1 From the Foundations of Quantum Theory to Quantum Technology – an Introduction

Gernot Alber

Nowadays, the new technological prospects of processing quantum information in quantum cryptography [1], quantum computation [2] and quantum communication [3] attract not only physicists but also researchers from other scientific communities, mainly computer scientists, discrete mathematicians and electrical engineers. Current developments demonstrate that characteristic quantum phenomena which appear to be surprising from the point of view of classical physics may enable one to perform tasks of practical interest better than by any other known method. In quantum cryptography, the no-cloning property of quantum states [4] or the phenomenon of entanglement [5] helps in the exchange of secret keys between various parties, thus ensuring the security of one-time-pad cryptosystems [6]. Quantum parallelism [7], which relies on quantum interference and which typically also involves entanglement [8], may be exploited for accelerating computations. Quantum algorithms are even capable of factorizing numbers more efficiently than any known classical method is [9], thus challenging the security of public-key cryptosystems such as the RSA system [6]. Classical information and quantum information based on entangled quantum systems can be used for quantum communication purposes such as teleporting quantum states [10, 11].

Owing to significant experimental advances, methods for processing quantum information have developed rapidly during the last few years.[1] Basic quantum communication schemes have been realized with photons [10, 11], and basic quantum logical operations have been demonstrated with trapped ions [13, 14] and with nuclear spins of organic molecules [15]. Also, cavity quantum electrodynamical setups [16], atom chips [17], ultracold atoms in optical lattices [18, 19], ions in an array of microtraps [20] and solid-state devices [21, 22, 23] are promising physical systems for future developments in this research area. All these technologically oriented, current developments rely on fundamental quantum phenomena, such as quantum interference, the measurement process and entanglement. These phenomena and their distinctive differences from basic concepts of classical physics have always been of central interest in research on the foundations of quantum theory. However, in emphasizing their technological potential, the advances in quantum infor-

[1] Numerous recent experimental and theoretical achievements are discussed in [12].

G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, A. Zeilinger: Quantum Information, STMP 173, 1–13 (2001)

mation processing reflect a profound change in the general attitude towards these fundamental phenomena. Thus, after almost two decades of impressive scientific achievements, it is time to retrace some of those significant early developments in quantum physics which are at the heart of quantum technology and which have shaped its present-day appearance.

1.1 Early Developments

Many of the current methods and developments in the processing of quantum information have grown out of a long struggle of physicists with the foundations of modern quantum theory. The famous considerations by Einstein, Podolsky and Rosen (EPR) [24] on reality, locality and completeness of physical theories are an early example in this respect. The critical questions raised by these authors inspired many researchers to study quantitatively the essential difference between quantum physics and the classical concepts of reality and locality. The breakthrough was the discovery by J.S. Bell [25] that the statistical correlations of entangled quantum states are incompatible with the predictions of any theory which is based on the concepts of reality and locality of EPR. The constraints imposed on statistical correlations within the framework of a local, realistic theory (LRT) are expressed by Bell's inequality [25]. As the concept of entanglement and its peculiar correlation properties have been of fundamental significance for the development of quantum information processing, it is worth recalling some of its most elementary features in more detail.

1.1.1 Entanglement and Local, Realistic Theories

In order to clarify the characteristic differences between quantum mechanical correlations originating from entangled states and classical correlations originating from local, realistic theories, let us consider the following basic experimental setup (Fig. 1.1). A quantum mechanical two-particle system,

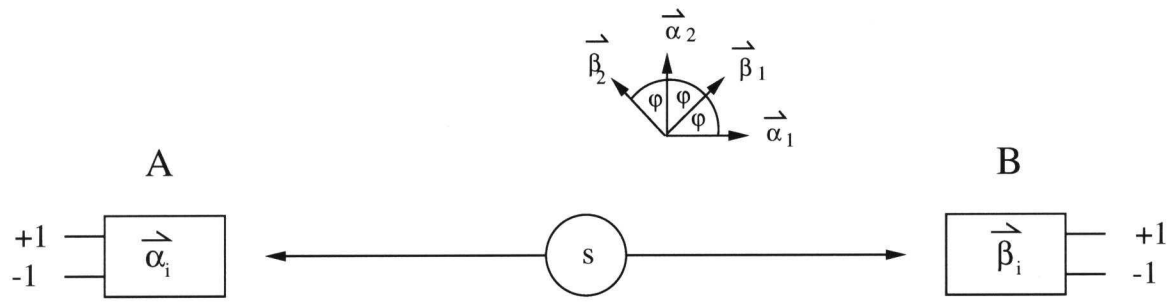

Fig. 1.1. Basic experimental setup for testing Bell's inequality; the choices of the directions of polarization on the Bloch sphere for optimal violation of the CHSH inequality (1.3) correspond to $\varphi = \pi/4$ for spin-1/2 systems

such as a photon pair, is produced by a source s. Polarization properties of each of these particles are measured subsequently by two distant observers A and B. Observers A and B perform polarization measurements by randomly selecting one of the directions $\boldsymbol{\alpha}_1$ or $\boldsymbol{\alpha}_2$, and $\boldsymbol{\beta}_1$ or $\boldsymbol{\beta}_2$, respectively, in each experiment. Furthermore, let us assume that for each of these directions only two measurement results are possible, namely $+1$ or -1. In the case of photons these measurement results would correspond to horizontal or vertical polarization.

What are the restrictions imposed on correlations of the measurement results if the physical process can be described by an underlying LRT with unknown (hidden) parameters? For this purpose, let us first of all summarize the minimal set of conditions any LRT should fulfill.

1. The state of the two-particle system is determined uniquely by a parameter λ, which may denote an arbitrary set of discrete or continuous labels. Thus the most general observable of observer A or B for the experimental setup depicted in Fig. 1.1 is a function of the variables $(\boldsymbol{\alpha}_i, \boldsymbol{\beta}_j, \lambda)$. If the actual value of the parameter λ is unknown (hidden), the state of the two-particle system has to be described by a normalized probability distribution $P(\lambda)$, i.e. $\int_\Lambda \mathrm{d}\lambda\, P(\lambda) = 1$, where Λ characterizes the set of all possible states. The state variable λ determines all results of all possible measurements, irrespective of whether these measurements are performed or not. It represents the element of physical reality inherent in the arguments of EPR: "If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity" [24].
2. The measurement results of each of the distant (space-like separated) observers are independent of the choice of polarizations of the other observer. This assumption reflects the locality concept inherent in the arguments of EPR: "The real factual situation of the system A is independent of what is done with the system B, which is spatially separated from the former" [24]. Thus, taking into account also this locality requirement, the most general observable of observer A for the experimental setup depicted in Fig. 1.1 can depend on the variables $\boldsymbol{\alpha}_i$ and λ (for B, $\boldsymbol{\beta}_j$ and λ) only.

These two assumptions, which reflect fundamental notions of classical physics as used in the arguments of EPR, restrict significantly the possible correlations of measurements performed by both distant observers. According to these assumptions, the following measurement results are possible: $a(\boldsymbol{\alpha}_i, \lambda) \equiv a_i = \pm 1$ $(i = 1, 2)$ for observer A, and $b(\boldsymbol{\beta}_i, \lambda) \equiv b_i = \pm 1$ $(i = 1, 2)$ for observer B. For a given value of the state variable λ, all these possible measurement results of the dichotomic (two-valued) variables a_i and b_i $(i = 1, 2)$ can be combined in the single relation

$$|(a_1 + a_2)b_1 + (a_2 - a_1)b_2| = 2\,. \tag{1.1}$$

It should be mentioned that this relation is counterfactual [26] in the sense that it involves both results of actually performed measurements and possible results of unperformed measurements. All these measurement results are determined uniquely by the state variable λ. If this state variable is unknown (hidden), (1.1) has to be averaged over the corresponding probability distribution $P(\lambda)$. This yields an inequality for the statistical mean values,

$$\langle a_i b_j \rangle_{\mathrm{LRT}} = \int_{\Lambda} \mathrm{d}\,\lambda\; P(\lambda) a(\boldsymbol{\alpha}_i, \lambda) b(\boldsymbol{\beta}_j, \lambda) \qquad (i,j=1,2), \tag{1.2}$$

which is a variant of Bell's inequality and which is due to Clauser, Horne, Shimony and Holt (CHSH) [27], namely

$$|\, \langle a_1 b_1 \rangle_{\mathrm{LRT}} + \langle a_2 b_1 \rangle_{\mathrm{LRT}} + \langle a_2 b_2 \rangle_{\mathrm{LRT}} - \langle a_1 b_2 \rangle_{\mathrm{LRT}} \,| \leq 2\,. \tag{1.3}$$

This inequality characterizes the restrictions imposed on the correlations between dichotomic variables of two distant observers within the framework of any LRT. There are other, equivalent forms of Bell's inequality, one of which was proposed by Wigner [28] and will be discussed in Chap. 3.

Quantum mechanical correlations can violate this inequality. For this purpose let us consider, for example, the spin-entangled singlet state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|+1\rangle_{\mathrm{A}}|-1\rangle_{\mathrm{B}} - |-1\rangle_{\mathrm{A}}|+1\rangle_{\mathrm{B}})\,, \tag{1.4}$$

where $|\pm 1\rangle_{\mathrm{A}}$ and $|\pm 1\rangle_{\mathrm{B}}$ denote the eigenstates of the Pauli spin operators σ_z^{A} and σ_z^{B}, with eigenvalues ± 1. Quantum mechanically, the measurement of the dichotomic polarization variables a_i and b_i is represented by the spin operators $\hat{a}_i = \boldsymbol{\alpha}_i \cdot \boldsymbol{\sigma}^{\mathrm{A}}$ and $\hat{b}_i = \boldsymbol{\beta}_i \cdot \boldsymbol{\sigma}^{\mathrm{B}}$. ($\boldsymbol{\sigma}^{\mathrm{A}}$, for example, denotes the vector of Pauli spin operators referring to observer A, i.e. $\boldsymbol{\sigma}^{\mathrm{A}} = \sum_{i=x,y,z} \sigma_i^{\mathrm{A}} \mathbf{e}_i$, where $\mathbf{e}_i$ are the unit vectors.) The corresponding quantum mechanical correlations entering the CHSH inequality (1.3) are given by

$$\langle \hat{a}_i \hat{b}_j \rangle_{\mathrm{QM}} = \langle \psi | \hat{a}_i \hat{b}_j | \psi \rangle = -\boldsymbol{\alpha}_i \cdot \boldsymbol{\beta}_j\,. \tag{1.5}$$

Choosing the directions of the polarizations $(\boldsymbol{\alpha}_1, \boldsymbol{\beta}_1)$, $(\boldsymbol{\beta}_1, \boldsymbol{\alpha}_2)$, $(\boldsymbol{\alpha}_2, \boldsymbol{\beta}_2)$ on the Bloch sphere so that they involve an angle of $\pi/4$ (see Fig. 109), one finds a maximal violation of inequality (1.3), namely

$$|\, \langle \hat{a}_1 \hat{b}_1 \rangle_{\mathrm{QM}} + \langle \hat{a}_2 \hat{b}_1 \rangle_{\mathrm{QM}} + \langle \hat{a}_2 \hat{b}_2 \rangle_{\mathrm{QM}} - \langle \hat{a}_1 \hat{b}_2 \rangle_{\mathrm{QM}} \,| = 2\sqrt{2} > 2\,. \tag{1.6}$$

Thus, for this entangled state, the quantum mechanical correlations between the measurement results of the distant observers A and B are stronger than any possible correlation within the framework of an LRT. Obviously, these correlations are incompatible with the classical notions of reality and locality of any LRT. It is these peculiar quantum correlations originating from entanglement which have been of central interest in research on the foundations of quantum theory and which are also of central interest for quantum information processing.

So far, numerous experiments testing and supporting violations of Bell's inequality [29, 30, 31] have been performed.[2] However, from a strictly logical point of view, the results of all these experiments could still be explained by an LRT, owing to two loopholes, namely the locality and the detection loopholes. The locality loophole concerns violations of the crucial locality assumption underlying the derivation of Bell's inequality. According to this assumption one has to ensure that any signaling between two distant observers A and B is impossible. The recently performed experiment of G. Weihs et al. [31] succeeded in fulfilling this locality requirement by choosing the separation between these observers to be sufficiently large. However, so far all experiments have involved low detection efficiencies, so that in principle the observed correlations which violate Bell's inequality can still be explained by an LRT [32, 33]. This latter detection loophole constitutes a major experimental challenge, and it is one of the current experimental aims to close both the detection loophole and the locality loophole simultaneously [34, 35, 36].

The concepts of physical reality and locality which lead to inequality (1.3) can also lead to logical contradictions with quantum theory which are not of statistical origin. This becomes particularly apparent when one considers an entangled three-particle state of the form

$$|\psi\rangle_{\mathrm{GHZ}} = \frac{1}{\sqrt{2}}(|+1\rangle_{\mathrm{A}}|+1\rangle_{\mathrm{B}}|+1\rangle_{\mathrm{C}} - |-1\rangle_{\mathrm{A}}|-1\rangle_{\mathrm{B}}|-1\rangle_{\mathrm{C}}) \,, \tag{1.7}$$

a so-called Greenberger–Horne–Zeilinger (GHZ) state [37]. Again $|\pm 1\rangle_{\mathrm{A}}$, $|\pm 1\rangle_{\mathrm{B}}$, and $|\pm 1\rangle_{\mathrm{C}}$ denote the eigenstates of the Pauli spin operators σ_z^{A}, σ_z^{B}, and σ_z^{C}, with eigenvalues ± 1. Similarly to Fig. 109, let us assume that the polarization properties of this entangled quantum state are investigated by three distant (space-like separated) observers A, B and C. Each of these observers chooses his or her direction of polarization randomly along either the x or the y axis.

What are the consequences an LRT would predict? As the three observers are space-like separated, the locality assumption implies that a polarization measurement by one of these observers cannot influence the results of the other observers. Following the notation of Fig. 109, the possible results of the polarization measurements of observers A, B and C along directions $\boldsymbol{\alpha}_i$, $\boldsymbol{\beta}_j$ and $\boldsymbol{\gamma}_k$ are $a_i = \pm 1$, $b_j = \pm 1$ and $c_k = \pm 1$. Let us now consider four possible coincidence measurements of these three distant observers, with results (a_x, b_x, c_x), (a_x, b_y, c_y), (a_y, b_x, c_y) and (a_y, b_y, c_x). As we are dealing with dichotomic variables, within an LRT the product of all these measurement results is always given by

$$R_{\mathrm{LRT}} = (a_x b_x c_x)(a_x b_y c_y)(a_y b_x c_y)(a_y b_y c_x) = a_x^2 b_x^2 c_x^2 a_y^2 b_y^2 c_y^2 = 1 \,. \tag{1.8}$$

What are the corresponding predictions of quantum theory? In quantum theory the variables a_i, b_j and c_k are replaced by the Pauli spin operators

[2] For a comprehensive discussion of experiments performed before 1989, see [29].

$\hat{a}_i = \boldsymbol{\alpha}_i \cdot \boldsymbol{\sigma}^{\mathrm{A}}$, $\hat{b}_j = \boldsymbol{\beta}_j \cdot \boldsymbol{\sigma}^{\mathrm{B}}$ and $\hat{c}_k = \boldsymbol{\gamma}_k \cdot \boldsymbol{\sigma}^{\mathrm{C}}$. The GHZ state of (1.7) fulfills the relations

$$\hat{a}_x \hat{b}_x \hat{c}_x |\psi\rangle_{\mathrm{GHZ}} = -|\psi\rangle_{\mathrm{GHZ}} ,$$

$$\hat{a}_x \hat{b}_y \hat{c}_y |\psi\rangle_{\mathrm{GHZ}} = \hat{a}_y \hat{b}_x \hat{c}_y |\psi\rangle_{\mathrm{GHZ}} = \hat{a}_y \hat{b}_y \hat{c}_x |\psi\rangle_{\mathrm{GHZ}} = |\psi\rangle_{\mathrm{GHZ}} . \tag{1.9}$$

Therefore the quantum mechanical result for the product of (1.8) is given by

$$\begin{aligned} R_{\mathrm{QM}} |\psi\rangle_{\mathrm{GHZ}} &= (\hat{a}_x \hat{b}_x \hat{c}_x)(\hat{a}_x \hat{b}_y \hat{c}_y)(\hat{a}_y \hat{b}_x \hat{c}_y)(\hat{a}_y \hat{b}_y \hat{c}_x) |\psi\rangle_{\mathrm{GHZ}} \\ &= (-1) |\psi\rangle_{\mathrm{GHZ}} \end{aligned} \tag{1.10}$$

and contradicts the corresponding result of an LRT. These peculiar quantum mechanical predictions have recently been observed experimentally [38]. The entanglement inherent in these states offers interesting perspectives on the possibility of distributing quantum information between three parties [39].

1.1.2 Characteristic Quantum Effects for Practical Purposes

According to a suggestion of Feynman [40], quantum systems are not only of interest for their own sake but might also serve specific practical purposes. Simple quantum systems may be used, for example, for simulating other, more complicated quantum systems. This early suggestion of Feynman emphasizes possible practical applications and thus indicates already a change in the attitude towards characteristic quantum phenomena.

In the same spirit, but independently, Wiesner suggested in the 1960s the use of nonorthogonal quantum states for the practical purpose of encoding secret classical information [41].[3] The security of such an encoding procedure is based on a characteristic quantum phenomenon which does not involve entanglement, namely the impossibility of copying (or cloning) nonorthogonal quantum states [4]. This impossibility becomes apparent from the following elementary consideration. Let us imagine a quantum process which is capable of copying two nonorthogonal quantum states, say $|0\rangle$ and $|1\rangle$, with $0 < |\langle 0|1\rangle| < 1$. This process is assumed to perform the transformation

$$|0\rangle|\varphi\rangle|a\rangle \rightarrow |0\rangle|0\rangle|a_0\rangle ,$$

$$|1\rangle|\varphi\rangle|a\rangle \rightarrow |1\rangle|1\rangle|a_1\rangle , \tag{1.11}$$

where $|\varphi\rangle$ represents the initial quantum state of the (empty) copy and $|a\rangle$, $|a_0\rangle$, $|a_1\rangle$ denote normalized quantum states of an ancilla system. This ancilla system describes the internal states of the copying device. As this copying process has to be unitary, it has to conserve the scalar product between the two input and the two output states. This implies the relation $\langle 0|1\rangle(1 - \langle 0|1\rangle\langle a_0|a_1\rangle) = 0$. This equality can be fulfilled only if either states

[3] Though this article was written in the 1960s, it was not published until 1983.

$|0\rangle$ and $|1\rangle$ are orthogonal, i.e. $\langle 0|1\rangle = 0$, or if $\langle 0|1\rangle = 1 = \langle a_0|a_1\rangle$. Both possibilities contradict the original assumption of nonorthogonal, nonidentical initial states. Therefore a quantum process capable of copying nonorthogonal quantum states is impossible. This is an early example of an impossible quantum process.

Soon afterwards, Bennett and Brassard [42] proposed the first quantum protocol (BB84) for secure transmission of a random, secret key using nonorthogonal states of polarized photons for the encoding (see Table 1.1). In the Vernam cipher, such a secret key is used for encoding and decoding messages safely [6, 43]. In this latter encoding procedure the message and the secret key are added bit by bit, and in the decoding procedure they are subtracted again. If the random key is secret, the safety of this protocol is guaranteed provided the key is used only once, has the same length as the message and is truly random [44]. Nonorthogonal quantum states can help in transmitting such a random, secret key safely. For this purpose A(lice) sends photons to B(ob) which are polarized randomly either horizontally (+1) or vertically (−1) along two directions of polarization. It is convenient to choose the magnitude of the angle between these two directions of polarization to be $\pi/8$. B(ob) also chooses his polarizers randomly to be polarized along these directions. After A(lice) has sent all photons to B(ob), both communicate to each other their choices of directions of polarization over a public channel. However, the sent or measured polarizations of the photons are kept secret. Whenever they chose the same direction (yes), their measured polarizations are correlated perfectly and they keep the corresponding measured results for their secret key. The other measurement results (no) cannot be used for the key. Provided the transmission channel is ideal, A(lice) and B(ob) can use part of the key for detecting a possible eavesdropper because in this case some of the measurements are not correlated perfectly. In practice, however, the transmission channel is not perfect and A(lice) and B(ob) have to process their raw key further to extract from it a secret key [45]. It took some more

Table 1.1. Part of a possible idealized protocol for transmitting a secret key, according to [42]

A(lice)'s direction i	1	2	1	1	2	1	2	2	1	2	$\cdots$
A(lice)'s polarization	+1	−1	−1	+1	+ 1	+1	−1	−1	−1	+1	$\cdots$
B(ob)'s direction i	2	1	1	2	2	1	2	1	1	2	$\cdots$
B(ob)'s measured polarization	+1	−1	−1	−1	+1	+1	−1	+1	−1	+1	$\cdots$
Public test of common direction	No	No	Yes	No	Yes	Yes	Yes	No	Yes	Yes	$\cdots$
Secret key			−1		+1	+1	−1		−1	+1	$\cdots$

years to realize that an exchange of secret keys can be achieved with the help of entangled quantum states [46]. Thereby, the characteristic quantum correlations of entangled states and the very fact that they are incompat-

ible with any LRT can be used for ensuring security of the key exchange. After the first proof-of-principle experiments [47, 48], the first practical implementation of quantum cryptography over a distance of about 1 km was realized at the University of Geneva using single, polarized photons transmitted through an optical fiber [49]. These developments launched the whole new field of quantum cryptography. Now, this field represents the most developed part of quantum information processing. Quantum cryptography based on the BB84 protocol has already been realized over a distance of 23 km [50]. Recent experiments [30, 31] have demonstrated that photon pairs can also be entangled over large distances, so that entanglement-based quantum cryptography over such large distances might become accessible soon. Some of these experiments are discussed in Chap. 3.

Simultaneously with these developments in quantum cryptography, numerous other physical processes were discovered which were either enabled by entanglement or in which entanglement led to an improvement of performance. The most prominent examples are dense coding [51], entanglement-assisted teleportation [10, 11, 52] and entanglement swapping [52, 53]. (These processes are discussed in detail in Chaps. 2 and 3.) In the spirit of Feynman's suggestion, all these developments demonstrate that characteristic quantum phenomena have practical applications in quantum information processing.

1.1.3 Quantum Algorithms

Feynman's suggestion also indicates interesting links between quantum physics and computer science. After the demonstration [54] that quantum systems can simulate reversible Turing machines [55], the first quantum generalization of Turing machines was developed [7]. (Turing machines are general models of computing devices and will be discussed in detail in Chap. 4.) Furthermore, it was pointed out that one of the remarkable properties of such a quantum Turing machine is quantum parallelism, by which certain tasks may be performed faster than by any classical computing device. Deutsch's algorithm [7, 56] was the first quantum algorithm demonstrating how the interplay between quantum interference, entanglement and the quantum mechanical measurement process could serve this practical purpose.

The computational problem solved by Deutsch's algorithm is the following. We are given a device, a so-called oracle, which computes a Boolean function f mapping all possible binary n-bit strings onto one single bit. Therefore, given a binary n-bit string x as input, this oracle can compute $f(x) \in \{0, 1\}$ in a single step. Furthermore, let us assume that this function is either constant or balanced. Thus, in the first case the 2^n possible input values of x are all mapped onto 0 or all onto 1. In the second case half of the input values are mapped onto either 0 or 1 and the remaining half are mapped onto the other value. The problem is to develop an algorithm which determines whether f is constant or balanced.

Let us first of all discuss briefly the classical complexity of this problem. In order to answer the question in the worst possible case, the oracle has to be queried more than 2^{n-1} times. It can happen, for example, that the first 2^{n-1} queries all give the same result, so that at least one more query of the oracle is required to decide whether f is constant or balanced. Thus, classically, it is apparent that the number of steps required grows exponentially with the number of bits.

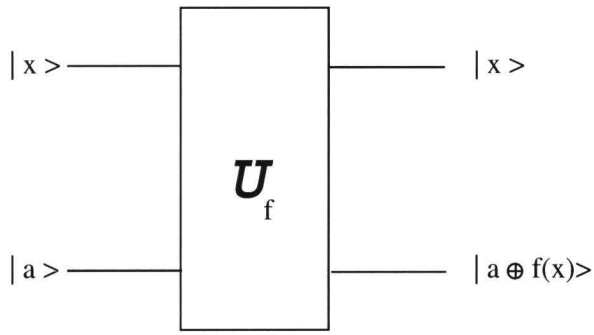

Fig. 1.2. Basic operation of a quantum oracle $\mathcal{U}_f$ which evaluates a Boolean function $f : x \in \mathbf{Z}_2^n \rightarrow f(x) \in \mathbf{Z}_2^1 \equiv \{0, 1\}$; $|x\rangle$ is the input state of an n-qubit quantum system; $|a\rangle$ is a one-qubit state and $\oplus$ denotes addition modulo 2

Quantum mechanically, the situation is different. The 2^n possible binary n-bit strings x can be represented by quantum states $|x\rangle$, which form a basis in a 2^n-dimensional Hilbert space $\mathcal{H}_{2^n}$, which is the state space of n qubits. Furthermore, we imagine that the classical oracle is replaced by a corresponding quantum oracle (Fig. 1.2). This is a unitary transformation $\mathcal{U}_f$ which maps basis states of the form $|x\rangle|a\rangle$, where $a \in \{0, 1\}$, to output states of the form $|x\rangle|a \oplus f(x)\rangle$ in a single step. Here, $|a\rangle$ denotes the quantum state of an ancilla qubit and $\oplus$ denotes addition modulo 2. If the initial state is $|x\rangle|0\rangle$, for example, the quantum oracle performs an evaluation of $f(x)$, resulting in the final state $|x\rangle|f(x)\rangle$. However, as this transformation is unitary, it can perform this task also for any linear combination of possible basis states in a single step. This is the key idea of quantum parallelism [7]. Deutsch's quantum algorithm obtains the solution to the problem posed above by the following steps (Fig. 1.3):

1. The n-qubit quantum system and the ancilla system are prepared in states $|0\rangle$ and $(|0\rangle - |1\rangle)/\sqrt{2}$. Then a Hadamard transformation

$$H : \; |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \,,$$
$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.12}$$

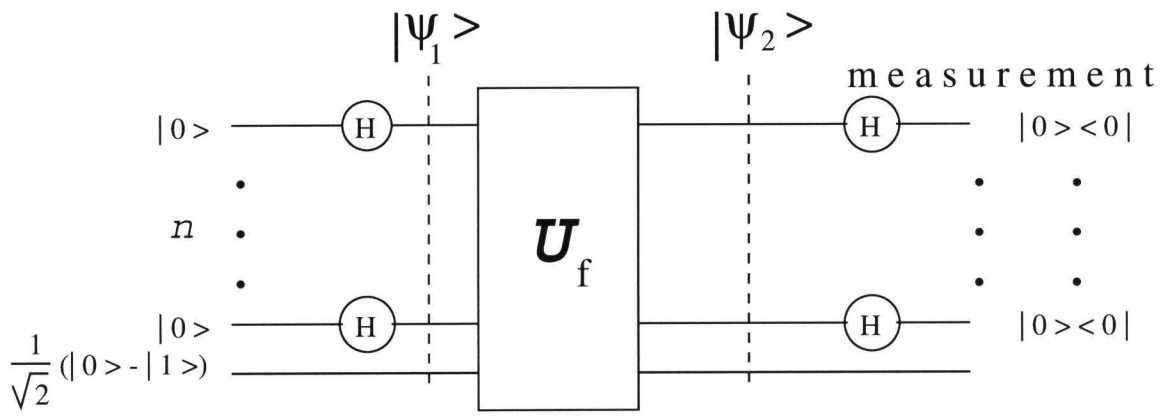

Fig. 1.3. Schematic representation of Deutsch's quantum algorithm

is applied to all of the first n qubits. We denote by $H^{(i)}$ the application of H to the ith qubit. Thus, the separable quantum state

$$|\psi_1\rangle \equiv \frac{1}{\sqrt{2}}[(\prod_{i=1}^{n} \otimes H^{(i)})|0\rangle](|0\rangle - |1\rangle) = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in 2^n} |x\rangle(|0\rangle - |1\rangle) \quad (1.13)$$

is prepared.

2. A single application of the quantum oracle $\mathcal{U}_f$ to state $|\psi_1\rangle$ yields the quantum state

$$|\psi_2\rangle \equiv \mathcal{U}_f|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in 2^n} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \, . \quad (1.14)$$

3. Subsequently a quantum measurement is performed to determine whether the system is in state $|\psi_1\rangle$ or not. With the help of n Hadamard transformations (as in step 1), this quantum measurement can be reduced to a measurement of whether the first n qubits of the quantum system are in state $|0\rangle$ or not.

If in step 3 the quantum system is found in state $|\psi_1\rangle$, f is constant, otherwise f is balanced. One of these two possibilities is observed with unit probability. The probability p of observing the quantum system in state $|\psi_1\rangle$ is given by

$$p \equiv |\, \langle\psi_1|\psi_2\rangle \,|^2 = \frac{1}{2^n} \, |\sum_{x \in 2^n} (-1)^{f(x)} \,|^2 \, . \quad (1.15)$$

Taking into account the single application of the quantum oracle in step 2 and the application of the Hadamard transformations in the preparation and measurement processes, Deutsch's quantum algorithm requires $O(n)$ steps to obtain the final answer, in contrast to any classical algorithm, which needs an exponential number of steps. Thus Deutsch's quantum algorithm leads to an exponential speedup.

A key element of this quantum algorithm and of those discovered later is the quantum parallelism involved in step 2, where the linear superposition

of the first n qubits comprises the requested global information about the function f. For most of the possible functions f this intermediate quantum state is expected to be entangled. An exception is the case of a constant function f, for which the quantum state $|\psi_2\rangle$ is separable. Furthermore, it is also crucial for the success of this quantum algorithm that the final measurement in step 3 yielding the required answer can be implemented by a fast quantum measurement whose complexity is polynomial in n. This is a requirement fulfilled by all other known fast quantum algorithms. The quantum algorithm described above was the first example demonstrating that quantum phenomena may speed up computations in such a way that an exponential gap appears between the complexity class of the quantum problem and the complexity class of the corresponding classical probabilistic problem.

Continuing this development initiated by Deutsch, other, new fast quantum algorithms were discovered in the subsequent years. The most prominent examples are Simon's quantum algorithm [57], Shor's celebrated algorithm [9] for factorizing numbers, and Grover's search algorithm [58]. (Quantum algorithms are discussed in detail in Chap. 4.) In addition, possible realizations of quantum computing devices were suggested which were based on trapped ions [59] and on cavity quantum electrodynamical setups [60]. These developments called for new methods for stabilizing quantum algorithms against perturbing environmental influences, which tend to destroy quantum interference and quantum entanglement [61]. This led to the development of the first error-correcting codes [62, 63, 64, 65, 66] by adaptation of classical error-correcting techniques to the quantum domain. An introduction to the theory of quantum error correction is presented in Chap. 4.

1.2 Quantum Physics and Information Processing

What are the common features of these early developments? The common element of these early developments in quantum cryptography and quantum computation is that they all involve the practical processing of information and they are all founded on and facilitated by characteristic quantum phenomena. These phenomena, among which the most prominent is entanglement, are in conflict with the classical concepts of physical reality and locality. Obviously, these early developments hint at a profound connection between the concept of information and some fundamental concepts of quantum theory, which is also promising from the technological point of view. It is these technologically oriented aspects of quantum information theory [67, 68, 69] which are at the heart of quantum information processing.

Methods for processing quantum information have developed rapidly during the last few years [12]. Owing to significant experimental advances, basic interference and entanglement phenomena which are of central interest for processing quantum information have been realized in the laboratory in various physical systems. Basic schemes for quantum communication have

been demonstrated with photons [10, 11, 49, 70]. Realizations of elementary quantum logical operations have been based on trapped ions [13, 14] and on nuclear magnetic resonance [15]. Recent experiments indicate that besides cavity quantum electrodynamical setups [16], trapped neutral atoms which are guided along magnetic wires (atom chips) might also be useful for quantum information processing [17]. There have also been theoretical proposals on using ultracold atoms in optical lattices [18, 19], on ions in an array of microtraps [20] and on solid-state devices [21, 22, 23] for the implementation of quantum logical gates.

By now, quantum information processing has become an interdisciplinary subject which attracts not only physicists but also researchers from other communities. The common interest is the practical, technologically oriented application of characteristic quantum phenomena. At this stage of development, it appears necessary to examine recent achievements and to emphasize the underlying, general, basic concepts, which have been developing gradually and which are now commonly adopted by all researchers in this field. This is one of the main intentions of the rest of the book.

In Chap. 2, Werner introduces the basic concepts of quantum information theory and describes the fundamental mathematical structures underlying recent and current developments. In particular, this chapter addresses a natural question appearing in connection with Feynman's suggestion, namely what can be done with the help of quantum systems and what cannot be done. A first example of an impossible quantum process, the copying of nonorthogonal quantum states, has already been mentioned. Other examples of possible and impossible quantum processes are discussed in detail in this contribution.

First experimental realizations of basic quantum communication schemes based on entangled photon pairs are discussed in Chap. 3 by Weinfurter and Zeilinger. These first experiments on entanglement-based quantum cryptography, dense coding and quantum teleportation demonstrate the important role photons play in current experiments. Furthermore, these experiments also emphasize once again the fundamental significance of entanglement for quantum information processing.

The basic theoretical concepts of quantum computation and the mathematical structure underlying quantum algorithms are discussed in Chap. 4 by Beth and Rötteler. In particular, it is demonstrated how recent results in the theory of signal processing can be used for the development of new fast quantum algorithms. A short introduction to the theory of quantum error correction is also presented.

A comprehensive account of the mathematical structure of entanglement and of the significance of mixed entangled states for quantum information processing is presented in Chap. 5 by M. Horodecki, P. Horodecki and R. Horodecki. One of the most surprising recent developments in this context has been the discovery of bound entanglement [71]. Though much is still unknown, this section gives a state-of-the-art presentation of what is known

about this new form of entanglement and its implications for processing quantum information.