X 5 Fundamental Concepts of Quantum Information Processing

Thomas Schäpers
Institut für Bio- und Nanosysteme (IBN-1)
Forschungszentrum Jülich GmbH

Contents

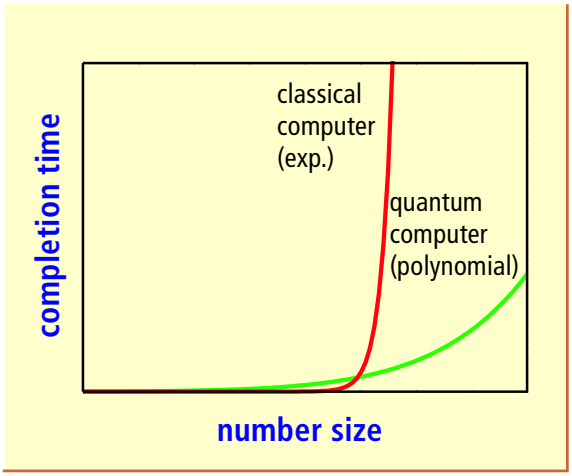

Fig. 1: *Completion time as a function of number size for a classical and a quantum factorization algorithm, respectively.*

1 Introduction

Quantum information technology is a fast developing field where the unique properties of quantum mechanics are used for computation or communication. In contrast to a bit processed in a conventional computer, which can only be in the state 0 or 1, here the bit is constituted by a quantum mechanical two-level system, the so-called qubit. A well-known example of a two-level system is the two states of an electron with spin 1/2 in a static magnetic field. What make the quantum bit so powerful is that superpositions of the two quantum states are allowed. If this property, which has no counterpart in conventional computers, is cleverly used, some computational problems can be solved much faster. The reason for this is that by employing a superposition of quantum states a quantum algorithm effectively calculates very many solutions in parallel. A prominent example of this kind of algorithm is Shor's prime number factorization, where a large number is decomposed into its prime factors [1]. As illustrated in Fig. 1, Shor's algorithm can factorize a large number exponentially fast compared to a classical computers.
A quantum computer is not commercially available, yet, as the technology to build such a device is still in an early stage and up to now systems with only a few quantum bits have been realized [2]. Of course, this is not sufficient for serious applications. One of the problems scientists face is the loss of coherence of the quantum mechanical state, due to the coupling of the quantum bit to the environment. If the coherence is lost during the computational sequence, the final result is meaningless.
Since quantum mechanics is one of the very fundamental principles in physics, many different experimental realizations in various fields of physics have been proposed. Quantum computing with a few quantum bits has been demonstrated by using nuclear magnetic resonance (NMR) [3]. Another possibility is to manipulate the electronic states of ions stored in a trap [4]. Quantum bits can also be realized in solid-state systems, in particular by using quantum dots [5, 6], single impurities in a semiconductor [7] or Josephson junctions [8, 9, 10].
In this lecture we will only discuss the basic principles of quantum computation. Quantum bits and quantum registers will be introduced first. Later on it will be discussed how the state of a quantum bit can be manipulated by means of a quantum gate. We will distinguish between two different gates, the single-qubit gate, where the state of single qubit is modified, and a

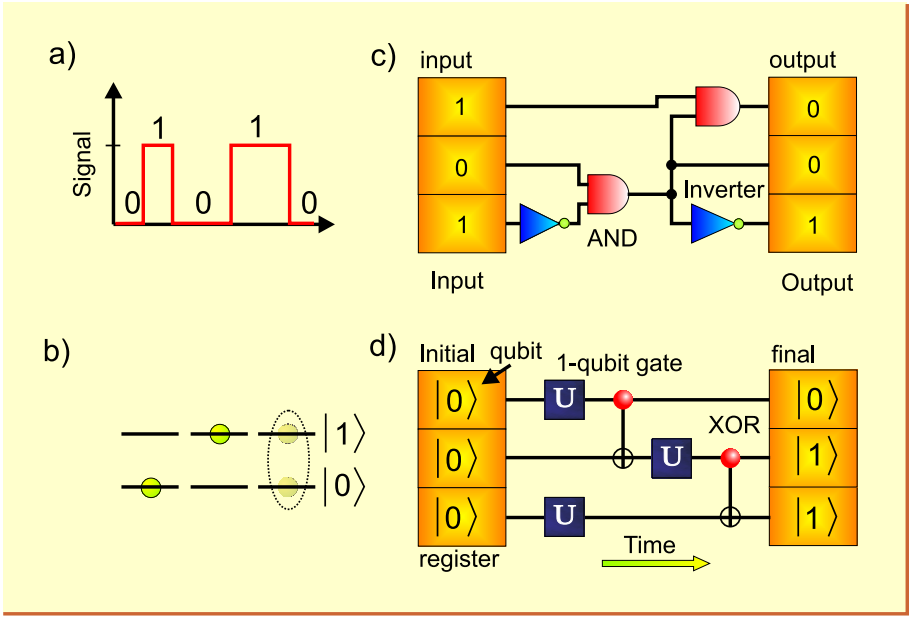

Fig. 2: *(a) Possible values in a digital computer. Here, the signal is switched between the values 0 and 1. (b) In a quantum mechanical two-level system the partical can be in the ground state $|0\rangle$ or in first excited state $|1\rangle$ but also in a superposition of both. (c) Schematic illustration of a digital computer. The calculation is performed by means of gates, e.g. inverters or NAND-gates (inverted AND). (d) Schematics of a 3-qubit quantum computer. The qubits are manipulated by single-qubit gates (U) and two-qubit gates (XOR).*

two-qubit gate, where the first qubit controls the state of the second one. Furthermore, we will discuss what else is required to build a properly operating quantum computer. In the last part the basic ideas of the two most popular quantum algorithms, the Shor and Grover algorithm will be explained.

2 Quantum Bits and Quantum Registers

In this section the basic elements of a quantum computer, the quantum bit and the quantum register are discussed. We will start by defining the smallest unit, the quantum bit and we will see what *strange* things can happen if more quantum bits are combined.

2.1 Quantum Bit

The basic element of a quantum computer is the quantum bit, or qubit, which can be viewed as an extension of the classical notion of a bit. As illustrated in Fig. 2 (a), in a classical computer only 0 and 1 are possible values corresponding to zero and a fixed finite voltage level [11]. Similarly, a qubit consists of a quantum mechanical two-level system. However, the crucial difference is that in addition to the two eigenstates $|0\rangle$ and $|1\rangle$ a qubit can be configured in any

superposition of these eigenstates[1]

$$|Q\rangle = c_0|0\rangle + c_1|1\rangle \ . \tag{1}$$

In contrast to the classical bit, a qubit can be prepared in an infinitive number of appropriate quantum states by choosing different coefficients c_0 and c_1. The qubit state is normalized so that $|c_0|^2 + |c_1|^2 = 1$. The two eigenstates usually correspond to the ground and excited states of a two-level system, as depicted in Fig.2 (b). A possible realization is the Zeeman splitting of the spin-up and spin-down state of a spin-1/2 particle ($s = \pm 1/2$), i.e. an electron, in a magnetic field $\mathbf{B}$. The corresponding two basis vectors can be represented by

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ , \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ . \tag{2}$$

The qubit can then be expressed by

$$|Q\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \ . \tag{3}$$

In case of an electron in a magnetic field $\mathbf{B}$, the two-level system is described by the Hamiltonian

$$H = \frac{1}{2} g^* \mu_B \mathbf{B} \sigma \ , \tag{4}$$

with g the effective gyromagnetic factor.[2] The Bohr magneton is defined as $\mu_B = e\hbar/2m_0$, with e the elementary charge and m_0 the free electron mass. The components of the $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ are the Pauli spin matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ , \ \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \ , \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \ . \tag{5}$$

As illustrated in Fig. 3, if one assumes a constant field along the z-direction: $\mathbf{B} = (0, 0, B_z)$, the Zeeman effect leads to a splitting of the spin-up and spin-down states. The level splitting is given by $\Delta E = g\mu_B B_z$, which can be rewritten as

$$\Delta E = \hbar\omega_p \ , \tag{6}$$

with

$$\omega_p = |g|\mu_B B_z/\hbar \tag{7}$$

the precession frequency. We will see below, ω_p plays an important role for the manipulation of a qubit.

The state of a spin-1/2 can best be visualized by using a Bloch sphere. Here, all possible spin orientations are mapped on a sphere. Using this scheme, the spin-up and spin-down state are illustrated in Fig. 4 a) and b), where the arrows representing the spin states point towards the $\pm z$-direction, respectively. For the superposition state $1/\sqrt{2}(|0\rangle + |1\rangle)$, which is an eigenstate of σ_x, the arrow points towards the x-direction, as shown in Fig. 4 c).

[1] Here, we used the Dirac notation which allows us to describe quantum mechanical states without defining a particular set of basis vectors.

[2] In order to be consistent with the usual notation in quantum computation, we assume a negative g^*-factor so that the spin-up state is the ground state, i.e. the state with the lower energy. A negative g^*-factor is found for example in GaAs.

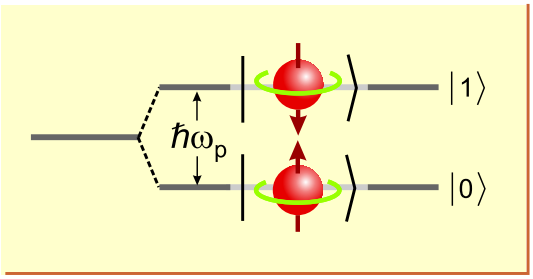

Fig. 3: *Zeeman-splitted spin up* $|0\rangle$ *and spin down* $|1\rangle$ *states representing a qubit. The energy splitting is given by* $\hbar\omega_p$*, with* ω_p *the cyclotron frequency.*

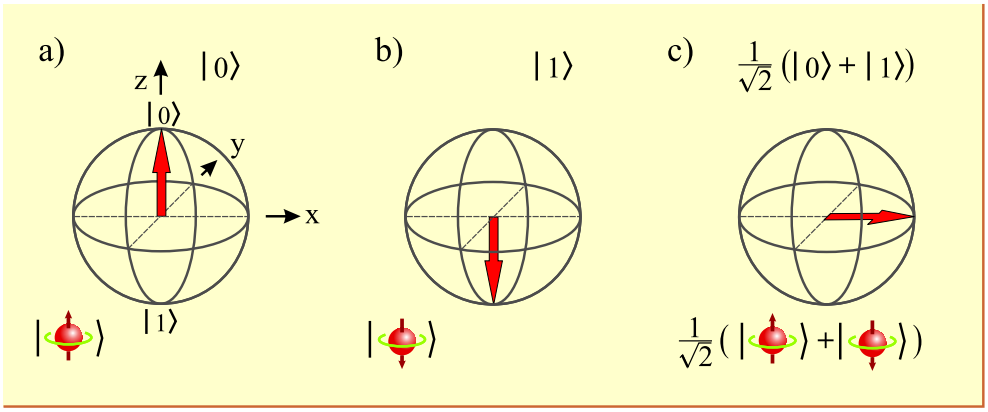

Fig. 4: *Bloch spheres illustrating different states of a spin 1/2-particle. (a) and (b) spin-up and spin-down state along the* z*-direction. (c) Superposition state* $1/\sqrt{2}(|0\rangle + |1\rangle)$ *pointing towards the* x*-direction. This state is an eigenstate of* σ_x*.*

Although an infinitive number of quantum states can be realized in a qubit state, a single qubit cannot be used to transmit more than one bit of information. This is due to the fact that in quantum mechanical systems only eigenstates of the quantum system are finally detected by the measurement procedure. For a superposition state, as given by Eq. (1), the final measurement will return 0 with probability $|c_0|^2$ and 1 with probability $|c_1|^2$. Thus, after the measurement the state of the qubit will either be the eigenstate $|0\rangle$ or $|1\rangle$ but definitely not in a superposition of both. Returning back to the spin 1/2-particle: If the spin orientation would be measured, e.g. by a Stern-Gerlach apparatus, the spin-up state would be measured with probability $|c_0|^2$ and the spin-down state with probability $|c_1|^2$.
Of course as a final result of a computation a superposition state is useless, because no unambiguous outcome is produced. Thus, at the end of a computation an eigenstate is required as a result. However, one should keep in mind that during calculation superposition states are very important, since they are responsible for the higher performance of quantum algorithms.

2.2 Quantum Register

A collection of qubits, which is usually called quantum register, can be used to encode more complex information. In the schematics of a quantum computer depicted in Fig. 2 (d) the quantum register contains three quantum bits. As a very simple example a two-qubit register can be composed from the following set of eigenvectors:

$$|0\rangle_2 \otimes |0\rangle_1 = |00\rangle \ , \quad |0\rangle_2 \otimes |1\rangle_1 = |01\rangle \ , \quad |1\rangle_2 \otimes |0\rangle_1 = |10\rangle \ , \quad |1\rangle_2 \otimes |1\rangle_1 = |11\rangle \ . \tag{8}$$

Here, $\otimes$ denotes the direct product of the vectors. The indices specify the first and second qubit. By using this set of basis vectors a general superposition of these state is given by

$$|\psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle \ . \tag{9}$$

Instead of writing the basis vectors as given in Eq. (8), we can also use the notation

$$|00\rangle = |0\rangle \ , \quad |01\rangle = |1\rangle \ , \quad |10\rangle = |2\rangle \ , \quad |11\rangle = |3\rangle \ , \tag{10}$$

which is sometimes easier to handle if many qubits are involved. Generally, for an n-bit quantum register we can write:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i|i\rangle \ . \tag{11}$$

For an n–qubit state we obtain 2^n states $|i\rangle$. Please note that by preparing a superposition state all these states are simultaneously present.

2.3 Entangled States

A closer look on two or more qubit registers reveal that states can be prepared where the states of constituting qubits in a register are not independent. This situation is called entanglement. A typical two-qubit entangled state is given by:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}} \left(|1\rangle_2 \otimes |0\rangle_1 - |0\rangle_2 \otimes |1\rangle_1 \right) \\ &= \frac{1}{\sqrt{2}} \left(|10\rangle - |01\rangle \right) \end{aligned} \tag{12}$$

Here, $|0\rangle_1$ and $|1\rangle_1$ are states constituting the first qubit, while $|0\rangle_2$ and $|1\rangle_2$ are the corresponding states of the second qubit. An entangled state cannot be factorized into an expression like:

$$|\psi\rangle = |m\rangle_2 \otimes |n\rangle_1 \ . \tag{13}$$

A typical representative of a state which can be factorized is given by

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|1\rangle_2 \otimes |0\rangle_1 - |1\rangle_2 \otimes |1\rangle_1 \right) \ , \tag{14}$$

since we can simplify it to

$$|\psi\rangle = \frac{1}{\sqrt{2}} |1\rangle_2 \otimes \left(|0\rangle_1 - |1\rangle_1 \right) \ , \tag{15}$$

corresponding to Eq. (13).
What is the consequence of entanglement? Let us assume that we are able to measure the state of the first qubit of the state given by Eq. (13). If the result would be $|0\rangle_1$, it directly implies that the second qubit is in the state $|1\rangle_2$. This behavior is of special importance, if the two qubits are represented by two polarized photons emitted in two opposite directions. A measurement of the polarization state of the first photon directly implies the polarization state of the second photon, although the detectors of the photons can be very far apart. Fundamental questions, how the second photon *knows* about the state of the first one are addressed in the famous article by Einstein-Podolsky-Rosen (EPR) [12]. Entanglement is also of outmost importance for quantum key distribution. Here, a secure key is generated by transmitting entangled photon between two parties. In the second step this key is used to encode information. The securities of this scheme is ensured by the fact that a possible eavesdropper can be discovered.

3 Quantum-Gates

The state of a qubit or of a set of qubits is controlled by quantum-gates. This is in analogy to boolean gates, e.g. to an inverter or AND gate in classical digital computers, where the corresponding truth tables are given in Table 1. Interestingly, by using an inverter (NOT gate)

a	*b*
0	1
1	0

a	*b*	*c*
0	0	0
0	1	0
1	0	0
1	1	1

Table 1: *Truth table of a NOT and AND gate. For the NOT gate a is the input parameter and b the output parameter. For the AND gate a and b are the input parameters and c the output.*

and an AND gate any boolean expression can be constructed. If we combine an AND and a NOT gate to form a NAND gate, even a single gate is sufficient to synthesize any boolean operation. In quantum computing the gates are represented by unitary transformations. Similar to conventional computers, one can define gates which are applied to a single qubit or gates, which connect two or more qubits. Furthermore, it was found that a set of two quantum gates is sufficient to implement all quantum computer operations.

3.1 Single-Qubit Gate: Basics Concept

By performing quantum computational operations, the qubit states are changed in course of time. The eigenstates $|0\rangle$ and $|1\rangle$ themselve are fixed, only the probabilities for their occupation, expressed by the coefficients $c_0(t)$ and $c_1(t)$ are explicitly time-dependent:

$$|Q(t)\rangle = c_0(t)|0\rangle + c_1(t)|1\rangle. \tag{16}$$

In quantum gate operations the coefficients $c_1(t)$ and $c_2(t)$ are changed in a defined manner, e.g. by applying an external magnetic field for a well-defined period of time.
In order to express the following single-qubit operations more compactly, the qubit state needs to be described a little bit more formally

$$|Q(t)\rangle = \sum_{i=0,1} c_i(t)|i\rangle \ . \tag{17}$$

The basis vectors defining the qubit are orthonormal which implies that they fulfill

$$\langle i|j\rangle = \delta_{ij} \ , \quad i,j = 0,1 \ . \tag{18}$$

Here, $\langle i|$ are the vectors of the dual space while $\langle \ldots | \ldots \rangle$ denotes the inner product. For example, by using the definition of the inner product the coefficients $c_i(t)$ can be extracted by:

$$\langle i|Q(t)\rangle = \langle i| \sum_{j=0,1} c_j(t)|j\rangle = c_i(t) \ . \tag{19}$$

In the framework of quantum mechanics the gate operation on a qubit corresponds to a transformation of the state in the course of time, which can be described by means of the Schrödinger equation

$$\mathrm{i}\hbar \frac{\partial}{\partial t}|Q(t)\rangle = H(t)|Q(t)\rangle \ , \tag{20}$$

where $H(t)$ is the Hamilton operator. Inserting the definition of $|Q(t)\rangle$, as given by Eq. (17), into the Schrödinger equation and multiplying by $\langle i|$, we obtain a set of two equations for the coefficients $c_0(t)$ and $c_1(t)$:

$$\begin{aligned} \langle i|\mathrm{i}\hbar \frac{\partial}{\partial t}|Q(t)\rangle &= \langle i|H(t)|Q(t)\rangle \\ \langle i|\mathrm{i}\hbar \sum_{j=1,2} \frac{\partial}{\partial t} c_j(t)|j\rangle &= \langle i|H(t) \sum_{j=1,2} c_j(t)|j\rangle \qquad (21) \\ \mathrm{i}\hbar \frac{\partial c_i(t)}{\partial t} &= \sum_{j=1,2} H_{ij}(t)c_j(t) \ . \qquad (22) \end{aligned}$$

Here, $H_{ij}(t) = \langle i|H(t)|j\rangle$ are the elements of the Hamilton matrix. In order to obtain the values of the coefficients $c_0(t_1)$ and $c_1(t_1)$ at time $t = t_1$, the two equations have to be integrated in the interval $[t_0, t_1]$, where t_0 is the initial time.
A single-qubit gate operation is realized by *switching on* a Hamiltonian for a period of time $\Delta t = t_1 - t_0$ and thus modifying the coefficients $c_1(t)$ and $c_2(t)$. As we will see below, for a spin-1/2 particle this can be realized by applying an oscillating magnetic field for a certain

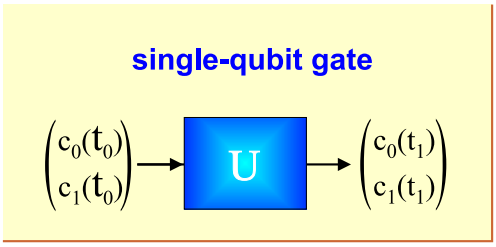

Fig. 5: *Quantum circuit diagram of an single-qubit gate. The gate operation is described by a unitary transformation.*

period of time. In this case the gate operation relies on the coupling of the magnetic moment of the particle to the field.
In order to clarify how the qubit is changed after a short period of time Δt we write the Schrödinger equation as follows

$$\frac{c_i(t_0+\Delta t)-c_i(t_0)}{\Delta t} = -\frac{i}{\hbar}\sum_j H_{ij}(t_0)c_j(t_0)\ . \tag{23}$$

By regrouping this equation we get for the final state of the qubit at time t_1:

$$c_i(t_1) = c_i(t_0+\Delta t) = \sum_j \left[\delta_{ij} - \frac{i}{\hbar}H_{ij}(t_0)\Delta t\right] c_j(t_0) \tag{24}$$

The matrix on the right side is a unitary matrix and can be summarized by defining:

$$U_{ij}(t_0+\Delta t, t_0) = \delta_{ij} - \frac{i}{\hbar}H_{ij}(t_0)\Delta t \tag{25}$$

Thus, the change of the qubit state between t_0 and t_1 calculated by integrating the Schrödinger equation what can be expressed by a unitary transformation U. For a qubit represented by a two component vector defined by Eq. (3), U can be described by a unitary 2×2 transformation matrix (Fig. 5):[3]

$$\begin{pmatrix} c_0(t_1) \\ c_1(t_1) \end{pmatrix} = U \begin{pmatrix} c_0(t_0) \\ c_1(t_0) \end{pmatrix} = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} c_0(t_0) \\ c_1(t_0) \end{pmatrix}\ . \tag{26}$$

This unitary matrix U represents the single-qubit gate operation. In the following two sections we will specify U in more detail by discussing two possible realizations of a single-qubit gate, i.e. the Hadamard transformation and the manipulation of a spin-1/2 quantum bit by an oscillating field.

3.2 The Hadarmard Transformation as a Single-Qubit Gate

A well-known representative of a single-qubit gate is the Hadamard transformation defined by the following unitary matrix

$$U_H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\ . \tag{27}$$

[3] An unitary matrix has the property: $U^\dagger U = 1$, with $U^\dagger$ the adjoint matrix defined by $U^\dagger = (U^*)^T$.

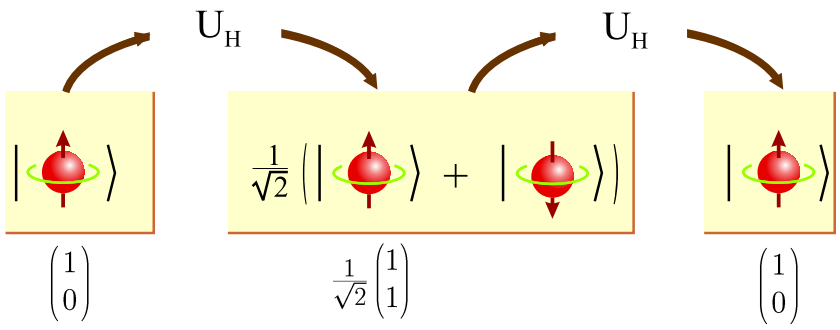

Fig. 6: *Hadamard transformation (single-qubit operation) on a spin-1/2 particle in the ground state. By applying the Hadamard transformation once again the initial spin orientation is recovered.*

The Hadamard transformation can be used to conveniently generate a superposition state out of an eigenstate. This operation is often the first processing step in quantum algorithms, e.g. the Deutsch-Josza algorithm [15]. Let us assume our qubit is in the ground state $|0\rangle$. Applying a Hadamard transformation results in

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \ . \tag{28}$$

Thus, as illustrated in Fig. 6, we end up with the superposition state $1/\sqrt{2}(|1\rangle + |0\rangle)$. One can easily verify that by applying a Hadamard transformation once again the superposition state returns back to the ground state $|0\rangle$ (see Fig. 6).
Of course Hadamard single-qubit gates can also be applied to qubit registers. For simplicity, let us consider a two-qubit register which is initially in the ground state $|00\rangle$. If we apply the transformations $U_{H,1}$ and $U_{H,2}$ to the first and to the second qubit, respectively, we end up with

$$U_{H,2}\,U_{H,1}\,|00\rangle = \frac{1}{2}\left(|00\rangle + |10\rangle + |01\rangle + |11\rangle\right) \ . \tag{29}$$

Thus by performing two simple one-qubit gate operation the ground state of a quantum register $|00\rangle$ is transformed to a superposition of all four basis states. As mentioned above, to be able to generate a superposition state is of outmost importance for quantum computation, since the strength of its concept lies in the parallel processing of all states.

3.3 Single-Qubit Manipulation by an Oscillating Magnetic Field

When we discussed the Hadamard transformation as a representative of a single-qubit gate we did not care how such a gate can actually be realized. Now we will explain how a single-qubit gate can be put into action by *switching on* a Hamiltonian. Let us return to our prototype qubit, i.e. the single electron with spin 1/2. By coupling the magnetic moment of the electron to an external magnetic field $\mathbf{B}$ the spin state can be modified. The process is illustrated in Fig. 7. The Hamiltonian describing this coupling was already given by Eq. (4). In contrast to the previous case with a constant magnetic field B_z, now a magnetic field rotating in the xy-plane with frequency ω_p and amplitude B_0 is applied for a certain period of time. Thus, in total the

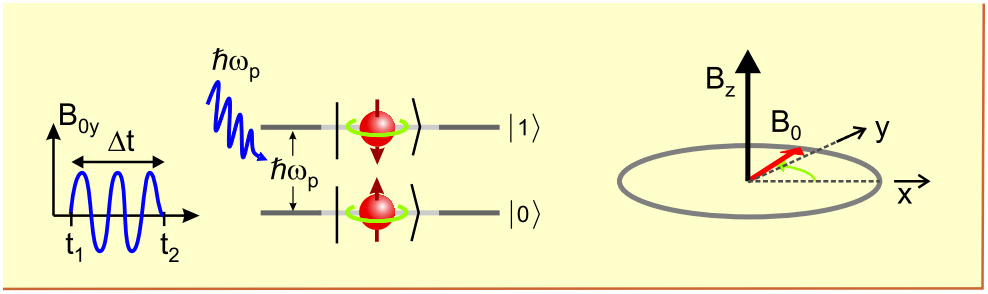

Fig. 7: *Coherent transitions of Zeeman-splitted electrons by applying a magnetic field rotating in the xy-plane with frequency ω_p. The level splitting is achieved by applying a constant field B_z along the z-direction.*

magnetic field is given by:

$$\mathbf{B} = \begin{pmatrix} B_0 \cos \omega_p t \\ B_0 \sin \omega_p t \\ B_z \end{pmatrix} \tag{30}$$

By inserting $\mathbf{B}$ into Eq. (4) one arrives at the following explicit form of the Schrödinger equation

$$i\hbar \frac{\partial}{\partial t} \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix} = \frac{1}{2} g \mu_B \begin{pmatrix} B_z & B_x - iB_y \\ B_x + iB_y & -B_z \end{pmatrix} \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix} . \tag{31}$$

Assuming the ground state $|Q(t_0)\rangle = (1, 0)$ to be the initial state at $t = t_0$ one finds the following solution for the quantum bit after the oscillating field is applied for a period of time $\Delta t = t_1 - t_0$:

$$|Q(t_1)\rangle = \begin{pmatrix} \cos(\Omega \Delta t/2) \exp(+i\omega_p \Delta t/2) \\ i \sin(\Omega \Delta t/2) \exp(-i\omega_p \Delta t/2) \end{pmatrix} , \tag{32}$$

with the characteristic frequency Ω defined by

$$\Omega = |g| \mu_B B_0 / \hbar . \tag{33}$$

In order to get some insight what happens to the qubit after the period of time Δt, one can calculate the expectation values of the spin in the different directions:

$$\langle s_x \rangle = \frac{\hbar}{2} \langle Q(t_2) | \sigma_x | Q(t_2) \rangle = \frac{\hbar}{2} \sin(\Omega \Delta t) \sin(\omega_p \Delta t) \tag{34}$$

$$\langle s_y \rangle = \frac{\hbar}{2} \langle Q(t_2) | \sigma_y | Q(t_2) \rangle = \frac{\hbar}{2} \sin(\Omega \Delta t) \cos(\omega_p \Delta t) \tag{35}$$

$$\langle s_z \rangle = \frac{\hbar}{2} \langle Q(t_2) | \sigma_z | Q(t_2) \rangle = \frac{\hbar}{2} \cos(\Omega \Delta t) \tag{36}$$

One finds by looking at $\langle s_z \rangle$ that in the course of time the spin oscillates with frequency Ω between the ground state $|0\rangle$ (spin-up) and the excited state $|1\rangle$ (spin-down), e.g. after applying the oscillation field for a period $\Delta t = \pi/\Omega$ the electron is transferred from the ground state $|0\rangle$ into the excited state $|1\rangle$. As can be inferred from Eq. (33), the time required to flip the spin is determined by the amplitude B_0 of the oscillation field.

The effect of the oscillation field on the qubit can best be visualized by making use of the Bloch sphere. For the case where the oscillation field is applied for a period $\Delta t = \pi/\Omega$ the

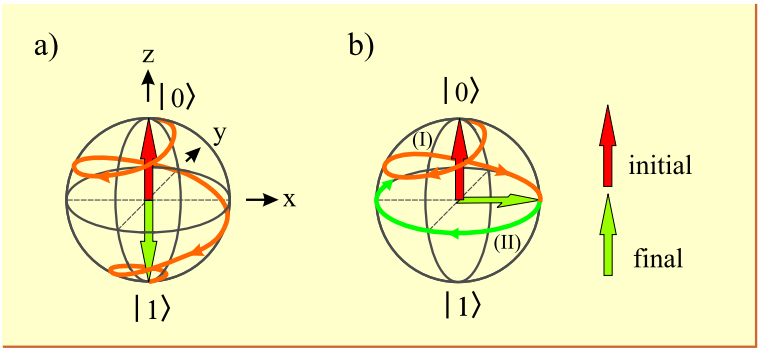

Fig. 8: *(a) Flip of the spin-up state $|0\rangle$ (red arrow) to the spin-down state $|1\rangle$ (green arrow). The trajectory of the spin is illustrated by the orange line. (b) Transition from the $|0\rangle$ state (red arrow) to the superposition state $1/\sqrt{2}(|0\rangle + |1\rangle)$ (green arrow). If the field is switched off after the transition, the spin precesses clockwise in the xy-plane as illustrated by the green line.*

spin is flipped from the top to the bottom pole, as illustrated in Fig. 8 a). However, the spin is not simply flipped but rather precesses about the z-axis while turning downwards. The spin precession is due to the second factors in Eqs. (34+35). The precession frequency is ω_p.
If the oscillation field is only applied for a period $\Delta t = \pi/2\Omega$ one can infer from Eq. (32) that a superposition state is obtained. The spin is now located in the xy-plane. If the amplitude B_0 of the oscillating field is properly adjusted one can for example transfer the $|0\rangle$ state to the $1/\sqrt{2}(|0\rangle + |1\rangle$ state, as illustrated in Fig. 8 b). Note, that after performing this transition and switching off the oscillating field the spin precesses about the z-axis with the precession frequency ω_p, thus the qubit does not keep its state in the course of time. Technically this is not a big problem. For example, one can compensate this effect by working in a reference frame rotating at with ω_p [16].
So far, we only considered the ground state as the initial state. One can generalize the special case discussed above by allowing any superposition state for the qubit. For this case the qubit manipulation can be expressed as

$$\begin{pmatrix} c_0(t_1) \\ c_1(t_1) \end{pmatrix} = U_R \begin{pmatrix} c_0(t_0) \\ c_1(t_0) \end{pmatrix} \tag{37}$$

with the corresponding unitary matrix given by

$$U_R = \begin{pmatrix} \cos(\Omega\Delta t/2)\exp(i\omega_p\Delta t/2) & i\sin(\Omega\Delta t/2)\exp(-i\omega_p\Delta t/2) \\ i\sin(\Omega\Delta t/2)\exp(i\omega_p\Delta t/2) & \cos(\Omega\Delta t/2)\exp(-i\omega_p\Delta t/2) \end{pmatrix} . \tag{38}$$

Interestingly, the matrix U_R can be decomposed in a product of two matrices

$$\begin{aligned} U_R &= \begin{pmatrix} \cos(\Omega\Delta t/2) & i\sin(\Omega\Delta t/2) \\ i\sin(\Omega\Delta t/2) & \cos(\Omega\Delta t/2) \end{pmatrix} \begin{pmatrix} \exp(i\omega_p\Delta t/2) & 0 \\ 0 & \exp(-i\omega_p\Delta t/2) \end{pmatrix} \\ &= R_x(\Omega\Delta t)R_z(\omega_p\Delta t) . \end{aligned}$$

We can interpret this outcome as a combination of two rotation of the spin, i.e. a rotation R_x with the angle $\Omega\Delta t$ about the x-axis and a rotation R_z with the angle $\omega_p\Delta t$ about the z-axis. After the period Δt the qubit is transferred to

$$|Q(t_1)\rangle = R_x(\Omega\Delta t)R_z(\omega_p\Delta t)|Q(t_0)\rangle .$$

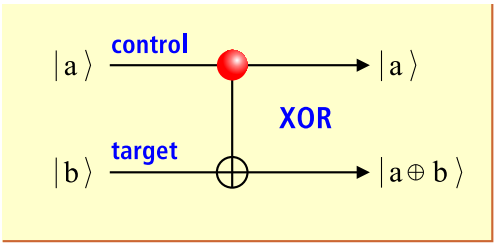

Fig. 9: *Quantum circuit diagram of an XOR gate. The lower bit $|b\rangle$ (target qubit) is flipped if $|a\rangle$ (source qubit) is set.*

a	b	$a \oplus b$		$\|a,b\rangle$	$\|a, a \oplus b\rangle$
0	0	0		$\|00\rangle$	$\|00\rangle$
0	1	1	$\Longleftrightarrow$	$\|01\rangle$	$\|01\rangle$
1	0	1		$\|10\rangle$	$\|11\rangle$
1	1	0		$\|11\rangle$	$\|10\rangle$

Table 2: *Truth table of a XOR (CNOT) gate for a boolean and for a quantum computer.*

In summary, spin rotation matrices can be used to generate any desired single-qubit gate. The spin rotation is determined by the time and amplitude of the applied oscillating field.

3.4 Two-Qubit Gates

We now turn to quantum gates, which are applied to two quantum bits. A typical two-qubit gate is the controlled NOT or exclusive OR (XOR) gate. In boolean computers the output is set to 1 if either the first or the second input is 1. If both are 1 the output is 0 again. The corresponding circuit diagram for qubits can be found in Fig. 9. In an XOR gate, a target qubit $|b\rangle$ is flipped if a control qubit $|a\rangle$ is in the $|1\rangle$ state. As long as $|a\rangle$ is in the state $|0\rangle$ no action is taken on $|b\rangle$. The corresponding truth table is given in Table 2. An important conceptual difference between the the XOR gate in boolean and quantum computers is that in quantum gates, the number of inputs and outputs are always identical. The quantum bits are both still present after the gate operation.
The XOR gate is an unitary transformation on states spanned by a set of four basis vectors. If we define the following set of basis vectors

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \tag{39}$$

we can express the XOR gate by the unitary 4×4 matrix

$$U_{XOR} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{40}$$

The XOR gate can be used to produce an entangled state out of two formerly non-entangled states. For this purpose we set the control qubit $|a\rangle$ (source-qubit) to a superposition state $1/\sqrt{2}(|0\rangle - |1\rangle)$ and the target qubit to $|b\rangle = |1\rangle$. The input state is thus given by $1/\sqrt{2}\,(|01\rangle - |11\rangle)$, which is non-entangled, since it can be factorized in $1/\sqrt{2}(|0\rangle - |1\rangle) \otimes |1\rangle$. Applying an XOR gate we obtain

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1/\sqrt{2} \\ 0 \\ -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 1/\sqrt{2} \\ -1/\sqrt{2} \\ 0 \end{pmatrix} . \tag{41}$$

Thus the result is an entangled state given by $1/\sqrt{2}\,(|01\rangle - |10\rangle)$.

The XOR gate can also be used as a measurement gate to obtain the output value of a calculation, since it can reproduce the result of one input state on both output gates [17]. For this purpose we set the target gate $|b\rangle$ to $|0\rangle$. As can be seen from the truth table of the XOR gate, both lines at the output reproduce the state of the source gate $|a\rangle$. The output is either $|00\rangle$ or $|11\rangle$. This process can be used to perform a non-demolition measurement of a qubit by generating a second one in the same state, which is used for the measurement process. Furthermore, this configuration can be used to produce fanout, i.e. coupling the output to more than one inputs, if a coupling to two gate inputs in the following calculation step is required.

The XOR gate is only one out of many possible two-qubit-gates. Another possible two-qubit gate is the so-called controlled rotation (CROT) [18], which is described by the matrix

$$U_{CROT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} . \tag{42}$$

Here, a rotation on the second qubit is performed if the control qubit is set to $|1\rangle$. The name controlled rotation originates from the fact that in case the control qubit is set, the σ_z Pauli spin matrix which describes a spin rotation about the z direction is applied to the target qubit.

One can show that any two-qubit gate can be transferred to the XOR gate by performing a sequence of single-qubit operation. In the case of a CROT gate this can be achieved by performing single-qubit rotations on the target qubit $|b\rangle$ about the y-axis:

$$R_{y,|b\rangle}(\theta) = \begin{pmatrix} \cos\theta/2 & \sin\theta/2 & 0 & 0 \\ -\sin\theta/2 & \cos\theta/2 & 0 & 0 \\ 0 & 0 & \cos\theta/2 & \sin\theta/2 \\ 0 & 0 & -\sin\theta/2 & \cos\theta/2 \end{pmatrix} \tag{43}$$

As can be easily verified, performing a $\theta = \pi/2$ rotation before the CROT operation and finally

a rotation with $\theta = \pi/2$ the XOR gate is recovered:

$$R_{y,|b\rangle}(-\frac{\pi}{2})U_{CROT}R_{y,|b\rangle}(\frac{\pi}{2}) = \frac{1}{2}\begin{pmatrix}1&-1&0&0\\1&1&0&0\\0&0&1&-1\\0&0&1&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}\begin{pmatrix}1&1&0&0\\-1&1&0&0\\0&0&1&1\\0&0&-1&1\end{pmatrix}$$
$$= \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} = U_{XOR} \tag{44}$$

It was shown that any possible quantum algorithm can be realized in the basis of only a single-qubit gate and a XOR gate. However, for some physical realizations of a quantum computer it is not always straightforward to realize a XOR gate, i.e. in case of a quantum computer based on trapped ions a CROT gate is easier to implement. In order to prove that a certain type of realization of a quantum computer can be used universally, it is sufficient to find a transformation of an implemented two-qubit gate to a XOR gate. As shown above, for the CROT gate this can be achieved by performing single qubit rotations.
If we take our spin-1/2 particles for the realization of a qubit, the exchange interaction between two particles can be used to implement a two-qubit gate. The corresponding Hamiltonian for two coupled electron spins can be expressed as:

$$H = J\sigma_1 \cdot \sigma_2 \,, \tag{45}$$

where J is the exchange coupling parameter and σ_1, σ_2 are the spins operators of particle 1 and 2, respectively. In the famous proposal of Loss and Divincenzo [5] the single electrons representing the qubit are confined in a split-gate quantum dot structure. The two-qubit gate operation is put into action by lowering the electrostatic barrier between both quantum dots. The onset of electron tunneling between both quantum dots results in the exchange interaction expressed by Eq. (45). Due to the coupling between both spins one qubit is changed as a function of the state of the other one.

4 Decoherence

So far, we discussed a rather ideal quantum computer composed of qubit registers and a set of quantum gates. However, reality is not that perfect. One important aspect, which has not been addressed yet, is the decoherence of quantum systems. Decoherence occurs due to the fact that a quantum system is not completely isolated from its environment. The quantum dynamics of the surrounding setup couple to a certain extent to the states of a quantum computer. Decoherence is a very serious problem, since the computational pathways which are separated at the beginning of the calculation are only recombined at the very end. Thus, if something gets wrong in between, the final result is completely meaningless.
The decoherence is characterized by the decoherence time τ_{dec}. Its inverse is a measure of the coupling of a single qubit with its environment. In order to perform a successful computation with a quantum computer, the decoherence time must be much longer than the expected operating time of the computation. The latter is determined by the number of computational switchings and the time required to perform each of these steps. Typical values of the minimum

Quantum system	t_{switch} [s]	τ_{dec} [s]	Ratio
Electrons GaAs	10^{-13}	10^{-10}	10^{3}
Electrons Au	10^{-14}	10^{-8}	10^{6}
Trapped ions: In	10^{-14}	10^{-1}	10^{13}
Optical microcavities	10^{-14}	10^{-5}	10^{9}
Electron spin	10^{-7}	10^{-3}	10^{4}
Electron quantum dot	10^{-6}	10^{-3}	10^{3}
Nuclear spin	10^{-3}	10^{4}	10^{7}

Table 3: *Typical times for quantum mechanical two-level systems, which are possible candidates for a realization of a qubit [19].*

switching time t_{switch}, the decoherence time τ_{dec} and the resulting maximum number of steps given by the ratio τ_{dec}/t_{switch} are summarized in Table 3 for various two-level systems [19]. Qubit states destroyed by decoherence can be recovered if error correction schemes are applied, as was first found out by Shor [20]. The major ingredient is the introduction of redundancy. The error correction relaxes somewhat the requirements resulting from the numbers given in Table 3. However, the circuit itself becomes more complex, since additional qubits have to be introduced.

5 The Five DiVincenzo Criteria

In the previous sections different parts of a quantum computer were discussed in detail. However, the fact that all components in itself are working does not mean that the device made out of these components can actually be used as a quantum computer. Exactly this issue was addressed by DiVincenzo [21, 22], who set up a list of five criteria, the so-called *DiVincenzo criteria*. The criteria are as follows:

- ⋆ Existence of a well-defined extendible qubit array.
- ⋆ It must be possible to define an initial state $|00\rangle$.
- ⋆ A sufficiently long decoherence time is required ($\tau_{dec}/t_{switch} > 10^4$).
- ⋆ An universal set of quantum gates exist.
- ⋆ A read-out of the qubit state must be possible.

Only if all criteria can in principle be fulfilled for an envisioned realization it makes sense to follow this approach. All criteria given above have been discussed in detail in the previous sections, except for the last one which is concerned with the read-out of the final state. For the spin-1/2 particle a direct read-out of the spin state by detecting its magnetic moment is difficult. For the quantum dot system, as proposed by Loss and DiVincenzo [5], a viable way is to transfer the spin degree of freedom into a charge degree of freedom. The latter can be accessed by electronic means.

6 Quantum Algorithms: A Brief Overview

In this section two different quantum algorithms will be discussed. Since most of the quantum algorithms are quite complex, we will omit a detailed treatment of the computational steps.
The probably most-cited quantum algorithm is the factorization algorithm invented by Peter Shor at IBM [1]. By using this algorithm it is possible to factorize large numbers with only a polynomial increase of computational time with the number of digits (see Fig. 1). In contrast, for digital computers the computational time increases exponentially with number size, so that it is literally impossible to factorize large numbers, i.e. numbers of more than 100 digits. This inability of digital computers is the reason why modern encryption schemes like the Rivest, Shamir, and Adleman (RSA) system [13] are based on factorizing large numbers. The fact that by employing Shor's algorithm large numbers can in principle be factorized is therefore a real threat for contemporary encryption methods.
In Shor's factorization algorithm a method is used where a large number N is factorized by finding a period of a sequence $f(x) = a^x \mod N$, where a is a randomly chosen small number with no factors in common with N. From the period of this series the prime factors of N can be extracted. However, for an ordinary computer it is as difficult to find the period of the series as finding the prime factors directly. The basic trick of Shor's algorithm is to find the period by performing a discrete Fourier transformation on a quantum mechanical superposition state. In practice only small numbers (number: 15) have been factorized so far, owing to the problem to build large-size quantum computer systems [2].
Another very prominent quantum algorithm is the search algorithm of Grover [14]. Due to the effective parallel computation in a quantum computer, Grover's algorithm can search for an item in a data base by only a single query, whereas multiple queries are required in a classical search algorithm. Once again, the speed of this algorithm is based on generating a superposition state given by Eq. (11) to address all entries of the data base at the same time.

References

[1] P. W. Shor. In S. Goldwasser, editor, *Proc. 35th Annual Symposium on the foundations of Computer Science*, pages 124–134. IEEE Compter Society Press, Los Alamitos, CA, 1994.

[2] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature **414**, 883 (2001).

[3] N. A. Gershenfeld and I. L. Chuang. Science **275**, 350 (1997).

[4] C. Monroe, D. M. Meekhof, B.E. King, W.M. Itano, and D.J.Wineland. Phys. Rev. Lett. **75**, 4714 (1995).

[5] D. Loss and D. P. DiVincenzo. Physical Review A **57**, 120 (1998).

[6] R. Hanson, L. P. Kouwenhoven, J. R. Petta, S. Tarucha, and L. M. K. Vandersypen, Reviews of Modern Physics **79**, 1217 (2007).

[7] B. E. Kane, Nature **393**, 133 (1998).

[8] Y. Nakamura, Yu. A. Pashkin, and J. S. Tsai. Nature **398**, 786 (1999).

[9] J.E. Mooij, T. P. Orlando, L. Levitov, Lin Tian, C. H. van der Wal, , and S. Lloyd, Science **285**, 1036 (1999).

[10] T. P. Orlando, J. E. Mooij, Lin Tian, C. H. van der Wal, L. S. Levitov, S. Lloyd, and J. J. Mazo, Phys. Rev. B **60**, 15398 (1999).

[11] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).

[12] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[13] R. Rivest, A. Shamir, and L. Adleman, Communications ACM **21** 120 (1978).

[14] L. K. Grover, Phys. Rev. Lett. **79**, 4709 (1997).

[15] D. Deutsch, Proc. R. Soc. Lond. A, **400**, 97 (1985).

[16] Vandersypen, L. Experimental quantum computation with nuclear spins in liquid solutions, Ph.D. Thesis, Stanford University, 2001 (quant-ph/0205193)

[17] D. Deutsch, Proc. R. Soc. Lond. A, **425**, 73 (1989).

[18] A. Steane, quant-ph/9608011, 1996, 1-36.

[19] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

[20] P. W. Shor, Phys. Rev. A **52**, 2493 (1995).

[21] D. P. DiVincenzo, Science 270, 255 (1995).

[22] D. P. DiVincenzo, Fortschr. Phys. **48**, 771 (2000).