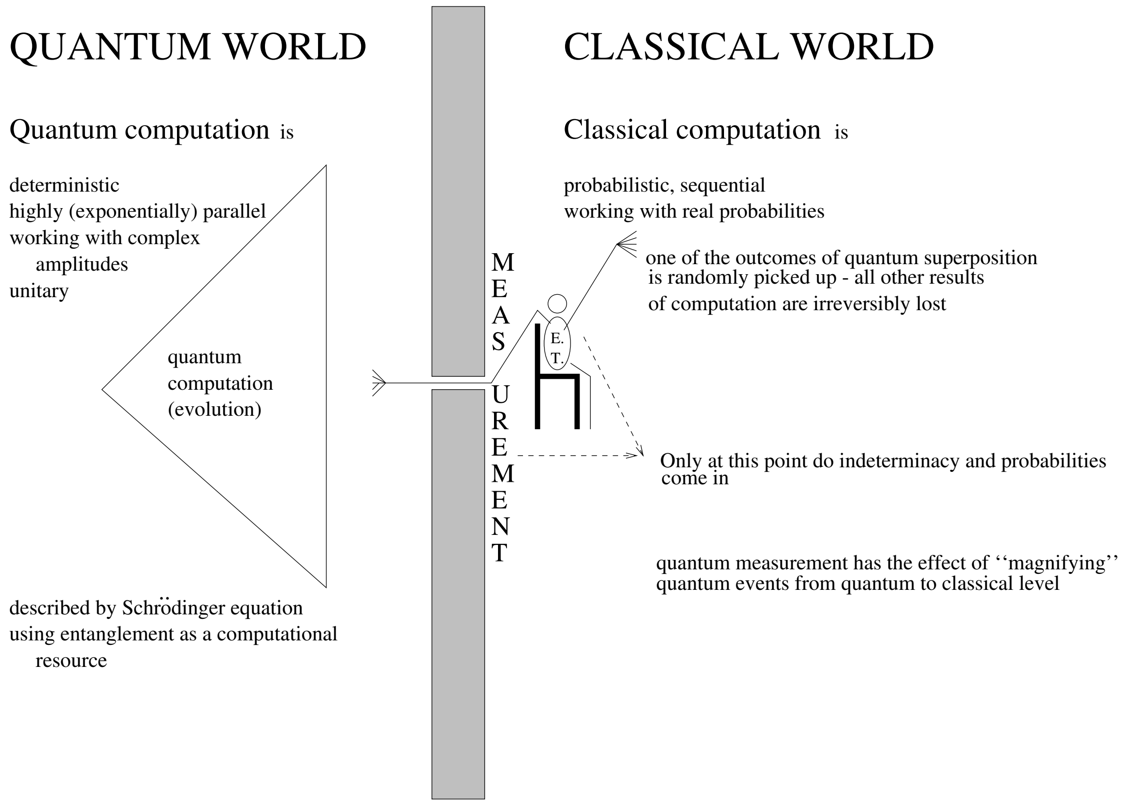
QUANTUM COMPUTING

Jozef Gruska



Chapter 2

ELEMENTS

INTRODUCTION

The basic elements of quantum computing are easy to identify: quantum bits, quantum registers, quantum gates and quantum networks. However, at this point an analogy with classical computing ends. Quantum bits, registers, gates and networks are very different, have other properties and larger power than their classical counterparts.

A quantum bit can be in any state within an infinite set of states. A quantum register of n quantum bits can be, at the same time, in any of the infinitely many superpositions of 2^n basis states. The parallelism a quantum register can exhibit is striking. The key new feature is that a quantum register can be in an entangled state. On one side, entangled states with their non-locality features are a hallmark of quantum mechanics. On the other side, quantum entanglement is an important resource of quantum information processing.

There is a larger variety of quantum gates than of classical gates. There are already infinitely many one-input/output quantum gates. In addition, almost any two-input/output quantum gate is universal. A simple two input/output gate together with one input rotation gates form a set of universal gates.

LEARNING OBJECTIVES

The aim of the chapter is to learn:

1. the basic concepts concerning quantum bits and registers;
2. the concept of quantum entanglement and the examples of its power;
3. the basic examples of quantum gates and of quantum circuits;
4. some examples of universal quantum gates and a method to show universality of quantum gates;
5. the basic quantum arithmetical circuits;
6. the concept of quantum superoperator circuits.

> What canst thou see elsewhere which thou canst not see here? Behold the heaven and the earth and all the elements: for of these are all things created.
>
> Thomas à Kempis (1380–1471)

Quantum algorithms and circuits work with quantum versions of the same basic elements as classical ones: quantum bits, quantum registers and quantum gates. However, all these new elements have specific properties and power. A good knowledge of them is a base for understanding more elaborate algorithms and networks presented in the next chapter, as well as for the understanding of the most of all other topics we deal with in this book.

2.1 Quantum Bits and Registers

Four key problems of quantum information processing are: how to represent, how to store, how to transmit and how to manipulate quantum information. Two key elements to deal with these problems are quantum bits and quantum registers.

2.1.1 Qubits

Let $\mathcal{S}$ be a two-dimensional quantum system with two orthonormal states, denoted $|0\rangle$ and $|1\rangle$, that can be considered as forming a natural, or standard, or preferred, basis of $\mathcal{S}$.

Definition 2.1.1 *A* **qubit** *(quantum bit) is a quantum state*

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle,^{1} \tag{2.1}$$

where $\alpha, \beta \in \mathbf{C}$ *and* $|\alpha|^2 + |\beta|^2 = 1$. [2]

Exercise 2.1.2 *Show that any qubit state* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ *can be expressed in the form* $|\psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$ *in the sense that* $|\alpha|^2 = |\cos\theta|^2$ *and* $|\beta|^2 = |e^{i\phi}\sin\theta|^2$.

---

[1] One can also say that a qubit is a unit vector in a two-dimensional inner-product space. For the representation of qubits we often assume that a particular basis, say $\{|0\rangle, |1\rangle\}$, has been fixed.

[2] The term qubit was coined by B. Schumacher (1995). A more classical term is a "two-level system", or a "two-state system".

For the purpose of quantum information processing two basis states $|0\rangle$ and $|1\rangle$ are usually taken as encoding classical bit values 0 and 1. A classical bit can be seen as a qubit promised to be in one of the basis states. In general, we can call any two-state system a physical bit and when the system is quantum and the two states are orthogonal quantum states, we can refer to it as a qubit. Therefore, any two-state quantum system is a potential candidate for a qubit.

In physics literature the following notation is often used for the states of the standard basis of various two-level quantum systems: in the case of spin$-\frac{1}{2}$ particles, and in the case of vertical or horizontal polarization of photons, $|\uparrow\rangle$ or $|\updownarrow\rangle$, is taken instead of $|0\rangle$ and $|\downarrow\rangle$, or $|\leftrightarrow\rangle$ is used instead of $|1\rangle$; in the case of diagonal polarizations of photons (45° and 135°), $|\nearrow\rangle$ ($|\searrow\rangle$) is used for $|0\rangle$ ($|1\rangle$) in the case of circular polarization $|\circlearrowleft\rangle$ ($|\circlearrowright\rangle$) is used for $|0\rangle$ ($|1\rangle$).

Remark 2.1.3 The term "qubit" is often used in a more abstract way—as a variable that can take on any qubit state (2.1). In such a case we can talk about a (particular) state of a qubit. This is in accordance with the use of the term "bit" in classical computing where we talk about a value, or a state, of a bit.

The above definition leaves the actual physical medium of a qubit completely undefined—as long as objects are treated according to the quantum principles discussed in the previous chapter.

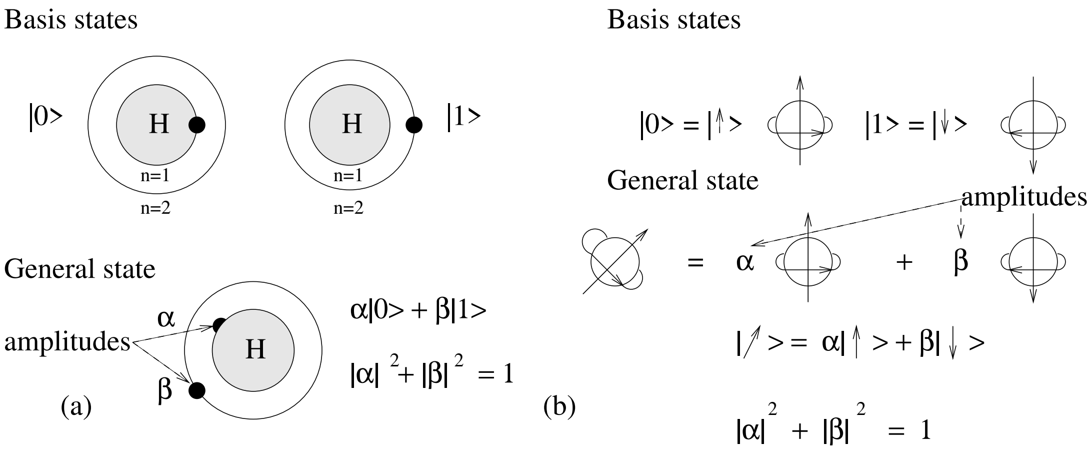


Figure 2.1: Qubit representations by energy levels of an electron in a hydrogen atom and by a spin-$\frac{1}{2}$ particle. The condition $|\alpha|^2 + |\beta|^2 = 1$ is a legal one if $|\alpha|^2$ and $|\beta|^2$ are to be the probabilities of being in one of two basis states (of electrons or photons).

There are many ways to realize qubits—there are many interesting/important two-dimensional quantum systems known in physics. For example, by the polarization of a photon or by the ground ($n = 1$) and excited ($n = 2$) states of an electron in the hydrogen atom (Figure 2.1a). One of the most often and best-explored two-level quantum systems is that of spin-$\frac{1}{2}$ particles with two basis states: spin-up (notation $|\uparrow\rangle$ or $|0\rangle$) and spin-down (notation $|\downarrow\rangle$ or $|1\rangle$) (Figure 2.1b).

From the implementation point of view the most promising candidates for qubits are so far photons, trapped ions and spins of atomic nuclei.

States $|0\rangle$ and $|1\rangle$ of a qubit can be seen, and are often referred to, as representing classical states (bits).[3] The main difference between classical bits and qubits is that while a classical bit can be set up only to one of the two states, namely 0 or 1, a qubit can take any quantum linear superposition of $|0\rangle$ and $|1\rangle$, i.e., in principle can be in any of uncountably many states. This means that a large, even infinite, amount of information could potentially be encoded in amplitudes of a single qubit by appropriately choosing α and β.[4] Of course, this does not mean that in any implementation a qubit can take any of its potentially infinite

[3] This is principally incorrect but often useful simplification, especially for getting an analogy with classical computing.

[4] For this reason, in order to study computational complexity problems of quantum computing a restriction will have to be made on α and β. In principle, it will be required that they can be computed in polynomial time and have logarithmic size.

number of theoretically possible states.[5]

One way to represent states of qubits geometrically is as points on the surface of a unit Riemann[6] sphere, where North and South poles correspond to the basis states (that correspond to bits) (see Figure 2.2a).[7] Qubits can be represented also by points on a Bloch[8] sphere (see Allen and Eberly, 1975), called also Poincaré sphere, and Figure 2.2b), using the spherical coordinate system. This representation is based on the fact that any qubit can be represented (see Exercise 2.1.2), as $\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$.[9]

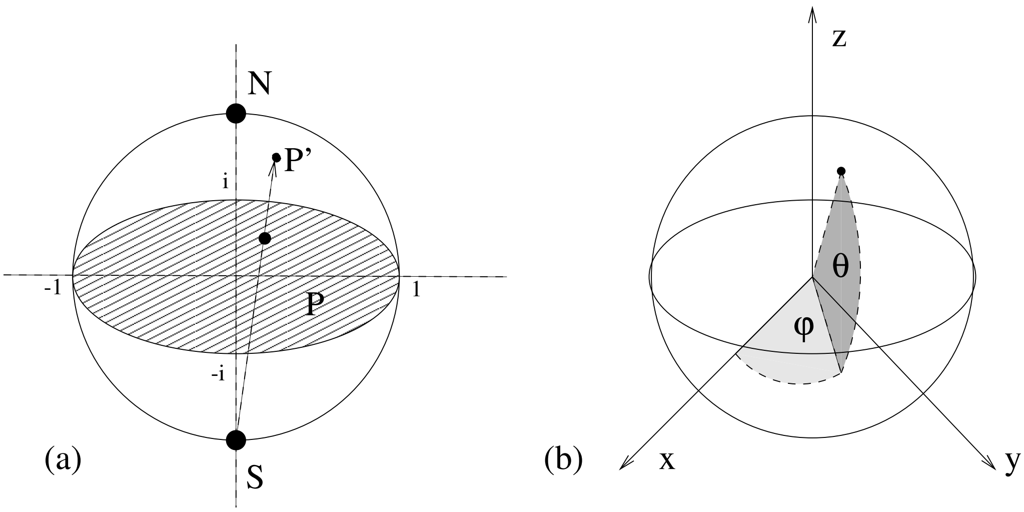


Figure 2.2: Representation of qubits on Riemann and Bloch spheres

Just as in the previous chapter, we can represent basis states as vectors as follows: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. In such a case we have representations:

$$|\nearrow\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, |\searrow\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}, |\circlearrowleft\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} \text{ and } |\circlearrowright\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{i}{\sqrt{2}} \end{pmatrix}.$$

[5]For example, a **trine** is a qubit that can be in only one of the following three states (see Peres and Wootters, 1991): $|0\rangle$, $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ or $\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$.

[6]Georg Friedrich Bernhard Riemann (1826–1866), a German mathematician. His main contributions was in the theory of complex variable functions and their representations (on Riemann surfaces), non-Euclidean geometry (representation of elliptic spaces and an extension of Gauss's work on differential geometry to n-dimensional objects), and electromagnetic theory.

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

[8]Felix Bloch (1905–1983), an American physicist of Swiss origin. His main contributions were in the quantum theory of solid bodies, ferromagnetism and quantum electrodynamics. Bloch developed methods to measure magnetic moments of atom nucleus.

[9]θ is the angle from z axis and ϕ the angle in the $x - y$ plane from the x axis—a phase. Representation of qubits by points on a Bloch sphere is of interest also because it provides an isomorphism between qubit operations and solid-body rotations.

Qubit measurements

Unfortunately, what goes into a qubit does not necessarily come out. A single qubit is in principle not fully identifiable, i.e., given an unknown state $|\psi\rangle$ of a qubit, it is in general not possible to identify it fully by a projection measurement. Quantum physics has strict rules on how to extract information out of an unknown quantum state. The outcome of any projection measurements of a qubit must be formulated in classical terms. More exactly, we can get out of any projection measurement of one qubit only one classical bit of information. Therefore, even though there is a continuum of possible quantum states of a single qubit, these states cannot all be distinguished reliably from each other. No (von Neumann) measurement can extract more than one expected bit of information from any given qubit.[10] From an information theory point of view, from a qubit one can obtain by a (projection) measurement exactly the same amount of (classical) information as a classical bit has, even if it has infinitely many potential states.

Example 2.1.4 *A measurement of a qubit state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, corresponding to the observable $\{E_0, E_1\}$, where E_0 (E_1) is the subspace spanned by the state $|0\rangle$ ($|1\rangle$), or, in other words, with respect to the standard basis $\{|0\rangle, |1\rangle\}$, provides as the output bit 0 (1) with the probability $|\alpha|^2$ ($|\beta|^2$) and the state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ collapses into the state $|0\rangle$ ($|1\rangle$). All other information about the superposition is irreversibly lost. For an observer a qubit represents therefore a probability distribution.*

However, the qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be measured also with respect to infinitely many other bases. For example, with respect to the often used dual basis $\mathcal{D} = \{|0'\rangle, |1'\rangle\}$, where

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

Since

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

we have

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

and a measurement of $|\phi\rangle$ with respect to the dual basis gives 0 (1) with probability $\frac{1}{2}|\alpha+\beta|^2$ ($\frac{1}{2}|\alpha-\beta|^2$).

Example 2.1.5 *If the state $|0\rangle$ is measured with respect to the standard basis we get as outcome 0 with probability 1 and the state collapses into itself. On the other hand, if $|0\rangle$ is measured with respect to the dual basis we get as the outcome 0 or 1, both with probability $\frac{1}{2}$, and the state will collapse either into the state $|0'\rangle$ or into the state $|1'\rangle$. The result of the measurement in this case is actually a random bit.*

[10] Of course, this is not the whole story. In order to illustrate the peculiarities of quantum measurement, let us consider again trines. No measurement on a trine can do better than rule out one of the three possibilities, leaving one bit of uncertainty about the original state of the trine. Thus, it is not possible to extract more than $\lg 3 - 1 \approx 0.585$ bits of classical information from a single trine. However, if we have two trines that are guaranteed to be identical, then (by Peres and Wootters, 1991), there is a measurement that can extract $\frac{\sqrt{2}}{3}(1 + \lg(17 + 12\sqrt{2})) - \frac{3}{2} \approx 1.369 > 2 \times 0.585$ bits of information from both trines. This implies that in some cases we can extract more than twice as much information from two identical qubits than from either one alone. In order to extract more information from two identical qubits than projection measurements allow, POV measurements, see Section 9.2.8, are used.

In addition, as discussed in Section 8.2.4, one can encode 3 bits into one qubit in such a way that any of them (but not all of them) can be retrieved (by a proper measurement) with success probability 0.79.

Remark 2.1.6 A measurement of a qubit with respect to the basis $\{|0\rangle, |1\rangle\}$ corresponds to the projection operator $\frac{1}{2}(I \pm \sigma_z)$. In the case of spin-$\frac{1}{2}$ particles this corresponds to measuring of the spin along the z-axis. Projections $\frac{1}{2}(I \pm \sigma_x)$ and $\frac{1}{2}(I \pm \sigma_y)$ correspond to measurements along the x-axis and y-axis, respectively.

Exercise 2.1.7 *Determine probabilities of the outcomes of the measurements of the qubit* $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ *with respect to the bases:*

(a) $\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(i|0\rangle - |1\rangle)\}$; *(b)* $\{\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle, \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\}$.

Exercise 2.1.8 *Given* $0 < p < 1$, *determine the basis with respect to which the measurement of a qubit* $\alpha|0\rangle + \beta|1\rangle$ *gives outcome* 0 *with probability* p.

Qubit evolution

Any quantum evolution of a qubit, or any quantum operation on a qubit is described, as already mentioned, by a unitary matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

which transforms any qubit state $\alpha|0\rangle + \beta|1\rangle$ into the state $(a\alpha + b\beta)|0\rangle + (c\alpha + d\beta)|1\rangle$. [11]

For example, the evolution given by the Hadamard matrix (transformation)

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

which is called also Hadamard rotation, transforms the states $|0\rangle$, $|1\rangle$, $|0'\rangle$ and $|1'\rangle$ as follows;

$$H|0\rangle = |0'\rangle, \qquad H|0'\rangle = |0\rangle,$$
$$H|1\rangle = |1'\rangle, \qquad H|1'\rangle = |1\rangle.$$

The Hadamard transformation can also be seen as the following mapping of the basis states:

$$H|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^i|1\rangle.$$

The basis $\mathcal{B} = \{|0\rangle, |1\rangle\}$ is called the **standard basis**, or the **computational basis**, $\mathcal{D} = \{|0'\rangle, |1'\rangle\}$ is called the **dual basis** or the **Hadamard basis** or the **Fourier basis**. As we could see, by applying H we can switch between the standard and the dual bases. Observe also that $H^2 = I$. The so-called **circular (polarization) basis**

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

[11] As basic textbooks on quantum mechanics show, the basic evolution of a spin-$\frac{1}{2}$ particle can be well controlled by a clever application of magnetic field and the 2×2 unitary matrix describing time evolution of the spin in the spin-up spin-down basis, from time $t = 0$ to time $t = T$, has, up to the phase factors, in general the form:

$$U = \begin{pmatrix} e^{i\omega T/2} & 0 \\ 0 & e^{-i\omega T/2} \end{pmatrix} \begin{pmatrix} \cos(\omega T/2) & -\sin(\omega T/2) \\ \sin(\omega T/2) & \cos(\omega T/2) \end{pmatrix},$$

where the second matrix is a rotation matrix. For $\omega T = \pi$ we get, up to the phase, the matrix for the NOT operation, and for $\omega T = -\frac{\pi}{2}$, the Hadamard rotation.

is also of importance.

Exercise 2.1.9 *Construct matrices to transform a qubit state from: (a) standard basis to circular polarization basis and vice versa; (b) dual basis to circular polarization basis and vice versa.*

If the states $|0'\rangle$ and $|1'\rangle$ are measured with respect to the standard basis $\mathcal{B}$, we get both outcomes—0 and 1—with the same probability $\frac{1}{2}$. The evolution H applied on the states of the standard basis can therefore be seen as implementing a **fair coin tossing**.

Example 2.1.10 *If the matrix*

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

is applied to the states of the standard basis, then $H'^2|0\rangle = -|1\rangle$, $H'^2|1\rangle = |0\rangle$, *and therefore* H'^2 *acts as a* NOT *operation, up to the phase sign.*

Exercise 2.1.11 *What do you get if the matrix from Figure 1.4e is applied: (a) once; (b) twice, to the standard basis states? (Transformation defined by this matrix is known as the* **square root of not**. *Explain why.)*

Three other important unitary operations on qubits are shown in Figure 2.3: rotation (by θ) $R(\theta)$; phase shift (with respect to α) $PS(\alpha)$; and scale (with respect to δ) $Scal(\delta)$.

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

Figure 2.3: Unitary matrices of degree 2

Exercise 2.1.12 *(Barenco, 1996) Show that the following properties hold for matrices* R, PS, $Scal$ *and the Pauli matrix* σ_x.
(a) $R(\theta_1) \cdot R(\theta_2) = R(\theta_1 + \theta_2)$;
(b) $PS(\alpha_1) \cdot PS(\alpha_2) = PS(\alpha_1 + \alpha_2)$;
(c) $Scal(\delta_1) \cdot Scal(\delta_2) = Scal(\delta_1 + \delta_2)$;
(d) $\sigma_x \cdot R(\theta) \cdot \sigma_x = R(-\theta)$; *(e)* $\sigma_x \cdot PS(\alpha) \cdot \sigma_x = PS(-\alpha)$.

A general form of the unitary matrices of degree 2 is well known:

Theorem 2.1.13 *Each unitary matrix* U *of degree* 2 *can be written as follows:*

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

Exercise 2.1.14 *Show how to construct from the rotation, phase shift and scale matrices: (a) the Hadamard matrix; (b) the matrix* $\begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}$.

Exercise 2.1.15 *Prove Theorem 2.1.13 using the fact that a matrix is unitary if and only if its rows and columns are orthogonal.*

Exercise 2.1.16 *(Vazirani, 1997) Given a matrix* M *and a real* λ, *define* $e^{i\lambda M} = \sum_{k=0}^{\infty} \frac{(i\lambda)^k}{k!} M^k$. *(a) Compute* $e^{i\sigma_x}$, $e^{i\sigma_y}$, $e^{i\sigma_z}$, *where* $\sigma_x, \sigma_y, \sigma_z$ *are Pauli matrices; (b) show that each unitary matrix of degree 2 has the form* $U = e^{i\gamma} e^{i\alpha\sigma_z} e^{i\theta\sigma_x} e^{i\beta\sigma_z}$.

In principle, there is a continuous range of rotation, phase shift and scale matrices. However, already finitely many of them are sufficient to perform all quantum computations with an arbitrary precision.

Exercise 2.1.17 *Show that any rotation* $R(\alpha)$ *can be decomposed, with an arbitrarily small error, into polynomially many, with respect to the error, gates* $R(\theta)$, *with* $\theta = 2\pi \sum_{k=0}^{\infty} \frac{1}{2^{2^k}}$.

One of the basic tools for unitary operations in H_2 is the **beam splitter**, see Figure 2.4 for two ways a beam splitter is depicted. The beam splitter has two input and two output ports. By varying both phases of the incoming beams and the reflectivity of the beam splitter, one can realize by a beam splitter any unitary operation in H_2. A beam splitter is often depicted with only one input and with no specification of phasing and reflecting. In such a case it is assumed that the second input refers to the vacuum or other reference state and the incoming basis state is transferred to an equally weighted superposition of both bases states.

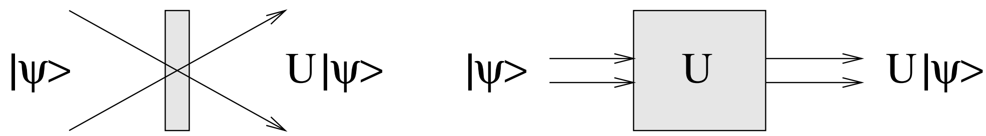


Figure 2.4: Beam splitter

Example 2.1.18 *In the case of photons a half-silver mirror (Figure 2.5b), acts as the beam splitter (see Figure 2.5a). A full-silver mirror (Figure 2.5c), reflects the photon. In the case of the half-silver mirror both detectors D1 and D2 detect the photon with the same probability. The fact that this cannot be interpreted as "photon goes one way with probability* $\frac{1}{2}$ *and the other way with the same probability" is well demonstrated using the so-called Mach–Zehnder interferometer (Figure 2.5d). In the case two half-silver mirrors and two full-silver mirrors are arranged as Figure 2.5d shows, then, as one can easily calculate, detector D1 detects the photon with probability* 1. *However, if we put an obstacle on one of the paths (Figure 2.5e), then both detectors detect with the same probability. If we put on one path an obstruction the photon can get through, but this obstruction acts as a measuring device, then both detectors* *detect the photon with the same probability (see Figure 2.5f). Finally, if we put on one path a glass that causes a precalculated delay (see Figure 2.5g), then only detector D2 detects the photon.*

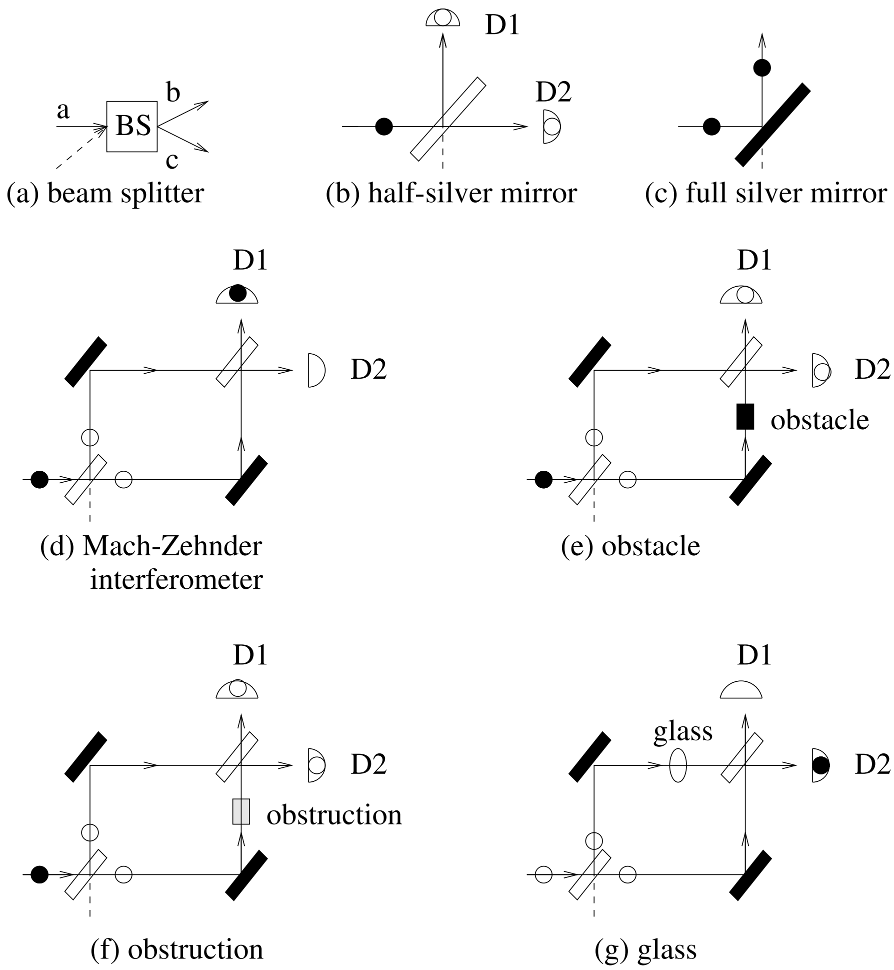


Figure 2.5: Mach–Zehnder interferometer in various situations

Remark 2.1.19 In addition to qubits as states of H_2, the special name **(qu)trit** is used for states in H_3, (for spin–1 particles). Their general form is

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle,$$

where $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$, and $(\{|0\rangle, |1\rangle, |2\rangle\})$ is its standard basis.

One cannot do too much computation with a single qubit. Actually, it is the concept of an n-bit **quantum register** that is a proper framework for designing quantum algorithms.

2.1.2 Two-qubit registers

A tensor product of two qubits is called a **2-qubit quantum register**. The corresponding Hilbert space is H_4. Several of its important/interesting bases are shown in Figure 2.6.

basis	basis state 1	basis state 2	basis state 3	basis state 4
standard	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
dual	$\|0'0'\rangle$	$\|0'1'\rangle$	$\|1'0'\rangle$	$\|1'1'\rangle$
Bell	Φ^+	Φ^-	Ψ^+	Ψ^-
	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$
magic	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{i}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{i}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$

Figure 2.6: Bases in H_4; Bell states are denoted by $\Phi^{\pm}$ and $\Psi^{\pm}$, and for each of these states the corresponding value is given one row below; the state Ψ^- is called **singleton**

It is usual to represent states of the standard basis in one of the following forms:

$$|0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ |1\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \ |2\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \ |3\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

A general state of a 2-qubit quantum register has the form

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \tag{2.2}$$

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

Exercise 2.1.20 *Express the basis states* $|00\rangle, |01\rangle, |10\rangle$ *and* $|11\rangle$ *in terms of the states* $|0'0'\rangle, |0'1'\rangle, |1'0'\rangle, |1'1'\rangle$ *and vice versa.*

Exercise 2.1.21 *(a) Design a unitary matrix that maps standard basis* $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ *into Bell's basis. (b) Design a unitary matrix that maps Bell's basis into the standard one; (c) Hadamard matrix transforms standard basis of* H_2 *into its dual basis and vice versa. Does there exist a unitary matrix that maps the standard basis of* H_4 *into Bell's basis and vice versa?*

Exercise 2.1.22 *Show that vectors of Bell's basis are eigenvectors of the unitary matrix implementing the mapping* $|x, y\rangle \to |\bar{x}, \bar{y}\rangle$.

Exercise 2.1.23 *(DiVincenzo et al. 1998a) For the following* 5 *states of two qutrits:* $|\phi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle)$, $|\phi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)||2\rangle$, $|\phi_3\rangle = \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle)$, $|\phi_4\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle$ *and* $|\phi_5\rangle = \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle)$ *show that they form "unextendable product base" of* H_9 *in the sense that: (a) they form an orthonormal set; (b) there is no state* $|\phi_1\rangle|\phi_2\rangle$*, where* $|\phi_1\rangle$ *and* $|\phi_2\rangle$ *are qutrit states, which is orthogonal to all* 5 *states above.*

Measurements of two-qubit registers

A measurement of the state $|\psi\rangle$, see (2.2), with respect to the standard basis produces as the outcome two bits ij with probability $|\alpha_{ij}|^2$, and causes the collapse of $|\psi\rangle$ into the state $|ij\rangle$.

> **Exercise 2.1.24** *Determine probabilities of possible outcomes when the state (2.2) is measured with respect to: (a) dual basis; (b) Bell's basis; (c) magic basis.*

It is often necessary to measure only one qubit. This can be done using observable

$$\begin{array}{ll} \mathcal{B}_1 = \{E_1^0, E_1^1\}, & \text{in the case of the first qubit;} \\ \mathcal{B}_2 = \{E_2^0, E_2^1\}, & \text{in the case of the second qubit.} \end{array}$$

where E_1^i, $i = 0, 1$, is the subspace spanned by the vectors $\{|i0\rangle, |i1\rangle\}$ and E_2^i, $i = 0, 1$ is the subspace spanned by the vectors $\{|0i\rangle, |1i\rangle\}$.

Hence, if the first qubit is measured, we get as the outcome bit 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$, and the post-measurement state

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

(Note that the state $|\psi'\rangle$ is projected and then renormalized.) In a similar way probabilities and resulting state are determined when outcome is 1 and when the second qubit is measured.

Quantum evolution of 2 qubits

Among unitary transformations on two qubits states the following transformation has a special role

$$\mathrm{XOR} : |x, y\rangle \to |x, x \oplus y\rangle,$$

with the matrix representation

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

XOR[12] matrix performs the same mapping as the CNOT gate considered in Section 1.7. (Observe that there is an infinite number of inequivalent quantum gates that reproduce the classical CNOT gate . Namely, all gates performing a transformation $|x, y\rangle \to e^{i\theta}|x, x \oplus y\rangle$.)

> **Exercise 2.1.25** *Verify that if I denotes the unit matrix of degree 2, then*
>
> $$XOR = |0\rangle\langle 0| \otimes \mathbf{1} + |1\rangle\langle 1| \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|).$$

[12] For the first implementation of the XOR gate see Monroe et al. (1995) and for an introductory description of it see Berman et al. (1998).

As discussed in detail in Section 2.3, the following unitary matrix is universal, in a reasonable sense, in the class of all unitary matrices

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

if α, ϕ and θ are irrational multiples of π and of each other.

Exercise 2.1.26 *Show that the tensor products of matrices and quantum states have the following property:*

$$(A \otimes B)(|\psi_1\rangle \otimes |\psi_2\rangle) = (A|\psi_1\rangle) \otimes (B|\psi_2\rangle).$$

Exercise 2.1.27 *Show that XOR matrix cannot be obtained as a tensor product of two unitary matrices of degree* 2.

2.1.3 No-cloning theorem

The following simply stated and easily proved theorem (see Wootters and Zurek, 1982, and Dieks, 1982), shows what a unitary transformation cannot do on two qubit registers. No-cloning theorem has far reaching consequences for quantum information processing.

Theorem 2.1.28 (No Cloning (copying) Theorem) *An unknown quantum state cannot be cloned. (Namely, there is no unitary transformation U, such that for any one-qubit state $|\psi\rangle$, $U(|\psi,0\rangle) = |\psi,\psi\rangle$.* [13]*) No cloning theorem holds for any Hilbert space.*

Proof 1. Assume that such a U exists and for two different orthogonal states $|\alpha\rangle$ and $|\beta\rangle$, $U(|\alpha,0\rangle) = |\alpha,\alpha\rangle$, $U(|\beta,0\rangle) = |\beta,\beta\rangle$. Let $|\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)$. Then $U(|\gamma,0\rangle) = \frac{1}{\sqrt{2}}(|\alpha,\alpha\rangle + |\beta,\beta\rangle) \neq |\gamma,\gamma\rangle = \frac{1}{2}(|\alpha,\alpha\rangle + |\beta,\beta\rangle + |\alpha,\beta\rangle + |\beta,\alpha\rangle)$.[14] ∎

Proof 2. Assume there is a unitary operator U such that $U|\phi,0\rangle = |\phi,\phi\rangle$, $U|\psi,0\rangle = |\psi,\psi\rangle$, for arbitrary ϕ,ψ. Since U is unitary we have

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

A contradiction is obtained if ϕ and ψ are chosen in such a way that $\langle\psi|\phi\rangle < 1$, which is always possible. ∎

[13]The no-cloning theorem seems to be bad news. However, this would be a very simplified view of its impacts. For example, very good news that unconditional secure quantum key generation is possible, see Section 6.2, is to a large extend due to this "bad news". In addition, new techniques have appeared that allow one to make approximate copies of qubits (Bužek and Hillery, 1996, and Bužek et al. 1997). They proposed the Universal Quantum Copy Machine that can produce two (imperfect, but equivalent in some weaker sense) copies of any qubit and the quality of copying is independent of particular qubits. It is even possible to make three imperfect copies. However, this good news has also 'bad" aspects. The copies obtained are entangled.

[14]The discovery that no general quantum copying procedure exists is a surprising and profound result of quantum mechanics. The reason behind it is that any attempt to copy a coherent superposition of states results in a state reduction, destruction of coherence, and the addition of noise. Moreover, the feasibility of cloning would have surprising consequences and would lead to paradoxes. For example, in combination with quantum teleportation, Section 6.4, it would allow faster-than-light transmission of information.

Exercise 2.1.29 *Design a classical circuit to copy an unknown classical bit.*

Exercise 2.1.30 *Show that we can learn an unknown quantum state with arbitrary precision when we have an unlimited number of copies of the state and can measure it with respect to any observable we need.*

Observe also that "No-cloning theorem" only implies that there is no general unitary transformation for perfect copying of quantum information without destroying the original copy of information. As we shall see in Section 6.4, quantum information can be teleported (a copy of it can be moved to some different place) but the original copy will get destroyed.

Exercise 2.1.31 *Show that to any qubit state $|\psi\rangle$ of a qubit there is a unitary transformation $U_{|\psi\rangle}$ such that $U_{|\psi\rangle}(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$.*

Exercise 2.1.32 *Show that if two different states $|\phi\rangle$ and $|\psi\rangle$ can be copied by the same circuit, then $\langle\phi|\psi\rangle = 0$.*

Exercise 2.1.33 *Show that there is no universal quantum NOT gate in the following sense—there is no unitary one-qubit transformation NOT such that $\langle NOT(\phi)|\phi\rangle = 0$ for any one qubit state $|\phi\rangle$.*[15]

2.1.4 Quantum registers

The generalization of 2-qubit registers to the case of n-qubit registers is straightforward.

Hilbert space of an n-qubit register

To deal with n-qubit registers we work within a 2^n-dimensional Hilbert space with the following set of basis vectors:

$$\mathcal{B} = \{|i\rangle \mid i \in \{0,1\}^n\}$$

or, another notation, used perhaps more often,

$$\mathcal{B} = \{|i\rangle \,|\, 0 \leq i < 2^n\},$$

which are said to form the **standard** or **computational** basis.

The general qubit state of the n-qubit register is

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i|i\rangle \quad \text{with} \quad \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

Remark 2.1.34 n-qubit registers have several remarkable properties:

1. The number of basis states and the size of superpositions grows exponentially with the number of qubits. Note that already for $n = 200$ the total number of states of any basis is larger than estimated number of atoms in the universe.[16]

[15] However, as shown by Bužek et al. (1999),
there is a method how to construct, to any qubit state $|\psi\rangle$ and any $\varepsilon > 0$ an (ε-orthgonal) state $|\psi_\varepsilon\rangle$ such that $\langle\psi|\psi_\varepsilon\rangle < \varepsilon$, provided a sufficient number $n_{\varepsilon,\psi}$ copies of $|\psi\rangle$ is available,

[16] Therefore, already 100-qubit computers should have, in some sense, incredible power.

2. In order to store a number n one requires $\lceil \lg(n+1) \rceil$ qubits and therefore one has to use a Hilbert space of dimension $2^{\lceil \lg(n+1) \rceil}$, i.e. with $2^{\lceil lg(n+1) \rceil} > n$ distinguished basis states.

3. In spite of the exponential size of the set of basis states there is a fast, linear time, access from one state of the standard basis to another. Indeed, at most n NOT operation applications to individual qubits can bring any state $|i\rangle$ into any state $|j\rangle$.

4. An n-qubit register seems to be able to store exponentially more information than an n-bit register. (However, as follows from Holevo theorem (1973), n is a maximum number of bits one can "store" in an n-qubit register in such a way that one can again retrieve them faithfully.)

Evolution of n-qubit registers

An evolution of an n-qubit register state is given by a unitary operator with a $2^n \times 2^n$ matrix. In order to perform classically such an evolution step an exponential number, $2^n(2 \cdot 2^n - 1)$, arithmetical operations are needed in general.

On the other hand, in designing quantum algorithms and networks we mostly use operators that have a simple structure due to which the overall effort to simulate an evolution step is significantly smaller than in the general case.

It is mostly the case that an evolution step is performed by applying a unitary rotation operator to a single qubit or by applying a unitary operation, especially XOR, to two qubits.

If a unitary matrix U is applied to the ith qubit, then the overall unitary operation applied to the n-qubit register states has the form $(\bigotimes_{k=1}^{i-1} I) \otimes U \otimes (\bigotimes_{k=i+1}^{n} I)$. In order to simulate such an evolution step only $3 \cdot 2^n$ arithmetical operations are needed.

Exercise 2.1.35 *Let* $U = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$. *Describe the structure of the following unitary matrices: (a)* $U \otimes I \otimes I$; *(b)* $U \otimes \bigotimes_{i=1}^{n-1} I$; *(c)* $\bigotimes_{i=1}^{k} I \otimes U \otimes \bigotimes_{i=1}^{k} I$; *(d)* $XOR \otimes I \otimes I$.

Example 2.1.36 *Let a unitary matrix* $U = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$ *be applied to the first qubit of an n-qubit register in the state* $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$. *In such a case*

$$U|\phi\rangle = \sum_{y_1 \dots y_n \in \{0,1\}^n} (\sum_{j=0}^{1} a_{y_1 j} \alpha_{j y_2 \dots y_n}) |y_1 \dots y_n\rangle.$$

One of the aims of quantum algorithms and network design is to decompose a problem-solving unitary operator into a sequence of one and two qubit operations from a small set of such available operations. As discussed in Section 2.3, for any reasonable set of such basic operations such a decomposition always exists. However, an important problem is to determine for particular unitary operations whether such a decomposition into a polynomial number of one or two qubit operations can be done. When a considered unitary operation can be decomposed into a polynomial number $p(n)$ of one and two qubit operations, then the overall quantum computation time is $\mathcal{O}(p(n))$. Where a classical simulation is to be performed the total number of operations needed is $\mathcal{O}(p(n)2^n)$.

Measurements

If the state $|\phi\rangle$ of an n-qubit register is measured with respect to the standard basis we get as the outcome n bits, each n-tuples of bits with a precalculated probability, and the state $|\phi\rangle$, in the (potential) superposition of 2^n basis states, collapses to just one of the basis states.

Let us now consider a measurement of the jth qubit only. The corresponding observable is $\mathcal{B}_j = \{E_j^0, E_j^1\}$, where E_j^0 (E_j^1) is the subspace of the 2^n-dimensional Hilbert space spanned by all basic vectors having 0 (1) in the jth component.

The measurement of the jth qubit gives

$$0\ (1) \text{ with probability } \sum_{i\,|\,i_j=0} |\alpha_i|^2 \ (\sum_{i\,|\,i_j=1} |\alpha_i|^2),$$

where i_j denotes the jth bit in the binary representation of i.

A measurement of n qubits of an $(n+m)$-qubit register reduces the dimensionality of the Hilbert space we work with by the factor 2^n.

When we want to measure the first m qubits of an $(n+m)$-qubit quantum register, it is convenient to express its states as:

$$|\psi\rangle = \sum_{i=0}^{2^n-1}\sum_{j=0}^{2^m-1} c_{ij}|i,j\rangle \quad \text{with} \quad \sum_{i,j}|c_{ij}|^2 = 1.$$

In this case the states of the basis are seen as pairs of integers $0 \le i < 2^n$ and $0 \le j < 2^m$.

If we now measure the first n qubits we get each number $i \in [0, 2^n)$, with probability

$$p(i) = \sum_{j=0}^{2^m-1} |c_{ij}|^2$$

and the state $|\psi\rangle$ collapses into the state

$$|\psi_i\rangle = \frac{1}{\sqrt{p(i)}} \sum_{j=0}^{2^m-1} c_{ij}|i,j\rangle.$$

Exercise 2.1.37 *What are the results of the measurement of the first qubit of the following states with respect to the dual basis: (a)* $\alpha|000\rangle + \beta|111\rangle$*; (b)* $\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$*; (c)* $\frac{1}{\sqrt{2}}(|0^{(n)}\rangle + |1^{(n)}\rangle$ *for an arbitrary* n*?*

Dual (Fourier) basis

It is the basis of the states $\{|i'\rangle \,|\, 0 \le i < 2^n\}$. Transformation between standard and dual (or Fourier) basis is given by the so-called **Hadamard transformation** or **Walsh transformation** or **Walsh–Hadamard transformation** or **discrete Fourier transformation over $\mathbf{Z}_2^n$**.[17]

$$H_n = \bigotimes_{i=1}^{n} H.$$

[17] Often the term "transform" is used instead of transformation .

It is easy to see that[18]

$$H_n|0^{(n)}\rangle = \bigoplus_{i=1}^{n} H|0\rangle = \bigoplus_{i=1}^{n} |0'\rangle = |0'^{(n)}\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle$$

and, in general, for $x \in \{0,1\}^n$

$$H_n|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle.^{19} \tag{2.3}$$

Example 2.1.38 (Setting of equally weighted superposition of basis states) *For many quantum algorithms the following initial state, which contains equally weighted distribution of all basis states, is of importance:*

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle. \tag{2.4}$$

Of key importance is the fact that it is very easy (theoretically at least) to set an "empty" register $|0^{(n)}\rangle$ into the state (2.4). One just needs to apply the Hadamard transformation H to each qubit as described above. In other words, using a linear number of operations we can transform one basis state into an exponential large and equally weighted superposition of all basis states.

Of importance in various areas of quantum information processing are the so-called **cat states** $\frac{1}{\sqrt{2}}(|0^{(n)}\rangle + |1^{(n)}\rangle)$. In the case $n = 2$ we have one of the Bell states, and in the case $n = 3$ one of the **GHZ states** (where GHZ stands for Greenberg, Horne and Zeilinger, 1998a). In general there are eight GHZ states of the form $\frac{1}{\sqrt{2}}(|abc\rangle \pm |\bar{a}\bar{b}\bar{c}\rangle)$, where $a, b, c \in \{0,1\}$ and at most one of a, b, c is one.

Exercise 2.1.39 *Describe unitary matrices that map the state $|0^{(n)}\rangle$ into the cat state $\frac{1}{\sqrt{2}}(|0^{(n)}\rangle + |1^{(n)}\rangle)$ for: (a) $n = 3$; (b) $n = 4$; (c) $n = 5$.*

Example 2.1.40 (Inversion about the average) *The unitary transformation*

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

where E is the average of $\{a_i \mid 0 \le i < 2^n\}$, can be performed by the matrix[20]

$$D_n = \begin{pmatrix} -1+\frac{2}{2^n} & \frac{2}{2^n} & \dots & \frac{2}{2^n} \\ \frac{2}{2^n} & -1+\frac{2}{2^n} & \ddots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \dots & -1+\frac{2}{2^n} \end{pmatrix}.$$

[18] The notation $0^{(n)}$ stands for n 0s.

[19] The dot product is defined as follows: $x \cdot y = \bigoplus_{i=1}^{n} x_i y_i$.

[20] The name of the operation comes from the fact that $2E - x = E + E - x$ and therefore the new value is as much above (below) the average as it was initially below (above) the average—which is precisely the inversion about the average.

The matrix D_n is clearly unitary and it can be shown to have the form $D_n = -H_n R_n^1 H_n$, where $R_n^1[i,j] = 0$ if $i \neq j$, $R_n^1[1,1] = -1$ and $R_n^1[i,i] = 1$ if $1 < i \leq n$.

Classical versus dual basis

In various considerations concerning Hilbert spaces H_{2^n}, especially in connection with quantum error-correcting codes, see Section 7.4, of large importance an interplay between the standard basis $\{|i\rangle \,|\, 0 \leq i \leq 2^n - 1\}$ and the dual basis $\{|i'\rangle \,|\, 0 \leq i \leq 2^n - 1\}$ is, where $|i'\rangle = |i'_{n-1}i'_{n-2}\ldots i'_0\rangle$ and $i = i_{n-1}i_{n-2}\ldots i_0$ in the binary representation.

Exercise 2.1.41 *(Steane, 1996) Let*

$$|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle = \sum_{x'\in\{0',1'\}^n} \alpha'_x |x'\rangle$$

and let $|\phi_j\rangle$ be obtained from $|\phi\rangle$ in the standard basis by the flipping jth bit of the basis states, i.e. $|\phi_j\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |flip_j(x)\rangle$. Show that then

$$|\phi_j\rangle = \sum_{x'\in\{0',1'\}^n} \alpha'_x (-1)^{x'_j} |x'\rangle.$$

Exercise 2.1.42 *(Steane, 1996) If $|\phi_c\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |flip(x)\rangle$, where flip$(x)$ flips all bits of the binary representation of x, then $|\phi_c\rangle = \sum_{x'\in\{0',1'\}^n} \alpha'_x (-1)^{parity(x')} |x'\rangle$, i.e if all basis words are flipped in the standard basis, then all odd parity words in the dual basis change their sign.*

Exercise 2.1.43 *Express the states $|1^{(n)}\rangle$ and $\frac{1}{\sqrt{2}}(|0^{(n)}\rangle + |1^{(n)}\rangle)$ in the dual basis.*

In all of the above exercises short states in one basis have long representation in another basis. This is inevitable because the following inequality holds (see Bialynicki-Birula and Mycielski, 1975, Deutsch, 1983, and Steane, 1996).

Theorem 2.1.44 *If a state $|\phi\rangle$ of a Hilbert space H_{2^n} can be written as a superposition of m_1 basis states in the standard basis and m_2 basis states in the dual basis, then*

$$m_1 m_2 \geq 2^n. \tag{2.5}$$

2.2 Quantum Entanglement

One of the most specific and also most important concepts for quantum computing and quantum information theory is that of quantum entanglement—also one of the most puzzling concepts of quantum physics.

2.2.1 Entanglement of pure states

Let us start with an example. A 2-qubit register can be in the state

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

If we observe the first bit of this state using the standard observable $\mathcal{B}_1$, then we get the value 0 with probability $\frac{1}{2}$ and the value 1 also with probability $\frac{1}{2}$. (Hence the outcome is completely random.) After such an observation the state $|\psi\rangle$ collapses into the state $|00\rangle$ in the first case and into the state $|11\rangle$ in the second case.[21] If, afterwards, we measure the second qubit its value is determined uniquely, with probability 1. We see that if a quantum register is in the above state $|\psi\rangle$, then the two qubits are not independent. In addition, in such a case particular qubits of the quantum register no longer have an identity! Each of them is actually in a totally mixed state—with probability $\frac{1}{2}$ in the state $|0\rangle$ and with probability $\frac{1}{2}$ in the state $|1\rangle$; only both together form a pure state.

How specific and important is this example? We naturally expect that there should be cases where the qubits are completely independent and therefore they can be separately acted on.

This is actually the case if a state $|\psi\rangle$ of a 2-qubit register is the tensor product $|\psi_1\rangle \otimes |\psi_2\rangle$ of two 1-qubit states $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$, i.e.,

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = (\sum_{i=0}^{1} \alpha_i|i\rangle) \otimes (\sum_{j=0}^{1} \beta_j|j\rangle). \tag{2.6}$$

Exercise 2.2.1 *Determine: (a)* $|\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$ *for* $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$*; (b)* $|\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$ *for* $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$*; (c)* $|\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$ *for* $\psi = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$.

If we now observe the first qubit of the state $|\psi\rangle$, in (2.6), we get:

$$0 \text{ with probability } |\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 = |\alpha_0|^2,$$
$$1 \text{ with probability } |\alpha_1\beta_0|^2 + |\alpha_1\beta_1|^2 = |\alpha_1|^2.$$

Moreover, after the observation of the first qubit the state $|\psi\rangle$ is reduced to $|\psi_2\rangle$; after the observation of the second qubit to $|\psi_1\rangle$.

If a quantum pure state of a Hilbert space H cannot be obtained as a tensor product of two quantum states from Hilberts spaces of the dimension smaller than that of H, then the state is called **entangled**. If this is a state of an n-qubit register, then we also say that all its qubits are entangled.

Entangled states arise in a natural way as a result of interactions between quantum systems. For example, if a pair of particles is created simultaneously and in such a way that some of their attributes (say spin or polarization) are preserved; for example, if one particle has spin $\frac{1}{2}$ and second has spin $-\frac{1}{2}$, or if one particle has polarization $0°$ and the second $90°$. In addition, some quantum operations create entangled states out of unentangled states. For example, if XOR operation is applied to the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$, the entangled state

[21] Two qubits in the state $|\psi\rangle$ therefore behave like a pair of magic coins with the property that if they are tossed one after another then the second of them yields head if and only if the first one does so.

$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is produced.[22] Observe that entangled states do not exist in classical systems.

Exercise 2.2.2 *(Cleve et al. 1998) Show that the state* $\sum_{y=0}^{2^n-1} e^{\frac{2\pi i a y}{2^n}}|y\rangle$ *is unentangled if* $a \in \{0,\ldots,2^n-1\}$ *and can be expressed in the form* $\bigotimes_{i=1}^{n}(|0\rangle + \alpha_i|1\rangle)$, *for proper amplitudes* α_i.

Exercise 2.2.3 *(Cleve et al. 1998) Show that the state* $\sum_{y=0}^{2^n-1} e^{2\pi i\phi y}|y\rangle$ *is unentangled for all* ϕ, *and find its decomposition into the tensor product of one-qubit states.*

A pair of two-state particles which is in the entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ or $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, is often said to be in the Bohm state or EPR state or Bell state or to form an EPR pair, or the EPR effect—"EPR" stands here for "Einstein, Podolsky and Rosen", see Section 9.1.5—and that it creates a so-called "EPR channel". Such a channel can be used to "teleport" quantum information as discussed in Section 6.4.

An EPR channel is created, for example, when certain types of atom or molecule decay with the emission of two photons, and consists of the fact that the two photons are always found to have opposite polarization, regardless of the basis used to measure them, provided both are measured with respect to the same basis. Figure 2.7 shows a way how an EPR-pair and channel can be generated.

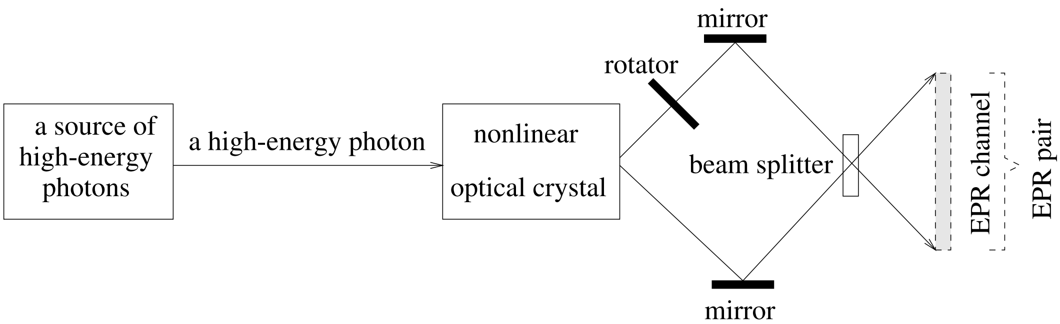


Figure 2.7: Generation of an EPR pair of polarized photons and an EPR-channel, adopted from Glanz (1995).

Exercise 2.2.4 *Show that by an appropriate choice of the basis any entagled (pure) state of two qubits can be written as* $|\phi\rangle = \cos\phi|00\rangle + \sin\phi|11\rangle$.

Paradoxical nature of entanglement

The source of various paradoxes related to entangled states (see Section 9.1.5), is the fact that a pair of particles in an entangled state can be much physically separated. Each

[22] Entangled are, for example, the states of Bell basis. Observe that XOR maps all states of Bell basis into states that are not entangled; it therefore performs **disentanglement** on the states of Bell basis.

The phenomenon of quantum entanglement was first noticed by Schrödinger, in 1935, and the English term "entanglement" is the direct translation of the German term "Verschränkung" used by Schrödinger.

measurement on one particle of such an entangled pair immediately determines the state of another one, no matter how far apart they are.

A measurement of an entangled particle exhibits therefore the so-called "non-local effect" (see page 20), something that cannot happen from the point of view of classical physics without an instantaneous communication among the particles.

Remark 2.2.5 The concept of an entangled state is an excellent example of a difference between thinking in terms of Hilbert space constructs and dealing with real quantum systems. Mathematically the concept of entanglement is a trivial one. Physically the existence of entangled states of distant particles is one of the most puzzling phenomena, and the Gedanken experiment devised by Einstein and his colleagues in 1935 concerning entanglement was to illustrate how unreasonable, from Einstein's point of view, quantum mechanics is (see Section 9.1.5). It was a very challenging experimental task to show experimentally entanglement of even 2 qubits. The entanglement of two spatially separated particles was experimentally demonstrated by Wu and Shaknov (1950), Kwiat et al. (1995) and Zeilinger et al. (1997)—polarized photons—and Hagley et al. (1997), pairs of atoms. The entanglement of two photons over 10 km has been demonstrated at the University of Geneva (see Tittel et al. 1998). Recent experimental demonstrations of GHZ states are considered as important achievements. First Laflamme et al. (1997) reported, using NMR technology, that three nuclear spins within a single molecule locally exhibited GHZ state. Later, Bouwmeester et al. (1998), demonstrated polarization entanglement in GHZ state for three spatially separated photons (such that each can be addressed separately).

The following set-up further illustrates peculiarities of entanglement.

Example 2.2.6 *Let both Alice and Bob possess one particle of an entangled pair in the state* $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ *and assume they travel to distant places and agree to measure their particles immediately after their arrival. Let us assume that Alice gets as the result of her measurement state the* $|0\rangle$. *She knows immediately that Bob's particle has the state* $|1\rangle$. *However, this situation could happen in two ways. The first possibility is that Alice has arrived first and her measurement determined the state of Bob's particle. The other possibility is that Bob has arrived first, got* $|1\rangle$ *as the result of his measurement, and that determined* $|0\rangle$ *as the state of Alice's particle. How to find out for Alice which of these two cases did really happen? She could call Bob to ask about the time of his measurement. Interestingly enough, such a classical communication seems to be the only way to solve this problem.*

Entanglement as a computational and communicational resource

Entanglement plays a central role in quantum information theory that extends classical information theory—see Chapter 8. According to Bennett (1998a), entanglement between a pair of quantum systems in a maximally entangled state is the purest form of inherently quantum information: it is capable interconnecting two parties far apart, it cannot be copied, eavesdropped without disturbance, nor it can be used by itself to send classical messages. At the same time it can assist in speeding up both classical and quantum communication.

Quantum entanglement is also the main reason why quantum computers cannot be efficiently simulated by classical ones.

To describe fully a state of n-qubit register we need to write down in general 2^n complex coefficients. Already for a small $n = 100$ this would require $2^{100} \approx 10^{30}$ numbers, which is outside the potential of foreseeable classical computers. (In addition, to simulate a quantum computer with 100-qubit register we would need to manipulate matrices of degree 10^{30}.) Since quantum computers are probabilistic it could seem that keeping a complete state description at each stage of simulation is not the only way to simulate quantum computers on probabilistic ones. It is therefore natural to ask whether it is possible to simulate quantum computers on probabilistic ones which do not always keep a complete description of the current quantum state and only provide various outcomes with the same probability as the simulated quantum computer does. Could not we perform some "local simulations" in which each qubit has a definite value at each computation step and each quantum gate can act on the input qubits in various possible ways, only one of which is always selected as determined by a (pseudo)random generator? Such simulations could avoid a need for exponential space! However, it is a consequence of quantum entanglement, of its non-local correlations, that we cannot always divide the state of the quantum system under consideration into parts and compute them separately. Due to the quantum entanglement there is in general no local probabilistic classical algorithm simulating quantum computers.

An easy way to demonstrate directly that it is exactly because of quantum entanglement that quantum computers cannot be efficiently simulated by classical ones goes as follows.

Let us assume that an evolution of a state $|\psi\rangle$ of an n qubit register goes through a sequence of states $|\psi_i\rangle$, $i \geq 1$, and $|\psi_i\rangle = |\phi_{i1}\rangle \otimes |\phi_{i2}\rangle \otimes \ldots \otimes |\phi_{in}\rangle$, where each $|\phi_{ij}\rangle$ is a qubit state. No matter how long such an evolution is, it can be easily simulated by a classical computer because it can simulate evolution qubit by qubit and there is no exponential increase in the number of coefficients a classical computer has to store.

It often used to be emphasized that quantum superposition is the root of the extraordinary power of quantum computing. However, it is nowadays clear that this is too simplified a view of quantum computing.

Indeed, as already discussed in Section 1.5, classical waves also exhibit superpositions. As a consequence, any effect depending on quantum interference alone seems to be readily simulated by classical waves. Entanglement can be seen as a very special type of superposition that has no classical analog. Jozsa (1997) provides arguments that we cannot always simulate quantum parallelism (see page 103), by classical waves.

Quantum entanglement should be seen as a computational resource that allows qualitatively and quantitatively new types of information processing. At the same time entanglement is a resource which is very difficult to create and to preserve.

Applications of quantum entanglement: speed-up of classical computations, Sections 3.1, 3.2, 3.3; quantum key generation, Sections 6.2 and 6.2.4; teleportation, Section 6.4; superdense coding, Section 6.4.4; entanglement enhanced classical communication (Bennett, Fuchs and Smolin, 1997); quantum data compression, Section 8.2; error-correction codes, Section 7.4; fault-tolerant computing, Section 7.5, dense coding, Section 8.2.4.

2.2.2 Quantifying entanglement

The amount of entanglement $E(\phi)$ in a pure state $|\phi\rangle$ of a compound (bipartite) quantum system $A \otimes B$ is defined (see Bennett et al. 1996a), using the concept of von Neumann quantum entropy by

$$E(\phi) = -Tr\rho_A \lg \rho_A = -Tr\rho_B \lg \rho_B,$$

where $\rho = |\phi\rangle\langle\phi|$. (See Sections 1.4.5 and 9.2.3 for references to density matrices and the tracing out operation.)

Bell states and GHZ states are an important example of maximally entangled two-qubit states.[23]

A pair of maximally entangled qubits forms the so-called **ebit**—the term coined by Ch. Bennett et al. (1996)[24].

An example of weakly entangled states in H_2 are states $\frac{1}{\sqrt{k}}|00\rangle + \sqrt{\frac{k-1}{k}}|11\rangle$ for large k.

Another examples of maximally entangled states in H_n are the states

$$|\phi_n\rangle = \frac{1}{\sqrt{n}} \sum_{1=1}^{n} |i\rangle|i\rangle.$$

It is easy to see that $|\phi_{2^n}\rangle = |\Phi^+\rangle^{\otimes n}$, i.e., $|\phi_{2^n}\rangle$ is the tensor product of the Bell state $|\Phi^+\rangle$ with itself n times.

There is a variety of technical results showing that entropy of entanglement as defined above is a reasonable measure of entanglement. For example, if two parties share an entangled pair, then they cannot change the entropy of entanglement by local actions (even with the help of classical communication). In addition, two pure entangled states with the same entropy of entanglement can be transferred into each other by local actions (see Bennett, 1998a).

The concept of entanglement is defined for mixed states and density matrices similarly as for pure states.

A mixed state $[\psi\rangle$ is **separable** or **disentangled** if $[\psi\rangle = \bigoplus_{i=1}^{n}(p_i, |\phi_i\rangle \otimes |\psi_i\rangle)$, where $\sum_{i=1}^{n} p_i = 1$ and $|\phi_i\rangle$, $|\psi_i\rangle$ are pure states. $[\psi\rangle$ is entangled if it is not disentangled.

A density matrix ρ is disentangled if $\rho = \sum_{i=1}^{n} p_i \rho_i \otimes \rho_i'$, $\sum_{i=1}^{n} p_i = 1$ and it is entangled if it is not disentangled.

Several approaches to quantification of entanglement of mixed states and density matrices are dealt with in Section 8.3 where various ways of creation and manipulation of entangled states are dealt with.

Remark 2.2.7 As illustrated in the rest of the book, entanglement can be used in various ways to make quantum communication more efficient and more secure. It is also well known in quantum mechanics that to any entangled state one can find operators whose correlation violate Bell inequalities and contradict "local realism" view of quantum physics (see Section 2.7). An important role in quantum information processing have quantum error-correcting codes whose highly entangled codewords protect quantum information. As discussed and illustrated by DiVincenzo and Peres(1997), entangled codewords appear to lead, under the assumption of local realism, to a reach variety of logical contradictions—"quantum paradoxis".

2.2.3 Substituting entanglement for communication

One of the surprising applications of entanglement was discovered in the area of multiparty communications. For example, as will now be shown, by sharing entangled particles communicating parties can reduce the amount of bits they need to broadcast in order to solve

[23] On the Bell states, that play an important role in the quantum theory of entanglement, one can also illustrate enormous difference between what is possible in quantum theory and practice. Theoretically, a single projection measurement can distinguish four Bell states. However, until now no experimental way to do that in H_4 is known! Only recently (see Kwiat and Weinfurter, 1998), a way has been demonstrated how to distinguish these four states, but only by working in a larger Hilbert space—making use of additional entanglement.

[24] The term "ebit" is also almost a trademark for "Electron-Beam Ion Trap".

together a special communication/cooperation problem—to compute together a function whose input data are distributed among the parties.

There are k parties $P_1, \ldots, P_k$ and a k-variable function f whose inputs are n-bit strings $x_1, \ldots, x_k$. The party P_j holds only the string x_j. All parties want to compute together $f(x_1, \ldots, x_k)$. In order to achieve it, the parties have to communicate. The average number of bits the parties have to broadcast if they work with classical information only, for valid inputs of length n, is called the communication complexity of f and denoted by $C(f, n, k)$. (This definition is a natural modification of the usual concepts in communication complexity.[25]) For the case where the parties can work also with quantum information, the corresponding communication complexity is denoted by $QC(f, n, k)$.

We show, following van Dam, Høyer and Tapp (1997), an example of functions $f_k, k = 1, 2, \ldots$ such that $QC(f_k, n, k)$ is asymptotically smaller, with respect to k, than $C(f_k, n, k)$.

An input $(x_1, \ldots, x_k) \in \{0, \ldots, 2^n - 1\}^k$ is defined to be **valid** if

$$\left(\sum_{i=1}^{k} x_i\right) \bmod 2^{n-1} = 0.$$

Denote by $f_k : \{0, \ldots, 2^n - 1\}^k \to \{0, 1\}$, the Boolean function defined, on valid inputs only, by

$$f_k(x_1, \ldots, x_k) = \left(\frac{1}{2^{n-1}} \sum_{i=1}^{k} x_i\right) \bmod 2.$$

Clearly, $f_k(x_1, \ldots, x_k) \in \{0, 1\}$ for all valid inputs.

At first we show that $QC(f_k, n, k) = k$ provided k communicating parties share k entangled qubits, each party having one. Later we show that $C(f_k, n, k) \geq k \lg k - k$ for $n \geq \lg k$. In this way we find that for functions f_k defined above communication with the help of entanglement is asymptotically better.

Let us assume that k parties share k qubits, the party P_i the qubit q_i and together these qubits are in the entangled state $|q_1 \ldots q_k\rangle = \frac{1}{\sqrt{2}}(|0^{(k)}\rangle + |1^{(k)}\rangle)$. Let each party P_j independently apply on its qubit q_j the following procedure.

1. A phase-changing transformation

$$|0\rangle \to |0\rangle, \quad |1\rangle \to e^{\frac{2\pi i x_j}{2^n}}|1\rangle.$$

2. Hadamard transformation.

3. A measurement of the jth qubit q_j, with respect to the standard observable $\{|0\rangle, |1\rangle\}$ providing an output $b_j \in \{0, 1\}$.

After the first step the resulting state is $\frac{1}{\sqrt{2}}\left(|0^{(k)}\rangle + (e^{\frac{2\pi i}{2^n}\sum_{j=1}^{k} x_j})|1^{(k)}\rangle\right)$. (Observe that for a valid input $e^{\frac{2\pi i}{2^n}\sum_{j=1}^{k} x_j}$ equals 1 or -1.) After the second step the resulting state is

$$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2^k}}\sum_{j=0}^{2^k-1}|j\rangle + e^{\frac{2\pi i}{2^n}\sum_{j=1}^{k} x_j}\frac{1}{\sqrt{2^k}}\sum_{j=0}^{2^k-1}(-1)^{parity(j)}|j\rangle\right),$$

[25] See Hromkovič (1997), Gruska (1997).

where $parity(j) = 0$ if j is even and 1, otherwise. Since $e^{\frac{2\pi i}{2^n}\sum_{j=1}^{k} x_j} = (-1)^{f_k(x_1,\ldots,x_k)}$ we see that the resulting state is

$$\frac{1}{\sqrt{2^{k-1}}} \sum_{parity(j)=f_k(x_1,\ldots,x_n)} |j\rangle.$$

It is now easy to determine that

$$b_1 \oplus b_2 \oplus \ldots \oplus b_k = f_k(x_1, \ldots, x_k),$$

no matter in which order parties perform their measurements.

Exercise 2.2.8 *Determine in detail that* $\oplus_{i=1}^{k} b_i = f_k(x_1, \ldots, x_n)$ *for: (a)* $k = 2, 3$*; (b) for an arbitrary* k*.*

All parties can compute the value of f_k if bits b_i, $i = 1, \ldots, k$ are broadcast. On the other hand, broadcasting of less than k bits cannot be sufficient to compute f_k because if one of the parties does not broadcast its bit, then no other party can compute the value of f_k.

Let us now consider communications between the parties in the case that only classical information is used.

The simplest way to communicate is that all but one of the parties broadcasts their inputs. The last party then computes the result and broadcast it to all other parties. This implies

$$C(f_k, n, k) \leq (k-1)n + 1.$$

Another possibility is that parties $P_1, P_2, \ldots, P_{k-1}$ broadcast the d most significant bits of their inputs, i.e., $y_i = x_i - x_i \bmod 2^{n-d}$ for some $d > 1$. The last party, say P_k, then computes the sum

$$(\sum_{i=1}^{k} x_i) - \delta,$$

where

$$\delta = \sum_{i=1}^{k-1} (x_i \bmod 2^{n-d}).$$

If $n \geq d = 1 + \lceil \lg(k-1) \rceil$, then

$$0 < \delta \leq (k-1)(2^{n-d} - 1) < 2^{n-1}.$$

This implies that P_k knows the value of the sum $\sum_{i=1}^{k} x_i$ up to an additional non-negative term smaller than 2^{n-1}. Since the sum $\sum_{i=1}^{k} x_i$ is divided by 2^{n-1} for valid inputs, P_k can determine the sum $\sum_{i=1}^{k} x_i$ exactly and therefore it can compute f_k.

In this case it holds, for the total number of bits to be broadcast,

$$C(f_k, n, k) \leq (k-1)(\lceil \lg(k-1) \rceil + 1) + 1.$$

□

Exercise 2.2.9 (Cleve and Buhrman, 1997) *Let each of three parties A, B and C possess an n bit string w^A, w^B and w^C, such that $w_i^A \oplus w_i^B \oplus w_i^C = 1$ for $1 \leq i \leq n$. In addition, let each party P possess one of the particles q_i^P, $1 \leq i \leq n$, of n triples of particles each in the entangled state $|\psi\rangle = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle - |111\rangle)$. Show that the three parties can compute the function $f(w^A, w^B, w^C) = \bigoplus_{i=1}^n w_i^A \wedge w_i^B \wedge w_i^C$ in such a way that each party $P \in \{A, B, C\}$ performs the following protocol:*

for i **from** 1 **to** n **do**

  if $w_i^P = 0$ **then** *apply Hadamard rotation to* q_i^P*;*

  get the bit s_i^P *by measuring* q_i^P*;*

compute $s^P \leftarrow \bigoplus_{i=1}^n s_i^P$.

and then let parties B and C send two bits, namely s^B and s^C, to A such that A can compute $s^A + s^B + s^C$ which equals $f(w^A, w^B, w^C)$. (It can be shown that the classical communication complexity of this problem is 3. Using quantum entanglement only two bits for communication are necessary, as demonstrated by the above protocol.)

Remark 2.2.10 In the result presented in this section it has been demonstrated that entanglement has the potential to act as a substitute for communication during multiparty cooperation. On the other hand, the potential of entanglement for direct communication is very restricted. This is discussed in more detail in Section 6.4 on teleportation—an another important application of entanglement.

Open problem 2.2.11 *Can quantum entanglement decrease also two-party communication complexity for some communication problems?*

2.3 Quantum Circuits

In a similar way as Boolean gates and circuits are building blocks of classical computers, quantum analogues of them are natural elements from which quantum computing devices are designed. However, the related theoretical, design and implementation problems for quantum gates and circuits are of significantly larger complexity.

2.3.1 Quantum gates

Unitarity is the main new requirement quantum gates have to satisfy.

Definition 2.3.1 *A* **quantum gate** *with n inputs and n outputs is specified by a unitary operator $U : \mathcal{H}_{2^n} \rightarrow \mathcal{H}_{2^n}$, and it is represented by a unitary matrix of degree 2^n.*

Example 2.3.2 *The so-called Hadamard (rotation) gates are represented by matrices*

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

Example 2.3.3 *The following one parameter set of* **rotation gates** *(represented by matrices) is also often used:*

$$R_x(\theta) = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}, \quad R_y(\theta) = \begin{pmatrix} i\cos\theta & \sin\theta \\ \sin\theta & i\cos\theta \end{pmatrix}, \quad R_z(\theta) = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix},$$

and

As already mentioned, of central importance for quantum computing is the XOR gate (Figure 2.8). Observe that if the target qubit has the input $|0\rangle$, then this gate can be used to copy qubits $|0\rangle$ and $|1\rangle$ from the control qubit. At the same time the gate in Figure 2.8 can be seen as a classical wire. Indeed, inputs $|0\rangle$ and $|1\rangle$ on the control qubit come out on the target qubit output, but a superposition $\alpha|0\rangle + \beta|1\rangle$ on the control qubit is transferred into the entangled state $\alpha|00\rangle + \beta|11\rangle$ and if we consider as the overall output that of the target qubit then this output is a mixed state: $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$, and if $|\alpha| = |\beta|$ then the output is a random $|0\rangle$ or $|1\rangle$.

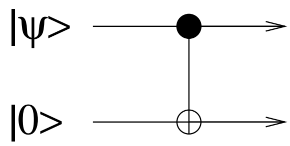


Figure 2.8: XOR gate as a real wire

Just as with classical gates, quantum gates also can be described by "truth tables" showing that the outputs for the case inputs are states $|0\rangle$ and $|1\rangle$. The point is that once such a truth table is given, linearity of quantum gate mappings allows us to determine gate outputs for all possible input states. In this way several often-used gates have been described in Figures 1.14 and 1.15: CNOT or XOR gate as well as Fredkin and Toffoli gates.

Exercise 2.3.4 *Describe unitary matrices for (a) Toffoli gate; (b) Fredkin gate.*

Exercise 2.3.5 *XOR gate can be expressed using outer and tensor products as follows:* $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_x$. *Find a similar representation for: (a) Toffoli gate; (b) Fredkin gate.*

The gates for basic Boolean reversible operations NOT, CNOT and CCNOT can be described also using a notation for registers as follows:

$$\begin{aligned} \text{NOT} &: |a\rangle \to |\bar{a}\rangle \\ \text{XOR} = \text{CNOT} &: |a, b\rangle \to |a, a \oplus b\rangle \\ \text{CCNOT} &: |a, b, c\rangle \to |a, b, (a \wedge b) \oplus c\rangle \end{aligned}$$

Observe that each of these gates is its own inverse.

An important difference between the classical and quantum computing is that for any n the number of n input/output quantum gates is uncountable. This immediately gives rise to several basic questions. Which of the gates are of real importance for quantum computing? Which of them can be well implemented with current or foreseeable technology?

A direct implementation of arbitrarily large/complex quantum gates is outside the possibilities of the current and foreseeable technology. This immediately arises another fundamental question: Can all large unitary matrices be effectively decomposed, in some reasonable sense, into a small (polynomial) number of unitary matrices of very small degree?

This brings us immediately to the concept of quantum circuits as an analogue of Boolean circuits.

Definition 2.3.6 *A* **quantum (Boolean) circuit** *is a collection of quantum gates acyclicly connected (by "quantum wires").*[26] *The* **size** *and the* **depth** *of a circuit refer to the number of nodes and depth of the underlying connection graph.*

A relation between a quantum circuit and the corresponding unitary matrix is far from being very transparent even for simple circuits and some experience is needed to get proper feelings in this respect. That is why there are quite a few (very simple) examples and exercises in this section, worth paying detailed attention to.

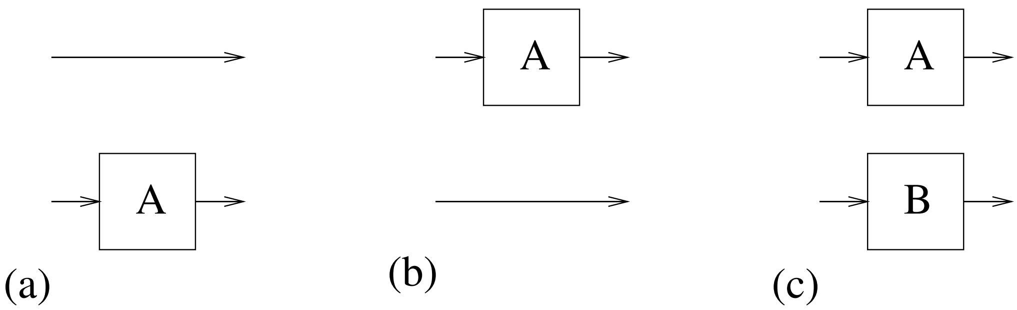


Figure 2.9: Elementary networks I

Exercise 2.3.7 *Let* $a = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ *be unitary matrices of degree* 2. *Design unitary matrices of degree 4 that represent mappings realized by networks: (a) in Figure 2.9a; (b) in Figure 2.9b; (c) in Figure 2.9c.*

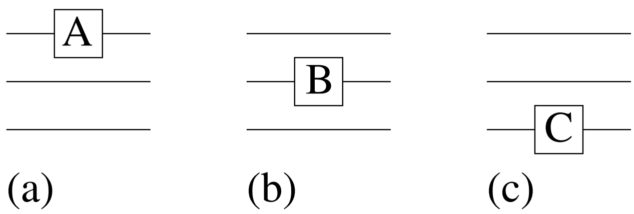


Figure 2.10: Elementary networks II

Exercise 2.3.8 *Let us assume that unitary matrices* A, B, C *of degree* 2 *are given. Design unitary matrices representing networks shown: (a) in Figure 2.10a; (b) in Figure 2.10b; (c) in Figure 2.10c; (d) for a network obtained by serial composition of networks in Figure 2.10a,b; (e) for a network obtained by serial composition of networks from Figure 2.10a,c.*

---

[26] We are using here similar terminology as for classical circuits, in spite of the fact that there are no real wires on the quantum level. Two ports of the gates communicate either by sharing a physical qubit or via field interactions or using other physical means.

When considering a class of quantum circuits $\{C_i\}_{i=1}^{n}$ of a certain type, it is necessary to assume, if we want to assign computations on such circuits to uniform complexity classes, that all such circuits can be designed (computed) by a single classical Turing machine in a polynomial time with respect to n.

If gates G_1 and G_2 realizes the mappings described by unitary matrices A_1 and A_2, then the network in Figure 2.11a realizes the mapping described by the matrix $A_1 \otimes A_2$.

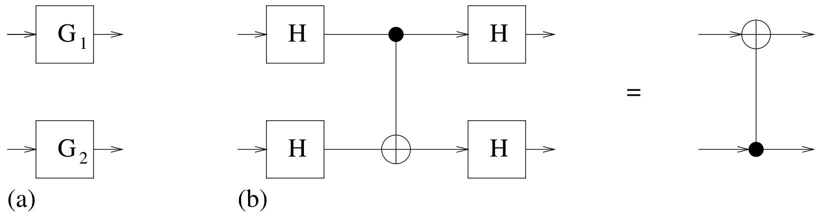


Figure 2.11: An implementation of the inverse of the XOR gate.

The processing in the network on the left side of the identity in Figure 2.11b for the input $|0\rangle|1\rangle$ can be depicted as follows:

$$
\begin{array}{lcl}
|0\rangle|1\rangle & \stackrel{H-\text{gates}}{\longrightarrow} & \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|1\rangle) \\
& \stackrel{\text{XOR gate}}{\longrightarrow} & \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle) \\
& \stackrel{H\ \text{gates}}{\longrightarrow} & |1\rangle|1\rangle.
\end{array}
$$

Exercise 2.3.9 *Prove the equivalence of networks shown in: (a) Figure 2.11b; (b) Figure 2.12.*

Exercise 2.3.10 *Show how to design quantum circuits producing the cat state* $\frac{1}{\sqrt{2}}(|0^{(l)}\rangle + |1^{(l)}\rangle)$ *for: (a)* $l = 2$*; (b)* $l = 3$*; (c) for an arbitrary* l.

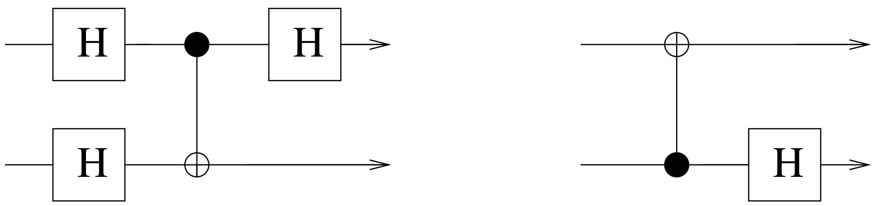


Figure 2.12: Two equivalent circuits

Example 2.3.11 *The XOR gate determined by the matrix XOR is an important example of a 2-qubit gate. If depicted as in Figure 1.14, then a simple circuit of three such gates, shown in Figure 2.13b, flips the qubits.*

Notation used for XOR and Toffoli gates in Figure 1.14 is often generalized to consider cases that target bits should flip if one of the control bits is 0 (represented by the empty circle) and for the cases there are several control and/or target bits or we have a controlled gate.

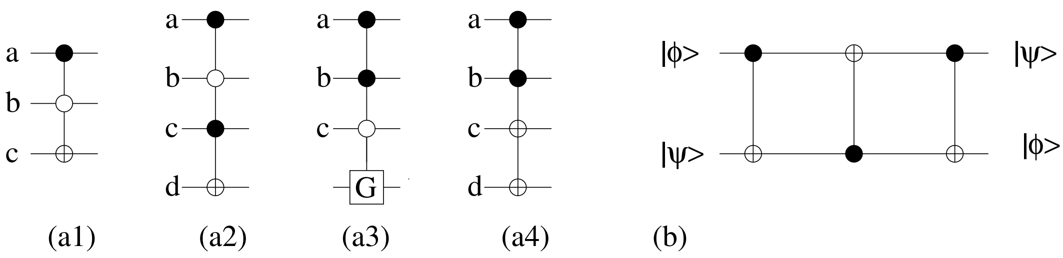


Figure 2.13: Generalized XOR gate notations and a quantum circuit to flip the qubits

For example, the circuit in Figure 2.13a1 realizes the mapping $(a,b,c) \to (a,b,(a\wedge \bar{b})\oplus c)$; the circuit in Figure 2.13a2, the mapping $(a,b,c,d) \to (a,b,c,(a\wedge \bar{b}\wedge c)\oplus d)$. In the circuit in Figure 2.13a3 the gate G is applied if and only if $a\wedge b\wedge \bar{c} = 1$. Finally, in the circuit from Figure 2.13a4 the last two bits flip if and only if $a \wedge b = 1$ (this stands actually for two consecutive XOR gates with the same control bits but different target bits). In addition, notation $\mathrm{XOR}_{i,j}$ will be used to denote the case that an XOR gate is applied to the ith and the jth qubit as the control and the target qubits.

Example 2.3.12 *Circuit in Figure 2.14a produces the Bell states.*

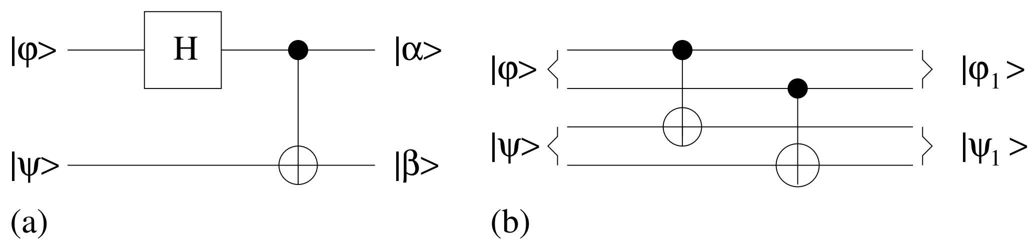


Figure 2.14: A circuit to produce Bell states and a circuit to map pairs of Bell states into pairs of Bell states

Exercise 2.3.13 *Show that the quantum circuit, so-called bilateral quantum XOR (BXOR), shown in Figure 2.14, transforms a pair of Bell states $|\phi\rangle$ and $|\psi\rangle$ into a pair of Bell states $|\phi_1\rangle$, $|\psi_1\rangle$.*

Exercise 2.3.14 *Show that each of the Pauli matrices maps in a one-to-one way states of the Bell basis on themselves if the matrix is applied to one of the two qubits of the given Bell state. (In other words, Bell states can be connected into one another by unilateral Pauli rotations.)*

XOR is an important example of quantum gates with two or more inputs that performs the so-called **conditional quantum dynamics**, in which one system (qubit) undergoes an evolution that depends on the quantum state of another system (of other qubits).

Exercise 2.3.15 *The circuit on Figure 2.15 (see Moore and Nilsson, 1998), performs a permutation of* 3 *qubit states using* 3 *ancilla qubits. Show: that any permutation of* n *qubit states can be performed: (a) using* 4 *layers of XOR gates with* n *ancilla qubits; (b) using* 6 *layers of XOR gates and no ancilla qubits.*

Exercise 2.3.16 *Show that any mapping* $(x_1, \ldots, x_n, b) \to (x_1, \ldots, x_n, b \oplus x_1 \oplus \ldots \oplus x_n)$ *can be performed by a* $\mathcal{O}(\lg n)$*-depth circuit using only XOR gates.*

Exercise 2.3.17 *Design: (a) a circuit to recognize Bell states; (b) a circuit to generate GHZ states; (c) a circuit to recognize GHZ states.*

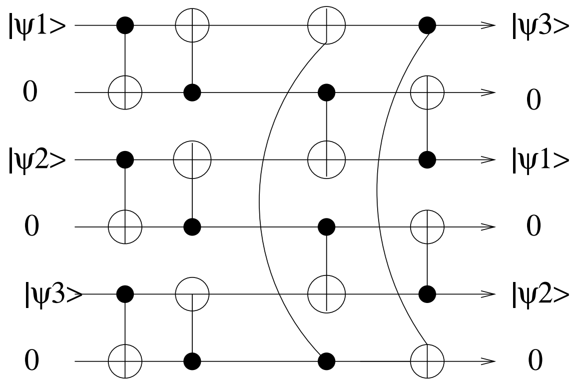


Figure 2.15: Permutation circuit

Example 2.3.18 *The Hadamard transform* H_n *is implemented by the circuit in Figure 2.16a, and Figure 2.16b contains the usual notation for the circuit for* H_n.

Exercise 2.3.19 *Apply the Hadamard transform* H_n *on the following states where* $x, y \in \{0,1\}^n$*: (a)* $\frac{1}{\sqrt{2}}(|x\rangle + |y\rangle)$*; (b)* $\frac{1}{\sqrt{2}}(|x\rangle - |y\rangle)$.

Exercise 2.3.20 *Design a quantum circuit transforming the state* $\alpha|0\rangle + \beta|1\rangle$ *into the state: (a)* $-\beta|0\rangle + \alpha|1\rangle$*; (b)* $\beta|0\rangle - \alpha|1\rangle$*; (c)* $\alpha|0\rangle - \beta|1\rangle$*; (d)* $-\alpha|0\rangle + \beta|1\rangle$.

XOR gate is also an example of so-called **measurements gates**. It is called so because if the value of the control input is 0, then the control qubit is in effect an apparatus to perform an accurate measurement of the target qubit.

Exercise 2.3.21 *Show that the operation* $AND : (x, y) \to (x, y, x \wedge y)$ *can be implemented: (a) up to a phase by a quantum circuit consisting of four Hadamard gates and three XOR gates; (b) by a quantum circuit consisting of six XOR gates and eight one-bit gates.*

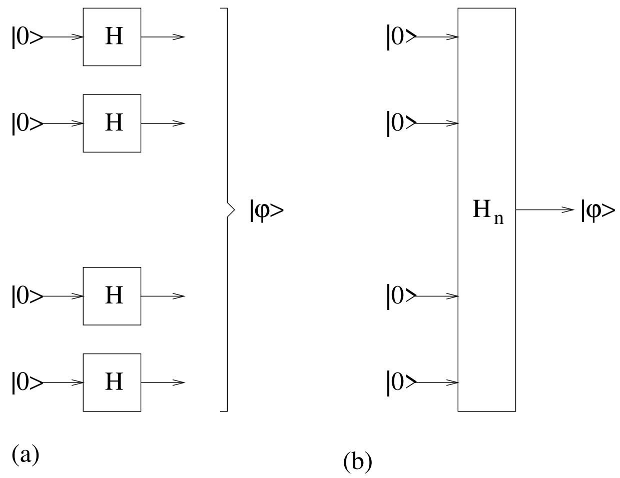


Figure 2.16: The Hadamard circuit H_n and its application to the state $|0^{(n)}\rangle$ with the outcome $|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$.

Exercise 2.3.22 *(Barenco et al. 1997) Design a quantum circuit to realize the unitary transformation* $U_k : |0^{(k)}\rangle \to \frac{1}{\sqrt{k}}(|0^{(k)}\rangle + \sum_{i=1}^{k-1} |2^i\rangle)$. *(Hint: use gates corresponding to the following unitary matrices:* $A_k = \frac{1}{\sqrt{k+1}} \begin{pmatrix} 1 & -\sqrt{k} \\ \sqrt{k} & 1 \end{pmatrix}$ *and*

$$T_{j,k} = \frac{1}{\sqrt{k-j+1}} \begin{pmatrix} \sqrt{k-j+1} & 0 & 0 & 0 \\ 0 & 1 & \sqrt{k-j} & 0 \\ 0 & -\sqrt{k-j} & 1 & 0 \\ 0 & 0 & 0 & \sqrt{k-j+1} \end{pmatrix}$$

for $1 \leq j < k$.*)*

The computational meaning of quantum circuits is defined as follows. For any quantum circuit C with input variables $x_1, \ldots, x_n$ and output variables $y_1, \ldots, y_m$, $m \leq n$ (they are to be a subset of outputs), we associate to any input $x \in \{0,1\}^n$ the probability distribution ρ_x over $\{0,1\}^m$ defined in the following way (see Yao, 1993).

For any input x the final quantum state v, corresponding to all output wires, not only to those carrying output variables, has the form

$$v = \sum_{y \in \{0,1\}^m} \alpha_y |y\rangle,$$

where α_y is the amplitude obtained by the projection of v when the output variables are set to the value y, i.e. α_y is the sum of amplitudes of these final outcomes having value y in the wires corresponding to output variables. Then $\pi_x(y) = |\alpha_y|^2$ is the corresponding probability and $\{\pi_x \,|\, x \in \{0,1\}^n\}$ is said to be the distribution generated by the circuit C.

One of the main results of classical computation theory says that each TM can be simulated in polynomial time by a uniform family of Boolean circuits. A similar result holds also for quantum Turing machines and quantum circuits, and due to this result one uses nowadays more quantum circuits than QTM to develop quantum algorithms. To present the corresponding result we need at first to introduce the concept of simulation of QTM by quantum circuit.

Definition 2.3.23 *A quantum circuit C with n input variables is said to (n,t)-simulate a QTM M, if for each $x \in \{0,1\}^n$ the probability distribution ρ_x generated by C is identical to the distribution of the configurations of M after t steps with x as input.*

Yao (1993) has shown the following result.

Theorem 2.3.24 *If M is a QTM and $n,t \in \mathbf{N}^{\geq 0}$, then there exists a quantum Boolean circuit C of size (number of gates) polynomial in n and t that (n,t)-simulates M.*

A **quantum program** is a quantum circuit together with some measurement (observation) gates/processes attached to some of the wires. There is a certain controversy about whether measurements can appear inside and not only at the end of quantum circuits. Arguments in favour are based on the observation that there are no physical reasons for not doing that. Arguments against are based on the point of view that measurement mostly changes a pure state into a mixed one.

Remark 2.3.25 Quantum gates are far from easy to implement. It seems safe to say that the potential computational power of quantum computers does not come from the intrinsic speed of quantum gates, but from the fact that quantum circuits to solve some problems can have exponentially less gates than their classical counterparts.

The task of designing efficient quantum algorithms can be seen as unitary matrix factorization problem: given a universal set $\mathcal{U}$ of basic unitary matrices, and an $n \times n$ unitary matrix U, how to decompose U into a product of $poly(\lg n)$ matrices from $\mathcal{U}$. Quantum programming—quantum algorithms and networks design and analysis—requires therefore quite a different expertise (see, for example Høyer, 1997). Development of efficient factorization methods and proper sets of basic unitary matrices is still task to deal with. In the next chapter we deal with quantum algorithm design problems in a more traditional spirit—as an art of composition of unitary transformation to perform the final unitary transformation.

2.3.2 Measurement gates

Measurement gates are not only to magnify results of quantum evolution to provide its outcomes to the classical world. They can be used also to influence, in an essential way, the whole process of quantum computation. Actually, some of the key results of the next chapter, fast quantum algorithms, are based on doing clever measurements in proper times.

Example 2.3.26 *Consider the two quantum circuits depicted in Figure 2.17. The first one consists at first of two Hadamard gates H_n and ends with the measurement gate, with respect to the standard observable. The second circuit has in addition a measurement gate also in between two Hadamard gates.*

There is an essential difference between these two circuits, and the inclusion of the measurement gate also between two Hadamard gates makes the second circuit more interesting.

Indeed, since $H_n^2 = 1$, the result of the measurement gate of the circuit in Figure 2.17a is $|0^n\rangle$ with probability 1. On the other hand, in the second circuit, the first measurement

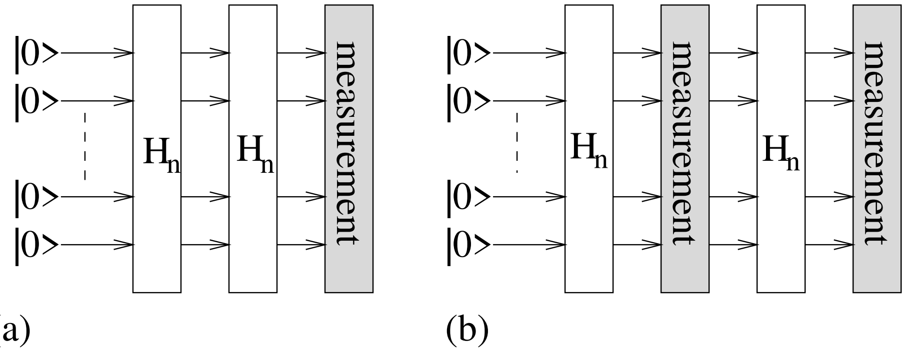


Figure 2.17: Measurement gates and their role

gate will observe a random n-bit string x with probability $\frac{1}{2^n}$. The output of the second gate is then $H_n|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{y\cdot x}|y\rangle$. The second measurement gate therefore observes any n-bit string with probability $\frac{1}{2^n}$.

Generation of a random string, as provided by the gates in Figure 2.17b, is often needed in quantum computation. It is therefore natural to ask whether the inclusion of an intermediate measurement is the only (easy) way of doing that or whether there is a simple way to avoid such intermediate measurements. As we shall see, there is—the so-called copying technique, using XOR gates. This will be illustrated in the following simple example using only H gates but the technique can be used in general. This techniques will play an important role in Sections 7.4 and 7.5.

Example 2.3.27 *As discussed in the previous example, the network in Figure 2.18a can be seen as generating a random bit. However, the same can do networks in Figure 2.18b,c.*

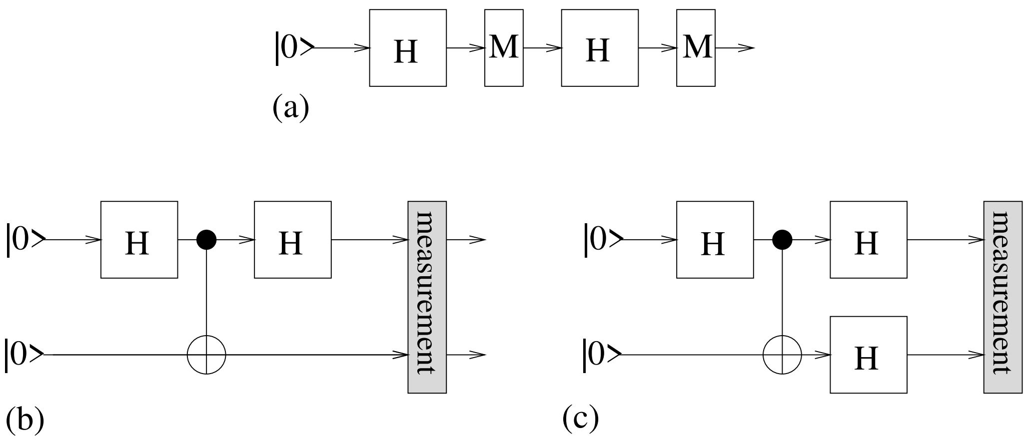


Figure 2.18: Power of copying circuits

In the circuit in Figure 2.18b, after the XOR gate the state is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and the first bit is random. After the next application of the Hadamard gate on the first bit we get

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

and the first bit is perfectly random.

In the circuit in Figure 2.18c, after the XOR gate we find the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. After the application of Hadamard gates on both bits we get

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

and the first bit is again perfectly random.

2.3.3 Universality of quantum gates

Since quantum operations can be seen as continuous, the concept of universality for a set of quantum gates is naturally a bit more complex than in the classical case. As a consequence, the maximum we can hope for is that any unitary transformation can be approximated by a transformation realized by a circuit consisting of gates from a fixed set of gates. The concept of an ε-approximation of a unitary matrix U by another matrix M is therefore of importance. Approximations of unitary transformations are defined as follows:

Definition 2.3.28 *A matrix M is ε-close to a unitary matrix U, or it is an ε-approximation U, if $||U - M|| \leq \varepsilon$.*

It is easy to see that if a matrix M is ε-close to a unitary matrix, then $1-\varepsilon \leq ||M|| \leq 1+\varepsilon$ and its rows, M_i, have the norm close to 1 and, in addition, they are almost orthogonal.

Exercise 2.3.29 *(Bernstein and Vazirani, 1997.) Show that if a matrix M of degree d is ε-close to a unitary matrix, then the following holds for its rows M_i: (a) $1 - \varepsilon \leq ||M_i|| \leq 1 + \varepsilon$; (b) if $i \neq j$, then $||M_i M_j^*|| \leq 2\varepsilon + 3\varepsilon^2$.*

Definition 2.3.30 *A set of quantum gates is* **universal** *if any unitary transformation U on any qubit register can be performed, with arbitrary precision $\varepsilon > 0$, by a quantum circuit $C_{U,\varepsilon}$, consisting of the gates from that set. (In other words, the unitary matrix defined by $C_{U,\varepsilon}$ is ε-close to U.) A quantum gate is* **universal** *if by itself it forms a universal set when supported by constant inputs $|0\rangle$ and $|1\rangle$*[27].

[27] One also says that a set of gates is universal if the subgroup of unitary transformations generated by the unitary transformations corresponding to the gates in the set is dense in the group of all unitary transformations $U(n)$, for any n.

Exercise 2.3.31 *Let ϕ_0 be an irrational fraction of π. (a) Show that any gate*

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

can be implemented with an arbitrary precision using (several copies of) a single gate U_{ϕ_0}; (b) show that the number of gates required to achieve ε accuracy of approximation is $\mathcal{O}(\frac{1}{\varepsilon})$.

The first result concerning the universality of quantum gates was due to Deutsch (1989), who has shown that any 3-qubit gate with the unitary matrix

$$D(\theta) = \begin{pmatrix} \mathbf{1} & & \mathbf{0} & \\ & \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix} & & \\ \mathbf{0} & \begin{matrix} 0 & 0 & i\cos\theta & \sin\theta \\ 0 & 0 & \sin\theta & i\cos\theta \end{matrix} & & \end{pmatrix},$$

where $\mathbf{0}$ and $\mathbf{1}$ are zero and unit matrices of degree 4, depicted in short in Figure 2.19a, with $D = R_y(\theta)$ (see page 81), is universal provided θ/π is irrational. Observe that the Deutsch gate can be seen as a quantum generalization of the Toffoli gate.

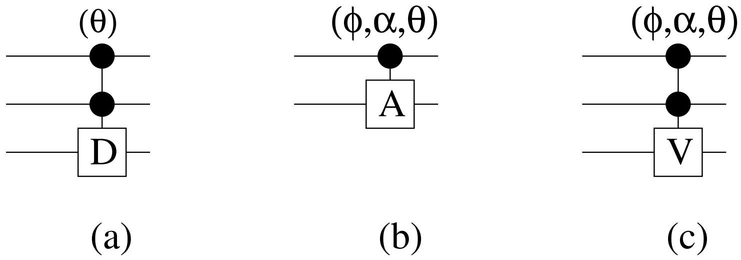


Figure 2.19: Short notation for gates $D(\theta)$, $A(\phi,\alpha,\theta)$ and $V(\phi,\alpha,\theta)$

The following example presents the first step which led to a universal 2-qubit gate.

Example 2.3.32 (Sleator and Weinfurter, 1995) *Consider the gates realizing the operators specified by the matrices:*

$$S(\tau) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{\frac{i\pi}{4}}\cos\frac{\pi\tau}{2} & e^{\frac{-i\pi}{4}}\sin\frac{\pi\tau}{2} \\ 0 & 0 & e^{\frac{-i\pi}{4}}\sin\frac{\pi\tau}{2} & e^{\frac{i\pi}{4}}\cos\frac{\pi\tau}{2} \end{pmatrix}, S^{-1}(\tau) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{\frac{-i\pi}{4}}\cos\frac{\pi\tau}{2} & e^{\frac{i\pi}{4}}\sin\frac{\pi\tau}{2} \\ 0 & 0 & e^{\frac{i\pi}{4}}\sin\frac{\pi\tau}{2} & e^{\frac{-i\pi}{4}}\cos\frac{\pi\tau}{2} \end{pmatrix}$$

Both gates perform transformations of the target bit conditional to the case that the control bit is 1. Clearly $S(\tau)S^{-1}(\tau) = I$. In addition, it holds

$$S^2(\frac{\tau}{2}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i\cos\pi\frac{\tau}{2} & \sin\pi\frac{\tau}{2} \\ 0 & 0 & \sin\pi\frac{\tau}{2} & i\cos\pi\frac{\tau}{2} \end{pmatrix},$$

and therefore $S^2(\frac{1}{2}) = XOR$.[28] *Since* $a \wedge b = \frac{1}{2}(a + b - a \oplus b)$, *it is easy to verify that the circuit in Figure 2.20a is an implementation of a generalization of the Toffoli gate provided that the schemes in 2.20b denote the gates for the matrices* $S(\frac{\tau}{2})$ *and* $S^{-1}(\frac{\tau}{2})$. *The gate* $S(\tau)$ *has been constructed by Sleator and Weinfurter as a universal gate provided* τ *is an irrational multiple of* π.

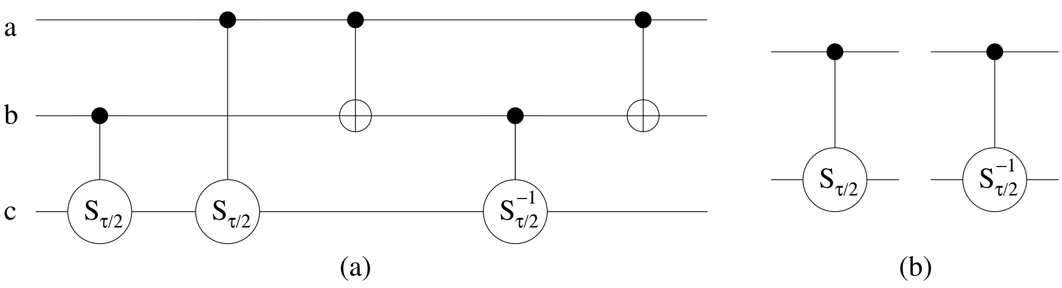


Figure 2.20: A circuit for the Toffoli gate

We show now a modified result, adopted from Barenco (1995), namely that any 2-input/output gate with the matrix

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

and with the short notation for the gate in Figure 2.19b, is universal if α, ϕ and θ are irrational multiples of π and of each other.

The proof is by providing an explicit construction of the circuit implementing the gate $D(\theta)$ via a 3-qubit gate specified by the matrix

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

with the short notation for the gate in Figure 2.19c.

Let us first observe that for any integer n

$$A^n(\phi,\alpha,\theta) = A(\phi, n\alpha \bmod 2\pi, n\theta \bmod 2\pi).$$

Since α and θ are irrational in the above sense, any transformation $A(\phi,\alpha_1,\theta_1)$, with $\alpha_1,\theta_1 \in [0,2\pi]$, can be implemented with arbitrary precision using several gates A.

Exercise 2.3.33 *Show that if* α_1 *and* θ_1 *are specified with accuracy* $\pm\varepsilon$, *then* $\mathcal{O}(\frac{1}{\varepsilon^2})$ *applications of the gate* A *are needed to approximate* $A(\phi,\alpha_1,\theta_1)$ *with a given precision* ε.

[28] $S(\frac{1}{2})$ is therefore called "a square root of XOR".

Let us call "repertoire of A" the set of unitary transformations that can be approximated with an arbitrary precision by networks composed of A-gates only. In this repertoire there is clearly the inverse of the transformation A because

$$A^{-1}(\phi,\alpha,\theta) = A(\phi, 2\pi-\alpha, 2\pi-\theta).$$

Let A_{ij}, $1 \leq i \neq j \leq 3$, denote the two-qubit gate obtained from A by having the ith qubit to be its control qubit and the jth qubit to be its target qubit. All such gates are clearly in the repertoire of A. It is now easy to verify that the network from Figure 2.21, described by the matrix

$$A_{23}(\phi,\frac{\alpha}{2},\frac{\theta}{2})A_{13}(\phi,\frac{\alpha}{2},\frac{\theta}{2})A_{12}(\phi,\frac{\pi}{2},\frac{\pi}{2})A_{23}^{-1}(\phi,\frac{\alpha}{2},\frac{\theta}{2})A_{12}(\phi,\frac{\pi}{2},\frac{\pi}{2})$$

implements the gate $V(\phi,\alpha,\theta)$—see Example 2.3.32.

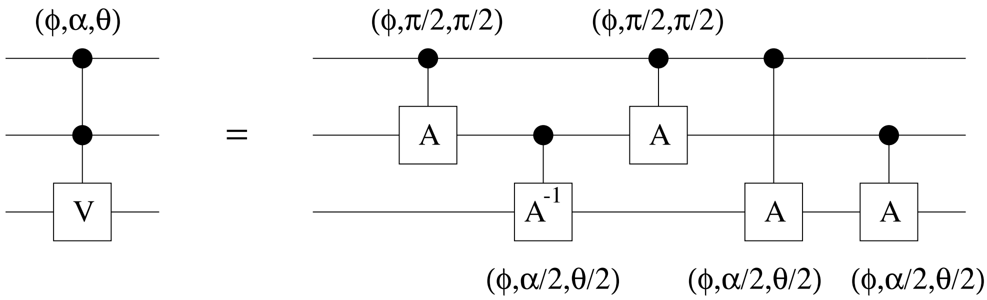


Figure 2.21: An implementation of the gate V -80%

Denote now by V' the gate obtained from V by exchanging the second and the third qubit, and let us denote by P the matrix (gate) $V'(\phi,\pi/2,\pi/2)$. In such a case

$$P = V'(\phi,\pi/2,\pi/2) = \left(\begin{array}{cc} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{-i\phi} \\ 0 & 0 & 1 & 0 \\ 0 & e^{i\phi} & 0 & 0 \end{array} \end{array}\right).$$

In addition, let us denote

$$Q = V'(\phi,\frac{\pi}{2},-\frac{\pi}{2})V(\phi,\frac{\pi}{2},-\frac{\pi}{2})V'(\phi,\frac{\pi}{2},-\frac{\pi}{2}) = \left(\begin{array}{cc} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array} \end{array}\right)$$

and

$$T(\phi,\beta) = Q[V(\phi,0,\beta)P]^2[V(\phi,0,-\beta)P]^2Q.$$

For very small β, we get

$$T(\phi,\beta) = \mathbf{1} + i\beta^2 \left(\begin{array}{cc} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & ie^{-i\phi} \\ 0 & 0 & -ie^{i\phi} & 0 \end{array} \end{array}\right) + \mathcal{O}(\beta^3),$$

where $\mathcal{O}(\beta^3)$ denotes a matrix the norm of which is $\mathcal{O}(\beta^3)$. Hence the transformation

$$V(\phi - \frac{\pi}{2}, 0, \beta) = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\beta & e^{-i\phi}\sin\beta \\ 0 & 0 & e^{i\phi}\sin\beta & \cos\beta \end{matrix} \end{pmatrix} = \lim_{n\to\infty} T(\phi, \sqrt{\beta/n})^n$$

can also be performed with an arbitrary precision by networks with the gate A as the only gate, and the same is therefore true for the transformation (gate).

$$\begin{aligned} R_z(\beta) &= \lim_{n\to\infty}[V\left(\phi, 0, \sqrt{\frac{\beta}{2n}}\right) V\left(\phi - \frac{\pi}{2}, 0, \sqrt{\frac{\beta}{2n}}\right) V\left(\phi, 0, -\sqrt{\frac{\beta}{2n}}\right) V\left(\phi - \frac{\pi}{2}, 0, -\sqrt{\frac{\beta}{2}n}\right)]^n \\ &= \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\beta} & 0 \\ 0 & 0 & 0 & e^{-i\beta} \end{matrix} \end{pmatrix}. \end{aligned}$$

The universal Deutsch gate can now be constructed as follows:

$$D(\phi) = R_z(\frac{\phi}{2})V(\phi, \frac{\pi}{2}, \phi)R_z(-\frac{\phi}{2}).$$

An additional significant step in the search for universal two qubit gates has been made by Deutsch, Barenco and Ekert (1995) and Lloyd (1995). They have shown that almost any nontrivial two-qubit gate is universal.

Exercise 2.3.34 *(Barenco, 1996) Show that: (a) there is no one-qubit universal gate; (b) no classical gate can be universal for quantum computing; (c) gate $A(\frac{\pi}{2}, \frac{\pi}{4}, \theta)$ is universal under certain conditions.*

Open problem 2.3.35 *Determine the set of all non-universal quantum gates.*

The task of finding 2-qubit universal gates is of theoretical and also practical importance. However, this is not the only way to go in searching for simple gates that can be used to design a quantum circuit.

As already mentioned, XOR gate is not universal for quantum computing. In spite of that it has its firm role in the search for universality in quantum computing.

Barenco et al. (1995) have shown that the XOR gate, when supplemented by a set of the following one-qubit gates (that perform general rotation of single qubits), is sufficient to implement any unitary transformation

$$\begin{pmatrix} e^{i(\delta+\frac{\alpha}{2}+\frac{\beta}{2})}\cos\frac{\theta}{2} & e^{i(\delta+\frac{\alpha}{2}-\frac{\beta}{2})}\sin\frac{\theta}{2} \\ -e^{i(\delta-\frac{\alpha}{2}+\frac{\beta}{2})}\sin\frac{\theta}{2} & e^{i(\delta-\frac{\alpha}{2}-\frac{\beta}{2})}\cos\frac{\theta}{2} \end{pmatrix}$$

On the base of the above results we see that while one- and two-bit operations are **classical computation primitives**, one- and two-qubit unitary operations are **quantum computation primitives**.

XOR gate has also been shown to be an important component of various decompositions of 3-qubit gates into 2-input/output gates. All these results make the XOR gate of central importance for quantum computation.

In addition, it can be shown that XOR gate and a single one-qubit gate form a universal set of gates (see Section 5.1).

Remark 2.3.36 Current quantum computing algorithms use qubits and quantum registers as the basic building blocks. This implies that current quantum mechanics systems used for quantum computing are composed of two-state quantum systems. Theoretically, we could use as basic quantum systems three or more states quantum systems. This would be a generalization of old attempts to use 3-valued or multi-valued logic for classical computing. In the classical case it has not been demonstrated that such a generalization brings some essential advantages. The quantum case has not yet been investigated and the situation may be quite different. Of interest is also the non-trivial question of universal quantum gates for 3-valued logic.

Remark 2.3.37 Presentation of quantum computations as an evolution of quantum states as presented usually in quantum computing, including this book, can be seen as corresponding to the Schrödinger view of quantum mechanics, see Section 9.1.1. An alternative approach, more corresponding to Heisenberger's matrix view of quantum mechanics, seeing a quantum computation as an evolution of operators in time, has been illustrated by Gottesman (1998) as useful in understanding an important class of quantum operators.

2.3.4 Arithmetical circuits

An efficient realization of networks for basic arithmetical and modular arithmetical operations (see Vedral, Barenco and Ekert, 1996), is of large importance for efficient implementation of various quantum algorithms, for example of those discussed in Section 3.2.

The two very basic problems are the design of networks for addition $(a, b) \to (a, a + b)$ and for modular addition $(a, b) \to (a, (a+b) \bmod N)$ of n-bit numbers a and b with $N = 2^n$.

Using an easy-to-design carry-gate (Figure 2.22a) and the summation gate (Figure 2.22b), the design of the adder is a straightforward application of the idea from Figure 1.17.

In the first phase all carry bits are computed using n carry gates. In the second phase at first $a_{n-1} \oplus b_{n-1}$ is transferred to b_{n-1}, using one XOR gate, and then, using $n-1$ reverse carry gates and n summation gates, all $(a+b)_i$ bits are computed and all carry bits are reset to 0 (to remove all garbage), for $i = n-2, \ldots, 0$.

Exercise 2.3.38 *(a) Design the carry gate from Figure 2.22a, using one XOR and one Toffoli gate; (b) design the summation gate from Figure 2.22b, using two XOR gates.*

Figure 2.23a shows a schematic notation for a binary adder. By reversing the order in which gates of an adder are applied we get a network, schematically shown in Figure 2.23b, to compute an ordinary subtraction $(a, b) \to (a, b - a)$ when $b \geq a$, and a "modulo 2^n subtraction" $(a, b) \to (a, 2^n + (b - a))$ if $a > b$. In the last case the most significant bit of the second register contains always 1. This will be essentially used in the next construction of the modular adder.

A modular adder for $(a+b) \bmod N$ is shown in Figure 2.24. The basic idea is very simple. Adder A1 provides the outputs $(a, a + b)$ and the subtractor S1 produces $a + b - N$ for the

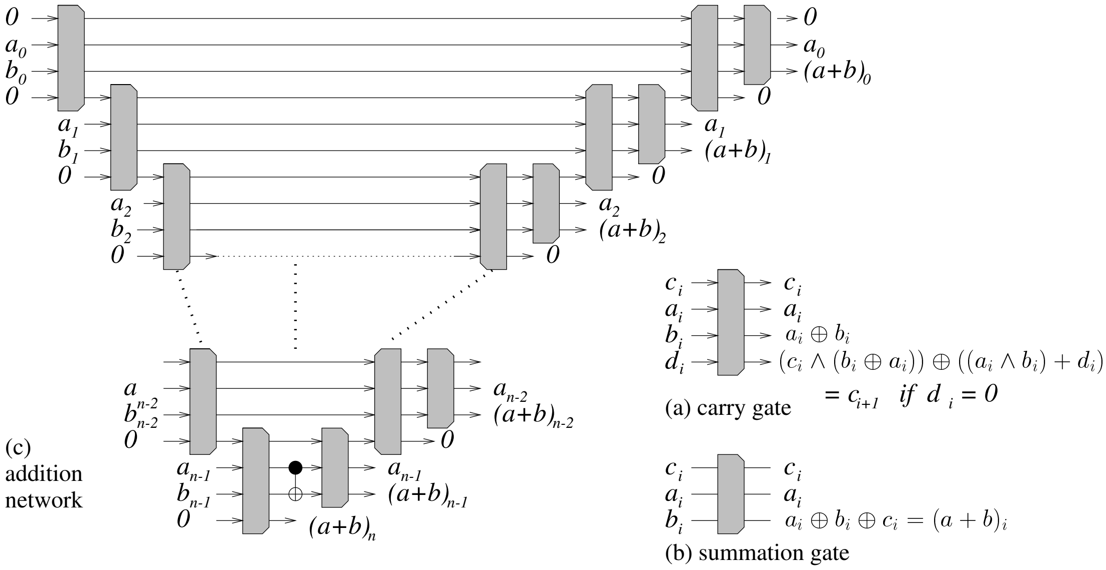


Figure 2.22: Quantum network for binary addition

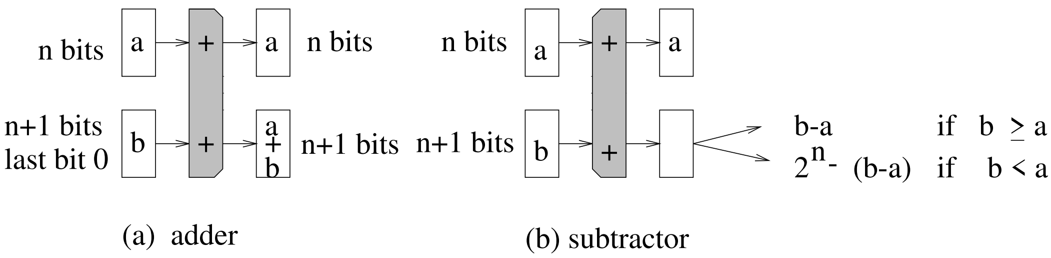


Figure 2.23: Gates for adders and subtractors

case $a+b \geq N$, which is exactly $(a+b) \bmod N$. However, in the case $a+b<N$ there is an overflow after S1 and the rest of the network is needed to handle this case. Overflow is first copied into the additional bit t set initially to 0, using the first XOR gate. Conditionally on that the gate G1 produces either N or 0. The second output of the adder A2 is therefore $(a+b) \bmod N$. The gate G2 resets the first register to N, if this is needed. The subtractor S2 then produces outputs $(a, (a+b) \bmod N - a)$. The second register has then the overflow exactly when S1 had and this is then used, with the help of the second XOR gate, to reset t to the value 0. The last adder is just to produce the output $(a, (a+b) \bmod N)$.

There are several natural ways to build networks for (modular) multiplication, and (modular) exponentiation on the base of networks for addition and modular addition. In the case of $f_{a,N}(b) = a \cdot b \bmod N$ we can use the decomposition of $f_{a,N}$:

$$\underbrace{(b+\ldots+b)}_{(a-1)-\text{plus operations}} \mod N \quad \text{or} \quad (\ldots\underbrace{((b+b) \bmod N) + b) \bmod N) + \ldots + b) \bmod N)}_{(a-1)-\text{plus operations}}$$

or as

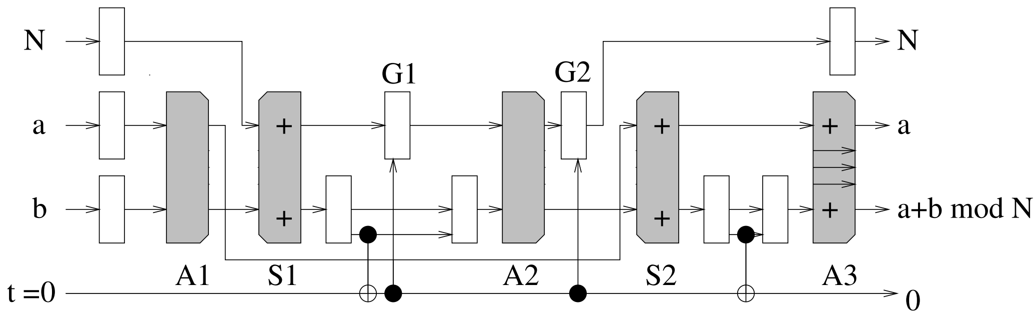


Figure 2.24: A quantum network for modular addition-75%

$$ab = (\sum_{i=0}^{n-1} a2^i b_i) \bmod N,$$

where $b = \sum_{i=0}^{n-1} b_i 2^i$, i.e. as $(n-1)$-additions, where in the ith addition $a2^i$ is added if and only if $b_i = 1$.

Exercise 2.3.39 *(a) Design a quantum network for modular multiplication; (b) design a quantum network for modular exponentiation.*

Similarly, $g_{a,N}(b) = a^b \bmod N$ can be computed using the decomposition

$$a^b = \prod_{i=0}^{n-1} (a^{2^i})^{b_i}.$$

Concerning the efficiency of networks for (modular) arithmetical operations two quantitative measures are of importance: the total number of elementary gates and the total number of qubits needed. The problem has received special attention because in Shor's algorithm efficiency of exponentiation $a^x \bmod n$ is of key importance for the overall efficiency. By Vedral, Barenco and Ekert (1996), $4n+3$ qubits are sufficient for exponentiation in Shor's factorization algorithm, where n is the number of qubits needed to store N, $2n$ is the number of qubits needed to store x (because x can be there as large as N^2), and $n+3$ temporary qubits are sufficient.

2.3.5 Quantum superoperator circuits

In spite of the fact that the model of quantum circuits from page 82 is fundamental for processing pure quantum states of an isolated quantum system, circuits processing density matrices with superoperators defined below (see Aharonov et al. 1998), are also of importance. They better correspond to computations in noisy environments.

Definition 2.3.40 *A superoperator gate G of type (k, l) is a completely positive map which maps density matrices on k qubits to density matrices on l qubits. Its action on a density matrix ρ will be denoted symbolically by $G \circ \rho$.*

Two important special cases of superoperator gates are unitary and measurement gates. In the case of a unitary gate U the corresponding operator is $U \cdot U^*$. For a pure state $|\phi\rangle$, U maps $\rho = |\phi\rangle\langle\phi|$ into $U \circ \rho = U\rho U^*$. A measurement gate represents a probabilistic projection into a set of mutually orthogonal subspaces, which produces a mixed state. Superoperators are in general not reversible.

There is a well-known and well-understood relation between superoperators and unitary operators.

Lemma 2.3.41 *The following conditions are equivalent for any two Hilbert spaces H_n and H_m and sets of linear operators $\mathcal{L}(H_n)$ and $\mathcal{L}(H_m)$.*

1. *A superoperator $T : \mathcal{L}(H_n) \to \mathcal{L}(H_m)$ is trace-preserving and completely positive.*
2. *There is a Hilbert space F with $\dim(F) \leq \dim(H_n)\dim(H_m)$, and a unitary embedding $E : H_n \to H_n \otimes F$ such that $T\rho = Tr_F(E\rho E^*)$ for all $\rho \in \mathcal{L}(H_n)$.*

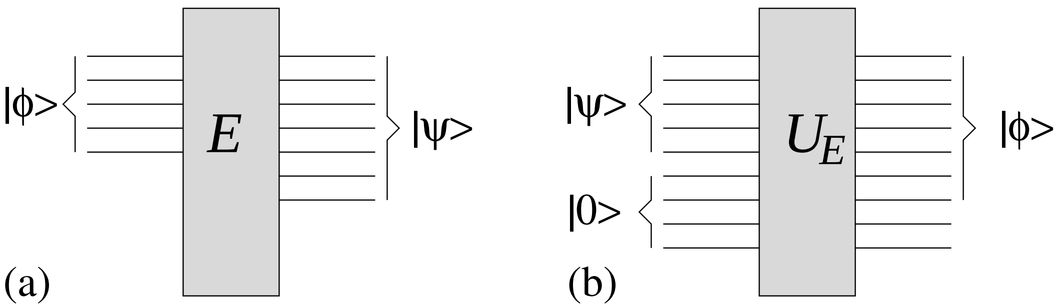


Figure 2.25: Encoder as superoperator and its unitary embedding

Example 2.3.42 *Superoperators of special interest for quantum information processing are encoders and decoders. An encoder E that maps n-qubits to m-qubits, $m \geq n$ (see Figure 2.25a), can be seen in a larger quantum space, extended by $k \geq m - n$ qubits in the initial state $0^{(k)}$, the so called* **ancilla** *qubits, as a unitary operator U_E, Figure 2.25b, some of the outputs of which are then discarded.*

Actually, any operation on quantum data can be represented as a superoperator, equivalent to a unitary interaction with ancilla qubits, followed by discarding some qubits (see Figure 2.25b).

Superoperators of any Hilbert space H can be naturally extended to superoperators operating on a composed Hilbert space $H \otimes H'$ by taking tensor product with the unit matrix of H'. This way any $T : \mathcal{L}(H) \to \mathcal{L}(H')$ can be extended to $T \otimes I : \mathcal{L}(H \otimes H') \to \mathcal{L}(H' \otimes H')$. This fact will be used below when the computation on superoperator circuits is defined.

Definition 2.3.43 *A quantum superoperator circuit over a set of superoperators $\mathcal{G}$ is a directed acyclic graph to whose nodes are assigned superoperators from $\mathcal{G}$ in such a way that if a node has indegree (outdegree) k (l), then the corresponding superoperator is of the type (k,l). A subset of inputs is labeled "blank" and a subset of outputs is labeled "results".*

Each superoperator circuit produces, for a given input density matrix, an output density matrix which is defined in the natural way as follows. If Q is a quantum superoperator circuit and $G_1, \ldots, G_t$ is a topological sort of its gates, then Q computes the density matrix

$$Q \circ \rho = G_t \circ G_{t-1} \circ \ldots \circ G_1 \circ \rho.$$

In order to show that this definition is consistent one has to show that the two different topological orderings of gates yield the same result. A step in this direction is to show that if G_1 and G_2 are superoperator gates operating on different qubits, then $G_1 \circ G_2 \circ \rho = G_2 \circ G_1 \circ \rho$, for any density matrix ρ. This can be shown easily if we consider an extension of superoperators by tensoring with unitary matrices as discussed above. The probability distribution that such a circuit computes is defined in the following way:

Definition 2.3.44 *Let Q be a quantum circuit with n inputs (blanks) and m outputs (results). The probability distribution $f_Q : \{0,1\}^n \rightarrow [0,1]^{\{0,1\}^m}$ that Q computes is defined as follows: For an input i the probability of the output j is*

$$f_Q(i)(j) = \langle j|(Q \circ |i\rangle\langle j|)_A|j\rangle,$$

where A is the set of "outputs".

As a quite straightforward corollary of Lemma 2.3.41 we have the main result concerning the computational power of superoperator gates.

Lemma 2.3.45 *If $G : \mathcal{L}(H_{2^n}) \rightarrow \mathcal{L}(H_{2^n})$ is a superoperator gate of type (n,m), then there exists a unitary quantum gate U_g on $2n+m$ qubits such that for any density matrix of the order n,*

$$G \circ \rho = (U_g \circ (\rho \otimes |0^{(n+m)}\rangle\langle 0^{(n+m)}|))|_A,$$

where A is the set of the first n qubits.

Proof. Let $G : \mathcal{L}(H_{2^n}) \rightarrow \mathcal{L}(H_{2^m})$. By Lemma 2.3.41, G has a representation of the form $G = Tr_{H_{2^{n+m}}}(V \cdot V^*)$, where $V : H_{2^n} \rightarrow H_{2^m} \otimes H_{2^{n+m}}$ is a unitary embedding. Let $\{|\phi_{ij}\rangle \,|\, 0 \leq i < 2^n, 0 \leq j < 2^{n+m}\}$ be an orthonormal basis on $H_{2^n} \otimes H_{2^{n+m}}$ such that $|\phi_{i,0^{n+m}}\rangle = V|i\rangle$, for any i and other basis vectors are arbitrary. Clearly, there is a unitary operator $U : |i,j\rangle \rightarrow |\phi_{ij}\rangle$ such that $V = UV_0$, where $V_0 : |x\rangle \rightarrow |x\rangle \otimes |0^{n+m}\rangle$. This implies

$$G = Tr_{H_{2^{n+m}}}(UV_0 \cdot V_0^* U^*).$$

As a corollary we get

Theorem 2.3.46 *The model of quantum circuits with mixed states is polynomially equivalent, in computational power, to the standard model of quantum circuits over pure states.*