Chapter 26
Quantum Information

Quantum information is one of the modern applications of quantum mechanics. Apart from quantum teleportation, we consider the fundamentals of quantum computers and the algorithms of Deutsch, Grover and Shor.

Quantum information (QI) means the transfer and processing of information, as far it is specifically quantum mechanical and not classical. In other words, quantum-mechanical principles such as superposition and entanglement of states play a central role in QI.

Hence in QI, we are dealing not with the fresh discovery of new principles of quantum mechanics, but rather with the new application of known relationships—QI was always implicit in quantum mechanics.[1] It is just the way of looking at things which has changed in the last two or three decades, probably because some concepts that had long been handled rather gingerly (entanglement, nonlocality, etc.) have proven their theoretical and practical significance.

With *quantum cryptography*, we already addressed a subtopic of quantum information in Chap. 10, Vol. 1. Two further topics that we outline below are *quantum teleportation* and *quantum computation*. But first, we show that there is no general quantum copier.

26.1 No-Cloning Theorem (Quantum Copier)

The *no-cloning theorem* states that it is impossible to duplicate *arbitrary* quantum-mechanical states. Thus, it is *not* possible to observe a state $|z\rangle$ non-destructively by producing an arbitrary number of (identical) copies of $|z\rangle$ and measuring this ensemble in leisurely fashion, as we will now demonstrate. We assume without loss of generality that all states are normalized.

[1] However, this is somewhat concealed by the fact that it makes use of a peculiar notation that (naturally) is oriented more to the needs of information processing than to those of theoretical physics.

J. Pade, *Quantum Mechanics for Pedestrians 2*, Undergraduate Lecture Notes in Physics, https://doi.org/10.1007/978-3-030-00467-5_26

We have an *unknown* state $|a\rangle$ which we want to duplicate. The system to which we want to transfer the copy is $|\varphi\rangle$; it plays the role of the blank sheet for copying and must be suitable, of course, to accept the copy. For instance, if we want to copy an unknown state $|a\rangle$ with spin 1, then $|\varphi\rangle$ must also allow spin 1. Thus, we want to transfer the product state[2] $|a \otimes \varphi\rangle$ by a unitary transformation U into the clone $|a \otimes a\rangle$. We do not have to go into details about U; it is enough to know that U must be independent of the state to be copied. We have:

$$U\,|a \otimes \varphi\rangle = |a \otimes a\rangle\,. \tag{26.1}$$

Now, a copier should be able to duplicate not only a single state (which here is $|a\rangle$); we need to have at least a second original state $|b\rangle$ which we can copy onto our blank sheet:

$$U\,|b \otimes \varphi\rangle = |b \otimes b\rangle\,. \tag{26.2}$$

We multiply the adjoint of the second equation into the first equation:

$$\langle b \otimes \varphi|\, U^\dagger U\,|a \otimes \varphi\rangle = \langle b \otimes b|\, a \otimes a\rangle\,. \tag{26.3}$$

We obtain

$$\langle b \otimes \varphi|\, a \otimes \varphi\rangle = \langle b \otimes b|\, a \otimes a\rangle\,, \tag{26.4}$$

or, with $\langle\varphi|\,\varphi\rangle = 1$,

$$\langle b|\, a\rangle = \langle b|\, a\rangle^2\,. \tag{26.5}$$

It follows that either $\langle b|\, a\rangle = 0$, or $\langle b|\, a\rangle = 1$. So we have either $|b\rangle \perp |a\rangle$ or $|b\rangle = |a\rangle$, which means that we cannot clone other states (recall that we assume normalized states).

Hence, strictly speaking, the name *no-cloning theorem* is not quite correct, because one can copy a state and the states orthogonal to it—but only those; all other states cannot be copied. If we know that *all* the states to be measured are parallel or orthogonal to a known state $|a\rangle$, we can make arbitrarily many copies of each state. This explains in retrospect why in quantum cryptography one uses *two different* orientations for the measurement of linear polarization: to spoil the possibility of reliably copying the states.

Another exceptional case in which copies of quantum states are possible occurs when there is a classical (i.e. non-quantum-mechanical) sub-step in the information processing. This of course can be copied perfectly.

Apart from these exceptional cases, the no-cloning theorem applies globally—there is no universal copier for pure quantum states.

[2]For reasons of greater clarity, we use here the detailed notation with $\otimes$, i.e. $|a \otimes b\rangle$.

26.2 Quantum Cryptography

We have already discussed this topic in Chap. 10, Vol. 1. Without going into detail, we want just briefly to mention here that there are protocols that work with entangled photons (e.g. the E91 protocol) and thereby provide an increase in security.

26.3 Quantum Teleportation

Teleportation is the (hypothetical) process whereby matter is transported from point A to point B without traversing the intervening space physically. This procedure, so much appreciated by sci-fi authors,[3] has in fact little in common with quantum teleportation, since in the latter, it is not the body, but rather its state—or more precisely, the quantum state—which is teleported. The tools are entangled states; in a certain part of the process, the information must be transmitted via a classical channel. We discuss the subject on the basis of quantum objects that can exist in two states, which we call $|0\rangle$ and $|1\rangle$.[4] The two states are normalized and mutually orthogonal.

Here we meet up again with Alice and Bob from Chap. 10, Vol. 1. The starting point is as follows: Alice wants to inform Bob of the state of a quantum object $Q1$, such as

$$|\varphi\rangle_1 = c\,|0\rangle_1 + d\,|1\rangle_1\,, \tag{26.6}$$

but without sending him the quantum object itself. Alice herself does not know the state and therefore cannot measure it reliably, since a single measurement gives no information about the constants c and d and will in general change the state (26.6). Preparing an ensemble by copying $Q1$ would indeed allow for the measurement of c and d with arbitrary precision, but it is prohibited according to the no-cloning theorem, as we have just seen. What to do?

The solution is achieved with a pair of entangled quantum objects QA and QB, transported to Alice and Bob (see Fig. 26.1) and containing the information about their status. To be concrete, the state of the entangled quantum objects QA and QB is

[3] Teleportation was made popular especially by 'Star Trek'. Apparently it was introduced in the series mainly for cost reasons—it simply would have been much more expensive to film / animate landings of spacecrafts on alien planets. "Beam me up, Scotty!"

[4] Instead of $|0\rangle$ and $|1\rangle$, we could choose other designations such as $|h\rangle$ and $|v\rangle$. But since $|0\rangle$ and $|1\rangle$ are used in quantum information exclusively, we adopt this notation. It should be mentioned in any case that $|0\rangle$ is *not* the zero vector (and of course, not the ground state of the harmonic oscillator). For concrete calculations, we use the representation

$$|0\rangle \cong \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |1\rangle \cong \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

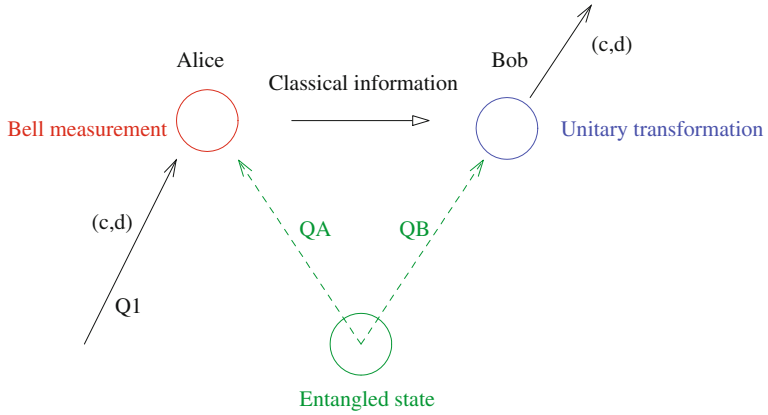

Fig. 26.1 Schematics of quantum teleportation

$$\left|\Phi^{-}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left[|01\rangle_{AB} - |10\rangle_{AB}\right]. \tag{26.7}$$

The total state $|\Psi\rangle_{1AB}$ of the three quantum objects is given by:

$$\begin{aligned} |\Psi\rangle_{1AB} &= |\varphi\rangle_1 \otimes \left|\Phi^{-}\right\rangle_{AB} \\ &= \frac{1}{\sqrt{2}}\left[c\,|001\rangle_{1AB} + d\,|101\rangle_{1AB} - c\,|010\rangle_{1AB} - d\,|110\rangle_{1AB}\right]. \end{aligned} \tag{26.8}$$

Alice now measures the quantum objects $Q1$ and QA (which are *not* entangled), using as a basis the Bell states, which we met up with already, in Chap. 20:

$$\begin{aligned} \left|\Phi^{\pm}\right\rangle_{1A} &= \frac{1}{\sqrt{2}}\left[|01\rangle_{1A} \pm |10\rangle_{1A}\right] \\ \left|\Psi^{\pm}\right\rangle_{1A} &= \frac{1}{\sqrt{2}}\left[|00\rangle_{1A} \pm |11\rangle_{1A}\right], \end{aligned} \tag{26.9}$$

with the inversions

$$\begin{aligned} |01\rangle_{1A} &= \frac{1}{\sqrt{2}}\left[\left|\Phi^{+}\right\rangle_{1A} + \left|\Phi^{-}\right\rangle_{1A}\right]; \quad |10\rangle_{1A} = \frac{1}{\sqrt{2}}\left[\left|\Phi^{+}\right\rangle_{1A} - \left|\Phi^{-}\right\rangle_{1A}\right] \\ |00\rangle_{1A} &= \frac{1}{\sqrt{2}}\left[\left|\Psi^{+}\right\rangle_{1A} + \left|\Psi^{-}\right\rangle_{1A}\right]; \quad |11\rangle_{1A} = \frac{1}{\sqrt{2}}\left[\left|\Psi^{+}\right\rangle_{1A} - \left|\Psi^{-}\right\rangle_{1A}\right]. \end{aligned} \tag{26.10}$$

We insert these inversions into the total state (26.8). It follows that:

$$|\Psi\rangle_{1AB} = \frac{1}{2}\left[\begin{array}{l} |\Psi^+\rangle_{1A}\,(-d\,|0\rangle_B + c\,|1\rangle_B) + |\Psi^-\rangle_{1A}\,(d\,|0\rangle_B + c\,|1\rangle_B) \\ +|\Phi^+\rangle_{1A}\,(-c\,|0\rangle_B + d\,|1\rangle_B) - |\Phi^-\rangle_{1A}\,(c\,|0\rangle_B + d\,|1\rangle_B) \end{array}\right]. \tag{26.11}$$

We can rewrite this with the help of the state $|\varphi\rangle_B = c\,|0\rangle_B + d\,|1\rangle_B$ and the (unitary) Pauli matrices (see the exercises):

$$|\Psi\rangle_{1AB} = \frac{1}{2}\left[\begin{array}{l} -|\Phi^-\rangle_{1A}\,|\varphi\rangle_B - |\Phi^+\rangle_{1A}\,\sigma_z\,|\varphi\rangle_B \\ +|\Psi^+\rangle_{1A}\,i\sigma_y\,|\varphi\rangle_B + |\Psi^-\rangle_{1A}\,\sigma_x\,|\varphi\rangle_B \end{array}\right]. \tag{26.12}$$

When Alice carries out her measurement, one of the four summands in the brackets is filtered out of the total state $|\Psi\rangle_{1AB}$, depending on which state $Q1QA$ she projects. Alice now tells Bob via a classical method (telephone, etc.) which state she has measured, so that Bob knows which unitary transformation he has to apply for preserving the original condition. In this way, the state $|\varphi\rangle_1$ of the quantum object 1 (but not $Q1$ itself!) has been teleported without ever measuring $Q1$ directly. Bob knows that QB now has precisely the unknown state that $Q1$ had before (i.e. 26.6).
A few remarks are in order:

1. The coefficients c and d are not measured. They are unknown for $|\varphi\rangle_1$, and likewise, after the teleportation, for $|\varphi\rangle_B$.
2. This is not copying, since the state $|\varphi\rangle_1$ is destroyed by Alice's measurement. So there is no contradiction with the no-cloning theorem.
3. Bob can prepare $|\varphi\rangle_B$ as soon as he receives the result of Alice's measurement. The transmission of this information is done via a classical channel, i.e. with a speed equal to or less than the speed of light. So there is no instantaneous non-local information transfer.
4. Quantum teleportation *never* involves the transport of matter.
5. Experimental realizations of quantum teleportation have been carried out since 1994. Outside the lab and over longer distances, they were performed e.g. in 2004 (in Vienna, over a distance of 600 m, using a fiber-optic cable in a sewer tunnel crossing the Danube River).[5] Methods for the teleportation of a beam of light including its temporal correlations have been proposed for instance in 2009.[6]

[5] Quantum teleportation is not restricted to the range of some few centimeters or meters; for 'records' see e.g. Xiao-Song Ma et al., 'Quantum teleportation over 143 kms using active feed-forward', *Nature* 489, 269–273 (2012), or Ji-Gang Ren et al., Ground-to-satellite quantum teleportation, *Nature* 549, 70–73 (2017) where quantum teleportation of independent single-photon qubits from a ground observatory to a low-Earth-orbit satellite over distances of up to 1400 km is reported.

[6] C. Noh et al., 'Quantum Teleportation of the Temporal Fluctuations of Light', *Phys. Rev. Lett.* 102, 230501 (2009).

26.4 The Quantum Computer

A quantum computer (QC) operates under the laws of quantum mechanics. In particular, it uses superposition and entanglement of states—principles which do not exist in classical mechanics. Due to this, a QC can (could)[7] carry out a large number of parallel operations (*quantum parallelism*), and solve suitable problems much faster than a classical computer. Although in a measurement, only *one* state is observed, it is nevertheless possible in certain cases to extract global information.

The topic experienced a big boost in 1994, when Peter W. Shor showed that a quantum computer can factorize large integers much faster[8] than a classical computer. However, it appears today (2018) that there is still a long road to a generally-applicable QC. The main problem is decoherence. The processes in a QC are essentially unitary transformations which must not be disturbed (or at least only in a manageable way) or even destroyed due to uncontrolled interactions with the environment.

All in all, this is a very active research area with a correspondingly extensive literature. We shall outline below a few basic ideas.

26.4.1 Qubits, Registers (Basic Concepts)

In classical information theory, the basic unit is the *bit* which can have one of *two* values. The bit is stored in a system that can assume only two states, and the system is *either* in the one *or* in the other state.[9] We call these states $|0\rangle$ and $|1\rangle$ once again.

In contrast, a quantum-mechanical system can be in a superposition $|z\rangle$ of the two states:

$$|z\rangle = a\,|0\rangle + b\,|1\rangle\,; \quad |a|^2 + |b|^2 = 1 \tag{26.13}$$

This system stores not a *bit*, but rather a *quantum bit*, a *qubit* for short.[10] A qubit can be implemented by any system with two states—such as a spin-1/2 quantum object (spin up or spin down), a polarized photon (vertical or horizontal), an atom (excited or not), and so on.

The initially indeterminate value of the system or the qubit is determined by a measurement. We obtain with a probability of $|a|^2$ the state $|0\rangle$, and with $|b|^2$ the state $|1\rangle$. This fact in itself is not remarkably useful. In other words, it is *not* the case

[7] The conditional 'could' is more appropriate insofar that until now (2018), a generally working, large QC exists only on paper.

[8] Under appropriate circumstances, the computation time of the classic computer grows exponentially with the number of digits of N, that of the quantum computer only polynomially. See the later section on the Shor algorithm.

[9] Possible realizations are familiar examples such as the ubiquitous coin with heads and tails, a switch (on/off), etc. Of course, all bi-stable systems are suitable in principle.

[10] Analogously, a linear combination of three states is called a *qutrit*, $a\,|0\rangle + b\,|1\rangle + c\,|2\rangle$.

that we can extract all the information—after the measurement, the system is either in the state $|0\rangle$ or in the state $|1\rangle$. In this sense, the information content of a qubit equals that of a classical bit. However, the superposition principle allows a certain parallelism in the calculations, as we shall see shortly.

Just as in a classical computer, one combines several qubits to give *registers*.[11] A quantum register of n qubits (register of size n or length n) is a state of the 2^n-dimensional product space (Hilbert space); for its basis, we can choose the product states. For a register $|a\rangle \otimes |b\rangle = |ab\rangle$ of two qubits, a possible basis is e.g. $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. If we understand this as a binary notation,[12] then the states are given in decimal notation by $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$. Unlike a classical bit, which can take on only *one* of these values, the qubit states can be superposed. We point out that a register can be entangled.

Example: Suppose we want to store a number between 0 and 7 in a register. For this we need 3 bits (in general, we need n bits to store one of the 2^n numbers between 0 and 2^{n-1}). A classical register would thus store *one* of the following configurations

$$\begin{array}{llll} 0 = (000) & 1 = (001) & 2 = (010) & 3 = (011) \\ 4 = (100) & 5 = (101) & 6 = (110) & 7 = (111)\,. \end{array} \tag{26.14}$$

A system of 3 qubits can occupy the following product states[13]:

$$\begin{array}{llll} 0 : |000\rangle & 1 : |001\rangle & 2 : |010\rangle & 3 : |011\rangle \\ 4 : |100\rangle & 5 : |101\rangle & 6 : |110\rangle & 7 : |111\rangle\,. \end{array} \tag{26.15}$$

Because we can generate superpositions like

$$|q\rangle = \sum_{x,y,z\in\{0,1\}} c_{xyz}\,|xyz\rangle\,, \tag{26.16}$$

one could conclude that the state vector allows us to store the $2^3 = 8$ numbers c_{xyz} at once, and generally 2^N numbers with N qubits.[14] But a measurement gives of course only one of the basis states. Thus, with the coefficients c_{xyz}, we have a remarkable virtual information store at our disposal, but we cannot read it out directly from the system. A measurement yields *one* of the numbers 0 to 7, and not all 8 in one sweep.

A remark on notation: As already indicated, there are different notations for qubits. Let us take as an example three qubits, which are all in the same superposition state[15];

---

[11] For the sake of simplicity, we assume that the quantum objects are distinguishable.

[12] So we have e.g. $10 \mathrel{\hat{=}} 1\cdot 2^1 + 0\cdot 2^0 = 2$ or $1101 \mathrel{\hat{=}} 1\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 = 13$.

[13] We use the abbreviation

$$|a\rangle \otimes |b\rangle \otimes |c\rangle = |abc\rangle$$

[14] For $N = 100$, we would have $2^N \approx 1.27\cdot 10^{30}$.

[15] For the sake of clarity, we leave off indexing: $|0\rangle\,|0\rangle\,|0\rangle \equiv |000\rangle \equiv |0_1 0_2 0_3\rangle$, and so on.

$$|z\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}. \tag{26.17}$$

Performing the multiplications yields:

$$|z\rangle = \frac{|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle}{2\sqrt{2}}. \tag{26.18}$$

This reads in decimal notation:

$$|z\rangle = \frac{|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle}{2\sqrt{2}} = \frac{1}{2\sqrt{2}} \sum_{k=0}^{7} |k\rangle\,. \tag{26.19}$$

The three notations (26.17)–(26.19) all denote exactly the same facts. In general, we have for a product of n qubits

$$|z\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle\,. \tag{26.20}$$

If it is not clear whether a ket is meant in decimal or binary notation, then $|0\rangle$ and $|1\rangle$ may be ambiguous, since it is not clear from the outset whether they are states of a single qubit or a register. This must be determined from context.

26.4.2 Quantum Gates and Quantum Computers

The manipulation of the registers is achieved by *gates*. A quantum gate is a device that acts on certain qubits of a register by means of a specific unitary operation. This means in the context of the following considerations that we can equate a gate with a unitary transformation. A *quantum network* or *quantum circuit* consists of gates which are interconnected in a certain way and which act in a specified time sequence.[16] The gates are connected by *quantum wires*, i.e. by ideal, loss-free and error-free connecting links.

A *quantum computer* is a quantum circuit which changes an input state according to a quantum algorithm[17] and yields the result as output or final state. It is important that the computation be reversible, as it involves only unitary transformations (=gates). The final state is measured as usual (by a projective measurement).

[16] The size of the network corresponds to the number of gates.

[17] An algorithm is a procedure for solving a problem (in finitely many steps).

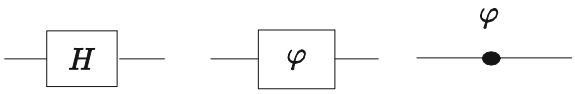

Fig. 26.2 Symbolic representation of the Hadamard gate and two different symbolic representations of the phase shift gate

The charm of the quantum gates is, *inter alia*, that only *three* of them are needed to perform all sorts of computational operations, namely two 1-qubit gates and a 2-qubit gate.[18]

26.4.2.1 1-Qubit Gates

The first 1-qubit gate that we will consider is the *Hadamard gate* or the Hadamard transformation (see also Appendix P, Vol. 2)[19]:

$$H \cong \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{26.21}$$

We obtain (see the exercises):

$$|q\rangle \to H\,|q\rangle = \frac{|1-q\rangle + (-1)^q\,|q\rangle}{\sqrt{2}}; \quad q \in \{0,1\}\,. \tag{26.22}$$

The second 1-qubit gate is the *phase shift gate* (phase shift, phase gate)[20]:

$$\Phi_\varphi \cong \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}, \tag{26.23}$$

or

$$|q\rangle \to \Phi_\varphi\,|q\rangle = e^{iq\varphi}\,|q\rangle\,; \quad q \in \{0,1\}\,. \tag{26.24}$$

These two components, schematically shown in Fig. 26.2, can be combined e.g. in such a way that they transform the state $|0\rangle$ into the general state of one bit (in other words, with these two gates we can construct any unitary 1-qubit operation). We have for example (see the exercises):

[18] We note that for this purpose there are other equivalent ways to choose three different 1 and 2-qubit gates. In addition, one can represent all the operations with *Toffoli gates*, which are 3-qubit gates.

[19] H here always means the Hadamard transformation. Since the Hamiltonian does not occur in this chapter, there is no risk of confusion.

[20] Also called 'rotation'.

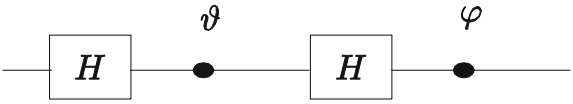

Fig. 26.3 Symbolic representation of the transformation (26.25)

$$|0\rangle \to \Phi_\varphi H \Phi_\vartheta H\,|0\rangle = e^{i\vartheta/2}\left(\cos\frac{\vartheta}{2}\,|0\rangle - i e^{i\varphi}\sin\frac{\vartheta}{2}\,|1\rangle\right). \tag{26.25}$$

Figure 26.3 shows the symbolic representation of the transformation (26.25).

26.4.2.2 2-Qubit Gate

Now one cannot perform all necessary operations with 1-bit gates. On the one hand, this is due to the fact that one wants to generate entangled states, and this requires at least two bits. The other reason is that certain classical operations are not reversible and therefore cannot be directly translated in terms of quantum information,[21] but this is achieved by using gates that process two or more bits.

We therefore introduce *two* qubits, one ($|p\rangle$, control) of length n and another ($|q\rangle$, target) of length m. The control bit remains unchanged, but the target bit is changed by the unitary transformation, in a way which is determined by the control bit[22]:

$$\begin{bmatrix} |p\rangle \\ |q\rangle \end{bmatrix} \to \begin{bmatrix} |p\rangle \\ |q \oplus f(p)\rangle \end{bmatrix}, \tag{26.26}$$

where $\oplus$ in quantum information always denotes the addition modulo 2^n and not (as in vector spaces) the direct sum (see Appendix C, Vol. 2).[23]

A simple and important example is the *controlled NOT gate* (CNOT gate, controlled not, CNOT, also called measuring gate) with $n = m = 1$, $|p, q\rangle \to |p, q \oplus p\rangle$. The symbolic representation is given in Fig. 26.4. Here, the second qubit $|q\rangle$ is changed when the first qubit $|p\rangle$ is in the state $|1\rangle$, otherwise nothing happens; in detail, this reads: $|00\rangle \to |00\rangle$, $|01\rangle \to |01\rangle$, $|10\rangle \to |11\rangle$, $|11\rangle \to |10\rangle$. We see in the target bit the (not uniquely reversible) XOR structure, but together with the control bit, a uniquely reversible unitary transformation results; it reads in matrix form:

[21] As an example, we consider the mod2 sum (=exclusive OR = XOR) $p \oplus q$ with $p, q \in \{0, 1\}$. Obviously this is not a reversible mapping, since we have $0 \oplus 0 = 1 \oplus 1$ and $0 \oplus 1 = 1 \oplus 0$. Similarly, the traditional gates AND and OR are not unitary and therefore are not directly eligible for quantum applications.

[22] This gate is also called a controlled-U gate.

[23] When using the notation $a \oplus b$, the information about n has to come from somewhere else.

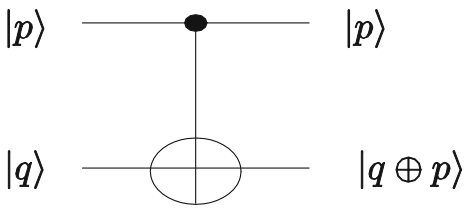

Fig. 26.4 Symbolic representation of the CNOT gate

$$C \cong \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{26.27}$$

If the target bit is in the state $|0\rangle$, we have

$$|p\rangle\,|0\rangle \to |p\rangle\,|p\rangle\,; \quad p \in \{0, 1\}\,. \tag{26.28}$$

This looks at first glance like a copier—but we know that copiers do not exist. In fact, the CNOT gate works as a copier only for $|0\rangle\,|0\rangle$ and $|1\rangle\,|0\rangle$.[24] Arbitrary states are not copied, but are entangled. To see this, we assume that the control bit is a superposition:

$$|p\rangle = a\,|0\rangle + b\,|1\rangle\,; \quad a, b \neq 0. \tag{26.29}$$

It follows that:

$$|p\rangle\,|0\rangle = (a\,|0\rangle + b\,|1\rangle)\,|0\rangle \to a\,|0\rangle\,|0\rangle + b\,|1\rangle\,|1\rangle\,, \tag{26.30}$$

and that is not a copy of the state $|p\rangle$, but rather an entangled state.

Another important operation is the *kickback*, with $m = 1$, while n is not specified. The otherwise arbitrary function f can take on the two values 0 and 1. For $|q\rangle$, we choose the superposition $|q\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Then we have, because of $|0 \oplus f(p)\rangle = |f(p)\rangle$:

$$|p\rangle\,\frac{|0\rangle - |1\rangle}{\sqrt{2}} \to |p\rangle\,\frac{|f(p)\rangle - |1 \oplus f(p)\rangle}{\sqrt{2}} = \begin{cases} |p\rangle\,\frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ |p\rangle\,\frac{|1\rangle - |0\rangle}{\sqrt{2}} \end{cases} \quad \text{for} \quad f(p) = \begin{cases} 0 \\ 1 \end{cases} \tag{26.31}$$

or briefly

$$|p\rangle\,\frac{|0\rangle - |1\rangle}{\sqrt{2}} \to |p\rangle\,(-1)^{f(p)}\,\frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{26.32}$$

The modular addition in the second register leaves it unchanged, apart from the change of sign controlled by p. As the overall result, we have $|p\rangle \to (-1)^{f(p)}\,|p\rangle$.

[24] Copying two (orthogonal) states is indeed allowed; see the section 'quantum copier'.

26.4.3 The Basic Idea of the Quantum Computer

Now that we have discussed some fundamental functions, we briefly describe the basic idea of the QC. There is an input register of N qubits, which are stored in a special state $|\psi\rangle$, namely in

$$|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{n=1}^{N} |\varphi_n\rangle \,. \tag{26.33}$$

The states $|\varphi_n\rangle$ are the state of the product basis; for the case $N = 3$, they are given in (26.15). This input state is now changed into a final state by a controlled sequence of unitary (i.e. reversible) transformations such as H.

We describe this by constructing the tensor product $|\Psi\rangle$ of $|\psi\rangle$ with the state $|\chi\rangle$ of an output register of 2^M qubits:

$$|\Psi\rangle = |\psi \otimes \chi\rangle = \frac{1}{\sqrt{2^N}} \sum_{n} |\varphi_n \otimes \chi\rangle \,. \tag{26.34}$$

The QC is thus essentially a unitary (total) operator U which transforms the system into the entangled state

$$|\Psi\rangle \to \left|\Psi'\right\rangle = U\,|\Psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{n} |\varphi_n \otimes f\,(\varphi_n)\rangle \,. \tag{26.35}$$

Both registers together now simultaneously contain 2^{N+M} values of the pair $(\varphi,\, f\,(\varphi))$.

The result of computations is read out by an (irreversible) measurement process. We thus have available significant virtual information, but cannot obtain it directly from the system, since the measurement returns only *one* couple $|\varphi_k \otimes f\,(\varphi_k)\rangle$.

However, it is possible to get more information from the state (26.35). There are several methods of doing this; we will consider the two simplest in more detail in the following, namely the algorithms of Deutsch and of Grover. After that, we give a brief comment on the Shor algorithm; more details on this topic are found in Appendix S, Vol. 2.

26.4.4 The Deutsch Algorithm

This section has the purpose of illustrating the principle of a quantum computation by means of a toy example. It is a black box (also called *oracle*). We know only that it calculates a (Boolean) function f:{0, 1} → {0, 1, }, but not which of the four possibilities:

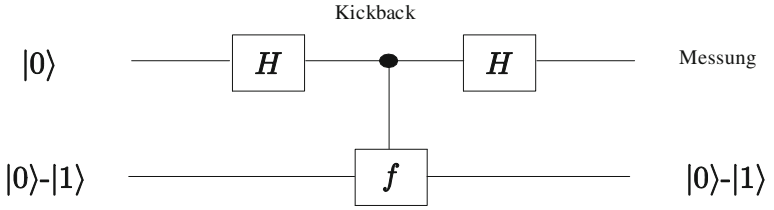

Fig. 26.5 Symbolic representation of the Deutsch algorithm

$$\begin{array}{ll} (1)\ f\,(0)=1; & f(1)=0 \\ (2)\ f\,(0)=0; & f(1)=1 \\ (3)\ f\,(0)=1; & f(1)=1 \\ (4)\ f\,(0)=0; & f(1)=0 \end{array} \tag{26.36}$$

is actually realized. One would like to know if it is one of the last two possibilities or not—in other words, if $f(0)$ and $f(1)$ are different or not.

Without quantum mechanics, we simply have to measure $f(0)$ and $f(1)$ to find the answer. Obviously, we need two measurement procedures. With quantum mechanics, we need only *one* measuring process.

For this purpose, we use the experimental setup shown in Fig. 26.5. The salient point is the use of the kickback transformation (26.32). We start with the state $|0\rangle\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ and transform as follows:

$$\begin{aligned} |0\rangle\,\frac{|0\rangle-|1\rangle}{\sqrt{2}} &\underset{\text{Hadamard}}{\rightarrow} \frac{|0\rangle+|1\rangle}{\sqrt{2}}\,\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\ &\underset{\text{kickback}}{\rightarrow} \frac{(-1)^{f(0)}\,|0\rangle+(-1)^{f(1)}\,|1\rangle}{\sqrt{2}}\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}. \end{aligned} \tag{26.37}$$

The second bit has done its duty in the transfer of f and we omit it now. It follows for the second Hadamard gate that:

$$\begin{aligned} &\frac{(-1)^{f(0)}\,|0\rangle+(-1)^{f(1)}\,|1\rangle}{\sqrt{2}} \\ &\underset{\text{Hadamard}}{\rightarrow} \frac{\left[(-1)^{f(0)}+(-1)^{f(1)}\right]|0\rangle+\left[(-1)^{f(0)}-(-1)^{f(1)}\right]|1\rangle}{2}. \end{aligned} \tag{26.38}$$

It is immediately obvious that for $f(0)=f(1)$, we measure $|0\rangle$; otherwise, $|1\rangle$. Thus, quantum mechanics answers the question (i.e. $f(0)=f(1)$—yes or no?) with *one* measurement, while the classical approach requires *two*.

This example is an improved version (1998) of the first quantum algorithm which was presented by David Deutsch in 1985. It shows that quantum calculations can run much faster than classical ones, provided one asks the right questions. In this toy example, we gain only a factor of 2. For other algorithms, however, the calculating

time depends polynomially on a system variable (e.g. the size of the system) for the quantum computer and exponentially for the classical computer, as is the case for the extension of this toy example to n inputs $|0\rangle$.

26.4.5 Grover's Search Algorithm

This algorithm, proposed by Lov K. Grover in 1996, performs a search in an unstructured data base. The problem can be thought of as the inverse phone book problem, i.e. looking for a name if only the phone number is known (where the phone book with N entries is arranged alphabetically, of course). Classically, one has to check each entry one by one; to find the right name, one has to make $\frac{N}{2}$ attempts on the average. In contrast, the Grover algorithm needs $\sim\sqrt{N}$ steps.

We assume that each number appears only once and that there are 2^n entries. We can describe the phone book with respect to our search by a function $f(k)$ that vanishes for all arguments except the desired one (κ):

$$f(k) = \delta_{k\kappa};\ k = 0, 1, \ldots, N-1; \quad N = 2^n; \quad 0 \leq \kappa \leq N-1. \tag{26.39}$$

$f(k)$ is again a black box (oracle). The position κ is not known and has to be identified.

We use two registers and the kickback discussed above. The first register is of length N, the second is in the state $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Since this is also the output state of the second register for the kickback, we consider in the following only the first register. Here, it holds that:

$$|k\rangle \to (-1)^{f(k)} |k\rangle\,, \tag{26.40}$$

where $\{|k\rangle\}$ is a CONS of dimension N. Because of (26.39), this means that all the states remain unchanged, except for the desired state $|\kappa\rangle$, where we have $|\kappa\rangle \to -|\kappa\rangle$. Due to this, the transformation can be written as (see the exercises):

$$U_\kappa = 1 - 2\,|\kappa\rangle\,\langle\kappa|\,. \tag{26.41}$$

Note that the last equation is just a different notation for the kickback. It does not mean that we know the value of κ at this point.

The initial state for the algorithm is a normalized equally-weighted superposition of all states

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle\,; \quad \langle s\,|s\rangle = 1. \tag{26.42}$$

Using this state, we define an operator

$$U_s = 2\,|s\rangle\,\langle s| - 1. \tag{26.43}$$

The Grover algorithm consists of a (repeated) application of $U_s U_\kappa$ to the initial state. We want to interpret this algorithm in the following in a geometrical way; the algebraic point of view can be found in Appendix R, Vol. 2.

The geometrical analogy is based on the fact that the two vectors $|\kappa\rangle$ and $|s\rangle$ define a plane. The two vectors are normalized, but due to

$$\langle \kappa \, | s \rangle = \frac{1}{\sqrt{N}} \tag{26.44}$$

they are not orthogonal (although 'almost' orthogonal for large N). We denote the vector lying in this plane which is orthogonal to $|\kappa\rangle$ as $\left|k'\right\rangle$. The angle between $|s\rangle$ and $\left|k'\right\rangle$ is φ. Because of $\langle \kappa \, | s \rangle = \frac{1}{\sqrt{N}} = \cos\left(\frac{\pi}{2} - \varphi\right) = \sin\varphi$, we have:

$$\varphi = \arcsin \frac{1}{\sqrt{N}}. \tag{26.45}$$

The two operators U_κ and U_s have a simple geometrical interpretation—they describe reflections (see the exercises). U_κ leaves the components of $|s\rangle$ which are orthogonal to $|\kappa\rangle$ unchanged, and reverses the sign of the $|\kappa\rangle$-component of $|s\rangle$. In the end, it is therefore a reflection around $\left|k'\right\rangle$. Analogously, the operator $U_s = 2\,|s\rangle\,\langle s| - 1$ produces a reflection in $|s\rangle$. The transformed vectors remain in the plane spanned by $|\kappa\rangle$ and $|s\rangle$.

If we apply U_κ to $|s\rangle$, we get a vector $\left|s'\right\rangle$ reflected at $\left|k'\right\rangle$, and this vector is transformed into $\left|s''\right\rangle$ by U_s. In sum we have the result that $U_s U_\kappa$ turns the vector $|s\rangle$ by the angle 2φ into the direction of $|\kappa\rangle$; see Fig. 26.6. By repeated application of $U_s U_\kappa$, we can rotate the initial state $|s\rangle$ closer and closer to $|\kappa\rangle$. This means that with each step, the relative amplitude of the $|\kappa\rangle$ component of $|s\rangle$ increases, and after a suitable number of steps a measurement we will almost certainly obtain the desired state $|\kappa\rangle$.

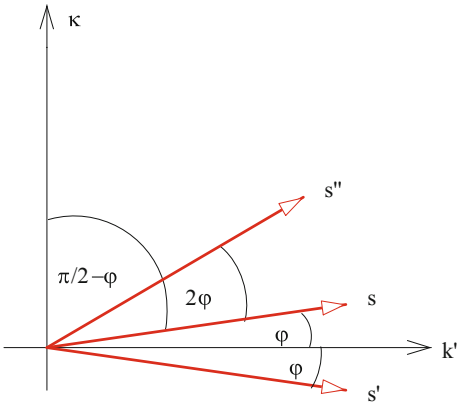

Fig. 26.6 Geometrical interpretation of the Grover algorithm

This behavior is called *amplitude amplification*. A superposition of states is thus changed by this unitary transformation in such a way that the amplitude of the state sought is particularly large. This state is then measured with a particularly high probability, especially if the amplification process is applied several times or iteratively; while wrong answers will cancel out. By the way, amplitude amplification is used also in Shor's algorithm.

The appropriate number of steps is given by the consideration that $\frac{\pi}{2} - \varphi$ must be in the vicinity of an integer multiple of 2φ, i.e.

$$\frac{\pi}{2} - \varphi \approx 2\varphi \cdot m \quad \text{or} \quad m \approx \frac{\pi}{4\varphi} - \frac{1}{2}. \tag{26.46}$$

With (26.45), we have for sufficiently large N:

$$m \approx \frac{\pi}{4}\sqrt{N}. \tag{26.47}$$

This also follows from the algebraic considerations (see Appendix R, Vol. 2), which lead to the formulation

$$\langle \kappa | \left(U_s U_\kappa\right)^m |s\rangle = \sin\left(2m+1\right)\varphi. \tag{26.48}$$

Thus we need $O(\sqrt{N})$ steps to answer (almost with certainty) the initial question. With this small number of steps (classical methods require $O(N)$ steps), the Grover algorithm is optimal in the sense that there is no algorithm that requires fewer than $O(\sqrt{N})$ steps.

26.4.6 Shor's Algorithm

This algorithm, proposed by Peter W. Shor in 1994, can be used for the factorization of very large numbers into prime factors. The problem is that while it is trivial to multiply two numbers, no matter how large, it is very time-consuming and far from trivial to find the prime factors of a given very large number. It is quickly computed that $179424673 \cdot 373587883$ gives the number $N = 67030883744037259$; but is is very hard to find the factors of a given N (try it yourself with 268898680104636581 or 170699960169639253, remembering that these numbers are small in this context). This fact is used for encryption (RSA algorithm). The basic idea is essentially that only Alice (sender) and Bob (receiver) know the prime factorization of a very large number $N = N_1 \cdot N_2$, whereas N may be known to the public. The security of the system depends crucially on the fact that the factorization of N takes so much time even with the fastest computers that it is a de facto insolvable problem (the computation times would be of the order of thousands or millions of years or more, depending on the number of digits of N).

The Shor algorithm is now a way to perform exactly this factorization relatively quickly. The algorithm is divided into a classical and a quantum-mechanical part. Similar to Grover's algorithm, it works on the basis of amplitude amplification. One possibility is to compute a Fourier transform of the state $\left|\Psi'\right\rangle$ as in

$$|\Psi\rangle \rightarrow \left|\Psi'\right\rangle = U\,|\Psi\rangle = \frac{1}{\sqrt{2^N}} \sum_n |\varphi_n \otimes f\,(\varphi_n)\rangle\,. \tag{26.49}$$

From the spectrum, one can infer the period of $f(\varphi_n)$, and from this period finally the prime factors. An algorithm running on a classical computer needs $O(N)$ steps to determine the period, while this figure is $O(\ln^3 N)$ for a quantum computer. It is this tremendous reduction in computation time which makes the Shor algorithm such a valuable tool. Since the detailed calculation is quite lengthy, we relegate it to Appendix S, Vol. 2.

26.4.7 On The Construction of Real Quantum Computers

As said above, quantum computing is a very active research area with a wide variety of issues, both in hardware and in software. The attempt to give an overview of the current state of affairs must be incomplete and will be quickly obsolete. Thus, a few remarks will be enough.

In the last years, there were quite often reports on quantum computers operating with different numbers of qubits. But apparently, most of them were special machines with very limited possibilities, designed for particular problems, and not every researcher was convinced that these devices kept their promises.

Note that there are marked and big differences between today's QC's and 'normal' PC's. For example, current QC's can usually not be programmed and reprogrammed, as is the case with PC's. Indeed, the first reprogrammable QC (operating with 5 qubits) was announced in 2016.[25] In addition, today's QC's are not cute devices to be comfortably placed on your lap. Most of them are big machines and have be cooled down elaborately to quite low temperatures (a few mK). In 2012 a QC was announced which was functional at room temperature, but it was operating with just 2 qubits, see P.C. Maurer et al., Room-Temperature Quantum Bit Memory Exceeding One Second, *Science* 336, 1283–1286, DOI: 10.1126/science.1220513 (08 june 2012).

The progress in the development of quantum computers is not as fast as hoped, although worldwide not only academic institutions, but also big players of the IT-military-industrial complex are engaged in research, as Google, Microsoft, IBM, NASA, to name a few. Despite all the efforts of the last years, the 'general-purpose QC for everybody' seems to be still far away, and the question remains whether it will be possible one day to produce 'real' quantum computers, perhaps even in

[25] S. Debnath et al., 'Demonstration of a small programmable quantum computer with atomic qubits'; *Nature* 536, 63–66 (04 August 2016); doi:10.1038/nature18648.

mass production. Opinions are divided on this issue, ranging from very pessimistic to very optimistic. The main problem is decoherence. That is, the quantum parallelism requires a unitary evolution, and this implies that uncontrollable interactions with the environment must be eliminated.

The experimental difficulties are obvious. A large number of quantum gates has to be 'wired' to each other and must be insulated from the environment as well as possible. Of course, such interactions cannot be eliminated completely. The task is therefore to minimize the perturbations induced by the environment and to offset the unavoidable errors by suitable correction algorithms. Thus, one needs good ideas on how to correct errors during a calculation, and how to restore superposition states.

It seems that quantum computers will not replace the classical computer by any means - and they will probably look very different. Which 'hardware' will ultimately prevail is not yet clear at the moment. Candidates for qubits presently include, among others, ion traps, molecular nuclear spins, entangled atoms, quantum dots in semiconductors, or spins of single atoms embedded in a semiconductor. More recent developments are photon–photon quantum gates, gates between a flying optical photon and a single trapped atom, and silicon quantum gates.[26]

Also on the theoretical side there are as yet unanswered questions. For example: Is there a general class of tasks which a quantum computer can solve better than a classical computer—or is it just a question of individual cases (such as the Shor algorithm), which have been found, at least so far, more or less by chance?

Concerning practical applications, there are a few calculations of difficult physical problems using QC's, for instance the first high-energy physics simulation on a quantum computer (2015, creation of pairs of particles and antiparticles) or real-time dynamics of lattice gauge theories.[27]

A further field of activity is the simulation of QC's (i.e., quantum simulators) with the help of supercomputers. The aim is to develop and to test algorithms suitable for 'real' QC's. In 2017, the Jülich Supercomputing Centre has announced a new world record by simulating a QC with 46 qubits.[28]

For those who want to gain experience with quantum devices, there are some interactive home pages. Among others, IBM provides a page where one can do own calculations, for instance write and run quantum algorithms on a real QC.[29]

---

[26] See e.g. D. M. Zajac et al., 'Quantum CNOT Gate for Spins in Silicon', *Science* 07 December 2017. DOI: 10.1126/science.aap5965.

[27] E.A. Martinez et al., 'Real-time dynamics of lattice gauge theories with a few-qubit quantum computer', *Nature* 534, 516–519 (23 June 2016), doi:10.1038/nature18318.

[28] http://www.fz-juelich.de/SharedDocs/Pressemitteilungen/UK/EN/2017/2017-12-15-world-record-juelich-researchers-simulate-quantum-computer.html?nn=897918.

[29] https://www.research.ibm.com/ibm-q/ as of december 2017.

26.5 Exercises

1. Above, it was proposed that you yourself try to find the prime factorization of 268898680104636581 and 170699960169639253. Did you find it?
2. Pauli matrices and qubits:

   (a) How do the Pauli matrices act on the qubit states $|0\rangle$ and $|1\rangle$?
   (b) How do the Pauli matrices act on the qubit state $|\varphi\rangle = c\,|0\rangle + d\,|1\rangle$?

3. Calculate the full expression containing N terms:

$$|z\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{26.50}$$

4. Show that:

$$|q\rangle \to H\,|q\rangle = \frac{|1-q\rangle + (-1)^q\,|q\rangle}{\sqrt{2}}; \quad q \in \{0,1\}, \tag{26.51}$$

   where H is the Hadamard matrix.
5. Calculate explicitly

$$\Phi_\varphi H \Phi_\vartheta H \tag{26.52}$$

   where H is the Hadamard transformation and Φ the phase shifter.
6. Kickback and Grover's algorithm: Given that:

$$f(k) = \delta_{k\kappa}; \quad k = 0, 1, \ldots, d-1; \quad d = 2^n; \quad 0 \le \kappa \le d-1. \tag{26.53}$$

   The effect of the kickback may be written as:

$$|k\rangle \to (-1)^{f(k)}\,|k\rangle \quad \text{or} \quad U_\kappa\,|k\rangle = (-1)^{f(k)}\,|k\rangle \tag{26.54}$$

   where $\{|k\rangle\}$ is a CONS. Show that

$$U_\kappa = 1 - 2\,|\kappa\rangle\,\langle\kappa|\,. \tag{26.55}$$

7. Given the normalized states $|x\rangle$ and $|y\rangle$, with $\langle x\ |y\rangle = 0$; show that the operator $U = 2\,|x\rangle\,\langle x| - 1$ describes a reflection at $|x\rangle$ and $-U$ a reflection at $|y\rangle$.
8. Given the normalized state

$$|\psi\rangle = \sum\nolimits_{n=1}^{N} c_n\,|\varphi_n\rangle \quad \text{with} \quad \langle\varphi_n\ |\varphi_m\rangle = \delta_{nm}. \tag{26.56}$$

   The probability of measuring the state $|\varphi_k\rangle$ is thus given by $|c_k|^2$. We selectively amplify the amplitude $c_m \neq 0$ by the following unitary transformation U (see Fig. 26.7):

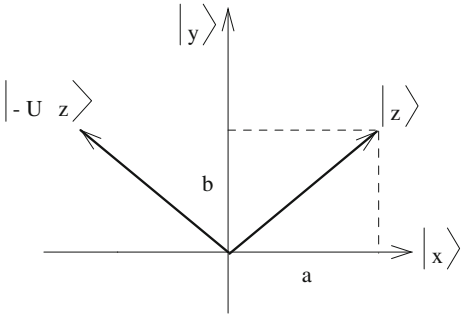

Fig. 26.7 Effect of $-U = 1 - 2\,|x\rangle\,\langle x|$ on a general state

$$U : c_n \to \alpha c_n \text{ for } n \neq m; \quad c_m \to \beta c_m \text{ for } n = m \tag{26.57}$$

with suitably chosen α, β.

(a) How are α and β connected?
(b) How do the measurement probabilities behave under a k-fold iteration of U?
(c) Specialize to the case of an initially uniform distribution $c_n = \frac{1}{\sqrt{N}}$ and $\alpha = \frac{1}{4}$. How often does one have to iterate in order to measure the state m with a probability of $w > 1 - 10^{-6}$ (assuming $N \gg 1$)?