

The proof is constructive. Again we show how it works in an example, the generalization being easy. Consider a three-qubit system, and a two-level unitary matrix

$$\begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & & & & & & 0 \\ 0 & & 1 & & & & & 0 \\ 0 & & & 1 & & & & 0 \\ 0 & & & & 1 & & & 0 \\ 0 & & & & & 1 & & 0 \\ 0 & & & & & & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \tag{18.10}$$

where the basis for the three-qubit vector space is lexicographically ordered $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, ... $|111\rangle$. This gate acts nontrivially only on the first and on the last basis states:

$$U|000\rangle = a|000\rangle + b|111\rangle \tag{18.11}$$

$$U|111\rangle = c|000\rangle + d|111\rangle \tag{18.12}$$

and we call $\tilde{U}$ the 2×2 (unitary) submatrix

$$\tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \tag{18.13}$$

Define then a *Gray code* connecting 000 to 111, i.e. a sequence of 3-bit numbers connecting 000 to 111 and differing by 1 bit at every step. For example:

$$000,\ 001,\ 011,\ 111 \tag{18.14}$$

Then the following circuit implements U:

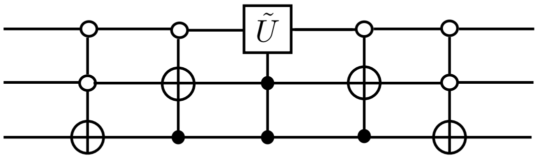


Fig. 18.1 Realization of a two-level unitary operator U using only Toffoli gates and a controlled $C^2(\tilde{U})$

- **Exercise:** prove it.

The Gray code indicates which generalized Toffoli's to use, the $\oplus$ placed on the bit change and empty (full) dots corresponding to 0 (1). Since Toffoli (and generalized Toffoli) gates, and $C^2(\tilde{U})$ can be realized with CNOT and single qubit gates, as shown in Section 17, Step II is proved. □

18.3 Step III: every single-qubit gate can be approximated with arbitrary precision with products of H and T gates.

We first define in next subsection a *distance* between unitary operators, and then prove **III**.

18.3.1 A distance between unitary operators

In order to understand how good is a given approximation, we define the distance (or error) E between the unitary operators U and V as:

$$E(U, V) \equiv \max_{|\psi\rangle} ||(U - V)|\psi\rangle|| \tag{18.15}$$

If P_U and P_V are respectively the probabilities of measuring a given result m in the states $U|\psi\rangle$ and $V|\psi\rangle$, then we can prove that:

$$|P_U - P_V| \leq 2E(U, V) \tag{18.16}$$

and this justifies our definition of the distance E.

Proof:

$$|P_U - P_V| = |\langle\psi|U^\dagger P_m U|\psi\rangle - \langle\psi|V^\dagger P_m V|\psi\rangle| \tag{18.17}$$

Let

$$|\Delta\rangle \equiv (U - V)|\psi\rangle \tag{18.18}$$

Then

$$\begin{aligned} |P_U - P_V| &= |\langle\psi|U^\dagger P_m|\Delta\rangle + \langle\Delta|P_m V|\psi\rangle| \leq |\langle\psi|U^\dagger P_m|\Delta\rangle| + |\langle\Delta|P_m V|\psi\rangle| \\ &\leq ||\Delta||\sqrt{\langle\psi|U^\dagger P_m U|\psi\rangle} + ||\Delta||\sqrt{\langle\psi|V^\dagger P_m V|\psi\rangle} \leq ||\Delta|| + ||\Delta|| \leq 2E(U,V) \end{aligned} \tag{18.19}$$

where we have used triangle (for moduli of complex numbers) and Schwarz inequalities, and the definitions (18.15) and (18.18). □

Using the definition (18.15), the distance between *products* of unitary operators can be shown to satisfy

$$E(U_m U_{m-1} \cdots U_1, V_m V_{m-1} \cdots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j) \tag{18.20}$$

Proof: take the case $m = 2$. Then for some state $|\psi\rangle$:

$$E(U_2U_1, V_2V_1) = ||(U_2U_1 - V_2V_1)|\psi\rangle|| \tag{18.21}$$

cf. the definition of E, and we find

$$\begin{aligned} &||(U_2U_1 - V_2V_1)|\psi\rangle|| = ||(U_2U_1 - V_2U_1)|\psi\rangle + (V_2U_1 - V_2V_1)|\psi\rangle|| \\ &\leq ||(U_2 - V_2)U_1|\psi\rangle|| + ||(V_2(U_1 - V_1)|\psi\rangle|| \leq E(U_2, V_2) + E(U_1, V_1) \end{aligned} \tag{18.22}$$

where we used the triangle inequality (for norms of vectors), and

$$||(U_2 - V_2)U_1|\psi\rangle| \leq E(U_2, V_2), \quad ||(V_2(U_1 - V_1)|\psi\rangle|| = ||(U_1 - V_1)|\psi\rangle|| \leq E(U_1, V_1) \tag{18.23}$$

from the definition of E and the fact that the norm of $U|\psi\rangle$ is the same as the norm of $|\psi\rangle$ if U is unitary. The proof is easily generalized to any m by induction. □

Exercise: prove that for small $\delta\varphi$

$$E(R_{\hat{n}}(\varphi), R_{\hat{n}}(\varphi + \delta\varphi)) \approx \frac{\delta\varphi}{2} \tag{18.24}$$

18.3.2 A rotation of a 2π-irrational angle

Defining the single qubit $\frac{\pi}{8}$ gate :

$$T = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{+i\frac{\pi}{8}} \end{pmatrix} = e^{-i\frac{\pi}{8}Z} \tag{18.25}$$

we find

$$HTH = He^{-i\frac{\pi}{8}Z}H = e^{-i\frac{\pi}{8}HZH} = e^{-i\frac{\pi}{8}X} \tag{18.26}$$

Thus T effects a rotation on the Bloch sphere around the z-axis of an angle $\frac{\pi}{4}$, and HTH a rotation around the x-axis of an angle $\frac{\pi}{4}$. Their product gives:

$$\begin{aligned} T\ HTH = e^{-i\frac{\pi}{8}Z}\ e^{-i\frac{\pi}{8}X} &= [\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}Z]\ [\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}X] = \\ &= \cos^2\frac{\pi}{8}I - i[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y]\sin\frac{\pi}{8} \\ &= \cos^2\frac{\pi}{8}I - \frac{i}{\sqrt{1+\cos^2\frac{\pi}{8}}}[\cos\frac{\pi}{8}X + \sin\frac{\pi}{8}Y + \cos\frac{\pi}{8}Z]\sin\frac{\pi}{8}\sqrt{1+\cos^2\frac{\pi}{8}} \end{aligned} \tag{18.27}$$

The product of rotations must be a rotation, so that

$$T\ HTH = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\hat{n}\cdot\vec{\sigma} \tag{18.28}$$

and comparing these two formulas for $THTH$ yields

$$\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}, \quad \hat{n} = \frac{1}{\sqrt{1+\cos^2\frac{\pi}{8}}}(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8}) \tag{18.29}$$

(remember that $\hat{n}$ must be normalized).

Thus we have constructed, using only products of T and H, a rotation $R_{\hat{n}}(\theta)$ of an angle θ around an axis $\hat{n}$ given in the above equation. The crucial fact is that here θ, as defined in (18.29), is not a rational multiple of 2π, i.e.

$$\theta \neq \frac{r}{s}\ 2\pi, \quad r, s\ integers \tag{18.30}$$

This can be shown using cyclotomic polynomial theory, see for ex. Boykin et al. in quant-ph/9906054.

Then iterating $R_{\hat{n}}(\theta)$ we can approximate with arbitrary accuracy a rotation $R_{\hat{n}}(\alpha)$ with any angle α.

Proof: if δ is the accuracy desired, take an integer N such that $N > 2\pi/\delta$. Then define the angle $\theta_k = (k\theta)\text{mod } 2\pi$. There must exist j and k in the set $\{1, ..., N\}$, with $j < k$, such that $|\theta_k - \theta_j| = |\theta_{k-j}| \leq \frac{2\pi}{N} < \delta$, simply because if we have N points in an interval $(0, 2\pi)$, at least two of them must be at a distance $\leq \frac{2\pi}{N}$. Observe that

θ_{k-j} cannot be 0, since it would imply $\theta_{k-j} = (k-j)\theta \mod 2\pi = 0 \Rightarrow (k-j)\theta = r2\pi$ (integer r) contradicting the fact that θ is not a rational multiple of 2π.

As a consequence, by taking the product of $k-j$ rotations $THTH$, we obtain a rotation around $\hat{n}$ by an angle $\theta_{k-j} < \delta$. Iterating this rotation we can approximate $R_{\hat{n}}(\alpha)$ with accuracy δ. □

Exercise: show that

$$\sin\frac{\theta}{2} = \sin\frac{\pi}{8}\sqrt{1+\cos^2\frac{\pi}{8}} \tag{18.31}$$

Exercise: show that

$$\cos^2\frac{\pi}{8} = \frac{2+\sqrt{2}}{4} \tag{18.32}$$

18.3.3 A different axis

Consider now the product with H gates

$$HR_{\hat{n}}(\theta)H = He^{-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}}H = e^{-i\frac{\theta}{2}\hat{n}\cdot H\vec{\sigma}H} = e^{-i\frac{\theta}{2}\hat{m}\cdot\vec{\sigma}} \tag{18.33}$$

This is a rotation, with the same angle θ as defined in (18.29), but around a new axis $\hat{m}$ defined by

$$\hat{m} = \frac{1}{\sqrt{1+\cos^2\frac{\pi}{8}}}(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8}) \tag{18.34}$$

since $HXH = Z, HYH = -Y, HZH = X$. For the same reason as in the preceding subsection, every rotation $R_{\hat{m}}(\alpha)$ can be approximated with arbitrary accuracy δ by a product of $R_{\hat{m}}(\theta)$ rotations.

18.3.4 Approximation for any single-qubit gate

Finally, any single-qubit gate U can be written as

$$U = R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\zeta) \tag{18.35}$$

Each of the three rotations can be approximated with precision δ, so that U can be approximated with arbitrary precision 3δ (cf. the product rule (18.20)) using only products of T and H. □

19 Lecture 19: Quantum circuits II

19.1 Another set of universal quantum gates: H, S, CNOT and TOFFOLI

Consider the circuit:

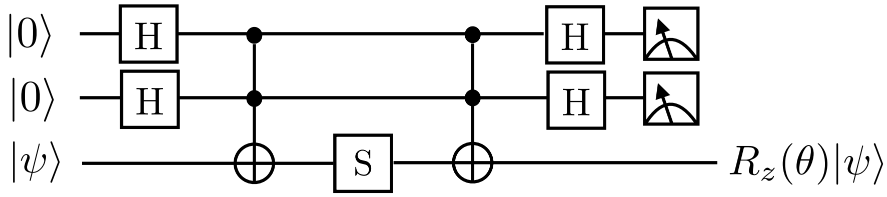


Fig. 19.1 Obtaining a 2π-irrational rotation with H, S, and TOFFOLI.

where S is the *phase* gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{19.1}$$

Exercise:

i): prove that the probability of measuring 0,0 on the first two qubits is $P(0,0) = 5/8$, and in that case the state $|\psi\rangle$ gets rotated around the z axis by an angle θ satisfying

$$\cos\theta = \frac{3}{5} \tag{19.2}$$

For any other results the state $|\psi\rangle$ is changed into $Z|\psi\rangle$.

Hint: before the measurements the state of the system is:

$$\frac{1}{4}[|00\rangle(3S{+}XSX)|\psi\rangle{+}|01\rangle(S{-}XSX)|\psi\rangle{+}|10\rangle(S{-}XSX)|\psi\rangle{+}|11\rangle(-S{+}XSX)|\psi\rangle] \tag{19.3}$$

Note also

$$\begin{aligned} 3S + XSX &= \begin{pmatrix} 3+i & 0 \\ 0 & 3i+1 \end{pmatrix} = (3+i)\begin{pmatrix} 1 & 0 \\ 0 & \frac{3i+1}{3+i} \end{pmatrix} = (3+i)\begin{pmatrix} 1 & 0 \\ 0 & \frac{3}{5}+i\frac{4}{5} \end{pmatrix} \\ S - XSX &= \begin{pmatrix} 1-i & 0 \\ 0 & i-1 \end{pmatrix} = (1-i)\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{19.4}$$

Since $(3{+}4i)/5$ has unit modulus, $(3{+}4i)/5 = e^{i\theta}$ with $\cos\theta = 3/5$, and $3S{+}XSX$ is proportional to a rotation $R_z(\theta)$, cf. Section 17.1. Moreover the matrix $S{-}XSX$ is proportional to Z.

ii): prove that θ satisfying (19.2) is an irrational multiple of 2π.

Hint: observe that

$$e^{i\theta} = \frac{3+4i}{5} \tag{19.5}$$

If θ was a rational multiple of 2π, we could write $\theta = (r/m)2\pi$, so that $e^{im\theta} = 1 \Rightarrow (3+4i)^m = 5^m$, implying $(3+4i)^m \equiv 0(mod\ 5)$. But this is contradicted by the Theorem:

$$(3+4i)^m \equiv 3+4i(mod\ 5) \tag{19.6}$$

which can be proved easily by induction.

We have therefore obtained (with probability 5/8) a rotation $R_z(\theta)$ on the qubit $|\psi\rangle$ with θ an irrational multiple of 2π. We can then proceed as in 18.3.2. Note that if the measurement of the first two qubits does not yield the result 0,0, then we can just apply Z to the third qubit and repeat the action of the circuit until 0,0 is obtained (and $|\psi\rangle$ has been changed into $R_z(\theta)|\psi\rangle$).

19.2 Principle of deferred measurement

Measurements can always be moved from an intermediate stage of a circuit to the end of the circuit. If the result of the measurement is used in the circuit, then the quantum gates controlled by classical bits can be substituted by quantum controlled gates.

Example: Teleportation circuit, with measurements by Alice moved to the end. Then the circuit becomes:

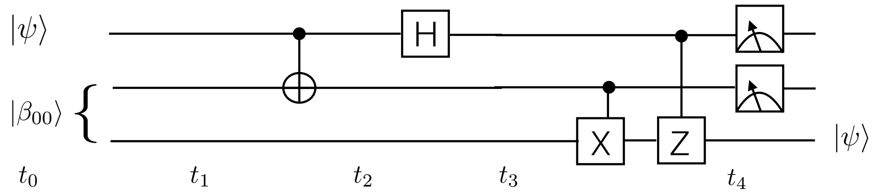


Fig. 19.2 Teleportation circuit with measurements moved to the end of the circuit.

The action of this circuit is identical to the original teleportation in Fig. 4.1. After the two controlled X and Z gates, the 3-qubit state becomes

$$|\Psi_4\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)|\psi\rangle \tag{19.7}$$

so that the state of Bob's qubit is again $|\psi\rangle$, whether Alice measures her qubits or not. There is no need of classical information sent by Alice to Bob. However the controlled gates X and Z are *extended* gates (connecting one qubit of Alice with Bob's qubit), and are responsible for a transfert of information, with speed $\leq c$.

Note: the original qubit $|\psi\rangle$ of Alice has been destroyed also in this case: even without measurements, Alice's 2-qubit state at the end of the circuit is given by the balanced superposition $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ that retains no information on $|\psi\rangle$.

19.3 Principle of implicit measurement

We have noted in previous Section that Bob's state does not depend on Alice measuring her qubits or not. This generalizes to the principle of implicit measurement: *any quantum wire, not terminated by a measurement, can be considered measured.*

Supposing that ρ is the density operator for a 2-qubit system, we can consider a measurement in the computational basis of the first qubit (Alice's). Suppose also that Alice does not communicate her result to Bob. What is the state of Bob's qubit after Alice's measurement ? Is this state different if Alice does not measure her qubit ? To answer, we recall that the collapse of ρ due to a measurement, if the result of the measurement is known, is given by $\rho_m = P_m \rho P_m / Tr(P_m \rho)$, see Section 8.2. If the result is *not* known, the density matrix becomes

$$\rho' = \sum_m p(m) \rho_m = \sum_m Tr(P_m \rho) \frac{P_m \rho P_m}{Tr(P_m \rho)} = \sum_m P_m \rho P_m \tag{19.8}$$

cf. Sect. 8.6. Thus, for a measurement by Alice in the computational basis, we find

$$\rho' = P_0 \rho P_0 + P_1 \rho P_1 = (|0\rangle\langle 0| \otimes I)\ \rho\ (|0\rangle\langle 0| \otimes I) + (|1\rangle\langle 1| \otimes I)\ \rho\ (|1\rangle\langle 1| \otimes I) \tag{19.9}$$

and the reduced density operator for Bob is

$$\rho'^B = Tr_A(\rho') = Tr_A(P_0 \rho P_0 + P_1 \rho P_1) = Tr_A((P_0 + P_1)\rho) = Tr_A(\rho) \tag{19.10}$$

where we used ciclicity of Tr_A since P_0, P_1 operate nontrivially only on the first qubit. Then we conclude that the reduced density operator for Bob is unchanged by the measurement of Alice. By the act of measurement, Alice cannot transfer information to Bob.

19.4 Measurement of an observable

Suppose that a unitary gate U is also hermitean. Then U is an observable. We can devise a circuit that effects the measurement of this observable on any state $|\psi_{in}\rangle$. Assume for simplicity that $|\psi_{in}\rangle$ is a single qubit state, and that the eigenvalues of U are +1 and -1. Then the circuit that realizes the measurement apparatus for U is as in Fig. 19.2.

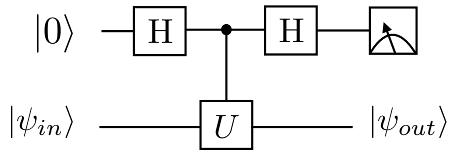


Fig. 19.3 Circuit realizing the measurement of an observable U with eigenvalues ±1.

Denoting by $|plus\rangle$ and $|minus\rangle$ the eigenvectors of U corresponding to the eigenvalues ±1, the state on which we want to measure U can be expanded as

$$|\psi_{in}\rangle = \alpha |plus\rangle + \beta |minus\rangle \tag{19.11}$$

The output of the circuit in Fig 19.2, before the measurement of the first qubit, is the 2-qubit state

$$\alpha|0\rangle|plus\rangle + \beta|1\rangle|minus\rangle \tag{19.12}$$

After the measurement it collapses into $|0\rangle|plus\rangle$ (with probability $|\alpha|^2$) or into $|1\rangle|minus\rangle$ (with probability $|\beta|^2$). Thus the measurement produces a collapse of the second qubit $|\psi_{in}\rangle$ into an eigenvector of U with the correct probabilities. $\square$

20 Lecture 20: Quantum Fourier Transform (QFT)

20.1 Discrete Fourier Transform

The discrete Fourier transform is defined as a transformation on N complex numbers $y_0, y_1, ..., y_{N-1}$ yielding N complex numbers $z_0, z_1, ..., z_{N-1}$ defined by:

$$z_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} y_j e^{2\pi i \; jk/N} \tag{20.1}$$

Note the analogy with the usual Fourier transform of a function $f(x)$:

$$\tilde{f}(k) = \frac{1}{\sqrt{2\pi}} \int dx f(x) e^{ikx} \tag{20.2}$$

where the sum on the discrete index j is replaced by an integral on the continuous "index" x, and y_j and z_k correspond respectively to $f(x)$ and $\tilde{f}(k)$.

20.2 Quantum Fourier Transform

It is a unitary operation QFT defined on basis vectors $|0\rangle, |1\rangle, ..., |N-1\rangle$ as

$$QFT|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \; jk/N} |k\rangle \tag{20.3}$$

Then the components y_j of a vector $|v\rangle = \sum_{j=0}^{N-1} y_j |j\rangle$ transform under QFT into new components z_k given by the discrete Fourier transform (prove it). We will show in the following that QFT is indeed unitary.

Using n qubits, the dimension N of the vector space of physical states is 2^n, and the basis vectors $|0\rangle, ..., |j\rangle, ..., |2^n - 1\rangle$ are given by the 2^n vectors of the computational basis $|00 \cdots 0\rangle$,...,$|j_1 j_2 \cdots j_n\rangle$,...,$|11 \cdots 1\rangle$, where $j_1, j_2, ..., j_n$ is the binary expression of the integer j.

20.3 Binary numbers and binary fractions

The binary representation of the integer j is $j_1 j_2 ... j_n$ where

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0 \tag{20.4}$$

Real numbers between 0 and 1 can be represented with *binary fractions*, defined by

$$0.j_1 j_2 \cdots j_n \equiv \frac{j_1}{2} + \frac{j_2}{2^2} + \cdots + \frac{j_n}{2^n} \tag{20.5}$$

and related to the binary integers $j_1 j_2 ... j_n$ by

$$0.j_1 j_2 \cdots j_n = \frac{1}{2^n} \; j_1 j_2 ... j_n \tag{20.6}$$

20.4 Product representation of QFT

Theorem: the unitary operator QFT can be written as the product

$$QFT|j_1 j_2 \cdots j_n\rangle = \frac{1}{2^{\frac{n}{2}}}(|0\rangle + e^{2\pi i\ 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i\ 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle + e^{2\pi i\ 0.j_1\cdots j_n}|1\rangle) \tag{20.7}$$

Proof:

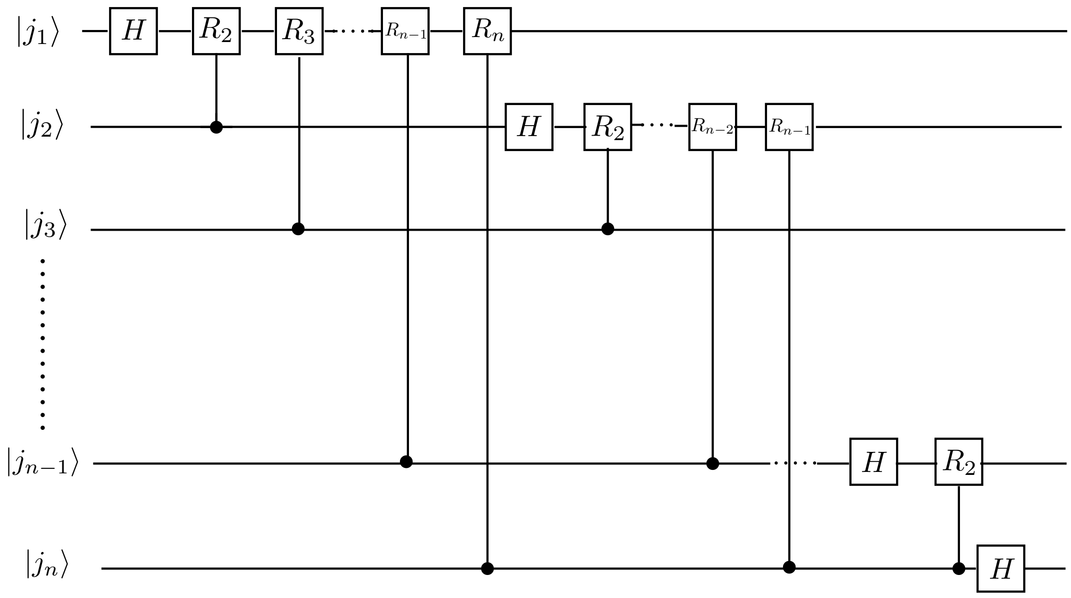
$$\begin{aligned} QFT|j\rangle &= \frac{1}{2^{\frac{n}{2}}}\sum_{k=0}^{2^n-1} e^{2\pi i\ jk/2^n}|k\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1} e^{2\pi i\ j/2^n(k_1 2^{n-1}+\cdots+k_n 2^0]}|k_1\cdots k_n\rangle \\ &= \frac{1}{2^{\frac{n}{2}}}\sum_{k_1=0}^{1} e^{2\pi i\ jk_1 2^{-1}}|k_1\rangle \sum_{k_2=0}^{1} e^{2\pi i\ jk_2 2^{-2}}|k_2\rangle \cdots \sum_{k_n=0}^{1} e^{2\pi i\ jk_n 2^{-n}}|k_n\rangle \\ &= \frac{1}{2^{\frac{n}{2}}}(|0\rangle + e^{2\pi i\ j/2}|1\rangle)(|0\rangle + e^{2\pi i\ j/2^2}|1\rangle)\cdots(|0\rangle + e^{2\pi i\ j/2^n}|1\rangle) \end{aligned} \tag{20.8}$$

and observing that

$$e^{2\pi i\ j/2} = e^{2\pi i\ 0.j_n}, \quad e^{2\pi i\ j/2^2} = e^{2\pi i\ 0.j_{n-1}j_n}, \ldots, e^{2\pi i\ j/2^n} = e^{2\pi i\ 0.j_1\cdots j_n} \tag{20.9}$$

the theorem follows. □

20.5 Efficient circuit for QFT



where

$$R_k \equiv \left(\begin{array}{cc} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{array} \right) \tag{20.10}$$

For example $R_1 = Z$, $R_2 = S$, $R_3 = T$, and in general $R_k^2 = R_{k-1}$.
The above circuit implements the QFT on the n-qubit input state $|j\rangle = |j_1\rangle \cdots |j_n\rangle$.

Proof: after the first H gate, the input state becomes (prove it):

$$\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{2\pi i \ 0.j_1}|1\rangle) \ |j_2\rangle \cdots |j_n\rangle \tag{20.11}$$

Applying next the controlled-R_2 gate produces the state (prove it):

$$\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{2\pi i \ 0.j_1 j_2}|1\rangle) \ |j_2\rangle \cdots |j_n\rangle \tag{20.12}$$

After the application of all controlled-R gates on the first qubit the state has become

$$\frac{1}{2^{\frac{1}{2}}}(|0\rangle + e^{2\pi i \ 0.j_1 j_2 \cdots j_n}|1\rangle) \ |j_2\rangle \cdots |j_n\rangle \tag{20.13}$$

Applying the same procedure to the second qubit leads to:

$$\frac{1}{2}(|0\rangle + e^{2\pi i \ 0.j_1 j_2 \cdots j_n}|1\rangle) \ (|0\rangle + e^{2\pi i \ 0.j_2 \cdots j_n}|1\rangle) \ |j_3\rangle \cdots |j_n\rangle \tag{20.14}$$

and repeating it on all the other input qubits yields the final state that coincides with the output of $QFT|j_1 j_2 \cdots j_n\rangle$ in (20.7), once we invert the order of the output qubits with CROSSOVER gates. □

The circuit proves that QFT is unitary, since all gates are unitary. The circuit uses $n + (n-1) + \cdots + 1 = n(n+1)/2 = \Theta(n^2)$ gates. In contrast, the best classical algorithms for the discrete Fourier transform use $\Theta(n2^n)$ gates, so that QFT has an exponential advantage on its classical counterpart.

21 Lecture 21: Phase estimation

21.1 The circuit

Consider the eigenvalue equation for a unitary operator U:

$$U|u\rangle = e^{2\pi i\varphi}|u\rangle \tag{21.1}$$

where U and the eigenvector $|u\rangle$ are known, and φ is unknown. The QFT provides an algorithm to find the phase φ, assuming that black boxes (circuits) are available to prepare the state $|u\rangle$ and to implement controlled-U^{2^j}.
The procedure of phase estimation uses two registers: the **first register** contains t qubits, each in the initial state $|0\rangle$. The number t will depend on:
- the accuracy we want to reach in the estimation of the phase
- the probability of success of the algorithm
The **second register** contains initially the eigenstate $|u\rangle$, with the appropriate number of qubits necessary to encode the eigenstate.

The circuit for the phase estimation is given in Fig. 21.1. The effect of the sequence of controlled-U gates on the state $|j\rangle|u\rangle$ is

$$|j_1\cdots j_t\rangle|u\rangle \longrightarrow |j_1\cdots j_t\rangle\; U^{2^{t-1}j_1}\cdots U^{2^0 j_t}\;|u\rangle = |j\rangle\; U^j|u\rangle \tag{21.2}$$

and recalling the eigenvalue equation (21.1):

$$|j\rangle|u\rangle \longrightarrow |j\rangle\; e^{2\pi i\varphi j}|u\rangle \tag{21.3}$$

The first register exits the H gates in the state:

$$|0\rangle \longrightarrow \frac{1}{2^{\frac{t}{2}}}\sum_{j=0}^{2^t-1}|j\rangle \tag{21.4}$$

(remember $(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)\cdots(|0\rangle+|1\rangle) = \sum_{j_1=0}^{1}\cdots\sum_{j_t=0}^{1}|j_1\cdots j_t\rangle = \sum_{j=0}^{2^t-1}|j\rangle$).
Thus the initial state of the two registers $|0\rangle|u\rangle$ is transformed by the circuit as:

$$|0\rangle|u\rangle \longrightarrow \frac{1}{2^{\frac{t}{2}}}\sum_{j=0}^{2^t-1}e^{2\pi i\varphi j}|j\rangle|u\rangle = \frac{1}{2^{\frac{t}{2}}}\sum_{j=0}^{2^t-1}e^{2\pi i\frac{(2^t\varphi)j}{2^t}}|j\rangle|u\rangle \tag{21.5}$$

Suppose now that the phase φ can be expressed *exactly* with t bits:

$$\varphi = 0.\varphi_1...\varphi_t \tag{21.6}$$

(remember that the phase as defined in (21.1) is a real number between 0 and 1). Then applying the inverse QFT to the first register gives

$$\frac{1}{2^{\frac{t}{2}}}\sum_{j=0}^{2^t-1}e^{2\pi i\frac{(2^t\varphi)j}{2^t}}|j\rangle \longrightarrow |2^t\varphi\rangle = |\varphi_1...\varphi_t\rangle \tag{21.7}$$

and measuring the register in the computational basis yields the phase φ.

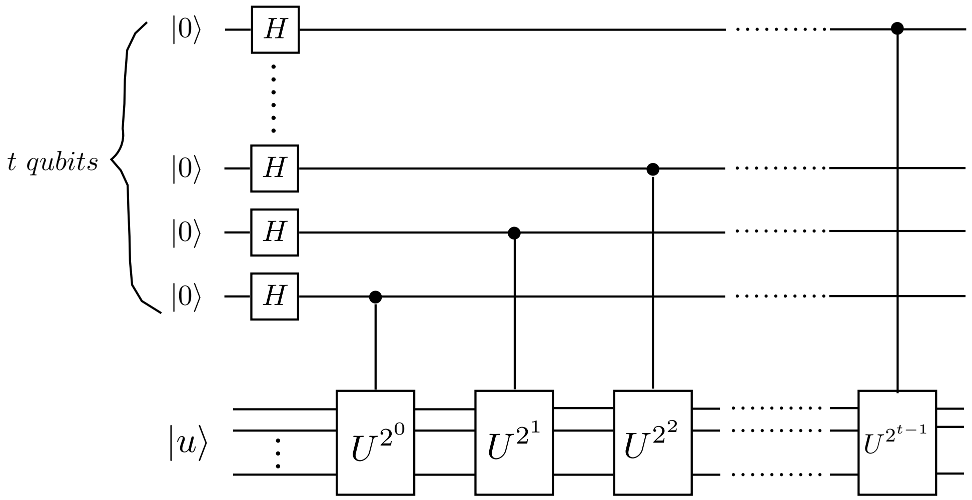


Fig. 21.1 The circuit for phase estimation.

21.2 Performance of the algorithm

And if the phase φ cannot be written exactly as $\varphi = 0.\varphi_1...\varphi_t$? For example φ could be irrational, and therefore have infinitely many φ_i bits in the binary fraction. The procedure of the previous section gives then an *approximation* of φ. Given a desired accuracy δ and a probability $1-\varepsilon$ of reaching this accuracy, we can compute the necessary number t in the first register of the phase estimation algorithm.

i) Consider the state of the first register emerging from the circuit for phase estimation, before the inverse QFT:

$$\frac{1}{2^{\frac{t}{2}}} \sum_{k=0}^{2^t-1} e^{2\pi i \varphi k} |k\rangle \tag{21.8}$$

Here φ can only be approximated by a binary fraction. Suppose that the best t-bit approximation of φ which is less than φ is given by the binary fraction $0.b_1...b_t = b/2^t$, i.e.

$$\varphi \approx b/2^t \tag{21.9}$$

where b is an integer in the interval $[0, 2^t - 1]$, with binary expression $b = b_1...b_t$.

The accuracy is then

$$\delta = \varphi - b/2^t \tag{21.10}$$

Now $\delta > 0$ because we have supposed that $b/2^t < \varphi$, and $\delta \leq 1/2^t$ because $1/2^t$ is the maximum error in a t-bit approximation. Thus

$$0 < \delta \leq 1/2^t \tag{21.11}$$

ii) Applying the inverse QFT to the first register in (21.8) produces

$$\frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{-\frac{2\pi ikl}{2^t}} e^{2\pi i\varphi k}|l\rangle \tag{21.12}$$

since the inverse QFT acts as:

$$QFT^{-1}|k\rangle = \frac{1}{2^{\frac{t}{2}}}\sum_{l=0}^{2^t-1} e^{-\frac{2\pi ikl}{2^t}}|l\rangle \tag{21.13}$$

(this can be simply shown by considering the matrix elements of QFT and of $QFT^{-1} = QFT^{\dagger}$ on the $|j\rangle$ basis). The state (21.12) can be rewritten as:

$$\frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{-\frac{2\pi ik(b+l)}{2^t}} e^{2\pi i\varphi k}|(b+l)\text{mod } 2^t\rangle \tag{21.14}$$

since translating the index l by the constant integer b just reshuffles the terms in the sum. We can even redefine the range of the sum on l, and the same state can be expressed by:

$$\frac{1}{2^t}\sum_{l=-2^{t-1}+1}^{2^{t-1}}\sum_{k=0}^{2^t-1} e^{-\frac{2\pi ik(b+l)}{2^t}} e^{2\pi i\varphi k}|(b+l)\text{mod } 2^t\rangle \tag{21.15}$$

The sum on l still involves 2^t terms and again addends are just reordered.

iii) consider now the amplitude α_l of the state $|(b+l)\text{mod } 2^t\rangle$:

$$\alpha_l = \frac{1}{2^t}\sum_{k=0}^{2^t-1} e^{-\frac{2\pi ik(b+l)}{2^t})} e^{2\pi i\varphi k} = \frac{1}{2^t}\sum_{k=0}^{2^t-1}(e^{2\pi i(\varphi-(b+l)/2^t)})^k = \tag{21.16}$$

$$= \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\varphi-(b+l))}}{1-e^{2\pi i(\varphi-(b+l)/2^t)}}\right) = \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\delta-l)}}{1-e^{2\pi i(\delta-l/2^t)}}\right) \tag{21.17}$$

(use $\sum_{n=0}^{N-1} x^n = (1-x^N)/(1-x)$, and the definition of δ in (21.10)). Its square modulus is the probability of obtaining, when measuring the qubits in the first register, the binary expression of the integer $(b+l)$ mod 2^t. Thus the square modulus of α_0 gives the probability of obtaining b, the best approximation of φ.

But what is the probability of obtaining a result m that differs more than a given e from b, i.e. such that $|m-b|>e$? The answer is the sum of all $|\alpha_l|^2$ such that $b+l$ differs by more than e from b, or equivalently such that l differs by more than e from 0. This sum is:

$$\mathrm{Prob}(|m-b|>e)=\sum_{l=-2^{t-1}+1}^{-(e+1)}|\alpha_l|^2+\sum_{l=e+1}^{2^{t-1}}|\alpha_l|^2 \tag{21.18}$$

iv) For any real θ, $|1-e^{i\theta}|\leq 2$, and therefore

$$|\alpha_l|\leq\frac{2}{2^t|1-e^{2\pi i(\delta-l/2^t)}|} \tag{21.19}$$

Moreover $|1-e^{i\theta}|\geq 2|\theta|/\pi$ when $-\pi\leq\theta\leq\pi$ (to prove it observe that $|1-e^{i\theta}|=\sqrt{2-2\cos\theta}=2|\sin\frac{\theta}{2}|$). As a consequence

$$|1-e^{2\pi i(\delta-l/2^t)}|\geq 4|(\delta-l/2^t)| \tag{21.20}$$

because indeed $-\pi\leq 2\pi(\delta-l/2^t)\leq\pi$ always (try with the extreme values $l=-2^{t-1}+1$ and $l=2^{t-1}$ and use $0<\delta\leq 1/2^t$). Then (21.19) implies also

$$|\alpha_l|\leq\frac{1}{2|2^t\delta-l|} \tag{21.21}$$

v) Applying this inequality to eq. (21.18) gives a bound on $\mathrm{Prob}(|m-b|>e)$:

$$\mathrm{Prob}(|m-b|>e)\leq\frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)}\frac{1}{(l-2^t\delta)^2}+\sum_{l=e+1}^{2^{t-1}}\frac{1}{(l-2^t\delta)^2}\right] \tag{21.22}$$

Remembering that $0<2^t\delta\leq 1$ we can write

$$\begin{aligned}\mathrm{Prob}(|m-b|>e)&\leq\frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)}\frac{1}{l^2}+\sum_{l=e+1}^{2^{t-1}}\frac{1}{(l-1)^2}\right]=\frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)}\frac{1}{l^2}+\sum_{l=e}^{2^{t-1}-1}\frac{1}{l^2}\right]\\&\leq\frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-e}\frac{1}{l^2}+\sum_{l=e}^{2^{t-1}-1}\frac{1}{l^2}\right]=\frac{1}{2}\sum_{l=e}^{2^{t-1}-1}\frac{1}{l^2}\leq\frac{1}{2}\int_{e-1}^{\infty}\frac{1}{l^2}dl=\frac{1}{2(e-1)}\end{aligned} \tag{21.23}$$

vi) Finally, if we set $e=2^{t-n}-1$, we find that $|m-b|>e$ is equivalent to:

$$|m-b|\geq 2^{t-n}\Longrightarrow\left|\frac{m}{2^t}-\frac{b}{2^t}\right|\geq\frac{1}{2^n} \tag{21.24}$$

Thus the probability that, measuring the first register, we find a result m that gives us an estimate of φ with an accuracy worse than $1/2^n$, is given by

$$\text{Prob}(|m-b|>e) \leq \frac{1}{2(e-1)} = \frac{1}{2(2^{t-n}-2)} \tag{21.25}$$

and conversely, the probability of obtaining a result m with accuracy *better* than (or at most equal to) $1/2^n$ is

$$\text{Prob}(|m-b| \leq e) \geq 1 - \frac{1}{2(2^{t-n}-2)} \equiv 1-\varepsilon \tag{21.26}$$

This result can be stated as follows:

Theorem: To obtain φ with an n-bit accuracy, and with a probability of at least $1-\varepsilon$, the phase estimation algorithm needs t qubits in the first register, where t is given by[2]

$$t = n + \left[\log_2(2+\frac{1}{2\varepsilon})\right] \tag{21.27}$$

(use the definition of ε given in (21.26) to express t in terms of n and ε). Thus if we want an n-bit accuracy with a probability of at least 90% (corresponding to $\varepsilon = 1/10$) we would need $t = n + \log_2 7 \approx n+3$ qubits in the first register.

Note: we have assumed the possibility of preparing the second register in the state $|u\rangle$. If $|u\rangle$ is not known, one can still use a (possibly unknown) state $|\psi\rangle$. This state can be expanded on the basis of the eigenvectors $|u\rangle$ of U, corresponding to the eigenvalues $e^{2\pi i\varphi_u}$:

$$|\psi\rangle = \sum_u c_u|u\rangle \tag{21.28}$$

The c_u are unknown if $|\psi\rangle$ is unknown. Using it as second register, the phase estimation protocol produces a final state $\sum_u c_u|\tilde{\varphi}_u\rangle|u\rangle$, with $|\tilde{\varphi}_u\rangle$ being a "good estimator" of the phase φ_u. Thus measuring the first register yields a good approximation of φ_u, where u is random with probability $|c_u|^2$. Measuring the second register gives the eigenvector corresponding to the eigenvalue $e^{2\pi i\varphi_u}$.

21.3 Summary of the algorithm

The circuit for the phase estimation algorithm can be schematically drawn as follows:

[2] the equal sign in formula (21.27) really means " = the closest integer bigger than".

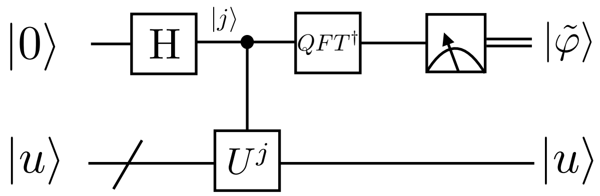


Fig. 21.2 Schematic circuit for phase estimation, where $|\tilde{\varphi}\rangle = |\varphi_1 ... \varphi_t\rangle$ is a good estimator of the phase φ in the eigenvalue $e^{2\pi i\varphi}$ of U, and $|u\rangle$ is the corresponding eigenvector.

The phase estimation algorithm is the core of the Shor algorithm for factorization in polynomial time, as will be discussed in Lecture 23.

21.4 Kitaev's algorithm

Consider the circuit

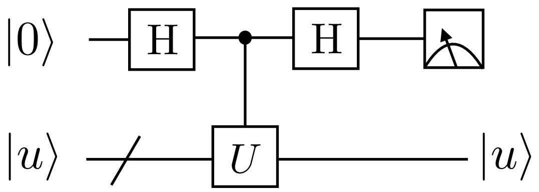


Fig. 21.3 Kitaev's algorithm for phase estimation.

where $|u\rangle$ is an eigenvector of U with eigenvalue $e^{2\pi i\varphi}$.

Exercise: show that the probability of obtaining 0 in the measurement of the first qubit is $p(0) = \cos^2(\pi\varphi)$.

Note that the input state $|u\rangle$ is unchanged at the end of the circuit, and can be re-used as input. Repeating the procedure yields a statistics of measurements that allows to estimate $p(0)$, and thus φ. This algorithm provides an alternative way to determine the phase φ of the eigenvalue of an unitary operator.

22 Lecture 22: Order finding

This is an application of the phase estimation algorithm, important for the factorization algorithm. Consider two integers, x and N, with $x < N$ and no common factors.

Definition: the **order** of x modulo N is the smallest positive integer r such that $x^r \equiv 1 \pmod{N}$.

The problem of finding the order is a difficult problem for a classical computer: no classical polynomial algorithm is known. By this we mean an algorithm polynomial in the number L of bits necessary to specify the problem, for example the number of bits necessary for the binary expression of N. Thus L satisfies $N \leq 2^L$.

Exercise: find the order of 5 modulo 21

Theorem: r always exists (provided x and N are coprime) and $r \leq N$. For the proof, see the Appendix.

22.1 The algorithm

The quantum algorithm for order finding is simply the algorithm for phase estimation applied to a unitary operator $U_{x,N}$ defined by

$$U_{x,N}|y\rangle \equiv |xy \text{ mod N}\rangle \tag{22.1}$$

where y is a L-bit integer, thus $0 \leq y \leq 2^L - 1$, and $U_{x,N}$ acts on a vector space of dimension 2^L.

Technical note: when $y \geq N$, the application $U_{x,N}$ is defined to act on $|y\rangle$ as the identity. Thus $U_{x,N}$ acts nontrivially on $|y\rangle$ only for $0 \leq y \leq N-1$.

Theorem: the states defined by

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \text{ mod N}\rangle \tag{22.2}$$

with integer s satisfying $0 \leq s \leq r-1$ (and r = order of x modulo N), are **eigenstates** of $U_{x,N}$:

$$U_{x,N}|u_s\rangle = \exp\left[\frac{2\pi i s}{r}\right] |u_s\rangle \tag{22.3}$$

Applying now the phase estimation algorithm gives an estimation the phase s/r of the eigenvalue $\exp[2\pi i s/r]$, and from s/r we can deduce r (via the continued fraction algorithm, see later), i.e. the order of x modulo N.

Proof:

$$\begin{aligned}
U_{x,N}|u_s\rangle &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]|x^{k+1}\text{ mod N}\rangle \\
&= \frac{1}{\sqrt{r}}\sum_{k=1}^{r}\exp\left[\frac{-2\pi is(k-1)}{r}\right]|x^{k}\text{ mod N}\rangle \\
&= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi is(k-1)}{r}\right]|x^{k}\text{ mod N}\rangle \\
&= \exp\left[\frac{2\pi is}{r}\right]\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]|x^{k}\text{ mod N}\rangle \\
&= \exp\left[\frac{2\pi is}{r}\right]|u_s\rangle \qquad (22.4)
\end{aligned}$$

We redefined $k \to k-1$ in the sum in the second line, and in the third line we wrote the sum from $k=1$ to $k=r$ as a sum from $k=0$ to $k=r-1$ since both the exponent and the vector $|x^k\text{mod N}\rangle$ do not change if $k \to k+r$, so that the term with $k=0$ is equal to the term with $k=r$. Indeed the exponent remains the same since $\exp[2\pi i \times integer] = 1$, and $|x^k \text{ mod N}\rangle = |x^{k+r} \text{ mod N}\rangle$ because $x^r \equiv 1$ mod N.

Exercise: prove that $U_{x,N}$ is unitary.

For the phase estimation algorithm, we need to know the eigenstate $|u_s\rangle$, but this is equivalent to know the order r (since it enters the definition (22.2) of $|u_s\rangle$), which is just the number we want to find ! There is a way out of this logical loop: we can choose as second register the state $|1\rangle = |00...01\rangle$, where all the L qubits are set to $|0\rangle$ except the last one which is set to $|1\rangle$. This state is in fact a sum of eigenstates $|u_s\rangle$:

$$|1\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle \qquad (22.5)$$

as can be seen from the inversion of formula (22.2):

$$|x^k \text{ mod N}\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\exp\left[\frac{2\pi isk}{r}\right]|u_s\rangle \qquad (22.6)$$

by taking $k=0$. The inversion formula can be verified easily noting that

$$\sum_{s=0}^{r-1}\exp[-2\pi isk/r] = r\delta_{k,0} \qquad (22.7)$$

(for $k=0$ this relation is trivial, for $k \neq 0$ use the formula for the geometric sum). Another way of proving (22.6) is to notice that the transformation matrix of (22.2) is unitary, and its inverse is given by its transpose conjugate.

In summary, taking as the input of the second register the state $|1\rangle$, the algorithm will estimate a phase s/r, where s can take the values $0 \leq s \leq r-1$ with equal probabilities $1/r$, but r is fixed to be the order of x modulo N. We now need a procedure to extract r if we know that it is the denominator of a rational number s/r. This procedure is the continued fraction algorithm we describe in next Section.

Note: one possible result of the algorithm is that the estimated phase is zero, since $s = 0 \to s/r = 0$ may happen with probability $1/r$. One has then to repeat the algorithm until one finds a nonvanishing phase.

22.2 Continued fraction algorithm

The procedure yields a fraction s/r which is close to the phase φ obtained by the phase estimation algorithm. It is based on the following

Theorem: if s/r satisfies

$$\left|\frac{s}{r} - \varphi\right| \leq \frac{1}{2r^2} \tag{22.8}$$

then s/r is a **convergent** of the continued fraction for φ (for the proof see Appendix 4 of Nielsen and Chuang).

To satisfy the condition of the Theorem, we need to know φ with a $(2L+1)$-bit precision. Indeed in this case

$$\left|\frac{s}{r} - \varphi\right| \leq 2^{-2L-1} \leq \frac{1}{2r^2} \tag{22.9}$$

since $r \leq N \leq 2^L$ and therefore $r^2 \leq 2^{2L} \Rightarrow 2r^2 \leq 2^{2L+1}$.

Definition: the **continued fraction** $[a_0, a_1, ..., a_M]$, where $a_0, ..., a_M$ are integers, $a_0 \geq 0$ and $a_1, ..., a_M$ are strictly positive, is defined by

$$[a_0, a_1, ..., a_M] \equiv a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{...+\frac{1}{a_M}}}} \tag{22.10}$$

Every positive rational number has a continued fraction representation.

Example: take the rational number 31/13. To find its continued fraction representation we perform repeatedly the operation of separating the integer part and inverting the fractional part:

$$\frac{31}{13} = 2 + 5/13 = 2 + \frac{1}{13/5} = 2 + \frac{1}{2+3/5} = 2 + \frac{1}{2+\frac{1}{5/3}} = 2 + \frac{1}{2+\frac{1}{1+2/3}} =$$

$$= 2 + \frac{1}{2+\frac{1}{1+\frac{1}{3/2}}} = 2 + \frac{1}{2+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}} \tag{22.11}$$

For any rational number only a finite number of steps is necessary, because the numerators in the fractional parts (5,3,2,1 in the example) are strictly decreasing and therefore have to terminate with 1. The example shows that the continued fraction expression for 31/13 is $[2, 2, 1, 1, 2]$.

Note 1: one advantage of the continued fraction representation, over the usual decimal representation, is that every rational number is represented by a finite string of integers $a_0, ..., a_M$, whereas this is not true in the decimal representation $(1/3 = [0, 3] = 0.33333....)$.

Note 2: the procedure of separating the integer part and writing the rest as 1/(1/rest) can be applied also to an irrational number. Then the procedure never stops, and irrational numbers have infinite continued fractions. For example

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, ...] \tag{22.12}$$

For a number given by $[a_0, ..., a_M]$, the m-th **convergent** is given by the continued fraction $[a_0, ...a_m]$ $(m \leq M)$. For example the convergents for 31/13 are:

$$\begin{aligned}&[2] = 2, \quad [2, 2] = 5/2 = 2.5, \quad [2, 2, 1] = 7/3 = 2.333..., \quad [2, 2, 1, 1] = 12/5 = 2.4,\\ &[2, 2, 1, 1, 2] = 31/13 = 2.3846...\end{aligned} \tag{22.13}$$

and are called convergents because they converge to $[a_0, ...a_M]$ (= 31/13 in the example).

The Theorem above ensures that if the phase estimation algorithm gives the phase φ with a $(2L + 1)$-bit accuracy, i.e.

$$\varphi = 0.\varphi_1...\varphi_{2L+1} = \frac{\varphi_1}{2} + ... + \frac{\varphi_{2L+1}}{2^{2L+1}}, \tag{22.14}$$

then the fraction s/r can be found in the convergents of the rational number φ. Which convergent ? One can try them all, starting from the end (those that approximate better the phase φ): each yields a particular r, and one can verify (in polynomial time) whether $x^r \equiv 1$ (mod N), until one finds the correct r. □

22.3 Summary of quantum order finding

- **Inputs:**
  1) black box $U_{x,N}$ to execute the operation $|j\rangle|k\rangle \to |j\rangle|x^j k(\text{mod N})\rangle$, where x, N are coprime and N is a L-bit integer.
  2) $t = 2L + 1 + [\log_2(2 + \frac{1}{2\varepsilon})]$ qubits in the state $|0\rangle$.
  3) L qubits in the state $|0....01\rangle$

- **Output:** the smallest $r > 0$ such that $x^r \equiv 1$ (mod N).

- **Runtime:** $O(L^3)$ operations. The algorithm succeeds with probability $O(1)$.

• **Procedure:**

1.	$\|0\rangle\|1\rangle$	initial state
2.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle\|1\rangle = \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} \|j\rangle\|u_s\rangle$	superposition with H gates
3.	$\rightarrow \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi isj/r}\|j\rangle\|u_s\rangle$	application of $U_{x,N}$
4.	$\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \|\widetilde{2^t\ \frac{s}{r}}\rangle\|u_s\rangle$	inverse QFT
5.	$\rightarrow$ estimation of $2^t\ \frac{s}{r}$	measuring first register
6.	$\rightarrow r$	continued fraction algorithm

Note: if s, r are L-bit integers, then the continued fraction for $\varphi = s/r$ can be computed using $0(L^3)$ operations: $0(L)$ for separation and inversion, and for each such operation, $0(L^2)$ for elementary arithmetic.

22.4 Period finding

Problem: find the period of a function $f(x)$ (mapping L bits into 1 bit), i.e. the smallest r, with $0 < r < 2^L$, such that

$$f(x+r) = f(x) \tag{22.15}$$

Preparatory observations:

We assume to have an oracle U_f (a circuit) that implements the unitary transformation on $t+1$ qubits

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle \tag{22.16}$$

We need $t = O(L + \log_2(\frac{1}{\varepsilon}))$ input qubits initialized to $|0\rangle$.
Finally we define the 1-qubit state:

$$|\widehat{f}(l)\rangle \equiv \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi ilx/r} |f(x)\rangle \tag{22.17}$$

If $f(x)$ has period r this relation can be inverted:

$$|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi ixl/r} |\widehat{f}(l)\rangle \tag{22.18}$$

To prove it, substitute (22.17) into (22.18), and use $\sum_{l=0}^{r-1} e^{2\pi ilx/r} = r$ for x integer multiple of r, otherwise $= 0$.

Procedure:

1. $|0\rangle|0\rangle$: input $t+1$ qubit state

2. $\longrightarrow \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle$: create superposition with $H^{\otimes t}$

3. $\longrightarrow \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{r}} \frac{1}{\sqrt{2^t}} \sum_{l=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i x l/r}|x\rangle|\widehat{f}(l)\rangle$: apply U_f

4. $\longrightarrow \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |\widetilde{l/r}\rangle|\widehat{f}(l)\rangle$: apply $QFT^\dagger$ to the first register (t qubits)

5. $\longrightarrow \widetilde{l/r}$: measurement of first register, a good estimate of l/r

6. $\longrightarrow r$: continued fraction algorithm.

22.5 Appendix: number theory

To prove the Theorem at the beginning of this Section, we need the following

Lemma 1: the GCD(a,b) is the least positive integer that can be written as $ax+by$, with x, y relative integers.

Proof: suppose that s is the least positive integer that can be written as $ax+by$. Since GCD(a,b) divides both a and b, it divides also s, and therefore GCD $\leq s$. Next we prove that $s \leq$ GCD by showing that s is a divisor of both a and b. Suppose that s does *not* divide a. Then $a = ks + \rho$, with $1 \leq \rho \leq s-1$, and therefore $a = k(ax+by) + \rho \Rightarrow \rho = a(1-kx) + b(-ky)$ is a positive integer that can be written as a linear combination of a and b, and *smaller* than s, and this is a contradiction. Hence s must divide a, and likewise we show that s divides b. This implies the Lemma. □

Multiplicative inverse (mod N)

Definition: if $ab \equiv 1$ (mod N), then b is the inverse of a (mod N) , and viceversa. The modular inverse does not exist always. For example $2 \times 3 = 1$ (mod 5) but 2 has no inverse (mod 4).

Lemma 2: a has a multiplicative inverse (mod N) iff GCD(a,N) = 1, i.e. iff a and N are coprime.

Proof: suppose that a has an inverse a^{-1} (mod N). This means $aa^{-1} = 1 + kN \Rightarrow aa^{-1} + (-k)N = 1$. Lemma 1 then implies GCD(a,N) = 1. Conversely, if GCD(a,N) = 1, then integers a^{-1} and b exist such that $aa^{-1} + bN = 1 \Rightarrow aa^{-1} \equiv 1$ (mod N). □

Note: all integers in the range 1 to $p-1$ have inverses (mod p) if p is prime. Indeed all integers 1,2,...,p are coprime with p.

Exercise: prove that the modular inverse is unique.

Using now Lemma 2 we prove the

Theorem: the order r of x modulo N always exists (provided x and N are coprime) and $r \leq N$.

Proof: Consider the sequence $x \pmod N$, $x^2 \pmod N$, ... $x^N \pmod N$. These are N integers in the interval [1,N-1]. (x^i can never be 0 (mod N) since x and N are coprime by hypothesis, and $x^i \equiv 0 \pmod N$ is incompatible with x having a modular inverse). If N integers can take values in the interval [1,N-1], at least two of them must be equal, i.e. there exist integers i and j in the interval [1,N] and with $i < j$ such that $x^i \equiv x^j \pmod N$. Multiplying both sides i times by the modular inverse of x yields $x^{j-i} \equiv 1 \pmod N$, and shows that the order is $r = j - i \leq N$.

23 Lecture 23: Factorization

23.1 Two theorems in number theory

Theorem 1: if N is a composite (i.e. not prime) L-bit integer, and y is a solution of $y^2 \equiv 1 \pmod{N}$ in the interval $1 < y < N-1$ (thus the trivial solutions $y = 1, y = N-1 \equiv -1 \pmod{N}$ are excluded), then $\mathrm{GCD}(y-1, N)$ and $\mathrm{GCD}(y+1, N)$ are nontrivial factors of N that can be computed with $O(L^3)$ operations.

Proof: since $y^2 \equiv 1 \pmod{N}$, N must divide $y^2 - 1 = (y+1)(y-1)$. Moreover $N > y+1 > y-1$ and therefore N cannot divide $(y+1)$ or $(y-1)$, but must have nontrivial common factors with $(y+1)$ and $(y-1)$. These common factors can be found by computing the GCD of N and $y \pm 1$ with Euclid's algorithm, which requires $O(L^3)$ operations.

Theorem 2: if we choose at random an integer x in the interval $[1, N-1]$, coprime with N, it is very probable that its order $\pmod{N}$ is even, and $x^{r/2}$ is *not* equal to $\pm 1 \pmod{N}$ (the probability is always $\geq 1/2$, see Appendix 4 of Nielsen and Chuang, where this probability is shown to be $1 - \frac{1}{2^m}$ where m is the number of different prime factors of N).

Then $y = x^{r/2}$ (mod N) is a nontrivial solution of $y^2 \equiv 1$ (mod N).

In conclusion, finding the order r modulo N of an integer x, chosen at random in the interval $[1, N-1]$, and coprime with N, allows to find in polynomial time a nontrivial solution of $y^2 \equiv 1 \pmod{N}$, and hence a nontrivial factor of N.

23.2 The factorization algorithm

We have seen that the two theorems of the previous section can be combined to construct a factorization algorithm. This algorithm was first proposed by P.W. Shor in 1994, and produces in polynomial time and with good probability a nontrivial factor of a composite integer N. All operations can be executed on a classical computer, except the order finding subroutine that requires a quantum computer (to find the order in polynomial time).

23.3 Summary of the algorithm

- **Input:** N
- **Output:** a nontrivial factor of N
- **Runtime:** $O((\log_2 N)^3)$ operations
- **Procedure:**

1. If N even. $\longrightarrow$ output $= 2$

2. Determine whether $N = a^b$ for $a \geq 1$, $b \geq 2$ (can be done by a classical algorithm in $O(L^3)$ operations). If yes, $\longrightarrow$ output $= a$.

3. Choose x in the interval $[1, N-1]$. Compute the GCD(x, N) , if it is > 1 then $\longrightarrow$ output $=$ GCD(x, N)

4. Quantum subroutine to find the order r of x modulo N.

5. If r is even and $x^{r/2} \neq -1 \pmod N$, compute GCD$(x^{r/2} - 1, N)$ and GCD$(x^{r/2} + 1, N)$, and test whether these are nontrivial factors of N. If yes, $\longrightarrow$ output $=$ these factors.

NB: $x^{r/2}$ cannot be $= +1 \pmod N$ because r is the *smallest* integer such that $x^r \equiv 1 \pmod N$.

23.4 Example: the factorization of $N = 91$

i) The steps 1. and 2. are passed without exiting.
ii) step 3. : choose for example $x = 4$, coprime with 91.
iii) compute order of 4 modulo 91. Result = 6 ($4^6 = 4096 = 1 + 45 \times 91$).
iv) check that $x^{r/2} \neq -1 \pmod N$, $\rightarrow 4^3 = 64 \neq -1 \pmod{91}$, ok.
v) GCD(64+1, 91) = 13, GCD(64-1, 91) = 7

23.5 Bibliography

P. W. Shor (1994), “Algorithms for quantum computation: discrete log and factoring”, Proc. of the 35-th Annual Symposium on the Foundations of Computer Science, 124-134, IEEE Computer Society Press.

24 Lecture 24: Quantum search algorithm (Grover)

24.1 The problem

The problem is to find, in a set of $N = 2^n$ elements, a subset of M elements that satisfies some given conditions. We say then that the search problem has M solutions.

We can assume the existence of a function $f(x)$ from n bits to 1 bit, that takes the value $f(x) = 1$ if x is a solution and $f(x) = 0$ if x is not a solution.

We also assume that there is a black box (an "oracle") U_f able to execute the operation on the $n + 1$ qubit state $|x\rangle|q\rangle$, where $|x\rangle$ is a n-qubit state and $|q\rangle$ is a 1-qubit state:

$$U_f|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle \tag{24.1}$$

In particular

$$U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle \tag{24.2}$$

In the quantum search algorithm it is useful to prepare the 1-bit initial state $|q\rangle$ in the state :

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{24.3}$$

Then it is easy to find that the action of U_f becomes:

$$U_f|x\rangle\frac{(|0\rangle - |1\rangle)}{\sqrt{2}} = (-1)^{f(x)}|x\rangle\frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \tag{24.4}$$

(prove it). The 1-qbit state does not change, and can be omitted from the discussion. We can then consider the action of U_f as follows:

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle. \tag{24.5}$$

i.e. the oracle *marks* the solutions of the search problem with a minus sign (corresponding to $f(x) = 1$).

The circuit that implements the quantum search is

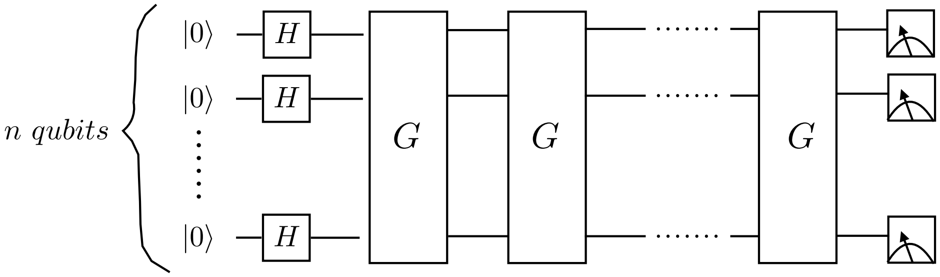


Fig. 24.1 The circuit for quantum search.

where G is the Grover unitary operator given by

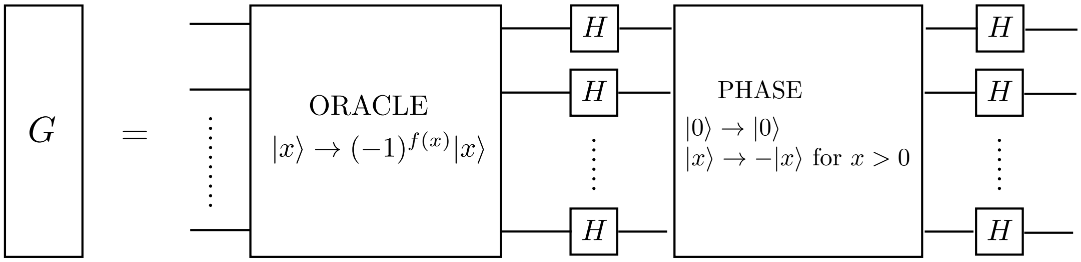

G
$=$
ORACLE
$|x\rangle \to (-1)^{f(x)}|x\rangle$
H
H
H
PHASE
$|0\rangle \to |0\rangle$
$|x\rangle \to -|x\rangle$ for $x > 0$
H
H
H

Fig. 24.2 The Grover operator.

and where we have omitted from the drawing the 1-qubit state (24.3), and possibly other work qubits for the functioning of G.

Let's trace the action of the quantum search circuit in Fig. 24.1.

1) Starting with the initial state $|0...0\rangle$, the H gates produce the complete superposition

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \tag{24.6}$$

To this state we repeatedly apply the Grover operator $G = H^{\otimes n}\ PHASE\ H^{\otimes n}\ ORACLE$. The box ORACLE is the unitary operator U_f, acting on the n-qubit state $|x\rangle$ as in (24.5). The box PHASE acts on the n-qubit basis vectors as indicated in the box: it multiplies all $|x\rangle$ by (-1) except the state $|0\rangle$ which is left untouched. It is immediate to see that this PHASE operator can be expressed as

$$PHASE = 2|0\rangle\langle 0| - I \tag{24.7}$$

as can be verified by acting on $|0\rangle$ and on $|x \neq 0\rangle$. Thus the Grover operator G can be written as

$$G = H^{\otimes n}\ (2|0\rangle\langle 0| - I)\ H^{\otimes n}\ U_f = (2|\psi\rangle\langle\psi| - I)\ U_f \tag{24.8}$$

where in the second equality we used $|\psi\rangle = H^{\otimes n}|0\rangle$.

2) We define the vectors $|\alpha\rangle$ and $|\beta\rangle$ as

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x{}'' \ |x\rangle, \quad |\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x{}' \ |x\rangle \tag{24.9}$$

where the symbols $\sum''$ and $\sum'$ are respectively sums on $x \neq$ solutions and $x =$ solutions. Then we can write $|\psi\rangle$ as

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \sqrt{\frac{N-M}{N}}\ |\alpha\rangle + \sqrt{\frac{M}{N}}\ |\beta\rangle \tag{24.10}$$

3) The action of the oracle U_f on any vector $a|\alpha\rangle + b|\beta\rangle$ is obtained by simply changing the sign of $|\beta\rangle$:

$$U_f(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle \tag{24.11}$$

(because all solutions $|x\rangle$ change sign under the action of U_f). It can be interpreted geometrically as a reflection about the vector $|\alpha\rangle$ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$. Similarly the operator $2|\psi\rangle\langle\psi| - I$ also performs a reflection in the same plane, about the vector $|\psi\rangle$. Indeed taking in this plane the basis given by $|\psi\rangle$ and $|\psi_\perp\rangle$, where $|\psi_\perp\rangle$ is a vector in the plane, perpendicular to $|\psi\rangle$, we find

$$(2|\psi\rangle\langle\psi| - I)(c|\psi\rangle + d|\psi_\perp\rangle) = c|\psi\rangle - d|\psi_\perp\rangle \tag{24.12}$$

Thus the Grover operator is the product of two reflections in the plane, which amounts to a rotation in this plane with an angle θ that we compute in next paragraph.

4) Here we study the action of G on $|\psi\rangle$. First, we rewrite the (real) coefficients in the expansion (24.10) of $|\psi\rangle$ on the basis vectors $|\alpha\rangle$ and $|\beta\rangle$ as:

$$|\psi\rangle = \cos\frac{\theta}{2}\ |\alpha\rangle + \sin\frac{\theta}{2}\ |\beta\rangle, \quad \cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}, \quad \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}} \tag{24.13}$$

with $0 \leq \theta \leq \pi$. Applying the Grover operator on $|\psi\rangle$ yields:

$$\begin{aligned} G|\psi\rangle &= (2|\psi\rangle\langle\psi| - I)\ U_f|\psi\rangle = \\ &= [2(\cos\frac{\theta}{2}\ |\alpha\rangle + \sin\frac{\theta}{2}\ |\beta\rangle)\ (\cos\frac{\theta}{2}\ \langle\alpha| + \sin\frac{\theta}{2}\ \langle\beta|) - I]\ (\cos\frac{\theta}{2}\ |\alpha\rangle - \sin\frac{\theta}{2}\ |\beta\rangle) \\ &= \cos\frac{3\theta}{2}\ |\alpha\rangle + \sin\frac{3\theta}{2}\ |\beta\rangle \end{aligned} \tag{24.14}$$

after using some elementary trigonometric identities. In general

$$G^k|\psi\rangle = \cos(\frac{\theta}{2} + k\theta)\ |\alpha\rangle + \sin(\frac{\theta}{2} + k\theta)\ |\beta\rangle \tag{24.15}$$

Thus G rotates $|\psi\rangle$ counterclockwise by an angle θ determined by (24.13), and is represented on the ($|\alpha\rangle$,$|\beta\rangle$) basis of the plane by the rotation matrix

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{24.16}$$

The geometry of the various vectors in the $\alpha\beta$ plane is given in the figure below:

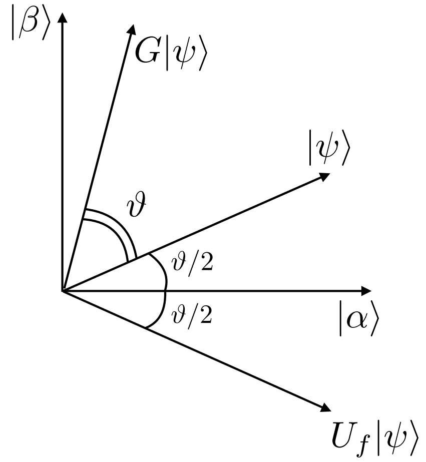


Fig. 24.3 Action of G and U_f on $|\psi\rangle$

Note: if $M \leq N/2$, $\Rightarrow \cos\frac{\theta}{2} \geq 1/\sqrt{2}$, and $0 \leq \theta \leq \pi/2$.

5) Performance: the idea is to use G to rotate $|\psi\rangle$ near $|\beta\rangle$. How many iterations of G are necessary ? The angle between $|\psi\rangle$ and $|\beta\rangle$ is arccos $\sqrt{M/N}$ (since the cosine of this angle is $\langle\beta|\psi\rangle = \sqrt{M/N}$, see (24.10)), and therefore we must repeat the Grover iteration R times, with

$$R = \text{CI}\left(\frac{\arccos\sqrt{\frac{M}{N}}}{\theta}\right) \tag{24.17}$$

and CI = closest integer. This will bring the rotated $|\psi\rangle$ within an angle $\theta/2$ from $|\beta\rangle$.

The rotated vector has a projection $\geq \cos\theta/2 = \sqrt{\frac{N-M}{N}}$ on $|\beta\rangle$, so that a measurement of the state in the computational basis yields a solution of the problem with a probability of at least $\cos^2\theta/2 = 1 - M/N$. Already with $M \leq N/2$ the probability of success exceeds 1/2. With $M \ll N$ this probability approaches 1, but the necessary number R of iterations increases.

6) This number R depends on the number of solutions M, but not on the nature of these solutions. Provided we know M, we can apply the quantum search algorithm. In fact the requirement of the knowledge of M can be lifted, see for ex. Nielsen and Chuang, Section 6.3.

An upper bound can be established on R. Since arccos $\sqrt{M/N} \leq \pi/2$, we find

$$R \leq \textit{integer part}\ \left[\frac{\pi/2}{\theta}\right] \tag{24.18}$$

From this equation we see that a lower bound on θ gives an upper bound on R. Since for $0 \leq \theta \leq \pi$ we have $\theta/2 \geq \sin\theta/2 = \sqrt{M/N}$, the corresponding upper bound on R is:

$$R \leq integer\ part\ \left[\frac{\pi}{4}\sqrt{\frac{N}{M}}\right] \tag{24.19}$$

Thus $R = O(\sqrt{N/M})$ Grover iterations are necessary to obtain a solution with high probability. This is a *quadratic improvement* over the $O(N/M)$ operations required classically.

24.2 Summary of the quantum search algorithm with $M = 1$ (one solution x_0)

- **Input:** a black box oracle U performing the transformation

$$U|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle \tag{24.20}$$

where $f(x) = 0$ for all $0 \leq x < 2^n$ except x_0, for which $f(x_0) = 1$

- $n + 1$ qubits in the state $|0\rangle$.

- **Output:** x_0

- **Runtime:** $O(\sqrt{2^n})$ operations

- **Procedure:**
  1. $|0\rangle^{\otimes n}|0\rangle$ initial state
  2. $\longrightarrow \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ apply $H^{\otimes n}$ to first n qubits, and HX to last qbit.
  3. $\longrightarrow [(2|\psi\rangle\langle\psi| - I)U]^R\ \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \approx |x_0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ apply R times the Grover operator, with $R \approx [\frac{\pi}{4}\sqrt{2^n}]$
  4. $\longrightarrow x_0$ measure the first n qubits

24.3 A two-bit example

In this example $N = 4$, and the oracle that tests x is one of the four gates:

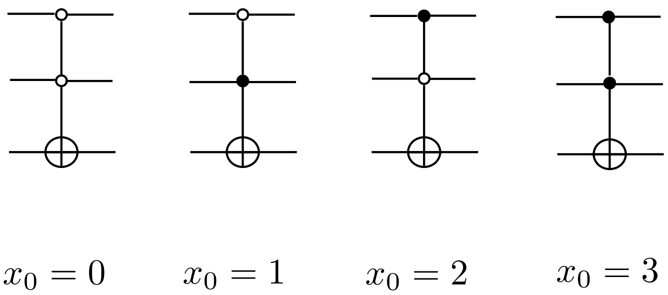


Fig. 24.4 Oracles for the four cases: solution $x_0 = 0$, ... solution $x_0 = 3$.

each corresponding to a particular solution x_0.

The first two qubits (the "query" qubits) encode x, the last qubit (the workspace qubit for the oracle, not to be confused with the last qubit in the procedure of previous section) is the oracle response. The circuit for the search of the solution is:

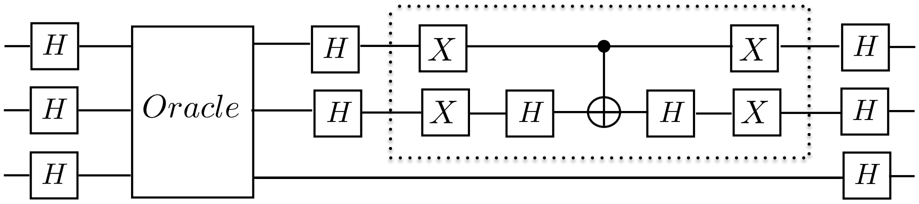


Fig. 24.5 circuit for the search of the solution x_0

Initially, the two query qubits are in the state $|00\rangle$, and the last qubit in the state $|1\rangle$. Gates in the dotted box perform the conditional phase shift operation $2|00\rangle\langle 00| - I$. For the present case, $N = 4, M = 1$ so that from (24.13) $\theta = \pi/3$, and the formula (24.17) for R yields exactly 1. Thus only one iteration is required to obtain exactly x_0. In other words, the two qubit query state after the first H gates:

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \tag{24.21}$$

is at an angle of 30 degrees from $|\alpha\rangle$, and a single rotation of $\theta = 60$ degrees moves it to $|\beta\rangle$. One can verify, using the circuit, that the measurement of the top two qubits gives x_0 after using the oracle only once.

By contrast, a classical computer trying to find x_0 by examining all the two-bit x (four of them) would require an average of 2.25 oracle calls.

Exercise: prove it.

References

[1] M.A. Nielsen, I.L. Chuang, “Quantum computation and quantum information”, CUP (2000).

[2] J. Preskill, Lecture Notes for Phys. 229: Quantum Information and Computation, http://theory.caltech.edu/∼preskill/ph219/

[3] V. Vedral, M. B. Plenio, “Basics of Quantum Computation”, arXiv:quant-ph/9802065

[4] W. Scherer, Mathematics of Quantum Computing, Springer 2019