81. Quantum Information

For many years atomic physicists had used quantum mechanics very successfully to calculate energy levels, cross sections and other practical quantities, and for the most part, left the philosophical issues of interpretation to others. But after the work of Bell in the 1960's showed that the peculiarly nonlocal nature of quantum correlations could be tested in the lab, a number of atomic physicists turned to the experimental study of entanglement and quantum measurement. A second phase began at the start of the 1990's when it was realized that correlations and quantum superpositions could be exploited in quantum information processing and secure communication. This has led to an explosive growth of the subject over the past 10 years, fuelled by the long-term prospects of quantum computing and the nearer goal of quantum cryptography. We review some of these developments in this chapter.

Quantum information theory is regarded as a mainly mathematics-based subject area which straddles the fields of theoretical physics (quantum mechanics and statistics), mathematics, and theoretical computer science. Its success stems from the introduction of novel methods into both physics and mathematics.

The fundamental quantity and resource in many applications in quantum information processing is quantum-mechanical entanglement between spatially separated subsystems. Entanglement is a purely quantum-mechanical effect and has led to numerous speculations about the validity of quantum mechanics itself for its apparent paradoxical implications. Most, if not all, of these difficulties have been resolved and can be mostly attributed to the simple fact that paradoxical behaviour is incompatible with common sense or everyday experience. This initial upsetting seems to be common to all revolutionary theories and has occurred most notably in Einstein's theory of relativity [81.1].

These quantum-mechanical correlations or entanglements have numerous applications in quantum cryptography [or rather quantum key distribution (QKD)], quantum communication, dense coding, and act as the main resource in quantum computing. We will briefly touch upon some mathematical issues concerning separability, quantification of entanglement and channel capacities before describing how quantum key distribution, teleportation and dense coding work. After that, a brief discussion of single-qubit and two-qubit quantum gates follows before we describe the simplest quantum algorithms. The issues of error correction and fault tolerant computation as well as DiVincenzo's checklist (which any realization should satisfy) provide the background for the discussion of some physical implementations.

We are acutely aware of the fact that we can give only a brief introduction into what has become a major field of investigation over the last decade. There are already a number of review articles and textbooks on the market that cover the vast literature on this emerging subject. Amongst those are the first quantum computing compendium by *Gruska* [81.2] and the quantum information textbooks by *Nielsen* and *Chuang* [81.3] and *Stolze* and *Suter* [81.4]. A regularly updated annotated bibliography on this subject, compiled by *Cabello*, forms an invaluable resource for those interested in the subject of this chapter [81.5].

81.1 Quantifying Information

As already noted, entanglement comes about if a quantum-mechanical system can be divided into several parts. As an example, consider a two-photon emission process from a spin-zero particle by which two photons escape in opposite directions. Given that the photons are spin-one particles, their spin projections onto some axis must be mutually opposite. As there is no prior information about the actual orientation of the spin, the part of the photon wave function associated with the spin degree is therefore

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right) . \qquad (81.1)$$

The striking feature of this type of quantum state is that it describes correlations of two spatially separated particles. If the polarization state of one photon is measured, the state of the other particle, which can be far away, is then instantly predetermined. These (nonlocal) correlations that exist between the particles are of purely quantum origin and are called entanglement. Note, however, that no information can be transmitted faster than the speed of light with this type of set up because the (classical) information concerning the measurement result on one particle needs to be transmitted via a necessarily causal classical channel.

The issue of nonlocality has been seen as a vital part in understanding of the foundations of quantum mechanics itself (Chapt. 80). In 1935, *Einstein*, *Podolsky*, and *Rosen* argued on the basis of entangled states that quantum mechanics is incomplete [81.6]. They were most concerned about the existence of elements of reality within strongly correlated quantum systems and initiated the debate on quantum nonlocality. The non-existence of so-called local hidden variable theories for the description of states like (81.1) was finally demonstrated by *Bell* [81.7]. He showed that maximally entangled states violate certain inequalities (now called Bell's inequalities) which local hidden variable models would have obeyed. Later experiments showed the correctness of Bell's demonstration [81.8].

In classical information theory, the unit of information is called a bit, which can be defined as the amount of information contained in a yes–no question. As a matter of fact, 'bit' is the abbreviation for 'binary digit' and refers to Boolean algebra in which the allowed states of a system are the logical 0 and the logical 1. Therefore, by abuse of language, one bit (as a unit) is the information carried by one bit (as a binary digit) [81.9].

In quantum mechanics, however, due to its inherent linearity, two 'quantum bits' (qubits for short) can be in superpositions of the logical states $|01\rangle$ and $|10\rangle$, or $|\uparrow\downarrow\rangle$ and $|\downarrow\uparrow\rangle$, as in the example above. This typical example of an entangled state shows that quantifying the amount of information contained in a quantum state is different from what is known in classical information theory because of the superposition property. The very same linearity prohibits us from copying an arbitrary quantum state. This effect is known as the No-cloning theorem [81.10]. However, universal copying machines can be constructed within the constraints of quantum mechanics [81.11].

81.1.1 Separability Criterion

From the above it is clear that entangled states play a major role in defining the differences between classical and quantum information. Let us begin by asking under which circumstances a particular given quantum state is entangled or not. For this, we need to give a criterion which allows one to decide this crucial question. Consider a bipartite quantum state, i. e., a state which is decomposed into two distinct, albeit possibly correlated, subsystems A and B. Note that these subsystems themselves might consist of ensembles of particles, in which case we are looking at a bipartite cut through the whole system. Then we say that a bipartite state is not entangled or separable if its density operator can be written as a convex combination of tensor product states, viz.

$$\hat{\varrho} = \sum_i p_i \hat{\varrho}_A^i \otimes \hat{\varrho}_B^i \,, \qquad \sum_i p_i = 1 \,. \tag{81.2}$$

The range of summation in (81.2) is limited by a theorem due to Caratheodory which states that every point in a convex set can be reached by suitable convex combinations of its extreme points. All states that cannot be written in the form of (81.2) are said to be entangled. Note that the set of separable states form a convex subset of the convex set of all possible states.

We will now give a simple criterion which decides whether a given state is actually separable or not. For this, one notes that by transposing the part of the density operator associated with the subsystem B, an operation which is called partial transposition, the resulting operator will not necessarily stay positive. However, if the density operator is separable, then its partial transpose is again a positive operator, and hence is a valid density operator. This condition of a state possessing a positive partial transpose is a necessary separability criterion [81.12] but sufficient only in the case of density matrices having Hilbert space dimensions 2×2 or 2×3 [81.13]. In higher-dimensional Hilbert spaces there exist states with positive partial transposes (PPT) which are nevertheless inseparable. This phenomenon is called bound entanglement [81.14].

Because of the convexity of the set of separable states, one can construct an operator (a hyperplane) $\hat{W}$ that separates an entangled state from the disentangled states,

$$\begin{aligned} &\operatorname{tr}\left(\hat{W}\hat{\varrho}_{AB}\right) < 0 \Leftrightarrow \hat{\varrho}_{AB} \text{ inseparable} \,, \\ &\operatorname{tr}\left(\hat{W}\hat{\varrho}_{AB}\right) \geq 0 \Leftrightarrow \hat{\varrho}_{AB} \text{ separable} \,. \end{aligned} \tag{81.3}$$

Such an operator is called an entanglement witness [81.15], and its existence is ensured by a consequence of the Hahn–Banach theorem [81.16].

A similar separability criterion can be found for a particularly interesting class of quantum states in infinite-dimensional Hilbert spaces, the Gaussian states. Gaussian states are most frequently encountered in quantum optics. They comprise all coherent, squeezed and thermal states, and combinations of them. Although being infinite-dimensional, these states permit a complete description in terms of their first and second moments. The characteristic function of a single-mode Gaussian state with $\boldsymbol{\lambda}^{\mathrm{T}} = (x, p)$ is given by [81.17]

$$\chi(\boldsymbol{\lambda}) = \exp\left\{ \mathrm{i}\boldsymbol{m}^{\mathrm{T}}\boldsymbol{\lambda} - \frac{1}{4}\boldsymbol{\lambda}^{\mathrm{T}}\boldsymbol{V}\boldsymbol{\lambda} \right\} \,, \tag{81.4}$$

where $\boldsymbol{V}$ is the covariance matrix containing the second moments. A necessary and sufficient criterion for separability of a bipartite Gaussian state is that the partially transposed covariance matrix still possesses positive symplectic eigenvalues [81.18].

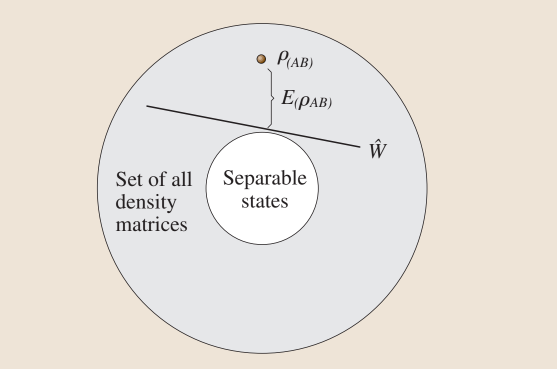

Fig. 81.1 Convex set of bipartite density matrices; the inner convex set represents the separable states. The witness operator $\hat{W}$ forms a hyperplane that separates $\hat{\varrho}_{AB}$ from the set of separable states

81.1.2 Entanglement Measures

Once one has checked for inseparability, the obvious question to ask concerns the amount of entanglement, hence the amount of nonclassical correlations in the given state. For bipartite pure states the answer is unique and given by the von Neumann entropy of one subsystem, viz.,

$$E(|\psi_{AB}\rangle) = S_A(\hat{\varrho}_B) = S_B(\hat{\varrho}_A) \,, \tag{81.5}$$

with $S_A(\hat{\varrho}_B) = -\operatorname{tr}\hat{\varrho}_B \ln \hat{\varrho}_B$ where $\hat{\varrho}_{A(B)} = \operatorname{tr}_{B(A)}|\psi_{AB}\rangle\langle\psi_{AB}|$. The second equality in (81.5) follows from the left-hand side of the Araki–Lieb inequality [81.19]

$$|S_A - S_B| \leq S_{AB} \leq S_A + S_B \tag{81.6}$$

when noting that the entropy of a pure state vanishes. Obviously, since $S_{AB} = 0$, no information can be extracted from the total state, all information is contained in the correlations between the subsystems A and B which are revealed by performing a measurement on one of the subsystems.

For bipartite quantum systems prepared in mixed states the answer is not so obvious. However, some insight can already be gained by looking at the Schmidt decomposition of the state (which, for bipartite states, always exists) [81.20], in particular, the number of elements in the decomposition, named the Schmidt number [81.21].

For a more precise definition of mixed bipartite entanglement, something more is needed. Recall that the set of separable density matrices forms a convex subset of all feasible density matrices. It therefore makes sense to look for a distance-type measure between the given state and the convex hull of product states. Note that the possibility of defining such a measure is provided by the convexity of the separable states and a consequence of the Hahn–Banach theorem [81.16]. Generally, agreement has been reached on what properties any feasible entanglement measure must fulfil [81.22,23]. Let $E(\hat{\varrho}_{AB})$ be a real-valued functional over the tensor-product Hilbert space of bipartite density matrices. If in addition $E(\hat{\varrho}_{AB})$ has the following properties:

1. $E(\hat{\varrho}_{AB}) = 0$ for all separable states;
2. $E(\hat{\varrho}_{AB})$ is invariant under local unitary transformations, viz., $E\big[\big(\hat{U}_A \otimes \hat{U}_B\big)\hat{\varrho}_{AB}\big(\hat{U}_A^\dagger \otimes \hat{U}_B^\dagger\big)\big] = E(\hat{\varrho}_{AB})$;
3. $E(\hat{\varrho}_{AB})$ is non-increasing under general local operations assisted by classical communication, viz., $E\big(\sum_i \hat{V}_A^i \otimes \hat{W}_B^i \hat{\varrho}_{AB} \hat{V}_A^{i\dagger} \hat{W}_B^{i\dagger}\big) \leq E(\hat{\varrho}_{AB})$;
4. $E(\hat{\varrho}_{AB})$ reduces to the reduced von Neumann entropy for pure states,

then $E(\hat{\varrho}_{AB})$ is called an entanglement measure.

Important examples of widely used entanglement measures are the entanglement of formation [81.24]

$$E_{\mathrm{F}}(\varrho_{AB}) = \min_{\hat{\varrho}_{AB}=\sum_i p_i|\psi_i\rangle\langle\psi_i|} \sum_i p_i E(|\psi_i\rangle)\,, \quad (81.7)$$

and the relative entropy of entanglement [81.22]

$$E_{\mathrm{R}}(\hat{\varrho}_{AB}) = \min_{\hat{\sigma}=\sum_i p_i \hat{\sigma}_i^A \otimes \hat{\sigma}_i^B} \operatorname{tr}\left[\hat{\varrho}_{AB}(\ln\hat{\varrho}_{AB} - \ln\hat{\sigma})\right]\,. \quad (81.8)$$

In general, both of these measures are hard to evaluate. Analytical formulas are known only in special cases. For qubits, the entanglement of formation is also a monotonic function of the concurrence [81.25]. The definition of the entanglement of formation, (81.7), can also be extended to cover Gaussian states [81.26].

The number of singlets, i. e., states of the form (81.1), that can be distilled from an ensemble of non-maximally entangled states is called the entanglement of distillation [81.27]. The entanglement of formation and the entanglement of distillation differ by the amount of bound entanglement (Sect. 81.1.1).

In some instances, when it is not necessary to comply with all of the above properties of entanglement measures, other quantities can be used to assess the entanglement content of a bipartite state. Particularly useful is the logarithmic negativity [81.28]

$$E_N(\hat{\varrho}_{AB}) = \log_2 \left\|\hat{\varrho}_{AB}^{\mathrm{P.T.}}\right\|_1\,, \quad (81.9)$$

where $\|\cdot\|_1$ denotes the trace norm and $\hat{\varrho}_{AB}^{\mathrm{P.T.}}$ the partial transpose of $\hat{\varrho}_{AB}$. This measure is often used in connection with Gaussian states.

In close analogy to classical information theory, the amount of nonclassical correlations is measured in ebits when one computes entropies with the dual logarithm ($\log_2$). For example, a pure state with state vector

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (81.10)$$

in an abstract two-particle Hilbert space spanned by the basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ contains 1 ebit of entanglement. It is also a maximally entangled state associated with this Hilbert space since the von Neumann entropy of any state in a Hilbert space of dimension N is bounded from above by $\log_2 \dim N$.

We have concentrated here on bipartite entanglement. The extension to multipartite systems is by no means trivial and much remains to be done on this subject [81.29].

81.2 Simple Quantum Protocols

In this section we describe the historically first and simplest quantum protocols – quantum key distribution, quantum teleportation, and super-dense coding – that make use of inherently 'quantum' properties of quantum-mechanical systems. These are either entanglement or, in the case of the simplest version of quantum key distribution, properties of the quantum-mechanical measurement process. We should mention here the pioneering work of Holevo [81.30] who showed how there are fundamental limits on the amount of information that can be extracted by measurements. The application of his ideas to channel capacity and communication [81.31] are well described in [81.3] and space limitations prevent us from elaborating on it in this chapter.

81.2.1 Quantum Key Distribution

Historically, the earliest protocol that used quantum-mechanical features in order to realize some specific task that could not have been performed classically was a protocol for secure distribution of a key in cryptography, known as the BB84-protocol after its inventors *Bennett* and *Brassard* and the year of its invention [81.32]. Although it is commonly referred to as the first example of quantum information processing, it does not make use of entanglement which was only done some years later, by *Ekert* [81.33].

The BB84 protocol works in the following way. The sender A prepares a random sequence (or string) of single photons in a polarization state which is chosen out of a set of four basis states, horizontally and vertically (H and V) polarized, and 45° and 135° (L and R) polarized. In each of the two basis sets $\{H, V\}$, $\{L, R\}$ one of the states is used to encode the logical value 0 (say in H and L) and the other states encode the logical value 1 (V and R). The random sequence is sent to the receiver B who performs measurements on the sequence of signals by randomly choosing analogous basis states. The result will be another string of 0's and 1's that generically does not coincide completely with the original string. To rectify this problem, sender and receiver communicate over a classical public channel where the sender announces the sequence of basis sets in which the photon states were prepared. The receiver compares its sequence of randomly chosen basis states with the announced string and keeps all measurement results for which the choice of basis had been the same. In that way a common secret key is established (Table 81.1).

The security against eavesdropping of this simple protocol comes from the fact that even by knowing the measurement basis (say $\{H, V\}$) no information has been revealed about the choice of the actual bit value (H or V). Hence, it is the quantum-mechanical measurement process itself that provides security of the protocol. The first quantum key distribution experiments were reported in [81.34]. However, imperfections in the generation and detection of photons, transmission losses and polarization drift causes an actual experimental realization to be far from ideal. In practise, encodings other than polarization may be used (for example a time-binned interferometric basis [81.35]). Despite these error sources, unconditionally secure quantum key distribution can be [81.36] and has been achieved [81.37]. Some fiber-based systems have reached distances of more than 100 km [81.38], but discussions of their security continue. For a review of theoretical and experimental aspects of quantum cryptography, see [81.39].

Table 81.1 BB84 protocol for secret key distribution. The sender A sends information encoded in either of two basis sets. The receiver B randomly chooses a measurement basis which is publicly communicated. For those cases when sender and receiver chose the same basis, the receiver's measurement yields a secure bit

Sender A	↗	↑	↘	→	↗	↑	→
Receiver B	+	×	×	+	×	×	+
Key			1	1	0		1

81.2.2 Quantum Teleportation

An important utilization of entanglement as a necessary resource can be found in what is commonly known as quantum teleportation. The task of teleportation is to transmit the complete information of an arbitrary unknown quantum state to a spatially different location with the aim of re-creating it. The simplest and obvious way to perform this task would be to take the quantum object which is prepared in the original state and physically transport it to a different location. But sometimes this is not possible because for example an ion needs to be stored in a trap and cannot be moved. The next obvious thing to do would be to measure the quantum state and to re-create it at a different position using the classical information obtained during the measurement. However, single measurements on a quantum system yield only partial information and multiple measurements on many identically prepared copies would have to be performed.

The protocol, which was originally proposed in [81.40] for qubits and later generalized to states in infinite-dimensional Hilbert spaces in [81.41], makes use of the existence of maximally entangled states. Let the unknown quantum state which is to be teleported be a qubit superposition state of the form

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle\ , \quad |\alpha|^2 + |\beta|^2 = 1\ . \tag{81.11}$$

Then one prepares a maximally entangled state of the form (81.10) which is one of the four so-called Bell states defined by

$$\begin{aligned} |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right)\ , \\ |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right)\ . \end{aligned} \tag{81.12}$$

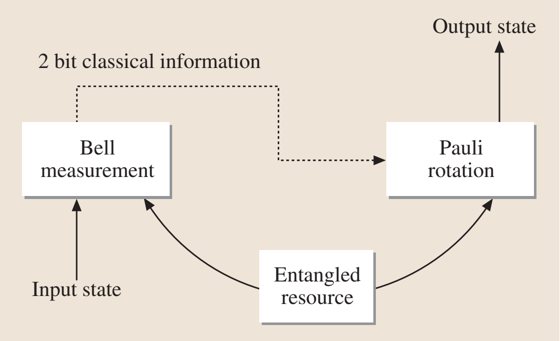

Fig. 81.2 Schematic outline of an ideal teleportation protocol

We then form the tensor product state $|\psi\rangle|\Psi^+\rangle$ as

$$
\begin{aligned}
|\psi_A\rangle|\Psi^+_{BC}\rangle &= \frac{\alpha}{\sqrt{2}}(|0_A 0_B 1_C\rangle + |0_A 1_B 0_C\rangle)\\
&\quad + \frac{\beta}{\sqrt{2}}(|1_A 0_B 1_C\rangle + |1_A 1_B 0_C\rangle)\\
&= \frac{1}{2}\Big[(\alpha|0_C\rangle + \beta|1_C\rangle)\big|\Psi^+_{AB}\big\rangle\\
&\quad + (\alpha|0_C\rangle - \beta|1_C\rangle)\big|\Psi^-_{AB}\big\rangle\\
&\quad + (\alpha|1_C\rangle + \beta|0_C\rangle)\big|\Phi^+_{AB}\big\rangle\\
&\quad + (\alpha|1_C\rangle - \beta|1_C\rangle)\big|\Phi^-_{AB}\big\rangle\Big]\,, \qquad (81.13)
\end{aligned}
$$

where we have explicitly indexed the relevant subsystems. After performing a joint measurement on subsystems A and B in the Bell basis (this is called a Bell-state measurement [81.42]) one obtains one of four possible results. If the measurement result was $|\Psi^+\rangle$, then the subsystem C is indeed prepared in the original unknown quantum state $|\psi\rangle$, hence the state has been 'teleported' from subsystem A to C. For all other measurement results the outcome is not exactly the same quantum state as intended, but the difference is just a unitary transformation which is uniquely determined by the outcome of the Bell measurement. For example, measuring $|\Psi^-\rangle$ means one has to perform a $\hat{\sigma}_z$-operation that flips the sign of the state $|1\rangle$, whereas on obtaining $|\Phi^+\rangle$ or $|\Phi^-\rangle$ the operations to be applied have to be $\hat{\sigma}_x$ or $\hat{\sigma}_z\hat{\sigma}_x$, respectively.

Note that this quantum teleportation protocol works with perfect fidelity only if a maximally entangled state has been used, i. e., a state containing 1 ebit of quantum information. In the course of the Bell measurement, the quantum information is used up, and two classical bits of information (the measurement result) have to be communicated to C in order to restore the original quantum state. In this sense, entanglement can be regarded as a resource or 'fuel' for certain tasks in quantum information processing. The first experimental demonstrations of teleportation of qubits were performed in [81.43] and of continuous variables in [81.44]. Recently, a teleportation experiment over 2 km standard telecommunication fibre has been reported [81.45]. A generalization of teleportation is entanglement swapping, in which EPR correlations are established between previously uncorrelated particles by Bell-state measurements [81.46].

81.2.3 Dense Coding

The complementary protocol to teleportation is characterized by the name of (super) dense coding [81.47]. The idea here is to transmit two classical bits of information at the expense of consuming 1 ebit of quantum information. The similarity to teleportation is best seen by noting that if the experimental apparatus of sender and receiver are interchanged and the protocol reversed (Fig. 81.3), then one reduces to the other. The mathematical equivalence of the teleportation and dense coding schemes has been beautifully shown in [81.48]. As in teleportation, sender and receiver initially share a two-particle maximally entangled state, i. e., one of the Bell states defined in (81.12). By acting with one of the four operations $\hat{I}$, $\hat{\sigma}_x$, $\hat{\sigma}_z$, or $\hat{\sigma}_z\hat{\sigma}_x$ on the qubit on the sender's side, the total two-qubit state is again in one of the four Bell states (81.12). Since they are mutually orthogonal to each other, the receiver can tell them apart by measuring in the Bell basis. In that way, two classical bits of information (the information about the single-qubit unitaries) can be transmitted using only a single qubit at a time.

An experiment using entangled photon pairs was reported in [81.49], which demonstrated dense coding in practise.

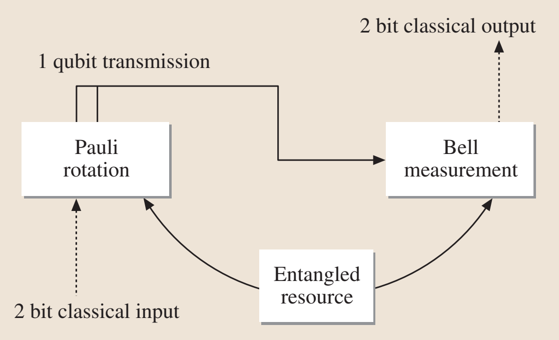

Fig. 81.3 Schematic outline of an ideal superdense coding protocol

http://www.springer.com/978-0-387-20802-2

Springer Handbook of Atomic, Molecular, and Optical
Physics
Drake, G. (Ed.)
2006, LVIII, 1506 p. 288 illus. in color. With CD-ROM.,
Hardcover
ISBN: 978-0-387-20802-2