Quantum entanglement

Ryszard Horodecki

Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland

Paweł Horodecki

Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-952 Gdańsk, Poland

Michał Horodecki

Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland

Karol Horodecki

Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland
and Faculty of Mathematics, Physics and Computer Science, University of Gdańsk, 80-952 Gdańsk, Poland

(Published 17 June 2009)

All our former experience with application of quantum theory seems to say that *what is predicted by quantum formalism must occur in the laboratory*. But the essence of quantum formalism—entanglement, recognized by Einstein, Podolsky, Rosen, and Schrödinger—waited over 70 years to enter laboratories as a new resource as real as energy. This holistic property of compound quantum systems, which involves nonclassical correlations between subsystems, has potential for many quantum processes, including canonical ones: quantum cryptography, quantum teleportation, and dense coding. However, it appears that this new resource is complex and difficult to detect. Although it is usually fragile to the environment, it is robust against conceptual and mathematical tools, the task of which is to decipher its rich structure. This article reviews basic aspects of entanglement including its characterization, detection, distillation, and quantification. In particular, various manifestations of entanglement via Bell inequalities, entropic inequalities, entanglement witnesses, and quantum cryptography are discussed, and some interrelations are pointed out. The basic role of entanglement in quantum communication within a distant laboratory paradigm is stressed, and some peculiarities such as the irreversibility of entanglement manipulations are also discussed including its extremal form—the bound entanglement phenomenon. The basic role of entanglement witnesses in detection of entanglement is emphasized.

DOI: 10.1103/RevModPhys.81.865 PACS number(s): 03.67.−a

CONTENTS

I. INTRODUCTION

Although in 1932 von Neumann had completed the basic elements of a nonrelativistic quantum description of the world, it was Einstein, Podolsky, and Rosen (EPR) and Schrödinger who first recognized a "spooky" feature of quantum machinery which lies at the center of interest of physics of the 21st century (von Neumann, 1932; Einstein *et al.*, 1935). This feature implies the existence of global states of a composite system which cannot be written as a product of the states of individual subsystems. This phenomenon, known as "entanglement," was originally called by Schrödinger "Verschränkung," which underlines the intrinsic order of statistical relations between subsystems of a compound quantum system (Schrödinger, 1935).

Paradoxically, entanglement, which is considered to be the most nonclassical manifestation of quantum formalism, was used by Einstein, Podolsky, and Rosen in their attempt to ascribe values to physical quantities prior to measurement. It was Bell who showed the opposite: it is just entanglement which irrevocably rules out such a possibility.

In 1964 Bell accepted the EPR conclusion—that the quantum description of physical reality is not complete—as a working hypothesis and formalized the EPR idea of deterministic world in terms of the local hidden variable model (LHVM) (Bell, 1964). The latter assumes that (i) measurement results are determined by properties the particles carry prior to, and independent of, the measurement ("realism"); (ii) results obtained at one location are independent of any actions performed at spacelike separation ("locality"); and (iii) the setting of local apparatus is independent of the hidden variables which determine the local results ("free will").[1] Bell proved that the above assumptions impose constraints in the form of the Bell inequalities on statistical correlations in experiments involving bipartite systems. He then showed that the probabilities for the outcomes obtained when some entangled quantum state is suitably measured violate the Bell inequality. In this way entanglement is that feature of quantum formalism which makes it impossible to simulate quantum correlations within any classical formalism.

Greenberger, Horne, and Zeilinger (GHZ) went beyond Bell inequalities showing that entanglement of more than two particles leads to a contradiction with the LHVM for nonstatistical predictions of quantum formalism (Greenberger *et al.*, 1989). Surprisingly, only at the beginning of the 1990s were general theoretical results concerning violation of Bell inequalities obtained (Gisin, 1991; Popescu and Rohrlich, 1992).

The transition of entanglement from gedanken experiments to laboratory began in the mid-1960s (Kocher and Commins, 1967; Freedman and Clauser, 1972). However it was Aspect *et al.* who first performed a convincing test of violation of the Bell inequalities (Aspect *et al.*, 1981, 1982). Since then many experimental tests of quantum formalism against the LHVM have been performed (Ou and Mandel, 1988; Kwiat *et al.*, 1995; Tittel *et al.*, 1998, 1999; Weihs *et al.*, 1998; Rowe *et al.*, 2001; Hasegawa *et al.*, 2004; Bovino, Castagnoli, *et al.*, 2006; Ursin *et al.*, 2007). These experiments strongly confirmed the predictions of the quantum description.[2]

In fact, a fundamental nonclassical aspect of entanglement was recognized in 1935. Inspired by the EPR paper, Schrödinger analyzed some physical consequences of quantum formalism and he noticed that the two-particle EPR state does not allow individual states to be ascribed to the subsystems, implying "entanglement of predictions" for the subsystems. Then he concluded: "Thus one disposes provisionally (until the entanglement is resolved by actual observation) of only a *common* description of the two in that space of higher dimension. This is the reason that knowledge of the individual systems can decline to the scantiest, even to zero, while that of the combined system remains continually maximal. The best possible knowledge of a whole does *not* include the best possible knowledge of its parts—and this is what keeps coming back to haunt us" (Schrödinger, 1935).[3]

This curious aspect of entanglement was long unintelligible, as it was related to the notion of "knowledge" in the quantum context. Only in the second half of the 1990s was it formalized in terms of entropic inequalities based on the von Neumann entropy (Horodecki and Horodecki, 1994; R. Horodecki *et al.*, 1996; Cerf and Adami, 1997).[4] Violation of these inequalities by entangled states is a signature of entanglement of quantum states; however, the physical meaning of this was unclear. An interesting attempt to solve this puzzle in terms of conditional entropy is due to Cerf and Adami (1997). Soon afterward it turned out that the latter, with a minus sign, called *coherent information*, is a fundamental quantity responsible the for capability of transmission of quantum information (Schumacher and Nielsen, 1996; Lloyd, 1997). Transmission is possible exactly in

[1]See, however, Norsen (2007) for derivation of the Bell theorem without involving the notion of "realism" (we thank Giancarlo Ghirardi for pointing out this problem).

[2]However so far, the above experiments suffer from a loophole; see Gill (2003), Brunner *et al.* (2007).

[3]An English translation appears in *Quantum Theory and Measurement*, edited by J. A. Wheeler and W. H. Zurek, Princeton University Press, Princeton, 1983, p. 167.

[4]The other formalization was proposed in terms of majorization relations (Nielsen and Kempe, 2001).

those situations in which "Schrödinger's demon" is "coming to haunt us," i.e., when the entropy of the output system exceeds the entropy of the total system. We mention that this story was given a new twist in terms of a quantum counterpart of the Slepian-Wolf theorem in classical communication (Horodecki, Oppenheiyn, *et al.*, 2005, 2007). In this approach the violation of entropic inequalities implies the existence of *negative quantum information*, which is an "extra" resource for quantum communication. Interestingly, only recently was a direct violation of the entropic inequalities experimentally demonstrated, confirming the breaking of classical statistical order in compound quantum systems (Bovino *et al.*, 2005).

The present-day entanglement theory has its roots in some key discoveries: quantum cryptography with the Bell theorem (Ekert, 1991), quantum dense coding (Bennett and Wiesner, 1992), and quantum teleportation (Bennett *et al.*, 1993),[5] including teleportation of entanglement of EPR pairs (so-called entanglement swapping) (Yurke and Stoler, 1992a, 1992b; Żukowski *et al.*, 1993; Bose *et al.*, 1998). All such effects are based on entanglement and all have been demonstrated in experiments (see Mattle *et al.*, 1996; Bouwmeester *et al.*, 1997; Boschi *et al.*, 1998; Furusawa *et al.*, 1998; Pan *et al.*, 1998; Jennewein *et al.*, 2000; Naik *et al.*, 2000; Tittel *et al.*, 2000). In fact, the above results including the paper on quantum cryptography (BB84) (Bennett and Brassard, 1984) and the idea of quantum computation (Feynman, 1982; Deutsch, 1985; Shor, 1995; Steane, 1996b) were the basis for a new interdisciplinary domain called quantum information (Lo *et al.*, 1999; Bouwmeester *et al.*, 2000; Nielsen and Chuang, 2000; Alber, Beth, *et al.*, 2001; Braunstein and Pati, 2003; Bruß and Leuchs, 2007), which incorporates entanglement as a central notion.

It has become clear that entanglement is not only the subject of philosophical debates, but a new quantum resource for tasks that cannot be performed by means of classical resources (Bennett, 1998). It can be manipulated (Popescu, 1995; Bennett, Brassard, *et al.*, 1996; Bennett, DiVincenzo, Smolin, *et al.*, 1996; Gisin, 1996; Raimond *et al.*, 2001), broadcast (Buzek *et al.*, 1997), controlled, and distributed (Beige *et al.*, 2000; Cirac and Zoller, 2004; Mandilara *et al.*, 2007).

Remarkably, entanglement is a resource which, though it does not carry information itself, can help in such tasks as the reduction of classical communication complexity (Cleve and Buhrman, 1997; Buhrman *et al.*, 2001; Brukner *et al.*, 2004), entanglement-assisted orientation in space (Brukner *et al.*, 2005; Bovino, Giardina, *et al.*, 2006b), quantum estimation of a damping constant (Venzl and Freyberger, 2007), frequency standards improvement (Wineland *et al.*, 1992; Huelga *et al.*, 1997; Giovannetti *et al.*, 2004) (see in this context Boto *et al.*, 2000), and clock synchronization (Jozsa *et al.*, 2000). Entanglement plays a fundamental role in quantum communication between parties separated by macroscopic distances (Bennett, DiVincenzo, Smolin, *et al.*, 1996).

Although the role of entanglement in quantum computational speedup is not clear (Kendon and Munro, 2006), it has played an important role in the development of quantum computing, including measurement-based schemes, one-way quantum computing (Raussendorf and Briegel, 2001),[6] and linear optics quantum computing (Knill *et al.*, 2001).[7] Entanglement has also given new insights for understanding many physical phenomena including super-radiance (Lambert *et al.*, 2004), superconductivity (Vedral, 2004), disordered systems (Dür *et al.*, 2005), and the emergence of classicality (Zurek, 2003). In particular, understanding the role of entanglement in existing methods of simulations of quantum spin systems allowed for significant improvement of the methods, as well as comprehension of their limitations (Vidal, 2003, 2004; Verstraete, Porras, and Cirac, 2004; Anders, Plenig, *et al.*, 2006). The role of entanglement in quantum phase transitions (Osborne and Nielsen, 2002; Osterloh *et al.*, 2002; Vidal *et al.*, 2003; Latorre *et al.*, 2004; Verstraete, Popp, and Cirac, 2004; Larsson and Johannesson, 2006) has been studied. Divergence of correlations at critical points is always accompanied by divergence of a suitably defined entanglement length (Verstraete, Popp, and Cirac, 2004). The concept of entanglement length originates from Aharonov, who studied a critical phenomenon in the context of fault-tolerant quantum computing (Aharonov, 1999). Last but not least, entanglement was also used on a more deep conceptual level to derive Born's rule with the help of the symmetry entanglement under local unitary operations, the property called "entanglement assisted invariance" or "envariance" (Zurek, 2005; see also Zurek, 2009).

Unfortunately, quantum entanglement has three disagreeable but interesting features: It has in general a very complex structure, it is fragile with respect to environment, and it cannot be increased on average when systems are not in direct contact but distributed in spatially separated regions. The theory of entanglement tries to give answers to fundamental questions such as (i) how to optimally detect entanglement theoretically and in the laboratory; (ii) how to reverse the inevitable process of degradation of entanglement; and (iii) how to characterize, control, and quantify entanglement.

The history of questions (i) and (ii) has its origin in the seminal papers of Werner and Popescu (Werner, 1989; Popescu, 1994). Werner not only gave an accurate definition of separable states (those mixed states that, are not entangled), but also noted that there exist entangled states that, like separable states, admit the LHV model, and hence do not violate Bell inequalities. Popescu

[5]Quantum teleportation with continuous variables in an infinite dimensional Hilbert space was first proposed by Vaidman (1994) and investigated by Braunstein and Kimble (1998).

[6]For a comprehensive review, see Browne and Briegel, 2006.

[7]It has been shown that linear optics quantum computing can be viewed as a measurement based on one-way computing (Popescu, 2006).

(1995) showed that, with the system in such a state, by means of local operations and postselection one can get a new state whose entanglement can be detected by Bell inequalities. This idea was developed by Gisin, who used so-called filters to enhance the violation of Bell inequalities (Gisin, 1996). In fact, this idea turned out to be a trigger for a theory of entanglement manipulations (Bennett, Brassard, *et al.*, 1996).

Soon afterwards, Peres showed that if, a state is separable,[8] then after *partial transpose*[9] of the density matrix on one subsystem of a compound bipartite system, it is still a legitimate state (Peres, 1996a). Surprisingly, the Peres condition appeared to be a good test for entanglement.[10] As the partial transpose is a *positive map*, it was realized that positive maps can serve as good detectors of entanglement. However, they cannot be implemented directly in the laboratory, because they are unphysical.[11] Fortunately there is a "footbridge" [Jamiołkowski (1972) isomorphism] which allows us to go to physical measurable quantities, Hermitians operators. This constitutes a necessary and sufficient condition for separability on both the physical level of observables and the nonphysical one engaging positive maps (M. Horodecki *et al.*, 1996). This characterization of entanglement, although nonoperational, provides a basis for the general theory of detection of entanglement. A historical note is in order here. That is, it turned out that both the general link between separability and positive maps as well as the Peres-Horodecki theorem were first known and expressed in a slightly different language in the 1970s (Choi, 1972) (see also Størmer, 1963; Woronowicz, 1976; Osaka, 1991). The rediscovery by Peres and Horodecki brought powerful methods to entanglement theory as well as caused a revival of research on positive maps, especially the so-called nondecomposable ones.

Terhal first constructed a family of nondecomposable positive linear maps based on entangled quantum states (Terhal, 2001). She also pointed out that a violation of a Bell inequality can be expressed as a witness for entanglement (Terhal, 2000).[12] Since then the theory of entanglement witnesses has been developed (Lewenstein *et al.*, 2000; Bruß *et al.*, 2002; Gühne *et al.*, 2003; Brandão, 2005; Kiesel *et al.*, 2005; Tóth and Gühne, 2005; Brandão and Vianna, 2006), including a nonlinear generalization (Gühne and Lewenstein, 2004b; Gühne and Lütkenhaus, 2006) and the study of indistinguishable systems (Schliemann *et al.*, 2001; Eckert *et al.*, 2003). The general methods for constructing entanglement witnesses for detecting genuine multipartite entanglement in experiments were presented by Tóth *et al.* (2009).

The concept of entanglement witness has been applied to different problems in statistical systems (Wieśniak *et al.*, 2005; Wu *et al.*, 2005; Brukner *et al.*, 2006; Cavalcanti *et al.*, 2006), quantum cryptography (Curty *et al.*, 2005), quantum optics (Stobińska and Wódkiewicz, 2005, 2006), condensed-matter nanophysics (Blaauboer and DiVincenzo, 2005), bound entanglement (Hyllus *et al.*, 2004), experimental realization of cluster states (Vallone *et al.*, 2007), and hidden nonlocality (Masanes *et al.*, 2007). At this time, in precision experiments multipartite entanglement was detected using entanglement witness operators (Barbieri *et al.*, 2003; Bourennane *et al.*, 2004; Roos *et al.*, 2004; Altepeter *et al.*, 2005; Häffner, Hänsel, *et al.*, 2005; Leibfried *et al.*, 2005; Mikami *et al.*, 2005; Resch *et al.*, 2005; Lu *et al.*, 2007).

As one knows, the main virtue of entanglement witnesses is that they provide an economic method of detection of entanglement that does not need full (tomographic) information about the state. A a natural question arises: How does one estimate optimally the amount of entanglement of a compound system in an unknown state if only incomplete data in the form of average values of some operators detecting entanglement are accessible? This question led to the new inference scheme for all processes where entanglement is measured. It involves a principle of minimization of entanglement under a chosen measure of entanglement with constraints in the form of an incomplete set of data from experiment (R. Horodecki *et al.*, 1999). In particular, minimization of entanglement measures (entanglement of formation and relative entropy of entanglement) under a fixed Bell-type witness constraint was obtained. Subsequently, the inference scheme based on the minimization of entanglement was successfully applied (Audenaert and Plenio, 2006; Eisert and Gross, 2007; Gühne, Reimpell, *et al.*, 2007; Wunderlich and Plenio, 2009) to estimate entanglement measures from recent experiments measuring entanglement witnesses. This result shows that the entanglement witnesses are not only economic indicators of entanglement but are also helpful in estimating the entanglement content.

In parallel to entanglement witnesses, the theory of positive maps was developed which provides, in particular, tools for the detection of entanglement (Cerf *et al.*, 1999; Horodecki and Horodecki, 1999; Terhal, 2001; Kossakowski, 2003; Benatti *et al.*, 2004; Majewski, 2004; Yu and le Liu, 2005; Breuer, 2006a; Chruściński and Kossakowski, 2006; Datta *et al.*, 2006; Hall, 2006; Piani, 2006; Piani and Mora, 2007). Strong inseparability criteria beyond the positive map approach were also found (Rudolph, 2000; Chen and Wu, 2003; Hofmann and Takeuchi, 2003; Gühne *et al.*, 2004; Mintert, Kus, *et al.*, 2005; Clarisse and Wocjan, 2006; Horodecki, Horodecki, *et al.*, 2006; Devi *et al.*, 2007; Gühne, Hyllus, *et al.*, 2007).

Separability criteria for continuous variables have also been proposed (see Sec. XVII.D). The necessary and sufficient condition for separability of Gaussian states of

[8]More formal definitions of entangled and separable states are given in the next section.

[9]The positive partial transpose condition is called the Peres criterion of separability.

[10]For low-dimensional systems it turned out to be a necessary and sufficient condition of separability called the Peres-Horodecki criterion (H. Horodecki *et al.*, 1996).

[11]See, however, Horodecki and Ekert, 2002.

[12]The term "entanglement witness" for operators detecting entanglement was introduced by Terhal, 2000.

a bipartite system of two harmonic oscillators was found independently by Simon and Duan *et al.* (Duan *et al.*, 2000; Simon, 2000). The two approaches are equivalent. Simon's criterion is a direct generalization of the partial transpose to continuous variable (CV) systems, while Duan *et al.* started with local uncertainty principles.

Soon afterward Werner and Wolf (2001c) found bound entangled Gaussian states. Since then the theory of entanglement for continuous variables has been developed in many directions, especially for Gaussian states, which are accessible in the current stage of technology (see Braunstein and Pati, 2003, and references therein). For the latter states the problem of entanglement versus separability was solved completely: operational necessary and sufficient conditions were provided by Giedke, Kraus, *et al.* (2001). This criterion therefore detects all bipartite bound entangled Gaussian states. Interestingly, McHugh *et al.* constructed a large class of non-Gaussian two-mode continuous variable states for which the separability criterion for Gaussian states can be employed (McHugh, Buzek, *et al.*, 2006).

Various criteria for continuous variables have been obtained (Mancini *et al.*, 2002; Raymer *et al.*, 2003; Agarwal and Biswas, 2005; Hillery and Zubairy, 2006). A powerful separability criterion of bipartite harmonic quantum states based on the partial transpose was derived which includes the above criteria as special cases (Shchukin and Vogel, 2005b; Miranowicz and Piani, 2006).

Undoubtedly, current entanglement theory owes its form to the discovery of entanglement manipulation (Popescu, 1995; Bennett, Brassard, *et al.*, 1996). It was realized (Bennett, Brassard, *et al.*, 1996) that a natural class of operations suitable for manipulating entanglement is that of local operations and classical communication (LOCC), neither of which can bring in entanglement for free. So the established *distant laboratory* (or LOCC) paradigm plays a fundamental role in entanglement theory. Within the paradigm many important results have been obtained. In particular, the framework for pure state manipulations has been established, including reversibility in asymptotic transitions of pure bipartite states (Bennett, Bernstein, *et al.*, 1996), connection between LOCC pure state transitions and majorization theory (Nielsen, 1999), as well as the effect of catalysis (Jonathan and Plenio, 1999; Vidal and Cirac, 2001, 2002). Moreover, inequivalent types of multipartite entanglement have been identified (Bennett *et al.*, 2000; Dür, Vidal, *et al.*, 2000).

Since in the laboratory one usually meets mixed states representing *noisy entanglement*, not very useful for quantum information processing, there was a big challenge: to reverse the process of degradation of entanglement by means of some active manipulation. Remarkably, Bennett, Brassard, *et al.* (1996) showed that it is possible to distill pure from noisy entanglement in an asymptotic regime. It should be noted that, in parallel, there was intense research aiming at protection of quantum information in quantum computers against decoherence. As a result, error-correcting codes were discovered (Shor, 1995; Steane, 1996). Soon it was realized that quantum error correction and distillation of entanglement are in fact inherently interrelated (Bennett, DiVincenzo, *et al.*, 1996).

A question fundamental for quantum information processing then immediately arose: Can noisy entanglement always be purified? A promising result was obtained by Horodecki *et al.* (1997), where all two-qubit noisy entanglement was shown to be distillable. However, soon afterward a no-go type result (M. Horodecki *et al.*, 1998) revealed a dramatic difference between pure and noisy entanglement: namely, there exists *bound entanglement*. This destroyed the hope that noisy entanglement can have a more or less uniform structure: instead we encounter peculiarity in the structure of entanglement. Namely, there is *free* entanglement, which can be distilled, and bound entanglement—a very weak form of entanglement. The passivity of the latter provoked research toward identifying any tasks that would reveal its quantum features. Existence of bound entangled states follows from the fact that a state with a so-called *positive partial transpose* cannot be distilled. The first explicit examples of such states were provided by Horodecki (1997). Further examples (called bound entangled states) were found by Bennett, DiVincenzo, Mor, *et al.* (1999), Bruß and Peres (2000), Werner and Wolf (2001c); see also Clarisse (2006), Bruß and Leuchs (2007), and references therein. Interestingly, it was shown recently that thermal states of some many-body systems can be bound entangled (Toth *et al.*, 2007).

The existence of bound entanglement has provoked many questions, including its relations to the local variable model as well as the long-standing and still open question of the existence of bound entangled states violating the positive portial transpose criterion, which would have severe consequences for communication theory.

Because of the existence of bound entanglement, the question "can every entanglement be used for some useful quantum task?" stayed open for a long time. Only recently was a positive answer for both bipartite and multipartite states given by Masanes (2005, 2006a) in terms of so-called activation (P. Horodecki *et al.*, 1999). This result allows us to define entanglement not only in the negative terms of Werner's definition (a state is entangled if it is not a mixture of product states) but also in positive terms (a state is entangled if it is a resource for a nonclassical task).

One most difficult and fundamental question in entanglement theory concerns the quantification of entanglement. Remarkably, two fundamental measures, *entanglement distillation* (Bennett, Bernstein, *et al.*, 1996; Bennett, Brassard, *et al.*, 1996; Bennett, DiVincenzo, *et al.*, 1996) and what is now called *entanglement cost* (Bennett, DiVincenzo, *et al.*, 1996; Hayden *et al.*, 2001), appeared in the context of manipulating entanglement, and have an operational meaning. Their definitions bring to mind a thermodynamical analogy (Popescu and Rohrlich, 1997; Horodecki *et al.*, 1998b; Vedral and Plenio, 1998), since they describe two opposite processes—

creation and distillation, which ideally should be the reverse of each other. Indeed, reversibility holds for pure bipartite states, but fails for noisy as well as for multipartite entanglement. The generic gap between these two measures shows a fundamental irreversibility (M. Horodecki *et al.*, 1998; Vidal and Cirac, 2001; Yang, Horodecki, *et al.*, 2005). This phenomenon has its origin in the nature of noisy entanglement, and its immediate consequence is the nonexistence of a unique measure of entanglement.

Vedral and co-workers (Vedral, Plenio, Rippin, *et al.*, 1997; Vedral and Plenio, 1998) proposed an axiomatic approach to quantifying entanglement, in which a "good" measure of entanglement is any function that satisfies some postulates. The leading idea (Bennett, DiVincenzo, *et al.*, 1996) is that entanglement should not increase under local operations and classical communication, the so-called monotonicity condition. They proposed a scheme to obtain measures satisfying this condition based on the concept of distance from separable states, and introduced one of the most important measures of entanglement, the so-called *relative entropy of entanglement* (Vedral, Plenio, Rippin, *et al.*, 1997; Vedral and Plenio, 1998) (for a more comprehensive review, see Vedral, 2002). Subsequently, a general mathematical framework for entanglement measures was worked out by Vidal (2000), who concentrated on the axiom of monotonicity (hence the term "entanglement monotone").

At first sight it could seem that measures of entanglement do not exhibit any ordered behavior. Eisert and Plenio showed numerically that entanglement measures do not necessarily imply the same ordering of states (Eisert and Plenio, 1999). It was further shown analytically by Miranowicz and Grudka (2004). However, it turns out that there are constraints for measures that satisfy suitable postulates relevant in an asymptotic regime. Namely, any such measure must lie between two extreme measures that are two basic operational measures: distillable entanglement E_D and entanglement cost E_C (Horodecki *et al.*, 2000b). This can be seen as a reflection of the more general fact that abstractly defined measures provide bounds for operational measures, which are of interest as they quantify how well some specific tasks can be performed.

The world of entanglement measures, even for bipartite states, still exhibits puzzles. One example may is the phenomenon of locking of entanglement (Horodecki *et al.*, 2005c). For most known bipartite measures we observe a kind of collapse: after removing a single qubit, for some states, entanglement dramatically decrease.

Concerning multipartite states, some bipartite entanglement measures such as the relative entropy of entanglement or robustness of entanglement (Vidal and Tarrach, 1999) easily generalize to multipartite states. See Barnum and Linden (2001) and Eisert and Briegel (2001) for early candidates for multipartite entanglement measures. In the multipartite case a new ingredient comes in: namely, one tries to single out and quantify "truly multipartite" entanglement. The first measure that reports genuinely multipartite properties is the "residual tangle" of Coffman *et al.* (2000). It is clear that in the multipartite case even the quantification of entanglement of pure states is a challenge. Interesting new schemes to construct measures for pure states have been proposed (Miyake, 2003; Verstraete *et al.*, 2003).

Entanglement measures allow for the analysis of dynamical aspects of entanglement,[13] including entanglement decay under interaction with the environment (Yi and Sun, 1999; Kim *et al.*, 2002; Życzkowski *et al.*, 2002; Dodd and Halliwell, 2004; Jakóbczyk and Jamróz, 2004; Miranowicz, 2004a; Montangero, 2004; Yu and Eberly, 2004; Carvalho *et al.*, 2005; Mintert, Carvalho, *et al.*, 2005; Shresta *et al.*, 2005; Ban, 2006; Ficek and Tanaś, 2006; Wang *et al.*, 2006; Maloyer and Kendon, 2007) and entanglement production, in the course of quantum computation (Parker and Plenio, 2002; Kendon and Munro, 2006) or due to interaction between subsystems. The latter problem gave rise to the notion of the "entangling power" (Zanardi *et al.*, 2000; Linden *et al.*, 2005) of a unitary transformation, which can be seen as a higher-level entanglement theory dealing with entanglement of operations, rather than entanglement of states (Eisert, Jacobs, *et al.*, 2000; Collins *et al.*, 2001; Harrow and Shor, 2005; Linden *et al.*, 2005).

Interestingly, even two-qubit systems can reveal nontrivial features of entanglement decay. That is, the state of two entangled qubits, treated with unitary dynamics and subjected to weak noise, can reach a set of separable states (see Sec. II) in finite time, while coherence vanishes asymptotically (Rajagopal and Rendell, 2001; Życzkowski *et al.*, 2002; Diósi, 2003). This effect was investigated in more realistic scenarios (Dodd and Halliwell, 2004; Jakóbczyk and Jamróz, 2004; Yu and Eberly, 2004, 2007b, 2009; Tolkunov *et al.*, 2005; Ficek and Tanaś, 2006; Wang *et al.*, 2006; Lastra *et al.*, 2007; Vaglica and Vetri, 2007) (see also Jordan *et al.*, 2007). It was called "sudden death of entanglement" (Yu and Eberly, 2006) and demonstrated by Almeida *et al.* (2007) (see Santos *et al.*, 2006).

Note that, apart from entanglement decay, positive effects of the environment have been investigated: entanglement generated by interference in the measurement process (Bose *et al.*, 1999; Cabrillo *et al.*, 1999) cavity-loss-induced generation of entangled atoms (Plenio *et al.*, 1999), atom-photon entanglement conditioned by photon detection (Horodecki, 2001b), generation of entanglement from white noise (Plenio and Huelga, 2002), entanglement generated by interaction with a common heat bath (Braun, 2002), noise-assisted preparation of entangled atoms inside a cavity (Yi *et al.*, 2003), environment-induced entanglement in Markovian dissipative dynamics (Benatti *et al.*, 2003), and entanglement induced by a spin chain (Yi *et al.*, 2006). It has been demonstrated (Lamata *et al.*, 2007) that it is possible to achieve an arbitrary amount of entanglement between

[13]See Amico *et al.* (2008), Yu and Eberly (2009), and references therein.

two atoms using spontaneously emitted photons, linear optics, and projective measurements.

One pillar of the theory of entanglement is, discovered by Ekert (1991), its connection with quantum cryptography (strictly speaking, with its subdomain—quantum key distribution) as well as with classical cryptography scenario called secure key agreement (Gisin and Wolf, 1999, 2000; Collins and Popescu, 2002). It seems that the most successful application of quantum entanglement is that it provides a basic framework for quantum key distribution (despite the fact that the basic key distribution protocol BB84 does not use entanglement directly). This is not just a coincidence. It appears that entanglement is the quantum equivalent of what is meant by privacy. Indeed, the main resource for privacy is a secret cryptographic key: correlations shared by interested persons but not known by any other person. Now, in the *single* notion of entanglement, two fundamental features of privacy are encompassed in an ingenious way. If systems are in a pure entangled state then at the same time (i) the systems are correlated and (ii) no other system is correlated with them. The interrelations between entanglement and privacy theory are so strong that in many cases cryptographic terminology seems to be the most accurate language to describe entanglement (see, e.g., Devetak and Winter, 2005). An example of a backreaction—from entanglement to privacy—is the question of existence of bound information as a counterpart of bound entanglement (Gisin and Wolf, 2000). In fact, the existence of such a phenomenon, conjectured by Gisin and Wolf, was found by Acín, Ciric, *et al.* (2004) for multipartite systems. There is a strong connection between quantum key distribution and distillation of entanglement. Protocols of entanglement distillation are based on techniques used in quantum key distribution, and vice versa (Bennett, DiVincenzo, *et al.*, 1996; Deutsch *et al.*, 1996; Lo and Chau, 1999; Shor and Preskill, 2000). However, quantum key distribution (QKD) is not equivalent just to distillation of singlets: one can obtain a secure key even from bound entangled states (Horodecki *et al.*, 2005d). This has fundamental implications: security can be obtained via channels that cannot faithfully transmit qubits (Horodecki *et al.*, 2008).

The fact that entanglement represents correlations that cannot be shared by third parties is deeply connected with *monogamy*—the basic feature of entanglement. In 1999 Coffman, Kundu, and Wootters first formalized monogamy in quantitative terms, observing that there is inevitable trade-off between the amount of entanglement that qubit A can share with qubit B_1 and the entanglement which the same qubit A shares with some other qubit B_2 (Coffman *et al.*, 2000). In fact, in 1996 the issue of monogamy was already touched on by Bennett, DiVincenzo, *et al.* (1996), where it was pointed out that no system can be EPR correlated with two systems at the same time; this has direct consequences for entanglement distillation. Monogamy expresses the nonshareability of entanglement (Terhal, 2004); it is not only central to cryptographic applications, but also allows us to shed new light on physical phenomena in many body systems such as frustration effects leading to a highly correlated ground state (see, e.g., Dawson and Nielsen, 2004).

Entanglement was also investigated within the framework of special relativity and quantum field theory (Summers and Werner, 1985; Czachor, 1997; Alsing and Milburn, 2002; Terno, 2004; Caban and Rembieliński, 2005; Peres *et al.*, 2005; Jordan *et al.*, 2006) [see the comprehensive review and references therein (Peres and Terno, 2004)]. In particular, entanglement for indistinguishable many-body systems was investigated in two complementary directions. The first (canonical) approach is based on the tensor product structure (Li *et al.*, 2001; Paskauskas and You, 2001; Schliemann *et al.*, 2001; Eckert *et al.*, 2002), while the second one is based on the occupation-number representation (Zanardi, 2002; Zanardi and Wang, 2002). Moreover, Verstraete and Cirac (2003) considered the notion of entanglement in the context of superselection rules more generally. However, it seems that there is still controversy concerning the meaning of entanglement for indistinguishable particles (Wiseman and Vaccaro, 2003). Recently, the group-theory approach to entanglement was developed by Korbicz and Lewenstein (2006) and its connection with noncommutativity was found.

In general, the structure of quantum entanglement appears to be complex and many different parameters, measures, and inequalities are needed to characterize its different aspects (see Alber, Beth, *et al.*, 2001; Bruß, 2002; Bruß *et al.*, 2002; Gurvits and Barnum, 2002; Terhal, 2002; Eckert *et al.*, 2003; Bengtsson and Życzkowski, 2006; Bruß and Leuchs, 2007).

Finally, the list of experiments dealing with entanglement[14] is growing quickly: entanglement over long distances (Tittel *et al.*, 1998, 1999; Weihs *et al.*, 1998; Marcikic *et al.*, 2004; Peng *et al.*, 2005), entanglement between many photons (Zhao *et al.*, 2004) and many ions (Häffner, Schmidt-Kaler, *et al.*, 2005), entanglement of an ion and a photon (Blinov *et al.*, 2004; Volz *et al.*, 2006), entanglement of mesoscopic systems (more precisely, entanglement between a few collective modes carried by many particles) (Altewischer *et al.*, 2002; Julsgaard *et al.*, 2004; Fasel *et al.*, 2005), entanglement swapping (Pan *et al.*, 1998; Jennewein *et al.*, 2001), and the transfer of entanglement between different carriers (Tanzilli *et al.*, 2005), etc. (Gisin, 2005). We now add a few recent experiments: multiphoton path entanglement (Eisenberg *et al.*, 2005), photon entanglement from semiconductor quantum dots (Akopian *et al.*, 2006)[15] teleportation between a photonic pulse and an atomic ensemble (Sherson *et al.*, 2006), violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality measured by two ob-

[14]Historically the first experimental realization of a two-qubit entangling quantum gate (controlled NOT) is due to Monroe *et al.* (1995).

[15]There was a controversy as to whether in the previous experiment of Stevenson *et al.* (2006) entanglement was actually detected (Lindner *et al.*, 2006).

servers separated by 144 km (Ursin *et al.*, 2007), purification of two-atom entanglement (Reichle *et al.*, 2006), increasing entanglement between Gaussian states (Ourjoumtsev *et al.*, 2007), and creation of entangled six-photon graph states (Lu *et al.*, 2007), generation and characterization of multipartite Dicke states (Prevendel *et al.*, 2009; Wieczorek *et al.*, 2009) and the invariance test of experimental correlation of photonic six-qubit singlet state (Radmark *et al.*, 2009).

II. ENTANGLEMENT AS A QUANTUM PROPERTY OF COMPOUND SYSTEMS

We are accustomed to the statement that on the fundamental level nature required a quantum rather than a classical description. However, the full meaning of this and all its possible experimental and theoretical implications are far from trivial (Jozsa, 1999). In particular, the "effect" of the replacement of the classical concept of phase space by the abstract Hilbert space makes a gap in the description of composite systems. To see this, consider a multipartite system consisting of n subsystems. According to the classical description the total (pure) state space of the system is the *Cartesian* product of the n subsystem spaces, implying that the total state is always a product state of the n separate systems. In contrast, according to the quantum formalism, the total Hilbert space H is a *tensor* product of the subsystem spaces $H=\otimes_{l=1}^{n}H_l$. Then the superposition principle allows us to write the total state of the system in the form

$$|\psi\rangle = \sum_{\mathbf{i}_1,\ldots,\mathbf{i}_n} c_{\mathbf{i}_1,\ldots,\mathbf{i}_n}|\mathbf{i}_1\rangle \otimes |\mathbf{i}_2\rangle \otimes \cdots \otimes |\mathbf{i}_n\rangle, \tag{1}$$

which cannot in general be described as a product of states of individual subsystems[16] $|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

This means that it is in general not possible to assign a single state vector to any one of n subsystems. It expresses formally the phenomenon of entanglement, which, in contrast to classical superposition, allows us to construct an exponentially large superposition with only a linear amount of physical resources. This is just what allows us to perform nonclassical tasks. The states on the left-hand side (LHS) of Eq. (1) appear usually as a result of direct physical interactions. However, entanglement can also be generated indirectly by application of the projection postulate (entanglement swapping).

In practice we encounter mixed rather than pure states. Entanglement of mixed states is no longer equivalent to being nonproduct states, as in the case of pure states. Instead, one calls a mixed state of n systems entangled if it cannot be written as a convex combination of product states[17] (Werner, 1989b):

$$\rho \neq \sum_i p_i \rho_1^i \otimes \cdots \otimes \rho_n^i. \tag{2}$$

The states that are not entangled in the light of the above definition are called *separable*. In practice, it is hard to decide if a given state is separable or entangled base on the definition itself. This so-called *separability* problem (see Secs. VI–X) is one of the fundamental problems concerning entanglement.

The above definition is negative, since a state is entangled if it cannot be written in the form (2). It should be noted in the above context that a positive definition of entangled states was proposed recently, namely, entangled states are those that cannot be simulated by classical correlations (Masanes *et al.*, 2007). This interpretation defines entanglement in terms of the behavior of the states rather than in terms of their preparation.

Example. For bipartite systems the Hilbert space $H=\mathcal{H}_1\otimes\mathcal{H}_2$ with $\dim\mathcal{H}_1=\dim\mathcal{H}_2=2$ is spanned by the four-Bell-state entangled basis

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle), \quad |\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle). \tag{3}$$

These states (called sometimes EPR states) have remarkable properties, namely, if one measures only at one of the subsystems one finds it with equal probability in state $|0\rangle$ or state $|1\rangle$. Thus the states give no knowledge about the subsystems. However, as a whole, the states are pure, hence they give maximal knowledge about the total system. This is just the feature which was first recognized by Schrödinger (see Sec. V). There is another holistic feature, that unitary operation applied to only one of the two subsystems suffices to transform from any Bell state to any one of the other three states. Moreover, Braunstein *et al.* showed that the Bell states are eigenstates of the Bell operator (16) and they maximally violate the Bell-CHSH inequality (17) (see Sec. IV) (Braunstein *et al.*, 1992).

The Bell states are special cases of bipartite maximally entangled states on the Hilbert space $C^d\otimes C^d$, given by

$$|\psi\rangle = U_A \otimes U_B|\Phi_d^+\rangle_{AB}, \tag{4}$$

where

$$|\Phi_d^+\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle|i\rangle \tag{5}$$

is the "canonical" maximally entangled state. Here a maximally entangled state will also be called an EPR state or a singlet state, since it is equivalent to the true singlet state up to local unitary transformations (for $d=2$ we call it also an e-bit). We will also often drop the index d.

The question of whether a mixture of Bell states is still entangled is quite nontrivial. Actually this is the

[16]Sometimes instead of the notation $|\psi\rangle\otimes|\phi\rangle$ we use $|\psi\rangle|\phi\rangle$ and for $|i\rangle\otimes|j\rangle$ the even shorter $|ij\rangle$.

[17]Note that classical probability distrubutions can *always* be written as mixtures of product distributions.

case if and only if one of the eigenvalues is greater than $\frac{1}{2}$ (see Sec. VI).

So far the most widely used source of entanglement is entangled-photon states produced by a nonlinear process of parametric down-conversion of type I or II corresponding to whether the entangled photons of the down-conversion pair are generated with the same polarization or orthogonal polarization, respectively. In particular, using parametric down-conversion one can produce a Bell-state entangled basis (3). There are also many other sources of entangled quantum systems, for instance, entangled photon pairs from calcium atoms (Kocher and Commins, 1967), entangled ions prepared in electromagnetic Paul traps (Meekhof *et al.*, 1996), entangled atoms in quantum electrodynamic cavities (Raimond *et al.*, 2001), long-living entanglement between macroscopic atomic ensembles (Hald *et al.*, 1999; Julsgaard *et al.*, 2001), entangled microwave photons from quantum dots (Emary *et al.*, 2005), entanglement between nuclear spins within a single molecule (Chen, He, *et al.*, 2006), and entanglement between light and atomic ensembles (Sherson *et al.*, 2006).

Next we present pioneering entanglement-based communication schemes using Bell entangled states.

III. PIONEERING EFFECTS BASED ON ENTANGLEMENT

A. Quantum key distribution based on entanglement

The first discovery within quantum information theory, which involves entanglement, is due to Ekert (1991). There were two well known facts: the existence of a highly correlated state,[18]

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle), \tag{6}$$

and the Bell inequalities (violated by these states). Ekert showed that, if put together, they become useful in producing a private cryptographic key. In this way he discovered entanglement-based quantum key distribution, as opposed to the original BB84 scheme which directly uses quantum communication. The essence of the protocol is as follows: Alice and Bob can obtain from a source the EPR pairs. Measuring them in the basis $\{|0\rangle, |1\rangle\}$, Alice and Bob obtain a string of perfectly (anti)correlated bits, i.e., the key. To verify whether it is secure, they check Bell inequalities on a selected portion of the pairs. Roughly speaking, if Eve knew the values that Alice and Bob obtained in their measurement, this would mean that the values existed before the measurement, hence Bell's inequalities would not be violated. Therefore, if the Bell inequalities are violated, the values do not exist before the Alice and Bob measurement, so it looks as if like nobody can know them.[19] The first implementations of Ekert's cryptography protocol were performed using polarization-entangled photons from spontaneous parametric down-conversion (Naik *et al.*, 2000) and photons entangled in energy-time (Tittel *et al.*, 2000).

After Ekert's idea, the research in quantum cryptography could have taken two paths. One is to treat the violation of the Bell inequality merely as a confirmation that Alice and Bob share good EPR states, as put forward by Bennett *et al.* (1992), because this is sufficient for privacy: if Alice and Bob have a true EPR state, then nobody can know the results of their measurements. This is what actually happened; for a long time only this approach was developed. In this case the eavesdropper, Eve, obeys the rules of quantum mechanics. We discuss this approach in Sec. XIX. The second path is to treat the EPR state as the source of strange correlations that violate the Bell inequality (see Sec. IV). This leads to a new definition of security: against the eavesdropper who does not have to obey the rules of quantum mechanics, but just the no-faster-than-light communication principle. The main task of this approach, which is an unconditionally secure protocol, has been achieved only recently (Barrett *et al.*, 2005; Masanes *et al.*, 2006; Masanes and Winter, 2006).

B. Quantum dense coding

In quantum communication there exists a reasonable bound on the possible miracles stemming from quantum formalism. This is the (Holevo bound) (Holevo, 1973). Roughly speaking it states that one qubit can carry at most only one bit of classical information. In 1992, Bennett and Wiesner discovered a fundamental primitive, called dense coding, which can evade the Holevo bound. Dense coding allows us to communicate two classical bits by sending one *a priori* entangled qubit.

Suppose Alice wants to send one of four messages to Bob, and can send only one qubit. To communicate two bits sending one qubit she needs to send a qubit in one of $2^2=4$ states. Moreover, the states need to be mutually orthogonal, as otherwise Bob will have problems with discriminating them, and hence the optimal bound 2 will not be reached. But there are only two orthogonal states of one qubit. Can entanglement help here? Let Alice and Bob instead share an EPR state. Now the clever idea comes: it is not the qubit that is sent that should be in one of four orthogonal states, but the pair of en-

[18]This state is also referred to as the singlet, EPR state, or EPR pair. If not explicitly stated, we use these names below to denote any maximally entangled state in higher dimensions; also see Sec. VI.B.3.

[19]In fact, the argument is more subtle. This is because in principle values that did not preexist could come to exist in a way that is immediately available to a third party—Eve, i.e., the values that were not known to anybody could happen to be known to everybody when they come to exist. To cope with this problem, Ekert used the fact that the singlet state cannot be correlated with any environment. Recently it turned out that one can argue based solely on Bell inequalities by means of so-called monogamy of nonlocal correlations (Barrett *et al.*, 2005, 2006; Acín *et al.*, 2006; Masanes and Winter, 2006).

tangled qubits together. We now check how it works. Suppose Alice and Bob share a singlet state (6). If Alice wants to tell Bob one of the four events $k \in \{0,1,2,3\}$, she rotates her qubit (entangled with Bob) with a corresponding transformation σ_k:

$$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\sigma_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad -i\sigma_3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{7}$$

The singlet state (6) rotated by σ_k on Alice's qubit becomes the corresponding $|\psi_k\rangle$ Bell state.[20] Hence $|\psi_k\rangle = [\sigma_k]_A \otimes I_B|\psi_0\rangle$ is *orthogonal* to $|\psi_{k'}\rangle = [\sigma_{k'}]_A \otimes I_B|\psi_0\rangle$ for $k \neq k'$ because Bell states are mutually orthogonal. Now if Bob gets Alice's half of the entangled state, after rotation he can discriminate between four Bell states, and infer k. In this way Alice sending one qubit has given Bob $\log_2 4 = 2$ bits of information.

Why does this not contradict the Holevo bound? This is because the communicated qubit was *a priori* entangled with Bob's qubit. This case is not covered by the Holevo bound, leaving a place for this strange phenomenon. Note also that as a whole two qubits have been sent: one was needed to share the EPR state. One can also interpret this in the following way: sending the first half of the singlet state (say it is during the night, when the channel is cheaper) corresponds to sending one bit of *potential communication*. It is thus creating the possibility of communicating one bit in the future: at this time Alice may not know what she will say to Bob in the future. During the day, she knows what to say, but can send only one qubit (the channel is expensive). That is, she sent only one bit of *actual communication*. However, at the same time, the potential communication gets actual; hence two bits in total are communicated. This explanation assumes that Alice and Bob have a good quantum memory for storing EPR states, which is still out of reach of current technology. In the original dense coding protocol, Alice and Bob share the pure maximally entangled state. The possibility of dense coding based on partially entangled pure and mixed states in multiparty settings was considered by Barenco and Ekert (1995); Hausladen *et al.* (1996); Bose *et al.* (2000); Hiroshima (2001); Ziman and Buzek (2003); Bruß *et al.* (2005); Mozes *et al.* (2005). The first experimental implementation of quantum dense coding was performed in Innsbruck (Mattle *et al.*, 1996), using a source of polarization-entangled photons [see experiments using nuclear magnetic resonance (Fang *et al.*, 2000), a two-mode squeezed vacuum state (Mizuno *et al.*, 2005), and controlled dense coding with an EPR state for a continuous variable (Jing *et al.*, 2003)].

[20] In correspondence with the Bell basis defined in Eq. (3) here $|\psi_0\rangle = |\psi^-\rangle$, $|\psi_1\rangle = |\phi^-\rangle$, $|\psi_2\rangle = |\psi^+\rangle$, $|\psi_3\rangle = |\phi^+\rangle$.

C. Quantum teleportation

Suppose Alice wants to communicate to Bob an unknown quantum bit. Suppose, further, that they have at their disposal only a classical telephone, and one pair of entangled qubits. One way would be for Alice to measure the qubit, guess the state based on the outcomes of measurement, and describe it to Bob via telephone. However, in this way the state will be transferred with very poor fidelity. In general an *unknown* qubit cannot be described by classical means, as it would become clonable, which would violate the main principle of quantum information theory: a qubit in an unknown quantum state cannot be cloned (Dieks, 1982; Wootters and Zurek, 1982).

However, Alice can send the qubit to Bob at the price of simultaneously erasing it at her site. This is the essence of *teleportation*: a quantum state is transferred from one place to another; not copied to the other place, but moved to that place. But how can this be performed with a pair of maximally entangled qubits? Bennett, Brassard, Crćpeau, Jozsa, Peres, and Wootters found the answer to this question in 1993 (Bennett *et al.*, 1993).

To perform teleportation, Alice needs to measure her qubit and part of a maximally entangled state. Interestingly, this measurement is itself entangling: it is projection onto the basis of four Bell states (3). Follow the situation in which she wants to communicate a qubit in state $|q\rangle = a|0\rangle + b|1\rangle$ on system A with the use of a singlet state residing on her system A' and Bob's system B. The total initial state, which is

$$|\psi_{AA'B}\rangle = |q\rangle_A \otimes \frac{1}{\sqrt{2}}[|0\rangle|0\rangle + |1\rangle|1\rangle]_{A'B}, \tag{8}$$

can be written using the Bell basis (3) on the system AA' in the following way:

$$\begin{aligned} |\psi_{AA'B}\rangle = \tfrac{1}{2}[&|\phi^+\rangle_{AA'}(a|0\rangle_B + b|1\rangle_B) + |\phi^-\rangle_{AA'}(a|0\rangle_B \\ &- b|1\rangle_B) + |\psi^+\rangle_{AA'}(a|1\rangle_B + b|0\rangle_B) \\ &+ |\psi^-\rangle_{AA'}(a|1\rangle_B - b|0\rangle_B)]. \end{aligned} \tag{9}$$

Now when Alice measures her systems AA' in this basis, she induces equiprobably the four corresponding states in Bob's system. The resulting states in system B are similar to the state of qubit $|q\rangle$ that Alice wanted to send him. Their mixture is, however, equal to the initial state of system B. Thus Bob does not get any information instantaneously. Yet, the output structure revealed in the above equation can be used: now Alice tells Bob her result via telephone. According to those two bits of information (which of the Bell states occurred on AA') Bob rotates his qubit by one of the four Pauli transformations (7). This is almost the end. After each rotation, Bob gets $|q\rangle$ at his site. At the same time, Alice has just one of the Bell states: the systems A and A' become entangled after measurement, and no information about the state $|q\rangle$ is left with her. That is, the *no-cloning* principle is observed, while the state $|q\rangle$ was transferred to Bob.

There is a much simpler way to send a qubit to Bob: Alice could just send it directly. Then, however, she has to use a quantum channel, just at the time she wants to transmit the qubit. With teleportation, she might have to send half of the EPR pair at an earlier time, so that only classical communication is needed later.

This is how quantum teleportation works in theory. This idea was also developed for other communication scenarios (see Murao *et al.*, 1999; Dür and Cirac, 2000c). It became immediately an essential ingredient of many quantum communication protocols. After pioneering experiments (Bouwmeester *et al.*, 1997; Boschi *et al.*, 1998; Furusawa *et al.*, 1998), there were experiments performing teleportation in different scenarios during the last decade (see, e.g., Nielsen *et al.*, 1998; Barrett *et al.*, 2004; Marcikic *et al.*, 2004; Riebe *et al.*, 2004; Ursin *et al.*, 2004). For the most recent one with mesoscopic objects, see Sherson *et al.* (2006).

D. Entanglement swapping

Usually quantum entanglement originates in a certain *direct interaction* between two particles placed close together. Is it possible to get entanglement (quantum correlation) between two particles which have never interacted in the past? The answer is positive (Yurke and Stoler, 1992b; Bennett *et al.*, 1993; Żukowski *et al.*, 1993).

Let Alice share a maximally entangled state $|\phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)_{AC}$ with Clare, and Bob share the same state with David:

$$|\phi^+\rangle_{AC} \otimes |\phi^+\rangle_{BD}. \tag{10}$$

Such a state can obviously be designed in such a way that particles A and D have never seen each other. Now, Clare and Bob perform a *joint* measurement in the Bell basis. It turns out that for any outcome the particles A and D collapse to some Bell state. If Alice and Bob will get to know the outcome, they can perform local rotation, to obtain the entangled state Φ^+_{AD}. In this way the particles of Alice and David are entangled although they never interacted directly with each other, as they originated from different sources.

One sees that this is equivalent to teleporting one member of the EPR pair through the second one; any of the pairs can be chosen to be either the channel or the teleported pair.

This idea has been adopted in order to perform *quantum repeaters* (Dür, Briegel, *et al.*, 1999), to allow for distributing entanglement in principle between arbitrarily distant parties. It was generalized to a multipartite scenario by Bose *et al.* (1998). Swapping can be used as a tool in multipartite state distribution, which is, for example, useful in quantum cryptography.

The conditions that should be met in optical implementation of entanglement swapping (as well as teleportation) have been derived by Żukowski *et al.* (1993). Along those lines entanglement swapping was realized in the laboratory (Pan *et al.*, 1998).

E. Beating classical communication complexity bounds with entanglement

Yao (1979) asked the following question: How much communication is needed in order to solve a given problem distributed among specially separated computers? To be more concrete, one can imagine Alice having the n-bit string x and Bob having the n-bit string y. Their task is to infer the value of some *a priori* given function $f(x,y)$ taking the value in $\{0, 1\}$, so that finally both parties know the value. The minimal number of bits needed in order to achieve this task is called the *communication complexity* of the function f.

Again, one can ask if entanglement can help in this case. This question was first asked by Cleve and Buhrman (1997) and independently by Grover (1997), who showed the advantage of entanglement-assisted over classical distributed computation.

Consider the following example, which is a three-party version of the same problem (Buhrman *et al.*, 2001). Alice, Bob, and Clare get two bits each, (a_1,a_0), (b_1,b_0), and (c_1,c_0), representing binary two-digit numbers $a=a_1a_0$, $b=b_1b_0$, and $c=c_1c_0$. They are promised to have

$$a_0 \oplus b_0 \oplus c_0 = 0. \tag{11}$$

The function that they are to compute is given by

$$f(a,b,c) = a_1 \oplus b_1 \oplus c_1 \oplus (a_0 \vee b_0 \vee c_0). \tag{12}$$

It is easy to see that the announcement of four bits is sufficient for all three parties to compute f. One party announces both bits (say it is Alice) a_1a_0. Now, if $a_0=1$, then the other parties announce their first bits b_1 and c_1. If $a_0=0$, then one of the other parties (say Bob) announces $b_1 \oplus b_0$ while Clare announces c_1. In both cases all parties compute the function by adding the announced bits modulo 2. Thus four bits are enough. It is a bit more tricky to show that four bits are *necessary*, so that the classical communication complexity of the above function equals 4 (Buhrman *et al.* 2001).

Suppose now that at the beginning of the protocol Alice, Bob, and Clare share a quantum three-partite entangled state:

$$|\psi_{ABC}\rangle = \tfrac{1}{2}[|000\rangle - |011\rangle - |101\rangle - |110\rangle]_{ABC}, \tag{13}$$

such that each party holds a corresponding qubit. It is enough to consider the action of Alice as the other parties will do the same with their classical and quantum data, respectively.

Alice checks her second bit. If $a_0=1$ she does a Hadamard transformation[21] on her qubit. Then she measures it in the $\{|0\rangle,|1\rangle\}$ basis, obtaining the result r_A. She then announces a bit $a_1 \oplus r_A$.

[21]The Hadamard transformation is a unitary transformation of basis which changes $|0\rangle$ into $1/\sqrt{2}(|0\rangle+|1\rangle)$ and $|1\rangle$ into $1/\sqrt{2}(|0\rangle-|1\rangle)$.

One can check that, if all three parties do the same, the bits r_A, r_B, r_C, i.e., those with "quantum origin" satisfy $r_A \oplus r_B \oplus r_C = a_0 \vee b_0 \vee c_0$. This gives in turn

$$\begin{aligned}(a_1 \oplus r_A) \oplus (b_1 \oplus r_B) \oplus (c_1 \oplus r_C) \\ = a_1 \oplus b_1 \oplus c_1 \oplus (r_A \oplus r_B \oplus r_C) \\ = a_1 \oplus b_1 \oplus c_1 \oplus (a_0 \vee b_0 \vee c_0) = f(a,b,c).\end{aligned} \tag{14}$$

Thus three bits are enough. The fourth, controlled by common quantum entanglement, was hidden in the three others and hence need not be announced.

Interestingly, although the effect is of practical importance, at its roots it is a purely philosophical question of the type, Is the Moon there, if nobody looks? (Mermin, 1985). Namely, if the outcomes of the Alice, Bob, and Clare measurements existed prior to measurement, then they could not lead to reduction of complexity, because the parties could have these results written on paper and they would offer a three-bit strategy, which is not possible. As a matter of fact, the discoveries of reduction of communication complexity used the GHZ paradox in the Mermin version, which says that the outcomes of the four possible measurements given by the values of a_0, b_0, and c_0 (recall the constraint $a_0 \oplus b_0 \oplus c_0$) performed on the state (13) cannot preexist.

Brukner *et al.* (2004) showed that this is quite generic: for any correlation Bell inequality for n systems, a state violating the inequality allows us to reduce the communication complexity of some problem. For a recent experiment see Trojek *et al.* (2005).

IV. CORRELATION MANIFESTATIONS OF ENTANGLEMENT: BELL INEQUALITIES

A. Bell theorem: CHSH inequality

The physical consequences of the existence of entangled (inseparable) states are continuously the subject of intensive investigations in the context of both the EPR paradox and quantum information theory. They are manifest, in particular, in correlation experiments via the Bell theorem, which states that the probabilities for the outcomes obtained when some quantum states are suitably measured cannot be generated from classical correlations. As a matter of fact, Bell in his proof assumed perfect correlations exhibited by the singlet state. However, in real experiments such correlations are practically impossible. Inspired by Bell's paper, Clauser, Horne, Shimony, and Holt (CHSH) (Clauser *et al.*, 1969) derived a correlation inequality, which provides a way of experimentally testing the local hidden variable model (LHVM) as an independent hypothesis separated from the quantum formalism. Consider a correlation experiment in which the variables (A_1, A_2) are measured on one subsystem of the whole system and (B_1, B_2) on the other system, and that the subsystems are spatially separated. Then the LHVM imposes the following constraints on the statistics of the measurements on the sufficiently large ensemble of systems[22]

$$|E(A_1,B_1) + E(A_1,B_2) + E(A_2,B_1) - E(A_2,B_2)| \leqslant 2, \tag{15}$$

where $E(A_i, B_j)$ is the expectation value of the correlation experiment A_iB_j.

This is the CHSH inequality, which gives a bound on any LHVM. It involves only a bipartite correlation function for two alternative dichotomic measurements and it is complete in the sense that if a full set of such inequalities (obtained by putting the minus in each of four possible positions) is satisfied there exists a joint probability distribution for the outcomes of the four observables, which returns the measured correlation probabilities as marginals (Fine, 1982).[23]

In the quantum case the variables convert into operators and one can introduce the CHSH operator

$$\mathcal{B}_{\mathrm{CHSH}} = \mathbf{A}_1 \otimes (\mathbf{B}_1 + \mathbf{B}_2) + \mathbf{A}_2 \otimes (\mathbf{B}_1 - \mathbf{B}_2), \tag{16}$$

where $\mathbf{A}_1 = \mathbf{a}_1 \cdot \sigma$, $\mathbf{A}_2 = \mathbf{a}_2 \cdot \sigma$ (similarly for $\mathbf{B}_1$ and $\mathbf{B}_2$), $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of Pauli operators, $\mathbf{a} = (a_x, a_y, a_z)$, etc., are unit vectors describing the measurements that the parties A (Alice) and B (Bob) perform. Then the CHSH inequality requires that the condition

$$|\mathrm{Tr}(\mathcal{B}_{\mathrm{CHSH}}\rho)| \leqslant 2 \tag{17}$$

is satisfied for all states ρ admitting a LHVM.

Quantum formalism predicts the Cirel'son inequality (Cirel'son, 1980),

$$|\langle \mathcal{B}_{\mathrm{CHSH}} \rangle_{QM}| = |\mathrm{Tr}(\mathcal{B}_{\mathrm{CHSH}}\rho)| \leqslant 2\sqrt{2}, \tag{18}$$

for all states ρ and all observables $\mathbf{A}_1, \mathbf{A}_2, \mathbf{B}_1, \mathbf{B}_2$. Clearly, the CHSH inequality can be violated for some choices of observables, implying nonexistence of LHVM. For the singlet state $\rho = |\psi^-\rangle\langle\psi^-|$, there is maximal violation $|\mathrm{Tr}(\mathcal{B}_{\mathrm{CHSH}\rho})| = 2\sqrt{2}$ which saturates the Cirel'son bound.

B. The optimal CHSH inequality for 2×2 systems

At the beginning of the 1990s there were two basic questions: First, it was hard to say whether a given state violates the CHSH inequality, because one has to construct a corresponding Bell observable for it. In addition, given a mixed state, there was no way to ensure whether it satisfies the CHSH inequality for each Bell

[22] It is assumed here that the variables A_i and B_i for $i = 1, 2$ are dichotomic, i.e., have values ± 1.

[23] Braunstein and Caves (1988) have considered modified CHSH inequalities based on Shannon entropies rather than on correlation functions. By the Fine result, they cannot be stronger than CHSH ones, but they are interesting in themselves in the information-theoretic context. This approach differs from the one we shall present in Sec. III, where von Neumann entropies are used.

observable. This problem was solved completely for an arbitrary quantum state ρ of two qubits using the Hilbert-Schmidt space approach (Horodecki *et al.*, 1995). That is, an n-qubit state can be written as

$$\rho = \frac{1}{2^n} \sum_{i_1 \cdots i_n=0}^{3} t_{i_1 \cdots i_n} \sigma_{i_1}^1 \otimes \cdots \otimes \sigma_{i_n}^n, \tag{19}$$

where σ_0^k is the identity operator in the Hilbert space of qubit k, and $\sigma_{i_k}^k$ correspond to the Pauli operators for three orthogonal directions $i_k = 1,2,3$. The set of real coefficients $t_{i_1 \cdots i_n} = \mathrm{Tr}[\rho(\sigma_{i_1} \otimes \cdots \otimes \sigma_{i_n})]$ forms a correlation tensor T_ρ. In particular, for the two-qubit system the (3×3)-dimensional tensor is given by $t_{ij} := \mathrm{Tr}[\rho(\sigma_i \otimes \sigma_j)]$ for $i,j = 1,2,3$.

In this case one can compute the mean value of an arbitrary $\mathcal{B}_{\mathrm{CHSH}}$ in an arbitrary fixed state ρ and then maximize it with respect to all $\mathcal{B}_{\mathrm{CHSH}}$ observables. As a result we have $\max_{\mathcal{B}_{\mathrm{CHSH}}} |\mathrm{Tr}(\mathcal{B}_{\mathrm{CHSH}}\rho)| = 2\sqrt{M(\rho)} = 2\sqrt{t_{11}^2 + t_{22}^2}$, where t_{11}^2 and t_{22}^2 are the two largest eigenvalues of $T_\rho^T T_\rho$, and T_ρ^T is the transpose of T_ρ.

It follows that for 2×2 systems the necessary and sufficient criterion for the violation of the CHSH inequality can be written as

$$M(\rho) > 1. \tag{20}$$

The quantity $M(\rho)$ depends only on the state parameters and contains all information that is needed to decide whether a state violates a CHSH inequality. The above inequality provides a practical tool for the investigation of nonlocality of the arbitrary two-qubit mixed states in different quantum information contexts (see, e.g., Scarani and Gisin, 2001a; Hyllus *et al.*, 2005; Walther *et al.*, 2005).

C. Violation of Bell inequalities by quantum states

1. Pure states

The second more fundamental question was "Are there many quantum states, that do not admit the LHV model?" More precisely, "Which quantum states do not admit the LHV model?" Even for pure states the problem is not completely solved.

Gisin proved that for the standard (i.e., nonsequential) projective measurements the only pure two-partite states which do not violate the correlation CHSH inequality (15) are product states and they are obviously local (Gisin, 1991; Gisin and Peres, 1992). Then Popescu and Rohrlich showed that any n-partite pure entangled state can always be projected onto a two-partite pure entangled state by projecting $n-2$ parties onto appropriate local pure states (Popescu and Rohrlich, 1992). Clearly, it needs an additional manipulation (postselection). Still the problem of whether the Gisin theorem can be generalized without postselection for an arbitrary n-partite pure entangled state remains open. In the case of three parties there are generalized GHZ states (Scarani and Gisin, 2001b; Żukowski *et al.*, 2002) that do not violate the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequalities (Mermin, 1990a; Ardehali, 1992; Belinskii and Klyshko, 1993) (see the next section). More generally, it has been shown (Żukowski *et al.*, 2002) that these states do not violate any Bell inequality for n-partite correlation functions for experiments involving two dichotomic observables per site. Acin *et al.* and Chen *et al.* considered a Bell inequality that shows numerical evidence that all three-partite pure entangled states violate it (Acín, Chen, *et al.*, 2004; Chen *et al.*, 2004). Recently, a stronger Bell inequality with more measurement settings was presented (Wu and Zong, 2003; Laskowski *et al.*, 2004), which can be violated by a wide class of states, including the generalized GHZ states (see also Chen, Albeverio, *et al.*, 2006).

2. Mixed states

In the case of noisy entangled states the problem appeared to be much more complex. A natural conjecture was that only separable mixed states of the form (34) admit a LHV model. Surprisingly, Werner constructed a one-parameter family of $U \otimes U$ invariant states (see Sec. VI.B.9) in $d \times d$ dimensions, where U is a unitary operator, and showed that some can be simulated by such a model (Werner, 1989b). In particular, two-qubit ($d=2$) Werner states are mixtures of the singlet $|\psi^-\rangle$ with white noise of the form

$$\rho = p|\psi^-\rangle\langle\psi^-| + (1-p)I/4. \tag{21}$$

Using the criterion (20), one finds that the CHSH inequality is violated when $2^{-1/2} < p \leqslant 1$.

However, Popescu noticed that Werner's model accounts only for correlations obtained for a reduced class of local experiments involving projective measurements, and found that some Werner mixtures if subjected to a sequence of local generalized measurements, including postselection, can violate the CHSH inequality (Popescu, 1995). Gisin then demonstrated that even for the case of two qubits the "hidden nonlocality" can be revealed using local filters in the first stage of the process (a procedure of this kind can be treated as a preprocessing consisting of stochastic LOCC) (Gisin, 1996). In the same year, Peres discovered that some states admitting a LHVM for a single copy violate Bell inequalities when more than one copy is jointly measured with the postselection procedure (Peres, 1996b). The merging of these two tests leads to a stronger detection of hidden nonlocality (Masanes, 2006b).

The above results allow us to understand the deep nature of noisy entanglement not just in the context of the LHV model. Clearly, the CHSH inequality can be used as a tool for two nonequivalent tasks: testing the quantum formalism against the LHV model (nonlocality witness) and testing for entanglement within the quantum formalism (entanglement witness). On the other hand, the idea of hidden nonlocality leads to the concept of distillation of entanglement—an important notion in quantum information theory (see Sec. XII). Finally, it turned out that hidden nonlocality allows us to reveal nonclassical features of arbitrary entangled state;

namely, Masanes *et al.* considered specific entanglement witnesses characterizing the states that violate the CHSH inequality after local filtering operators (Masanes *et al.*, 2007). Then they proved that any bipartite entangled state σ exhibits a hidden nonlocality which can be "activated" in the sense that there exists another state ρ not violating the CHSH inequality such that the state $\rho\otimes\sigma$ does violate it (see Sec. XII.I).

D. All $n\times 2\times 2$ Bell inequalities for correlation functions

The CHSH inequality is one elementary inequality that can be viewed as a special case of an infinite hierarchy of Bell inequalities related to the type of correlation measurements with n-partite systems, where each of the parties can measure m observables, each being l-valued. For the CHSH inequality $n=m=l=2$.

As early as 1990 several generalizations of the latter were derived for the case $n,2,2$ (MABK inequalities). The complete set of such inequalities was constructed by Werner and Wolf (2001a) and independently by Żukowski and Brukner (2002); see also Weinfurter and Żukowski (2001). The WWZB inequalities are given by linear combinations of the correlation expectation values

$$\sum_k f(k)E(k)\leqslant 2^n, \tag{22}$$

where coefficients are given by $f(k)=\Sigma_s S(s)(-1)^{\langle k,s\rangle}$, $S(s)$ is an arbitrary function of $s=s_1\cdots s_n\in\{-1,1\}^n$, such that $S(s_1\cdots s_n)=\pm 1$; $\langle k,s\rangle=\Sigma_{j=1}^n k_j s_j$, and $E(k)=\langle\Pi_{j=1}^n A_j(k_j)\rangle_{\mathrm{av}}$ is the correlation function (average over many runs of experiment) labeled by a bit string $k=k_1\cdots k_n$, and the binary variables $k_j\in 0,1$ indicate the choice of the ± 1-valued observable $A_j(k_j)$ at site j.

There are 2^{2^n} different functions $S(s)$, and correspondingly 2^{2^n} inequalities. In particular, putting $S(s_1\cdots s_n)=\sqrt{2}\cos[-\pi/4+(s_1+\cdots+s_n-n)\pi/4]$ one recovers the Mermin-type inequalities, and for $n=2$ the CHSH inequality (15) follows.

Fortunately, the set of linear inequalities (22) is equivalent to a single nonlinear inequality

$$\sum_s\left|\sum_k(-1)^{\langle k,s\rangle}E(k)\right|\leqslant 2^n, \tag{23}$$

which characterizes the structure of the accessible classical region for the correlation function for n-partite systems, a hyperoctahedron in 2^n dimensions, as the unit sphere of the Banach space l^1 (Werner and Wolf, 2001a).

The WWZB inequalities are an important tool for the investigation of possible connections among quantum nonlocality, distillability, and entanglement for n-qubit systems. In particular, it has been shown that violation of the WWZB inequality by a multiqubit state implies that pure entanglement can be distilled from it. But the protocol may require that some of the parties join into several groups (Acín, 2001; Acin *et al.*, 2003). This result was generalized to the asymptotic scenario (Masanes, 2006b). For further development, see Horodecki *et al.*, (2007).

E. Logical versions of Bell's theorem

The violation of Bell inequalities as a paradigmatic test of quantum formalism has some unsatisfactory features as it applies only to a statistical measurement procedure. It is intriguing that the quantum formalism via quantum entanglement offers an even stronger departure from classical intuition based on the logical argument which discusses only perfectly correlated states. This kind of argument was discovered by Greenberger, Horne, and Zeilinger and applies for *individual* systems that are in the GHZ state, i.e., $|\psi\rangle_{ABC}=(1/\sqrt{2})(|000\rangle+|111\rangle)_{ABC}$. They showed that any deterministic LHVM predicts that a certain outcome always happens while quantum formalism predicts it never happens.

The original GHZ argument for qubits has been subsequently developed (Mermin, 1990b; Hardy, 1993; Cabello, 2001a, 2001b; Cerf, Massar, and Pironio 2002; Chen *et al.*, 2003; Greenberger *et al.*, 2005a, 2005b) and extended to continuous variables (Clifton, 2000; Massar and Pironio, 2001; Chen and Zhang, 2002) and it is known as the "all-versus-nothing" proof of the Bell theorem or "the Bell theorem without inequalities." The proofs are purely logical. An important step was the reduction of the GHZ proof to two-particle nonmaximally (Hardy, 1993) and maximally entangled systems of high dimensionality (Torgerson *et al.*, 1995; Kaszlikowski *et al.*, 2000; Durt *et al.*, 2001; Pan *et al.*, 2001; Chen, Chen, *et al.*, 2005).

However, in real experiments ideal measurements and perfect correlations are practically impossible. To overcome the problem of a "null experiment" Bell-type inequalities are needed. Recently two-particle all-versus-nothing nonlocality tests were performed using two-photon so-called hyperentanglement (Cinelli *et al.*, 2005; Yang, Zhang, *et al.*, 2005). A novel nonlocality test, the "stronger two observer all versus nothing" test (Cabello, 2005), has been performed using a four-qubit linear cluster state via two photons entangled in both polarization and linear momentum (Vallone *et al.*, 2007).

F. Violation of Bell inequalities: General remarks

There is much literature concerning interpretation of the "Bell effect." The most evident conclusion from those experiments is that it is not possible to construct a LHVM simulating all correlations observed for quantum states of composite systems. But such a conclusion is not surprising. What is crucial in the context of the Bell theorem is just a *gap* between the quantum and classical descriptions of the correlations, which gets out of hand.

Nature on its fundamental level offers us a new kind of statistical non-message-bearing correlation, which is encoded in the quantum description of states of com-

pound systems via entanglement. They are "nonlocal"[24] in the sense that they cannot be described by a LHVM; but they are *nonsignaling*, as local measurements performed on spatially separated systems cannot be used to transmit messages.

Generally speaking, quantum compound systems can reveal *holistic nonsignaling* effects even if their subsystems are spatially separated by macroscopic distances. In this sense quantum formalism offers a holistic description of nature (Primas, 1983), where in a nontrivial way the system is more than a combination of its subsystems.

It is intriguing that entanglement does not exhaust the full potential of nonlocality under the constraints of no signaling. Indeed, it does not violate Cirel'son's bound (18) for CHSH inequalities. On the other hand, one can design a family of probability distributions (see Gisin, 2005, and references therein), which would violate this bound but still do not allow for signaling. They are called Popescu-Rohrlich nonlocal boxes, and represent extremal nonlocality admissible without signaling (Popescu and Rohrlich, 1994). We see therefore that quantum entanglement is situated at an intermediate level between locality and maximal non-signaling nonlocality. Needless to say, the Bell inequalities still involve many fascinating open problems interesting for both philosophers and physicists (see Gisin, 2007).

V. ENTROPIC MANIFESTATIONS OF ENTANGLEMENT

A. Entropic inequalities: Classical versus quantum order

As mentioned in the Introduction Schrödinger first pointed out that entanglement does not manifest itself only as correlations of outputs of local measurements. In fact, he recognized another aspect of entanglement, which involves a profoundly nonclassical relation between the information that an entangled state gives us about the whole system and the information that it gives us about subsystems.

This new "nonintuitive" property of compound quantum systems, intimately connected with entanglement, was a long-standing puzzle from both a physical and a mathematical point of view. The main difficulty was that, in contrast the concept of correlation, which has a clear operational meaning, the concept of information in quantum theory was obscure until 1995, when Schumacher showed that the von Neumann entropy

$$S(\rho) = -\operatorname{Tr}\rho\log\rho \tag{24}$$

has the operational interpretation of the number of qubits needed to transmit quantum states emitted by a statistical source (Schumacher, 1995). The von Neumann entropy can be viewed as the quantum counterpart of the Shannon entropy $H(X)=-\Sigma_i p_i\log p_i$, $\Sigma_i p_i=1$, which is defined operationally as the minimum number of bits needed to communicate a message produced by a classical statistical source associated to a random variable X.

In 1994 Schrödinger's observation that an entangled state provides more information about the total system than about subsystems was quantified by means of the von Neumann entropy. It was shown that the entropy of a subsystem can be greater than the entropy of the total system only when the state is entangled (Horodecki and Horodecki, 1994). In other words, the subsystems of the entangled system may exhibit more disorder than the system as a whole. In the classical world this never happens. Indeed, the Shannon entropy $H(X)$ of a single random variable is never larger than the entropy of two variables,

$$H(X,Y) \geqslant H(X), \quad H(X,Y) \geqslant H(Y). \tag{25}$$

It has been proven (Horodecki and Horodecki, 1996; R. Horodecki *et al.*, 1996; Terhal, 2002; Vollbrecht and Wolf, 2002b), that analogous α entropy inequalities hold for separable states,

$$S_\alpha(\rho_{AB}) \geqslant S_\alpha(\rho_A), \quad S_\alpha(\rho_{AB}) \geqslant S_\alpha(\rho_B), \tag{26}$$

where $S_\alpha(\rho)=(1-\alpha)^{-1}\log\operatorname{Tr}\rho^\alpha$ is the α Renyi entropy for $\alpha\geqslant 0$; here $\rho_A=\operatorname{Tr}_B(\rho_{AB})$ and similarly for ρ_B. If α tends to 1, one obtains the von Neumann entropy $S_1(\rho)\equiv S(\rho)$ as the limiting case.

B. Entropic inequalities and negativity of information

Entropic inequalities (26) involve a nonlinear functional of a state ρ, so they can be interpreted as *scalar separability criteria* based on a nonlinear entanglement witness (see Sec. VI). This role is analogous to that of Bell inequalities as entanglement witnesses. In this context a natural question arises: Is this all we should expect from violation of entropic inequalities? Surprisingly enough, entropic inequalities are only the tip of the iceberg which reveals dramatic differences between classical and quantum communication due to quantum entanglement. To see this, consider again the entropic inequalities based on the von Neumann entropy ($\alpha=1$) which hold for separable states. They may be equivalently expressed as

$$S(\rho_{AB}) - S(\rho_B) \geqslant 0, \quad S(\rho_{AB}) - S(\rho_A) \geqslant 0 \tag{27}$$

and interpreted as the constraints imposed on the correlations of the bipartite system by positivity of some function

$$S(A|B) = S(\rho_{AB}) - S(\rho_B), \tag{28}$$

and similarly for $S(B|A)$. Clearly, the entropy of the subsystem $S(\rho_A)$ can be greater than the total entropy

[24]The term nonlocality is somewhat misleading. In fact there is a breaking of the conjunction of locality and counterfactuality. Recently, responsibility for breaking this conjunction has been shifted toward violation of counterfactuality itself. Namely, there are *nonlocal* hidden variable models (Leggett, 2003) with more or less reasonable nonlocal influences, which imply inequalities violated by quantum mechanics. Groeblacher *et al.* (2007) performed an experiment verifying this violation.

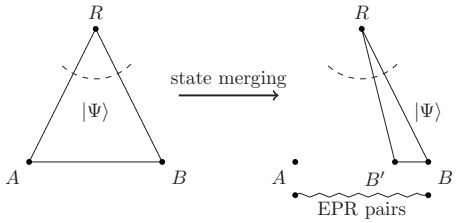

FIG. 1. The concept of state merging: before and after.

$S(\rho_{AB})$ of the system only when the state is entangled. However, there are entangled states which do not exhibit this exotic property, i.e., they satisfy the constraints. Thus the physical meaning of the function $S(A|B)$ $[S(B|A)]$ and its peculiar behavior were an enigma for physicists. It can be viewed as an analog of classical conditional entropy (Werhl, 1978)

$$H(X|Y) = H(X,Y) - H(X). \tag{29}$$

What is intriguing is that this classical function is always positive, while, as we have seen, its quantum version can be negative. Remarkably, just this negative part, if taken with the minus sign, is known under the name of "coherent information"[25] (Schumacher and Nielsen, 1996), and it determines quantum channel capacity (see Sec. XIV.B).

An early attempt to understand the negativity was due to Cerf and Adami (1997). Recently, the solution of the problem was presented within the quantum counterpart of the classical Slepian-Wolf theorem called "quantum state merging" (Horodecki, Oppenheim, *et al.*, 2005; Horodecki *et al.*, 2007). In 1971, Slepian and Wolf considered the following problem: How many bits does the sender (Alice) need to send to transmit a message from the source, provided the receiver (Bob) already has some prior information about the source? The number of bits is called the partial information. Slepian and Wolf (1971) proved that the partial information is equal to the conditional entropy (29), which is always positive: $H(X|Y) \geqslant 0$.

In the quantum state merging scenario, an unknown quantum state is distributed to spatially separated observers Alice and Bob. The question is: How much quantum communication is needed to transfer Alice's part of the state to Bob in such a way that finally Bob has the total state (Fig. 1)? This communication measures the partial information that Bob needs conditioned on its prior information $S(B)$. Surprisingly, Horodecki *et al.* proved that a necessary and sufficient number of qubits is given by (28), even if this quantity is negative.

Remarkably, there are two regimes, classical and quantum, depending on the sign of the partial information $S(A|B)$: (i) Partial information $S(A|B)$ is positive [the inequalities (27) are not violated]: the optimal state merging protocol requires sending $r \cong S(A|B)$ qubits. (ii) Partial information $S(A|B)$ is negative [the inequalities (27) are violated]: optimal state merging does require the sending of qubits; in addition Alice and Bob gain $r \cong -S(A|B)$ pairs of qubits in a maximally entangled state. The quantum and classical regimes are determined by the relations between knowledge about the system as a whole and that about its subsystems, as considered by Schrödinger.

Finally, we note that early manifestations of entanglement [nonlocality (EPR, Bell) and what we can call *insubordination* (Schrödinger)] were seemingly academic issues, of merely philosophical relevance. What is perhaps the most surprising twist is that both the above features qualify entanglement as a resource for performing some concrete tasks.

Indeed, the violation of the Bell inequalities determines the usefulness of quantum states for specific nonclassical tasks, such as, for example reduction of communication complexity, or quantum cryptography (see Sec. III). Similarly, the violation of the entropic inequalities based on the von Neumann entropy (27) determines the usefulness of states as a *potential* for quantum communication. It is in agreement with the earlier results that the negative value of the function $S(A|B)$ is connected with the ability of the system to perform teleportation (Horodecki and Horodecki, 1996; Cerf and Adami, 1997) as well as with a nonzero capacity of a quantum channel (Schumacher and Nielsen 1996; Lloyd, 1997; Devetak, 2003).

C. Majorization relations

In 2001 Nielsen and Kempe discovered a stronger version of the classical versus quantum order (Nielsen and Kempe, 2001), which connects the majorization concept and entanglement; namely, they proved that if a state is separable then the inequalities

$$\lambda(\rho) \prec \lambda(\rho_A), \quad \lambda(\rho) \prec \lambda(\rho_B) \tag{30}$$

have to be satisfied. Here $\lambda(\rho)$ is a vector of eigenvalues of ρ; $\lambda(\rho_A)$ and $\lambda(\rho_B)$ are defined similarly. The relation $x \prec y$ between d-dimensional vectors x and y (x is majorized by y) means that $\Sigma_{i=1}^{k} x_i^{\downarrow} \leqslant \Sigma_{i=1}^{k} y_i^{\downarrow}$, $1 \leqslant k \leqslant d$, and the equality holds for $k=d$, $x_i^{\downarrow} (1 \leqslant i \leqslant d)$ are components of vector x rearranged in decreasing order; $y_i^{\downarrow}$ $(1 \leqslant i \leqslant d)$ are defined similarly. Zeros are appended to the vectors $\lambda(\rho_A)$ and $\lambda(\rho_B)$ in Eq. (30), in order to make their dimension equal to that of $\lambda(\rho)$.

The above inequalities constitute a necessary condition for separability of bipartite states in arbitrary dimensions in terms of the local and global spectra of a state. This criterion is stronger than entropic criterion (26) and it again supports the view that separable states are more disordered globally than locally (Nielsen and Kempe, 2001). An alternative proof of this result has been given (Gurvits and Barnum, 2005).

[25]The term "coherent information" was originally defined to be a function of a state of a single system and a channel, but, further, its use has been extended to apply to a bipartite state.

VI. BIPARTITE ENTANGLEMENT

A. Definition and basic properties

The fundamental question in quantum entanglement theory is which states are entangled and which are not. Only in a few cases does this question have a simple answer. The simplest is the case of pure bipartite states. In accordance with the definition of multipartite entangled states (Sec. II), any bipartite pure state $|\Psi_{AB}\rangle \in \mathcal{H}_{AB}=\mathcal{H}_A\otimes\mathcal{H}_B$ is called separable (entangled) if and only if it can (cannot) be written as a product of two vectors corresponding to Hilbert spaces of subsystems:

$$|\Psi_{AB}\rangle = |\phi_A\rangle|\psi_B\rangle. \tag{31}$$

In general, if the vector Ψ_{AB} is written in any orthonormal product basis $\{|e_A^i\rangle\otimes|e_B^j\rangle\}$ as follows:[26]

$$|\Psi_{AB}\rangle = \sum_{i=0}^{d_A-1}\sum_{j=0}^{d_B-1} A_{ij}^{\Psi}|e_A^i\rangle\otimes|e_B^j\rangle, \tag{32}$$

then it is a product if and only if the matrix of coefficients $A^{\Psi}=\{A_{ij}^{\Psi}\}$ is of rank 1. In general, the rank $r(\Psi)\leqslant k\equiv\min[d_A,d_B]$ of this matrix is called the Schmidt rank of vector Ψ and it is equal to either of the ranks of the reduced density matrices $\varrho_A^{\Psi}=\mathrm{Tr}_B|\Psi_{AB}\rangle\langle\Psi_{AB}|$, $\varrho_B^{\Psi}=\mathrm{Tr}_A|\Psi_{AB}\rangle\langle\Psi_{AB}|$ (which satisfy $\varrho_A^{\Psi}=A^{\Psi}(A^{\Psi})^{\dagger}$ and $\varrho_A^{\Psi}=[(A^{\Psi})^{\dagger}A^{\Psi}]^T$, respectively[27]). In particular, there always exists such a product basis $\{|\tilde{e}_A^i\rangle\otimes|\tilde{e}_B^j\rangle\}$ in which the vector takes the Schmidt decomposition

$$|\Psi_{AB}\rangle = \sum_{i=0}^{r(\Psi)} a_i|\tilde{e}_A^i\rangle\otimes|\tilde{e}_B^i\rangle, \tag{33}$$

where the strictly positive numbers $a_i=\{\sqrt{p_i}\}$ correspond to the nonzero singular eigenvalues (Nielsen and Chuang, 2000) of A^{Ψ}, and p_i are the nonzero elements of the spectrum of either reduced density matrix.

Quantum entanglement is in general both quantitatively and qualitatively considered to be a property *invariant* under product unitary operations $U_A\otimes U_B$. Since in the case of a pure vector and the corresponding pure state (projector) $|\Psi_{AB}\rangle\langle\Psi_{AB}|$ the coefficients $\{a_i\}$ are the only parameters that are invariant under such operations, they completely determine the entanglement of the bipartite pure state.

As already mentioned, the pure state (projector) $|\Psi_{AB}\rangle\langle\Psi_{AB}|$ is separable if and only if the vector Ψ_{AB} is a product. Equivalently, the rank of either of the reduced density matrices ϱ_A, ϱ_B is equal to 1, or there is a single nonzero Schmidt coefficient. Thus for bipartite pure states it is elementary to decide whether the state is separable or not by diagonalizing its reduced density matrix.

[26]Here the orthonormal basis $\{|e_X^i\rangle\}$ spans subspace $\mathcal{H}_X$, $X=A,B$.

[27]T denotes transposition.

So far we have considered entanglement of pure states. Due to the decoherence phenomenon, in laboratories we unavoidably deal with mixed states rather than pure ones. However, a mixed state still can contain some entanglement. In accordance with the general definition for the n-partite state (Sec. II) any bipartite state ϱ_{AB} defined on Hilbert space $\mathcal{H}_{AB}=\mathcal{H}_A\otimes\mathcal{H}_B$ is separable (see Werner, 1989b) if and only if it can neither be represented nor approximated by states of the following form:

$$\varrho_{AB} = \sum_{i=1}^{k} p_i\varrho_A^i\otimes\varrho_B^i, \tag{34}$$

where ϱ_A^i, ϱ_B^i are defined on local Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$. In the case of finite-dimensional systems, i.e., when $\dim\mathcal{H}_{AB}<\infty$, the states ϱ_A^i, ϱ_B^i can be chosen to be pure. Then, from the Caratheodory theorem, it follows (see Horodecki, 1997; Vedral and Plenio, 1998) that the number k in the convex combination can be bounded by the square of the dimension of the global Hilbert space: $k\leqslant d_{AB}^2=(d_Ad_B)^2$, where $d_{AB}=\dim\mathcal{H}_{AB}$, etc., It happens that for two qubits the number of states (sometimes called the cardinality) needed in the separable decomposition is always 4, which corresponds to the dimension of the Hilbert space itself (see Sanpera *et al.*, 1998; Wootters, 1998). There are, however, $d\otimes d$ states that for $d\geqslant 3$ have cardinality of order of $d^4/2$ (see DiVincenzo, Terhal, *et al.*, 2000). We restrict subsequent analysis to the case of finite dimensions unless stated otherwise.

The set $\mathcal{S}_{AB}$ of all separable states defined in this way is convex, compact, and invariant under the product unitary operations $U_A\otimes U_B$. Moreover, the separability property is preserved under so-called (stochastic) separable operations (see Sec. XI.B).

The problem is that, given any state ϱ_{AB}, it is hard to check whether it is separable or not. In particular, its separable decomposition may have nothing in common with the eigendecomposition, i.e., there are many separable states that have their eigenvectors entangled or nonproduct.

It is important to repeat what the term entanglement means on the level of mixed states: all states that do not belong to $\mathcal{S}$, i.e., are not separable (in terms of the above definition), are called *entangled*. In general, the problem of characterization of the set of separable mixed states appears to be extremely complex, as we show next. However, the operational criteria are known which partially describe the set.

B. Main separability criteria in the bipartite case

1. Positive partial transpose criterion

A very strong necessary condition for separability has been provided by Peres (1996b), called the positive partial transpose (PPT) criterion. It says that if ϱ_{AB} is separable then the new matrix $\varrho_{AB}^{T_B}$ with matrix elements defined in some fixed product basis as

$$\langle m|\langle \mu|\varrho_{AB}^{T_B}|n\rangle|\nu\rangle \equiv \langle m|\langle \nu|\varrho_{AB}|n\rangle|\mu\rangle \tag{35}$$

is a density operator (i.e., has a non-negative spectrum), which means that $\varrho_{AB}^{T_B}$ is also a quantum state (it also guarantees the positivity of $\varrho_{AB}^{T_A}$ defined in an analogous way). The operation T_B, called a partial transpose,[28] corresponds to transposition of indices corresponding to the second subsystem and has an interpretation as a partial time reversal (Sanpera *et al.*, 1998).

The PPT condition is known to be stronger than all entropic criteria based on Renyi α entropy (Sec. V) for $\alpha \in [0,\infty]$ (Vollbrecht and Wolf, 2002b). A fundamental fact is (M. Horodecki *et al.*, 1996) that the PPT condition is not only a necessary but also a sufficient condition for separability of the $2\otimes 2$ and $2\otimes 3$ cases. Thus it gives a complete characterization of separability in those cases (for more details and further improvements see Sec. VI.B.2).

2. Separability via positive, but not completely positive, maps

The Peres PPT condition initiated a general analysis of the problem of separable (equivalently entangled) states in terms of linear positive maps (M. Horodecki *et al.*, 1996); namely, it can be seen that the PPT condition is equivalent to demanding the positivity[29] of the operator $[I_A \otimes T_B](\varrho_{AB})$, where T_B is the transposition map acting on the second subsystem. The transposition map is a positive map (i.e., it maps any positive operator on $\mathcal{H}_B$ into a positive one), but it is not completely positive.[30] In fact, $I_A \otimes T_B$ is not a positive map and this is the source of success of the Peres criterion.

It has been recognized that any positive (P) but not completely positive (CP) map $\Lambda: \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_{A'})$ with a codomain related to some new Hilbert space $\mathcal{H}_{A'}$ provides a nontrivial necessary separability criterion in the form

$$[I_A \otimes \Lambda_B](\varrho_{AB}) \geqslant 0. \tag{36}$$

This corresponds to non-negativity of the spectrum of the following matrix:

$$[I_A \otimes \Lambda_B](\varrho_{AB}) = \begin{pmatrix} \Lambda(\varrho_{00}) & \cdots & \Lambda(\varrho_{0d_A-1}) \\ \Lambda(\varrho_{10}) & \cdots & \Lambda(\varrho_{1\,d_A-1}) \\ \cdots & \cdots & \cdots \\ \Lambda(\varrho_{d_A-10}) & \cdots & \Lambda(\varrho_{d_A-1d_A-1}) \end{pmatrix} \tag{37}$$

with $\varrho_{ij} \equiv \langle i| \otimes \mathrm{I}\, |\varrho_{AB}|j\rangle \otimes I$.

It happens that using the above technique one can provide a necessary and sufficient condition for separability (see M. Horodecki *et al.*, 1996): the state ϱ_{AB} is separable if and only if the condition (36) is satisfied for all P but not CP maps $\Lambda: \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A)$ where $\mathcal{H}_A$ and $\mathcal{H}_B$ describe the left and right subsystems of the system AB.

Note that the set of maps can be further restricted to all P but not CP maps that are identity preserving (Horodecki, 2001a) (the set of witnesses can then also be restricted via the isomorphism). One could also restrict the maps to trace preserving ones, but then one has to enlarge the codomain (M. Horodecki *et al.*, 2006).

Given the characterization in terms of maps and witnesses it was natural to ask about a more practical characterization of separability and entanglement. The problem is that in general the set of P but not CP maps is not characterized and it involves a hard problem in contemporary linear algebra (for progress in this direction, see Kossakowski, 2003, and references therein).

However, for very low-dimensional systems there is a surprisingly useful solution (M. Horodecki *et al.*, 1996a): the states of $d_A \otimes d_B$ with $d_A d_B \leqslant 6$ (two-qubit or qubit-qutrit systems) are separable if and only if they are PPT. For two qubits (and only for them) there is an even simpler condition (see Slater, 2005b; Augusiak *et al.*, 2008) important for physical detection (see Sec. VIII.B.2): the two-qubit state ϱ_{AB} is separable if and only if

$$\det(\varrho_{AB}^{\Gamma}) \geqslant 0. \tag{38}$$

This is the simplest two-qubit separability condition. It is a direct consequence of two facts known earlier: the partial transpose of any entangled two-qubit state is of full rank and has only one negative eigenvalue (Sanpera *et al.*, 1998; Verstraete, Audenaert, Dehane, *et al.*, 2001). Note that some generalizations of Eq. (38) for other maps and dimensions are also possible (Augusiak *et al.*, 2008).

The sufficiency of the PPT condition for separability in low dimensions follows from the fact (Størmer, 1963; Woronowicz, 1976) that all positive maps $\Lambda: \mathcal{B}(\mathcal{C}^d) \to \mathcal{B}(\mathcal{C}^{d'})$ where $d=2$, $d'=2$, and $d=2$, $d'=3$ are *decomposable*, i.e., are of the form

$$\Lambda^{\mathrm{dec}} = \Lambda_{CP}^{(1)} + \Lambda_{CP}^{(2)} \circ T, \tag{39}$$

where $\Lambda_{CP}^{(i)}$ stand for some CP maps and T stands for transposition. It can be shown (M. Horodecki *et al.*, 1996) that among all decomposable maps the transposition map T is the "strongest" map, i.e., there is no decomposable map that can reveal entanglement which is not detected by transposition.

3. Separability via entanglement witnesses

Entanglement witnesses (M. Horodecki *et al.*, 1996; Terhal, 2000) are fundamental tools in quantum entanglement theory. They are observables that completely characterize separable states and allow us to detect entanglement physically. Their origin stems from geometry: the convex sets can be described by hyperplanes. This translates into the statement (see M. Horodecki *et*

[28] Following Rains (1998) instead of $\varrho_{AB}^{T_B}$ we write ϱ_{AB}^{Γ} (as Γ is the right "part" of the letter T).

[29] The operator is called positive and only if it is Hermitian and has a non-negative spectrum.

[30] The map Θ is completely positive if and only if $I \otimes \Theta$ is positive for identity map I on any finite-dimensional system.

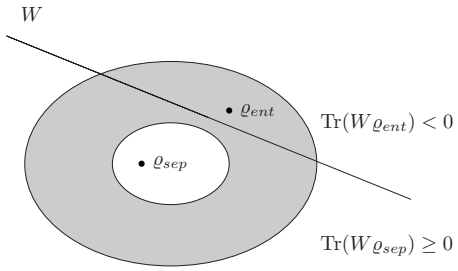

FIG. 2. The line represents a hyperplane corresponding to the entanglement witness W. All states located to the left of the hyperplane or belonging to it (in particular, all separable states) provide non-negative mean value of the witness, i.e., $\mathrm{Tr}(W\varrho_{\mathrm{sep}})\geqslant 0$ while those located to the right are entangled states detected by the witness.

al., 1996; Terhal, 2000) that the state ϱ_{AB} belongs to the set of separable states if it has a non-negative mean value

$$\mathrm{Tr}(W\varrho_{AB})\geqslant 0 \tag{40}$$

for all observables W that (i) have at least one negative eigenvalue and (ii) have a non-negative mean value on product states or equivalently satisfy the non-negativity condition

$$\langle\psi_A|\langle\phi_B|W|\psi_A\rangle|\phi_B\rangle\geqslant 0 \tag{41}$$

for all pure product states $|\psi_A\rangle|\phi_B\rangle$. The observables W satisfying conditions (i) and (ii) above[31] have been named *entanglement witnesses* by Terhal (2000) who stressed their physical importance as entanglement detectors; in particular, one says that entanglement of ϱ is detected by witness W if and only if $\mathrm{Tr}(W\varrho)<0$; see Fig. 2. (We discuss physical aspects of entanglement detection in more detail subsequently.) An example of the entanglement witness for the $d\otimes d$ case is (Werner, 1989b) the Hermitian swap operator

$$V=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes|j\rangle\langle i|. \tag{42}$$

To see that V is an entanglement witness note that we have $\langle\psi_A|\langle\phi_B|V|\psi_A\rangle|\phi_B\rangle=|\langle\psi_A|\phi_B\rangle|^2\geqslant 0$ which ensures property (ii) above. At the same time $V=P^{(+)}-P^{(-)}$ where $P^{(+)}=\frac{1}{2}(I+V)$ and $P^{(-)}=\frac{1}{2}(I-V)$ correspond to projectors onto the symmetric and antisymmetric subspaces of the Hilbert space $\mathcal{C}^d\otimes\mathcal{C}^d$, respectively. Hence V also satisfies (i) since it has some eigenvalues equal to -1. It is interesting to note that V is an example of the so-called decomposable entanglement witness [see Eq. (39) and analysis below].

The P but not CP maps and entanglement witnesses are linked by the so-called Choi-Jamiołkowski isomorphism (Jamiołkowski, 1972; Choi, 1982):

$$W_\Lambda=[I\otimes\Lambda](P_d^+) \tag{43}$$

with pure projector

$$P_d^+=|\Phi_d^+\rangle\langle\Phi_d^+|, \tag{44}$$

where the state vector $\Phi_d^+\in\mathcal{H}_A\otimes\mathcal{H}_A$ is defined as

$$|\Phi_d^+\rangle=\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle\otimes|i\rangle,\quad d=\dim\mathcal{H}_A. \tag{45}$$

The pure projector P_d^+ is an example of a maximally entangled state[32] on the space $\mathcal{H}_A\otimes\mathcal{H}_A$.

An important observation is that while the condition (40) as a whole is equivalent to Eq. (36), a particular witness is not equivalent to a positive map associated via isomorphism: the map provides a stronger condition (see later discussion).

As we have already said, a special class of decomposable P but not CP maps [i.e., of the form (39)] which provide no stronger criterion than the PPT one, is distinguished. Consequently, all corresponding entanglement witnesses are called decomposable and are of the form (see Lewenstein *et al.*, 2000)

$$W^{\mathrm{dec}}=P+Q^\Gamma, \tag{46}$$

where P,Q are some positive operators. It can be shown that decomposable witnesses (equivalently, decomposable maps) describe the set $\mathcal{S}_{\mathrm{PPT}}$ of all states that satisfy the PPT criterion. Like the set $\mathcal{S}$ of separable states this set is also convex, compact, and invariant under product unitary operations. It has also been found that stochastic separable operations preserve the PPT property (M. Horodecki *et al.*, 1998). In general, we have $\mathcal{S}\subsetneq\mathcal{S}_{\mathrm{PPT}}$. As described previously the two sets are equal for $d_Ad_B\leqslant 6$. In all other cases, they differ (Horodecki, 1997) (see Sec. VI.B.7 for examples), i.e., there are entangled states that are PPT. The latter states give rise to the so-called bound entanglement phenomenon (see Sec. XI).

To describe $\mathcal{S}_{\mathrm{PPT}}$ it is enough to consider only a subset of decomposable witnesses where $P=0$ and Q is a pure projector corresponding to entangled vector $|\Phi\rangle$. This gives a minimal set of entanglement witnesses that describe the set of PPT states. The required witnesses are thus of the form

$$W=|\Phi\rangle\langle\Phi|^\Gamma \tag{47}$$

with an entangled vector $|\Phi\rangle$. The swap V is proportional to a witness of this kind. Indeed, we have $V=dP_+^\Gamma$ (hence the swap is a decomposable witness).

For $d\otimes d$ systems there is one distinguished decomposable witness which is not of the form (47) but is useful and looks simple. This is the operator

[31]The witnesses can be shown to be isomorphic to P but not CP maps; see Eq. (43).

[32]For simplicity we drop the dimension denoting the projector onto $\Phi^+\equiv\Phi_d^+$ as $P^+\equiv P_d^+$ provided it does not lead to ambiguity.

$$W(P^+) = d^{-1}I - P^+. \tag{48}$$

One can prove that the condition $\langle W(P^+)\rangle_{\varrho_{\rm PPT}} \geqslant 0$ provides immediately the restriction on the parameter called fidelity or singlet fraction:[33]

$$F(\varrho) = \mathrm{Tr}[P^+\varrho]; \tag{49}$$

namely (see Rains, 2001),

$$F(\varrho_{\rm PPT}) \leqslant 1/d. \tag{50}$$

In particular, this inequality was found first for separable states and its violation was shown to be sufficient for entanglement distillation (Horodecki and Horodecki, 1999).

As already mentioned, the set of map conditions (36) is equivalent to the set of witness conditions (40). Nevertheless, any single witness W_Λ condition is much weaker than the condition given by the map Λ. This is because the first is of scalar type, while the second represents an operator inequality condition. To see this difference it is enough to consider the two-qubit case and compare the transposition map T (which detects all entanglement in the sense of the PPT test) with the entanglement witness isomorphic to it, which is the swap operation V, that does not detect entanglement of any symmetric pure state. Indeed it is not difficult to see (see Horodecki and Ekert, 2002) that the condition based on one map Λ is equivalent to a continuous set of conditions defined by all witnesses of the form $W_{\Lambda,A} \equiv A \otimes I W_\Lambda A^\dagger \otimes I$ where A are operators on $\mathcal{C}^d$ of rank more than 1. It implies, in particular, that the PPT condition associated with *a single* map (transposition T) is equivalent to the set of all the conditions provided by the witnesses of the form (47).

On the other hand, one must stress that the condition based on a witness is naturally directly measurable (Terhal, 2000) while physical implementation of the separability condition based on (unphysical) P but not CP maps is much more complicated, though still possible (see Sec. VIII.B.1).

The important question one can ask about entanglement witnesses regards their optimality (Lewenstein *et al.*, 2000, 2001). We say that an entanglement witness W_1 is *finer* than W_2 if and only if the entanglement of any ϱ detected by W_2 is also detected by W_1. A given witness W is called optimal if and only if there is no witness finer than it. The useful sufficient condition of optimality (Lewenstein *et al.*, 2000) is expressed in terms of the Hilbert subspace $\mathcal{P}_W = \{|\phi\rangle|\psi\rangle : \langle\phi|\langle\psi|W|\phi\rangle|\psi\rangle = 0\}$; namely, if $\mathcal{P}_W$ spans the whole Hilbert space then the witness is optimal. In a sense it is then fully "tangent" to the set of separable states. The systematic method of optimization of a given entanglement witness was worked out first by Lewenstein *et al.* (2000, 2001) [for an alternative optimization procedure, see Eisert *et al.* (2004); cf. the optimization of witnesses for continuous variables (Hyllus and Eisert, 2006)].

In some analogy to the pure bipartite case, we can define the Schmidt rank for density matrices (Terhal and Horodecki, 2000) as $r_S(\varrho) = \min\{\max_i[r_S(\psi_i)]\}$ where the minimum is over all decompositions $\varrho = \Sigma_i p_i |\psi_i\rangle\langle\psi_i|$ and $r_S(\psi_i)$ are the Schmidt ranks of the corresponding pure states (see Sec. VI.A). One can easily prove that separable operations[34] cannot increase it.

Now, for any k in the range $\{1, \ldots, r_{\max}\}$ with $r_{\max} = \min[d_A, d_B]$, we have a set $\mathcal{S}_k$ of states with a Schmidt number not greater than k. For each such set we can build a theory similar to that of separable/entangled states, with Schmidt-number witnesses in place of usual witnesses. The family of sets $\mathcal{S}_k$ satisfies inclusion relations $\mathcal{S}_1 \subset \mathcal{S}_2 \subset \cdots \subset \mathcal{S}_{r_{\max}}$. Note here that $\mathcal{S}_1$ corresponds to the set of separable states, while $\mathcal{S}_{r_{max}}$ corresponds to the set of all states. Each set is compact, convex, and again closed under separable operations. Moreover, each such set is described by k-positive maps (Terhal and Horodecki, 2000) or by Schmidt rank k witnesses (Sanpera *et al.*, 2001). A Schmidt rank k witness is an observable W_k that satisfies the following two conditions: (i) it must have at least one negative eigenvalue, and (ii) it must satisfy

$$\langle\Psi_k|W_k|\Psi_k\rangle \geqslant 0, \tag{51}$$

for all Schmidt rank k vectors $\Psi_k \in \mathcal{H}_{AB}$. As in the case of the separability problem the k-positive maps are related via Choi-Jamiołkowski isomorphism to special maps that are called k positive (i.e., such that $[I_k \otimes \Lambda_k]$ is positive for I_k being identity on $\mathcal{B}(\mathcal{C}^k)$) but not completely positive. The isomorphism is virtually the same as the one that links entanglement witnesses $W = W_1$ with 1-positive (i.e., just positive) maps Λ_1. Many techniques have been generalized from separability to mixed state Schmidt rank analysis (see Sanpera *et al.*, 2001). For a general review of the separability problem including especially entanglement witnesses, see Bruß (2002), Bruß *et al.* (2002), Terhal (2002). The Schmidt number witnesses and maps description has been reviewed by Bruß *et al.* (2002).

4. Estimating entanglement from incomplete data

As mentioned, entanglement witnesses have been found important in experimental detection of entanglement: for any entangled state $\varrho_{\rm ent}$ there are witnesses that are signatures of entanglement in a sense that they are negative on this state $\mathrm{Tr}(W\varrho_{\rm ent}) < 0$. Here we describe applications of entanglement witnesses for evaluation of entanglement based on incomplete experimental data, or macroscopic parameters.

The first issue concerns the following question (R. Horodecki *et al.*, 1999): Given experimental mean values of an incomplete set of observables $\langle A_i\rangle = a_i$ what information about entanglement should be concluded based on those data? The idea was that if entanglement is finally needed as a resource then the observer should con-

[33] One has $0 \leqslant F(\varrho) \leqslant 1$ and $F(\varrho) = 1$ if and only if $\varrho = P^+$.

[34] Separable operations are described in Sec. XIII.

sider the worst case scenario, i.e., should minimize entanglement under experimental constraints. In other words, experimental entanglement should be of the form

$$E(a_1, \ldots, a_k) = \inf_{\{\langle A_i\rangle_\varrho = a_i\}_{i=1}^k} E(\varrho). \tag{52}$$

Such minimization of the entanglement of formation and relative entropy of entanglement was performed for a given mean of the Bell observable on an unknown two-qubit state.

Recently the idea of minimization of entanglement under experimental constraints was applied with the help of entanglement witnesses (Eisert *et al.*, 2007; Gühne, Reimpell, *et al.*, 2007). Gühne, Reimpell, *et al.* (2007) using convex analysis performed a minimization of convex entanglement measures for given mean values of entanglement witnesses based on approximation of convex function by affine functions from below. Specific estimates have been performed for existing experimental data. Independently a similar analysis of lower bounds for many entanglement measures was performed by Eisert *et al.* (2007), where the emphasis was on analytical formulas for specific examples. The derived formulas (Eisert *et al.*, 2007; Gühne, Reimpell, *et al.*, 2007) provide a direct quantitative role for results of entanglement witnesses measurements. Note that a more refined analysis was focused on correlations obtained in the experiment, identifying which types of correlations measured in incomplete experiments may be already a signature of entanglement (Audenaert and Plenio, 2006).

Another issue, where entanglement witnesses have been applied, is the problem of macroscopic entanglement at finite temperature. A threshold temperature for existence of entanglement can be identified. The relation between the thermal equilibrium state and entanglement was hidden in a two-qubit analysis of the Jaynes principle and entanglement (R. Horodecki *et al.*, 1999). The first explicit analysis of entanglement in the thermal state was provided by Nielsen (1998) where first calculation of temperatures for which entanglement is present in the two-qubit Gibbs state was performed. A fundamental observation is that entanglement witness theory can be exploited to detect entanglement in general (multipartite) thermal states including systems with a large number of particles (Brukner and Vedral, 2004; Toth, 2005). In the most elegant approach, for any observable O one defines an entanglement witness as follows (see Toth, 2005)

$$W_O = O - \inf_{|\Psi_{\text{prod}}\rangle} \langle \Psi_{\text{prod}}|O|\Psi_{\text{prod}}\rangle, \tag{53}$$

where the infimum is taken over all product pure states Ψ_{prod} (note that the method can be extended to take into account partial separability[35] as well). Now if W_O has a negative eigenvalue it becomes immediately an entanglement witness by construction. In the case of spin lattices one takes $O=H$ where H is a Hamiltonian of the system and calculates $\langle W_H\rangle_\varrho$ for quantum Gibbs state $\varrho_{\text{Gibbs}}=\exp(-H/kT)/\text{Tr}[\exp(-H/kT)]$. It can be seen that for H with a discrete spectrum the observable W_H has a negative eigenvalue if the lowest-energy state is entangled and then the observable becomes an entanglement witness by construction [see Eq. (53)]. In this way one can estimate the range of temperatures for which the mean value $\langle W_H\rangle_{\varrho_{\text{Gibbs}}}$ is negative (Toth, 2005). Further improvements involve uncertainty based entanglement witnesses (Anders, Kaszlikowski, *et al.*, 2006) and applications of entanglement measures like robustness of entanglement (Markham *et al.*, 2006) to thermal entanglement.

5. Entanglement witnesses and Bell inequalities

Entanglement witnesses (see Sec. VI) are Hermitian operators that are designed directly for detection of entanglement. In 2000 Terhal first considered a possible connection between entanglement witnesses and Bell inequalities (Terhal, 2000). From a "quantum" point of view, Bell inequalities are just nonoptimal entanglement witnesses. For example, one can define a CHSH-type witness which is positive on all states that admit the LHVM,

$$W_{\text{CHSH}} = 2I - \mathcal{B}_{\text{CHSH}}, \tag{54}$$

where $\mathcal{B}_{\text{CHSH}}$ is the CHSH operator (16).

In 1999 Peres conjectured (Peres, 1999) that PPT states do not violate Bell inequalities:

$$\text{LHVM} \Leftrightarrow \text{PPT}. \tag{55}$$

The answer to this question will give important insight into our understanding of classical versus quantum behavior of states of composite systems.

In the multipartite case, Bell inequalities can even detect so-called bound entanglement [Kaszlikowski *et al.*, 2000; Werner and Wolf, 2000, 2001b; Dür, 2001; Sen(De) *et al.*, 2002; Augusiak and Horodecki, 2006].

In general, the problem of the relation between Bell inequalities and entanglement witnesses is very complex. It follows from the very large number of "degrees of freedom" of the Bell inequalities. Nevertheless, it is a basic problem, as the Bell observable is a *double* witness. It detects not only entanglement but also nonlocality.

6. Distinguished map criteria: Reduction criterion and its extensions

There are two important separability criteria provided by P but not CP maps. The first one is the so-called reduction criterion (Cerf *et al.*, 1999; Horodecki and Horodecki, 1999) defined by Eq. (36) with the reduction map: $\Lambda^{red}(\varrho)=I\,\text{Tr}(\varrho)-\varrho$. This map is decomposable but, as we show subsequently, plays an important role in entanglement distillation theory (Horodecki and Horodecki, 1999). Only in the case of a two-dimensional Hilbert space does the map represent a reflection in the Bloch sphere representation (Bengtsson and Życzkowski, 2006), and it can be easily shown to be equal

[35]See Sec. VII.

to the transpose map T followed by σ_y, i.e., $\sigma_y T(\varrho)\sigma_y$. As such it provides a separability condition completely equivalent to PPT in this special (two-qubit) case. In general, the reduction separability criterion $[I_A \otimes \Lambda_B^{\mathrm{red}}](\varrho_{AB}) \geqslant 0$ generated by Λ^{red} can be written as

$$\varrho_A \otimes I - \varrho_{AB} \geqslant 0 \tag{56}$$

and since Λ^{red} is decomposable (Horodecki and Horodecki, 1999) the corresponding separability criterion is weaker than the PPT one (see Sec. VI.B.2). On the other hand, it is interesting that this criterion is stronger (Hiroshima, 2003) than majorization separability criteria (Nielsen and Kempe, 2001) as well as some entropic criteria with $\alpha \in [0,1]$ and $\alpha=\infty$ (for the proofs see Vollbrecht and Wolf, 2002b, and Horodecki and Horodecki, 1999, respectively).

Another important criterion is the one based on the map due to Breuer and, independently, Hall (Breuer, 2006a; Hall, 2006) which is a modification of the reduction map on the even-dimensional Hilbert space $d=2k$. On this subspace there exist antisymmetric unitary operations $U^T=-U$ (for instance, $U=\mathrm{antidiag}[1,-1,1,-1,\ldots,1,-1]$ (Breuer, 2006a)). The corresponding antiunitary map $U(\cdot)^T U$ maps any pure state to some state that is orthogonal to it. This leads to the conclusion that the map which acts on the state ϱ as

$$\Lambda(\varrho) = \Lambda^{\mathrm{red}}(\varrho) - U(\varrho)^T U^\dagger \tag{57}$$

is positive for any antisymmetric U. This map is *not decomposable* and the entanglement witness W_Λ corresponding to it has an optimality property since the corresponding space $\mathcal{P}_{W_\Lambda}$ (see Sec. VI.B.3) is the full Hilbert space (Breuer, 2006b). This nondecomposability property allows the map to detect a special class of very weak entanglement, namely, the PPT entanglement mentioned before.

7. Range criterion and its applications; PPT entanglement

The existence of nondecomposable maps (witnesses) with $d_A\, d_B > 6$ implies that there are states that are entangled but PPT in all those cases. Thus the PPT test is no longer a sufficient test of separability in those cases. This has striking consequences for quantum communication theory, including entanglement distillation (where PPT entanglement represents so-called bound entanglement phenomenon, Sec. XII) and quantum key distribution (Sec. XIX.B) discused later. The existence of PPT entangled states was known already in terms of cones in the mathematical literature [see, e.g., Choi (1982)], sometimes expressed in direct sum language.

On physical grounds, the first examples of entangled states that are PPT were provided by Horodecki (1997), following the Woronowicz construction (Woronowicz, 1976). Their entanglement was found by a criterion that is independent of the PPT one. As mentioned, this might be done with a properly chosen P but not CP nondecomposable map (see Sec. VI.B.2). Horodecki (1997) formulated another criterion for this purpose, which is useful for other applications (see below). This is the range criterion: if ϱ_{AB} is separable, then there exists a set of product vectors $\{\psi_A^i \otimes \phi_B^i\}$ that spans the range of ϱ_{AB} while $\{\psi_A^i \otimes (\phi_B^i)^*\}$ spans the range of $\varrho_{AB}^{T_B}$, where the complex conjugate is taken in the same basis in which the PPT operation on ϱ_{AB} has been performed. In particular, an example of the $3\otimes 3$ PPT entangled state revealed by the range criterion (written in a standard basis) was provided:

$$\varrho_a = \frac{1}{8a+1}\begin{bmatrix} a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1+a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ a & 0 & 0 & 0 & a & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1+a}{2} \end{bmatrix}, \tag{58}$$

where $0<a<1$. Further examples of PPT states that are entangled can be found in Alber, Beth, *et al.* (2001).

An interesting application of the range criterion to finding PPT states is the unextendible product basis (UPB) method by Bennett, DiVincenzo, Mor, *et al.* (1999) and DiVincenzo *et al.* (2003) (for further development see, e.g., Pittenger, 2003; Bandyopadhyay, Ghosh, *et al.*, 2005). The UPB is a set $\mathcal{S}_{\mathrm{UPB}}$ of orthonormal product vectors in $\mathcal{H}_{AB}=\mathcal{H}_A\otimes\mathcal{H}_B$ such that there is no product vector that is orthogonal to all of them.

Example. An example in the $3\otimes 3$ case is (Bennett, DiVincenzo, Mor, *et al.*, 1999) $S_{\mathrm{UPB}} \equiv \{|0\rangle(|0\rangle+|1\rangle), (|0\rangle+|1\rangle)|2\rangle, |2\rangle(|1\rangle+|2\rangle)(|1\rangle+|2\rangle)|0\rangle, (|0\rangle-|1\rangle+|2\rangle)(|0\rangle-|1\rangle+|2\rangle)\}$.

Since there is no product vector orthogonal to the subspace $\mathcal{H}_{\mathrm{UPB}}$ spanned by elements of $\mathcal{S}_{\mathrm{UPB}}$, any vector from the orthogonal subspace $\mathcal{H}_{\mathrm{UPB}}^\perp$ (spanned by vectors orthogonal to $\mathcal{H}_{\mathrm{UPB}}$) is entangled. Consequently, by the above range criterion, any mixed state with support contained in $\mathcal{H}_{\mathrm{UPB}}^\perp$ is entangled. In particular, a special class of states proportional to the projector $P_{\mathcal{H}_{\mathrm{UPB}}^\perp}=\mathrm{I}-P_{\mathcal{H}_{\mathrm{UPB}}}$ (here $P_{\mathcal{H}}$ stands for the projection onto the subspace $\mathcal{H}$) is also entangled, but it can be shown to be PPT because of the special way in which the projector $P_{\mathcal{H}_{\mathrm{UPB}}}$ was constructed. In this way the notion of the UPB leads to the construction of PPT entangled states. This result was further exploited to provide new nondecomposable maps (Terhal, 2001). The idea was to take a projector on UPB space $P_{\mathcal{H}_{\mathrm{UPB}}}$ and observe that the following quantity $\epsilon=\min_{\Psi_{\mathrm{sep}}}\langle\Psi_{\mathrm{sep}}|P_{\mathcal{H}_{\mathrm{UPB}}}|\Psi_{\mathrm{sep}}\rangle$ is strictly positive because of the unextendibility property. Then consider the operator on $d\otimes d$ space:

$$W_{\mathrm{UPB}} = P_{\mathcal{H}_{\mathrm{UPB}}} - d\epsilon|\Psi_{\max}\rangle\langle\Psi_{\max}|, \tag{59}$$

where $\Psi_{\max}$ is a maximally entangled state such that $|\Psi_{\max}\rangle \notin \mathcal{H}_{\mathrm{UPB}}$ (one can always show that such a vector exists). Any entanglement witness of the above form de-

tects PPT entanglement of $\varrho_{\mathrm{UPB}}=(1/\mathcal{N})(\mathrm{I}-P_{\mathcal{H}_{\mathrm{UPB}}})$ since the mean value $\mathrm{Tr}(W_{\mathrm{UPB}}\varrho_{\mathrm{UPB}})$ will gain only the (negative) contribution from the second term of the Eq. (59). At the same time, the optimization of the ϵ above guarantees that the W_{UPB} has nonnegative mean value on any product state; hence it is indeed a legitimate witness. Terhal calculated explicitly the lower bounds for the parameter ϵ for a few examples of UPBs.

This idea was further generalized to the case of *edge* states (Lewenstein *et al.*, 2000) (see also Lewenstein and Sanpera, 1998; Horodecki *et al.*, 2000; Kraus *et al.*, 2000). A state is called an "edge" and denoted as δ_{edge} if it satisfies the following properties: (i) the PPT property and (ii) extremal violation of the range criterion [i.e., there should be no $|\phi\rangle|\psi\rangle\in\mathcal{R}(\varrho)$ such that $|\phi\rangle|\psi^*\rangle\in\mathcal{R}(\varrho^{\Gamma})$]. It can be seen that entanglement of any PPT entangled state is due to some "nonvanishing" admixture of the edge state. In particular, convex null of separable and edge states is equal to PPT states. An example of an edge state is any state based on the UPB construction, ϱ_{UPB}. Another edge state is the $2\otimes 4$ PPT entangled state from Horodecki (1997).

Now the generalization of the Terhal construction leads to a method that in fact detects any PPT entanglement (Lewenstein *et al.*, 2001):

$$W=P+Q^{\Gamma}-\epsilon C/c, \tag{60}$$

with P, Q positive operators supported on kernels of δ_{edge} and $\delta_{\mathrm{edge}}^{\Gamma}$ respectively, while $\epsilon=\min_{\Psi_{\mathrm{sep}}}\langle\Psi_{\mathrm{sep}}|P+Q^{\Gamma}|\Psi_{\mathrm{sep}}\rangle$ can be shown to be strictly positive (by extremal violation of the range criterion by the δ_{edge} state) while C is an arbitrary positive operator with $\mathrm{Tr}(C\delta_{\mathrm{edge}})>0$ and $c=\max_{\Psi_{\mathrm{sep}}}\langle\Psi_{\mathrm{sep}}|C|\Psi_{\mathrm{sep}}\rangle$. All the above witnesses are nondecomposable, and it is interesting that entanglement of all PPT entangled states can be detected even by a restricted subclass of the above, when P, Q are projectors on the kernels of δ_{edge}, while C is the identity operator (then $c=1$). Of course all maps isomorphic to the above witnesses are also nondecomposable.

Returning to the range criterion introduced above, there is an interesting application: the so-called Lewenstein-Sanpera decomposition; namely, any bipartite state ϱ can be uniquely decomposed (see Karnas and Lewenstein, 2000) in the following way (Lewenstein and Sanpera, 1998):

$$\varrho=(1-p)\varrho_{\mathrm{sep}}+p\sigma, \tag{61}$$

where ϱ_{sep} [called the best separable approximation (BSA)] is a separable state, and p is a minimal probability $p\in[0,1]$, such that σ is still a legitimate state. Clearly, ϱ is separable if and only if $p=1$. Otherwise, ϱ is entangled and so is σ. For two qubits the entangled part σ is always pure (Lewenstein and Sanpera, 1998). Moreover, the decomposition can then be found in a fully algebraic way without an optimization procedure (Wellens and Kuś, 2001); in particular, if ϱ_{sep} is of full rank, then σ is maximally entangled and p^* is equal to the so-called Wootters concurrence (see Wellens and Kuś, 2001, for the proof).

The range criterion takes into account vectors from the range. A significant step further is to take into account the ensemble of—in general, nonorthogonal—vectors v_i, which reproduce the state $\rho=\Sigma_i|v_i\rangle\langle v_i|$. The possibility to make them all product *at once* defines separability. This leads to necessary and sufficient separabilty criteria via biconcurrence (Badziag *et al.*, 2002, 2007) and is related to the entanglement measure called concurrence (see Sec. XV.C.2.a). Recently this type of approach (i.e., basing directly on analysis of ensemble) resulted in the useful characterization of bipartite separability in terms of families of commuting normal matrices (Samsonowicz *et al.*, 2007).

8. Matrix realignment criterion and linear contraction criteria

There is yet another class of strong criteria based on linear contractions on product states. They stem from the new criterion discovered by Chen and Wu (2003) and Rudolph (2003) called the computable cross-norm (CCN) criterion or the matrix realignment criterion which is operational and independent the PPT test (Peres, 1996b). In terms of matrix elements it can be stated as follows: If the state ϱ_{AB} is separable then the matrix $\mathcal{R}(\varrho)$ with elements

$$\langle m|\langle\mu|\mathcal{R}(\varrho_{AB})|n\rangle|\nu\rangle\equiv\langle m|\langle n|\varrho|\nu\rangle|\mu\rangle \tag{62}$$

has a trace norm not greater than 1 (there are many other variants; see Horodecki, Horodecki, *et al.*, 2006).

It can be formally generalized as follows: if Λ satisfies

$$\|\Lambda(|\phi_A\rangle\langle\phi_A|\otimes|\phi_B\rangle\langle\phi_B|)\|_1\leqslant 1 \tag{63}$$

for all pure product states $|\phi_A\rangle\langle\phi_A|\otimes|\phi_B\rangle\langle\phi_B|$ then for any separable state ϱ_{AB} one has $\|\Lambda(\varrho_{AB})\|_1\leqslant 1$.[36] The matrix realignment map $\mathcal{R}$ which permutes matrix elements satisfies the above contraction condition on products (63). To find other interesting contractions of that type that are not equivalent to realignment is an open problem.

Quite remarkably, the realignment criterion has been found to detect some of the PPT entanglement (Chen and Wu, 2003) (see also Rudolph, 2003) and to be useful for construction of some nondecomposable maps. It also provides a lower bound on an entanglement measure—concurrence (see Chen *et al.*, 2005b). On the other hand, it happens that for any state that violates the realignment criterion there is a local uncertainty relation (LUR) (see Sec. VIII.A) that is violated, but the converse statement is not always true (Gühne *et al.*, 2006). On the other hand, finding LURs (like finding original entanglement witnesses) is not easy in general and there is no practical characterization of LURs known so far, while the realignment criterion is elementary, fast in application, and still powerful enough to detect PPT entanglement.

[36]Here $\|X\|_1=\mathrm{Tr}\sqrt{XX^{\dagger}}$ denote the trace norm.

9. Some important classes of quantum states

In this section we recall classes of states for which the PPT property is equivalent to separability. We start from Werner states that are linked to one intriguing problem of entanglement theory,namely, the NPT bound entanglement problem (DiVincenzo, Shor, *et al.*, 2000; Dür, Cirac, *et al.*, 2001) (see Sec. XII).

Werner $d\otimes d$ states (Werner, 1989b). Define projectors $P^{(+)}=(I+V)/2$, $P^{(-)}=(I-V)/2$ with identity I, and "flip" operation V (42). The $d\otimes d$ state

$$W(p)=(1-p)\frac{2}{d^2+d}P^{(+)}+p\frac{2}{d^2-d}P^{(-)},\quad 0\leqslant p\leqslant 1, \tag{64}$$

is invariant under any $U\otimes U$ operation for any unitary U. $W(p)$ is separable if and only if it is PPT, which holds for $0\leqslant p\leqslant\frac{1}{2}$.

Isotropic states (Horodecki and Horodecki, 1999). They are $U\otimes U^*$ invariant (for any unitary U) $d\otimes d$ states. They are of the form

$$\varrho_F=\frac{1-F}{d^2-1}(I-P_+)+\frac{Fd^2-1}{d^2-1}P_+,\quad 0\leqslant F\leqslant 1 \tag{65}$$

[with P^+ defined by Eq. (44)]. An isotropic state is separable if and only if it is a PPT, which holds for $0\leqslant F\leqslant\frac{1}{d}$.

Low global rank class (Horodecki, Lewenstein, et al., 2000). The general class of the $d_A\otimes d_B$ states which have global rank not greater than the local ones: $r(\varrho_{AB})\leqslant\max[r(\varrho_A),r(\varrho_B)]$. Here again the PPT condition is equivalent to separability. If $r(\varrho_{AB})<\max[r(\varrho_A),r(\varrho_B)]$ (which corresponds to a violation of the entropic criterion for $\alpha=\infty$) then the PPT test is violated, because the reduction criterion (weaker than PPT) is stronger than the S_∞ entropy criterion (Horodecki, Smolin, *et al.*, 2003).

VII. MULTIPARTITE ENTANGLEMENT—SIMILARITIES AND DIFFERENCES

In the multipartite case the qualitative definition of separability and entanglement is much richer than in bipartite case. There is so-called full separability, which is the direct generalization of bipartite separability. Moreover, there are many types of *partial* separability. Below we discuss the separability criteria in this more complicated situation.

A. Notion of full (m-partite) separability

The definition of full multipartite separability (or m separability) of m systems $A_1\cdots A_m$ with Hilbert space $\mathcal{H}_{A_1\cdots A_n}=\mathcal{H}_{A_1}\otimes\cdots\otimes\mathcal{H}_{A_m}$ is analogous to that in the bipartite case: $\varrho_{AB}=\Sigma_{i=1}^k p_i\varrho_{A_1}^i\otimes\cdots\otimes\varrho_{A_m}^i$. The Carathéodory bound is kept, $k\leqslant\dim\mathcal{H}_{A_1\cdots A_m}^2$. Such a defined set of m-separable states is again (i) convex and (ii) closed (with respect to the trace norm). Moreover, separability is preserved under m-separable operations (see Sec. XIII), which are an immediate generalization of the bipartite separable ones,

$$\varrho_{A_1,\ldots,A_m}\to\frac{\sum_i A_i^1\otimes\cdots\otimes A_i^n\varrho_{A_1,\ldots,A_m}(A_i^1\otimes\cdots\otimes A_i^n)^\dagger}{\mathrm{Tr}\left[\sum_i A_i^1\otimes\cdots\otimes A_i^n\varrho_{A_1,\ldots,A_m}(A_i^1\otimes\cdots\otimes A_i^n)^\dagger\right]}. \tag{66}$$

The separability characterization in terms of positive, but not completely positive, maps and witnesses generalizes in a natural way (M. Horodecki *et al.*, 2001). There is a condition analogous to Eq. (36) with I acting on one first subsystem $\mathcal{H}_{A_1}$ and the map $\Lambda_{A_2\cdots A_m}$: $\mathcal{B}(\mathcal{H}_{A_2,\ldots,A_m})\to\mathcal{B}(\mathcal{H}_{A_1})$. Namely, in Eq. (36) we take maps $\Lambda_{A_2\cdots A_m}$: $\mathcal{B}(\mathcal{H}_{A_2,\ldots,A_m})\to\mathcal{B}(\mathcal{H}_{A_1})$ that are positive on product states, i.e., $\Lambda_{A_2\cdots A_m}(|\phi_{A_2}\rangle\langle\phi_{A_2}|\otimes\cdots\otimes|\phi_{A_m}\rangle\langle\phi_{A_m}|)\geqslant 0$ (with arbitrary states $\phi_{A_i}\in\mathcal{H}_{A_i}$) but not completely positive. The corresponding entanglement witness must have again (i) at least one negative eigenvalue and also satisfy (ii)

$$\langle\phi_{A_1}|\cdots\langle\phi_{A_m}|W|\phi_{A_1}\rangle\cdots|\phi_{A_m}\rangle\geqslant 0. \tag{67}$$

Maps and witnesses are again related by the isomorphism (43) with the maximally entangled state P_+ on the bipartite system A_1A_1.

The above description provides a full characterization of m separability of the m partite system. An example of maps positive on product states is a product of positive maps. Of course there exist maps that are positive on product states, but are not of the latter form [those are in particular maps (M. Horodecki *et al.*, 2001) detecting entanglement of some semiseparable states constructed in Bennett, DiVincenzo, Mor, *et al.* (1999); see one of the examples below]. Multipartite witnesses and related maps were investigated by Jafarizadeh *et al.* (2006) by means of linear programming.

Example. An elementary example of a fully separable three-qubit state is

$$\varrho = p|0\rangle\langle 0|^{\otimes 3} + (1-p)|1\rangle\langle 1|^{\otimes 3}. \tag{68}$$

We now consider the case of pure states in more detail. A pure m-partite state is fully separable if and only if it is a product of pure states describing m elementary subsystems. To check it, it is enough to compute the reduced density matrices of elementary subsystems and check whether they are pure. However, if one asks about the possible ways this simple separability condition is violated then the situation becomes more complicated.

The first problem is that in the multipartite case (in comparison to the bipartite one) only rarely do pure states admit the generalized Schmidt decomposition $|\Psi_{A_1,\ldots,A_m}\rangle = \Sigma_{i=1}^{\min[d_{A_1},\ldots,d_{A_m}]} a_i |\tilde{e}^i_{A_1}\rangle \otimes \cdots \otimes |\tilde{e}^i_{A_m}\rangle$ (see Peres, 1995; Thapliyal, 1999). An example of state admitting Schmidt decomposition in the $d^{\otimes m}$ case is the generalized Greenberger-Horne-Zeilinger state

$$|\mathrm{GHZ}\rangle_d^{(m)} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} (|i\rangle^{\otimes m}), \tag{69}$$

which is a generalization of the original GHZ state (Greenberger *et al.*, 1989) that is a three-qubit vector $|\mathrm{GHZ}\rangle = 1/\sqrt{2}(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle)$. To give an example of a state which does not admit Schmidt decomposition, note that the latter implies that if we trace out any subsystem, the rest is in a fully separable state. One easily finds that the state

$$|W\rangle = \frac{1}{\sqrt{3}}(|0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |1\rangle|0\rangle|0\rangle) \tag{70}$$

has an entangled two-qubit subsystem, and hence does not admit Schmidt decomposition (Dür, Vidal, *et al.*, 2000).

Thus in general the entanglement of a pure state is described by the spectra of reduced density matrices produced by all bipartite partitions. As implied by the full separability definition it is said to be fully m-partite separable if and if only

$$|\Psi_{A_1,\ldots,A_m}\rangle = |\psi_{A_1}\rangle \otimes \cdots \otimes |\psi_{A_m}\rangle. \tag{71}$$

However, violation of this condition does not automatically guarantee what can be intuitively considered as "truly" m-partite entanglement (to understand this, see, for instance, the four-system state $\Psi_{A_1A_2A_3A_4} = |\Phi_{A_1A_2}\rangle \otimes |\Phi_{A_3A_4}\rangle$ where at least one vector $\Phi_{A_1A_2}$, $\Phi_{A_3A_4}$ is entangled).

One says that an m-partite state is *m-partite entangled* if and only if all bipartite partitions produce mixed reduced density matrices (note that both reduced states produced in this way have the same nonzero eigenvalues). This means that there does not exist a cut, against which the state is a product. To this class belong all those pure states that satisfy the generalized Schmidt decomposition (like the GHZ state above). But there are many others, for example, the mentioned W state. In Sec. XIII we discuss how one can introduce a classification within the set of m-partite entangled states. One can introduce a further classification by means of stochastic LOCC (SLOCC) (see Sec. XIII), according to which for three qubits there are two classes of truly three-partite entangled states, represented by the GHZ and W states. There are, furthermore, three classes of pure states which are partially entangled and partially separable: this is the state $|\Phi^+\rangle|0\rangle$, where $\Phi^+ = (1/\sqrt{2})(|0\rangle|0\rangle + |1\rangle|1\rangle)$ and its twins produced by two cyclic permutations of subsystems. We see that in the latter case only two-qubit entanglement is present and explicitly "partial" separability can be seen. This leads us to the various notions of partial separability described in the next section. Here we present an important family of pure entangled states.

Example: Quantum graph states. The general form of graph states has been introduced by Raussendorf *et al.* (2003) as a generalization of *cluster states* (Briegel and Raussendorf, 2001) that have been shown to be a resource for a one-way quantum computer (Raussendorf and Briegel, 2001). The universality of quantum computers based on graph states is an important application of quantum entanglement in the theory of quantum computation (see Hein *et al.*, 2005). In general, any graph state is a pure m-qubit state $|G\rangle$ corresponding to a graph $G(V,E)$. The graph is described by the set V of vertices with cardinality $|V|=m$ (corresponding to qubits of $|G\rangle$) and the set E of edges, i.e., pairs of vertices (corresponding to pairs of qubits of $|G\rangle$).[37] Now, the mechanism of creating $|G\rangle$ is simple. One takes as the initial state $|+\rangle^{\otimes m}$ with $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$. Then, according to the graph $G(V,E)$, to any of pairs of qubits corresponding to vertices connected by an edge from E one applies a controlled phase gate: $U_{C\ \mathrm{phase}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_3$. Note that since all such operations commute even if performed according to the edges with a common vertex, the order of applying the operations is arbitrary. Remarkably, the set of graph states is described by a polynomial number $m(m-1)/2$ of discrete parameters, while in general the set of all states in the m-qubit Hilbert space is described by an exponential 2^m number of continuous parameters. Moreover, local unitary interconvertibility under $\otimes_{i=1}^m U_i$ of two graphs states is equivalent to their interconvertibility under stochastic local operations and classical communications.

B. Partial separability

Here we consider two other important notions of partial separability. The first one is separability with respect to partitions. In this case, the state of $A_1,\ldots,A_m$ elementary subsystems is separable with respect to a given partition $\{I_1,\ldots,I_k\}$, where I_i are disjoint subsets of the set of indices $I=\{1,\ldots,m\}$ $(\cup_{l=1}^k I_l = I)$ if and only if $\varrho = \Sigma_{i=1}^N p_i \varrho_1^i \otimes \cdots \otimes \varrho_k^i$, where any state ϱ_l^i is defined on the tensor product of all elementary Hilbert spaces corre-

[37] Usually E is represented by a symmetric adjacency matrix with elements $A_{uv} = A_{vu} = 1$ if and only if $u \neq v$ are connected by the edge and $A_{uv} = 0$ otherwise. Note that there are no more than $m(m-1)/2$ edges or pairs of vertices.

sponding to indices belonging to set I_i. Now, one may combine several separability conditions with respect to several different partitions. This gives many possible choices for partial separability.

We show an interesting example of partial separability which requires an even number of qubits in general.

Example. Consider four-qubit Smolin states (Smolin, 2001)

$$\varrho_{ABCD}^{\text{unlock}} = \frac{1}{4}\sum_{i=1}^{4} |\Psi_{AB}^{i}\rangle\langle\Psi_{AB}^{i}| \otimes |\Psi_{CD}^{i}\rangle\langle\Psi_{CD}^{i}|, \tag{72}$$

where $|\Psi^i\rangle$ are four Bell states. It happens that it is symmetrically invariant under any permutations [to see it one can use the symmetric Hilbert-Schmidt representation $\varrho_{ABCD}^{\text{unlock}} = \frac{1}{4}(\mathrm{I}^{\otimes 4} + \Sigma_{i=1}^{3}\sigma_i^{\otimes 4})$]. Thus the state is separable under any partition into two two-qubit parts. Still, it is entangled under any partition 1 vs 3 qubits since it violates the PPT criterion with respect to this partition, i.e., $(\varrho_{ABCD}^{\text{unlock}})^{T_A} \ngeq 0$. This state has been shown to have applications in remote concentration of quantum information (Murao and Vedral, 2001). The Smolin state has also been shown to be useful in reduction of communication complexity via violation of Bell inequalities (Augusiak and Horodecki, 2006).

Particularly interesting from the point of view of low-partite case systems is a special class of partially separable states called *semiseparable*. They are separable under all 1 versus $m-1$ partitions: $\{I_1=\{k\}, I_2=\{1,\ldots,k-1,k+1,\ldots,m\}\}$, $1 \leqslant k \leqslant m$. It allows us to show a new type of entanglement: there are semiseparable three-qubit states which are still entangled as seen in the example below. There is also another notion of separability/entanglement which is related to the concept of being "at most n-partite entangled" (Vedral, Plenio, Jacobs, and Knight, 1997). For instance, the state $\rho = p\rho_{AB} \otimes \rho_{CDE} + (1-p)\rho_{ACDE} \otimes \rho_B$ is at most bipartite entangled. One may also define the notions of "at most (at least) k-subsystem entanglement" and then the above state may contain at most 4-subsystem (at least 2-subsystem) entanglement. Finally, one can consider mixtures of type "clusters" like, for instance, mixtures of states product under (arbitrary) k versus m-k-type partitions [see Seevinck and Svetlichny (2002) for $k=1$]. However, criteria for this type of entanglement have not been well developed yet.

Examples. Consider the following product states (DiVincenzo *et al.*, 2003): a $2 \otimes 2 \otimes 2$ state composed on three parts ABC generated by a set defined as $S_{\text{shift}} = \{|0\rangle|0\rangle|0\rangle, |+\rangle|1\rangle|-\rangle, |1\rangle|-\rangle|+\rangle, |-\rangle|+\rangle|1\rangle\}$, with $|\pm\rangle = (1/\sqrt{2})(|0\rangle \pm |1\rangle)$. This set can be proven to define the multipartite unextendible product basis in full analogy to the bipartite case discussed in Sec. VI.B.7: there is no product state orthogonal to the subspace spanned by S_{shift}. Thus in analogy to bipartite construction, the state $\varrho_{\text{shift}} = (I - P_{\text{shift}})/4$ where P_{shift} projects onto the subspace spanned by S_{shift} can be easily shown to be entangled as a whole (i.e., not fully separable) but PPT under all bipartite cuts (i.e., $A|BC$, $AB|C$, $B|AC$). However, it happens that it is not only PPT but also *separable* under all bipartite cuts (i.e., semiseparable). This means that semiseparability is not equivalent to full separability even in the most simple multipartite case like the three-qubit one.

Another interesting class is the set of $U \otimes U \otimes U$ invariant $d \otimes d \otimes d$ states which comprises semiseparable and fully three-separable subclasses of states in one five-parameter family of states (see Eggeling and Werner, 2001).

The moral of the story is that checking bipartite separability with respect to all possible cuts is not enough to guarantee full separability. However, separability with respect to some partial splittings still gives an important generalization of separability and has interesting applications (see Dür, Cirac, *et al.*, 1999; Dür and Cirac, 2000a, 2000b; Smolin, 2001) (see Sec. XII). In this context we describe below a useful family of states.

Example. The separability of the family of states presented below (Dür, Cirac, *et al.*, 1999a; Dür and Cirac, 2000b) is determined by checking the PPT criterion under any possible partitions. To be more specific, the PPT condition with respect to some partition guarantees separability along that partition. The states found some important applications in the activation of bound entanglement (Dür and Cirac, 2000a), nonadditivity of multipartite quantum channels (Dür *et al.*, 2004), and the multipartite bound information phenomenon (Acín, Cirac, *et al.*, 2004). This is the following m-qubit family (Dür, Cirac, *et al.*, 1999):

$$\varrho^{(m)} = \sum_{a=\pm} \lambda_0^a |\Psi_0^a\rangle\langle\Psi_0^a| + \sum_{k\neq 0} \lambda_k (|\Psi_k^+\rangle\langle\Psi_k^+| + |\Psi_k^-\rangle\langle\Psi_k^-|), \tag{73}$$

where $|\Psi_k^{\pm}\rangle = (1/\sqrt{2})(|k_1\rangle\,|k_2\rangle\cdots|k_{m-1}\rangle|0\rangle \pm |\bar{k}_1\rangle|\bar{k}_2\rangle\cdots \times |\bar{k}_{m-1}\rangle|1\rangle$ with $k_i = 0,1$, $\bar{k}_i = k_i \oplus 1 \equiv (k_i+1) \bmod 2$, and k one of 2^{m-1} real numbers defined by the binary sequence $k_1,\ldots,k_{m-1}$.

We put $\Delta = \lambda_0^+ - \lambda_0^- \geqslant 0$ and define bipartite splitting into two disjoint parts, $A(k) = \{$subset with the last (mth) qubit$\}$, $B(k) = \{$subset without the last qubit$\}$, with the help a of binary sequence k such that the ith qubit belongs to $A(k)$ [and not to $B(k)$] if and only if the sequence $k_1,\ldots,k_{m-1}$ contains $k_i = 0$. Then one can prove (Dür, Cirac, *et al.*, 1999) that (i) $\varrho^{(m)}$ is separable with respect to the partition $\{A(k), B(k)\}$ if and only if $\lambda_k \geqslant \Delta/2$, which happens to be equivalent to the PPT condition with respect to that partition (i.e., $\varrho^{T_B} \geqslant 0$); (ii) if the PPT condition is satisfied for all bipartite splittings then $\varrho^{(m)}$ is fully separable. Note that condition (ii) above does not hold in general for other mixed states, which can be seen easily on the three-qubit semiseparable state ϱ_{shift} recalled in this section. That state is entangled but clearly satisfies the PPT condition under all bipartite splittings.

VIII. FURTHER IMPROVEMENTS OF ENTANGLEMENT TESTS: NONLINEAR SEPARABILITY CRITERIA

The nonlinear separability criteria fall into two different classes. The first class is based on *nonlinear* functions of results of a few different measurements performed in the usual, noncollective manner (on one copy of ϱ_{AB} at a time). To this class belong all separability conditions formulated in terms of uncertainty relations which were first developed for continuous variables but then also strongly pursued for finite dimensions, for example, in terms of spin-sqeezing inequalities.[38] Such conditions will be described in Sec. VIII.A.[39]

The second class of nonlinear separability conditions is based on *collective* measurements on several copies and has attracted more and more attention recently. We present them in Sec. VIII.B.

A. Uncertainty-relation-based separability tests

Separability tests based on uncertainty relations have first been developed for continuous variables and applied to Gaussian states (Duan *et al.*, 2000; Simon, 2000; see also Mancini *et al.*, 2002). For the bipartite case nonlinear inequalities for approximations of finite-dimensional Hilbert spaces in the limit of high dimensions have been exploited in terms of global angular-momentum-like uncertainties by Kuzmich and Polzik (2000) with further experimental application (Julsgaard *et al.*, 2001).[40]

General separability criteria based on an uncertainty relation and valid for both discrete and continuous variables (CVs) were introduced by Giovannetti *et al.* (2003) and Hofmann and Takeuchi (2003) (the second one was introduced for discrete variables but its general formulation is valid also for the CV case). Further, it was shown (Hofmann, 2003) that PPT entanglement can be detected by means of the uncertainty relation introduced by Hofmann and Takeuchi (2003). This approach was further developed and simplified by Gühne (2004) and developed also in entropic terms (Gühne and Lewenstein, 2004a). Another separability criterion in two-mode continuous systems based on uncertainty relations with the particle number and the destruction operators has been presented (Tóth *et al.*, 2003), which may be used to detect entanglement of light modes or in Bose-Einstein condensates.

We recall briefly the key of the approach of local uncertainty relations (Hofmann and Takeuchi, 2003) which has found application in the idea of macroscopic entanglement detection via magnetic susceptibility (Wieśniak *et al.*, 2005). Consider the set of local observables $\{A_i\}_{i=1}^N$, $\{B_i\}_{i=1}^N$ on Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$, respectively. Suppose that one has bounds on the sum of local variances, i.e., $\Sigma_i \delta(A_i)^2 \geqslant c_a, \Sigma_i \delta(B_i)^2 \geqslant c_b$ with some nonnegative values c_a, c_b and the variance definition $\delta(M)_\varrho^2 \equiv \langle M^2\rangle_\varrho - \langle M\rangle_\varrho^2$. Then for any separable state ϱ_{AB} the following inequality holds (Hofmann and Takeuchi, 2003):

$$\sum_i \delta(A_i \otimes I + I \otimes B_i)_{\varrho_{AB}}^2 \geqslant c_A + c_B. \tag{74}$$

Note that by induction the above inequality can be extended to the multipartite case. Quite remarkably, if the observables A_i and B_i are chosen in a special asymmetric way, the above inequality can be shown (Hofmann, 2003) to detect entanglement of the family of PPT states (58). The LUR approach was generalized by Gühne (2004) to separability criteria via nonlocal uncertainty relations. That approach is based on the observation that, for any $\mathcal{S}$ (here we choose it to be a set of product states), any set of observables M_i, and the state $\varrho = \Sigma_i p_i \varrho_i$, $\varrho_i \in \mathcal{S}$, the following inequality holds:

$$\sum_i \delta(M_i)_\varrho^2 \geqslant \sum_k p_k \sum_i \delta(M_i)_{\varrho_k}^2. \tag{75}$$

It happens that in many cases it is easy to show that right-hand side (RHS) is separated from zero for separable ϱ, while at the same time the LHS vanishes for some entangled states.[41]

B. Detecting entanglement with collective measurements

1. Physical implementations of entanglement criteria with collective measurements

The idea of direct measurement of pure state entanglement was first considered by Sancho and Huelga (2000) and involved the explicit application of collective measurements to entanglement detection (Acín *et al.* 2000). In general, the question here is how to detect entanglement physically by means of a small number of collective measurements that do not lead to complete tomography of the state. Here we focus on the number of estimated parameters (means of observables) and try to diminish it. The fact that the mean of an observable may be interpreted as a single binary estimated parameter (equivalent to one-qubit polarization) has been proven by Horodecki (2003c), and Paz and Roncaglia (2003), cf. Brun (2004).

The power of positive map separability criteria and entanglement measures has motivated work on implementations of separability criteria via collective measurements, introduced by Horodecki and Ekert (2002)

[38]We stress here that we do not consider entanglement measures which are also nonlinear functions of the state, but belong to a special class that has, in a sense, its own philosophy.

[39]There are also nonlinear criteria which do not belong to this class, see, e.g., Badziag *et al.*, 2008.

[40]The first use of an uncertainty relation to detect entanglement (theoretically and experimentally) can be found in Hald *et al.* (1999) for spins of atomic ensembles.

[41]There is also a separability criterion in terms of covariance matrices, which is equivalent to all LUR criteria (Gühne, Hyllus, *et al.*, 2007) (see also Abascal and Björk, 2007, in this context). Other criteria for symmetric n-qubit states have been presented in the form of a hierarchy of inseparability conditions on the intergroup covariance matrices of even order (Devi *et al.*, 2007).

and Horodecki (2003d) and improved by Carteret (2005), and Horodecki, Augusiak, *et al.* (2006). On the other hand, the entropic separability criteria have led to the separate notion of collective entanglement witnesses (Horodecki, 2003b) described next.

The evaluation of nonlinear state functions via collective measurement (Ekert, Alves, *et al.*, 2002; Filip, 2002) (see also Fiurášek, 2002b; Horodecki, 2003b) was implemented experimentally in the distant laboratory paradigm (Bovino *et al.*, 2005). The method takes an especially striking form in the two-qubit case, when not only unambiguous entanglement detection (Horodecki and Ekert, 2002) but also estimation of such complicated entanglement measures as entanglement of formation and Wootters concurrence can be achieved by measuring only four collective observables (Horodecki, 2003d), much smaller than the 15 required by state estimation. The key idea of the latter scheme is to measure four collective observables $A^{(2k)}$ on $2k$ copies of the state that previously have been subjected to physical action of some maps.[42] The mean values of these observables reproduce all four moments $\langle A^{(2k)}\rangle=\Sigma_i\lambda_i^k$ of spectrum $\{\lambda_k\}$ of the square of the Wootters concurrence matrix $\hat{C}(\varrho)=\sqrt{\sqrt{\varrho}\sigma_2\otimes\sigma_2\varrho^*\sigma_2\otimes\sigma_2\sqrt{\varrho}}$. Note that, due to the link (Wootters, 1998) between Wootters concurrence and entanglement of formation, the latter can be also inferred in such an experiment. Recently, a collective observable acting on two copies of quantum state which detect two-qubit concurrence has been constructed and implemented (Walborn *et al.*, 2006). The observable is much simpler, however, the method works under the promise that the state is pure. This approach can be also generalized to the multiparty case using a suitable factorizable observable corresponding to the concurrence (see Aolita and Mintert, 2006).

In methods involving positive map criteria the unphysical character of given map L (equal to, say, partial transpose) has been overcome first with the help of affine rescaling [referred to as so-called structural physical approximation (SPA)] which allows us to measure the spectrum $L(\varrho)$ with d^2 collective observables instead of the d^4-1 required if one checks the map condition with prior tomography. The approach easily generalizes to multipartite map criteria like realignment or linear contractions (Horodecki, 2003a). The implementation with the help of local measurements has also been developed (see Alves *et al.*, 2003).

However, as pointed out by Carteret (2005), the disadvantage of the method is that SPA involved here requires in general a significant amount of noise added to the system. The improved method of noiseless detection of PPT criterion, concurrence, and tangle has been worked out (Carteret, 2003, 2005) with the help of the polynomial invariants technique which allows for very simple and elegant quantum network designing. Later, general noiseless networks working for arbitrary positive (or contraction) maps have been solved where general noiseless networks have been designed (Horodecki, Augusiak, *et al.*, 2006).

Finally we note that the above techniques have been also developed on the ground of continuous variables (Fiurášek and Cerf, 2004; Stobińska and Wódkiewicz, 2005; Pregnell, 2006).

2. Collective entanglement witnesses

There is yet another technique (Horodecki, 2003b) that seems to be more important in the context of experimental implementations. This is the notion of the collective entanglement witness. Consider a bipartite system AB on the space $\mathcal{H}_{AB}=\mathcal{H}_A\otimes\mathcal{H}_B$. One introduces here the notion of collective observable $A^{(n)}$ with respect to the single system Hilbert space $\mathcal{H}$ as an observable defined on $\mathcal{H}^{\otimes n}$ and measured on n copies $\varrho^{\otimes n}$ of given state ϱ. Also one defines the notion of the mean of collective observable in a single copy of state $\varrho^{\otimes n}$ as $\langle\langle A^{(n)}\rangle\rangle:=\mathrm{Tr}(A^{(n)}\varrho^{\otimes n})$. Now any observable $W^{(n)}$ defined on $(\mathcal{H}_{AB})^{\otimes n}$ that satisfies the condition

$$\langle\langle W^{(n)}\rangle\rangle_{\varrho_{\mathrm{sep}}}:=\mathrm{Tr}(W^{(n)}\varrho_{\mathrm{sep}}^{\otimes n})\geqslant 0 \tag{76}$$

when there exists an entangled state ϱ_{ent} such that

$$\langle\langle W^{(n)}\rangle\rangle_{\varrho_{\mathrm{ent}}}<0 \tag{77}$$

is called a collective n-copy entanglement witness.

Recently it has been observed that there is a single four-copy collective entanglement witness that detects all (unknown) two-qubit entanglement (Augusiak *et al.*, 2008). On this basis a corresponding universal quantum device, that can be interpreted as a quantum computing device, has been designed.

It is very interesting that the following collective entanglement witness (Mintert and Buchleitner, 2006):

$$\tilde{W}^{(2)}_{AA'BB'}=2P^{(+)}_{AA'}\otimes P^{(-)}_{BB'}+2P^{(-)}_{AA'}\otimes P^{(-)}_{BB'}-4P^{(-)}_{AA'}\otimes P^{(-)}_{BB'}, \tag{78}$$

with $P^{(+)}$ and $P^{(-)}$ projectors onto symmetric and antisymmetric subspace, respectively (see Sec. VI.B.3), has been shown to provide a lower bound on bipartite concurrence $\mathcal{C}(\varrho_{AB})$ (Mintert *et al.*, 2004),

$$\mathcal{C}(\varrho_{AB})\geqslant-\langle\langle\tilde{W}^{(2)}_{AA'BB'}\rangle\rangle_{\varrho_{AB}}. \tag{79}$$

IX. CLASSICAL ALGORITHMS DETECTING ENTANGLEMENT

The first systematic methods of checking entanglement of a given state was worked out in terms of finding the decomposition onto separable and entangled parts of the state (see Lewenstein and Sanpera, 1998) and generalizations to the case of PPT states (Kraus *et al.*, 2000; Lewenstein *et al.*, 2001). The methods were based on the systematic application of the range criterion involving, however, the difficult analytical part of finding product

[42]They are so-called physical structural approximations, described further in this section.

states in the range of a matrix. A further attempt to provide an algorithm deciding entanglement was based on checking the variational problem based on a concurrence vector (Audenaert, Verstraeter, *et al.*, 2001). The problem of the existence of a classical algorithm that unavoidably identifies entanglement has been analyzed by Doherty *et al.* (2002, 2004) both theoretically and numerically and implemented by semidefinite programming methods. This approach is based on a theorem concerning the symmetric extensions of a bipartite quantum state (Fannes *et al.*, 1988; Raggio and Werner, 1989). It has the following interpretation. For a given bipartite state ϱ_{AB} one asks about the existence of a hierarchy of symmetric extensions, i.e., whether there exists a family of states $\varrho_{AB_1\cdots B_n}$ (with n arbitrary high) such that $\varrho_{AB_i}=\varrho_{AB}$ for all $i=1,\ldots,n$. It happens that the state ϱ_{AB} is separable if and only if such a hierarchy exists for each natural n (see Sec. XVI). However, for any fixed n checking the existence of such a symmetric extension is equivalent to an instance of semidefinite programming. This leads to an algorithm consisting of checking the above extendability for increasing n, which always stops if the initial state ϱ_{AB} is entangled. However, the algorithm never stops if the state is separable. Further, another hierarchy has been provided together with the corresponding algorithm in Eisert *et al.* (2004), extended to involve higher order polynomial constraints and to address the multipartite entanglement question.

The idea of the dual algorithm was provided by Hulpke and Bruß (2005), based on the observation that in checking the separability of a given state it is enough to consider a countable set of product vectors spanning the range of the state. The constructed algorithm is dual to that described above, in the sense that its termination is guaranteed if the state is separable, otherwise it will not stop. It has been further realized that running both the algorithms (i.e., the one that always stops if the state is entangled with the one that stops if the state is separable) in parallel gives an algorithm that always stops and decides entanglement definitely (Hulpke and Bruß, 2005).

The complexity of both algorithms is exponential in the size of the problem. It seems that it must be so. The milestone result that has been proven in a meantime was that solving separability is a so-called *NP hard* problem (Gurvits, 2002, 2003, 2004). Namely, it is known (Yudin and Nemirovskii, 1976) that if a largest ball contained in the convex set scales properly, and moreover there exists an efficient algorithm for deciding membership, then one can efficiently minimize linear functionals over the convex set. Now, Gurvits has shown that for some entanglement witness (corresponding to linear functional) the optimization problem was intractable. This, together with the results on the radius of the ball contained within separable states (see Sec. X), shows that the problem of separability cannot be efficiently solved.

Recently the new algorithm via the analysis of a weak membership problem has been developed together with analysis of NP hardness (Ioannou *et al.*, 2004; Ioannou and Travaglione, 2006; Ioannou, 2007). The goal of the algorithm is to solve the "witness" problem. This is either (i) to write a separable decomposition up to the given precision δ or (ii) to find an (according to a slightly modified definition) entanglement witness that separates the state from a set of separable states by more than δ (the notion of the separation is precisely defined). The analysis shows that one can find more precisely a likely entanglement witness that detects the entanglement of the state (or find that it is impossible) reducing the set of "good" (i.e., possibly detecting the state entanglement) witnesses by each step of the algorithm. The algorithm singles out a subroutine which can be, to some extent, interpreted as an oracle calculating a "distance" of the given witness to the set of separable states.

Finally, note that there are also other proposals of algorithms deciding separability like Zapatrin (2005) (for a review, see Ioannou, 2007, and references therein).

X. QUANTUM ENTANGLEMENT AND GEOMETRY

The geometry of entangled and separable states is a wide branch of entanglement theory (Bengtsson and Życzkowski, 2006). The most simple and elementary example of geometrical representation of separable and entangled states in three dimensions is a representation of a two-qubit state with maximally mixed subsystems (Horodecki and Horodecki, 1996); namely, any two-qubit state can be represented in the Hilbert-Schmidt basis $\{\sigma_i\otimes\sigma_j\}$ where $\sigma_0=I$, and in this case the correlation matrix T with elements $t_{ij}=\mathrm{Tr}(\varrho\sigma_i\otimes\sigma_j)$, $i,j=1,2,3$ can be transformed by local unitary operations to the diagonal form. This matrix completely characterizes the state if local density matrices are maximally mixed [which corresponds to the vanishing of the parameters $r_i=\mathrm{Tr}(\sigma_i\otimes I\varrho)$, $s_j=\mathrm{Tr}(I\otimes\sigma_j\varrho)$, for $i,j=1,2,3$]. It happens that after diagonalizing,[43] T is always a convex combination of four matrices $T_0=\mathrm{diag}[1,-1,1]$, $T_1=\mathrm{diag}[-1,1,1]$, $T_2=\mathrm{diag}[1,1,-1]$, $T_3=\mathrm{diag}[-1,-1,-1]$ which corresponds to the maximally mixed Bell basis. This has a simple interpretation in three-dimensional real space: a tetrahedron $\mathcal{T}$ with four vertices and their coordinates corresponding to the diagonals above [(1,1,−1), etc.]. The subset of separable states is an octahedron that comes out from intersection of $\mathcal{T}$ with its reflection by the map $(x,y,z)\to(-x,-y,-z)$. It is remarkable that all states with maximally mixed subsystems are equivalent (up to product unitary operations $U_A\otimes U_B$) to Bell diagonal states [a mixture of four Bell states (3)]. Moreover, for all states (not only those with maximally mixed subsystems) the singular values of the correlation matrix T are invariants under such product unitary transformations. The Euclidean lengths of the real three-dimensional vectors with coordinates r_i, s_j defined above are also similarly invariant.

Note that an analog of the tetrahedron $\mathcal{T}$ in the state space for entangled two qudits was defined and investi-

[43]The diagonalizing matrix T corresponds to applying the product $U_A\otimes U_B$ unitary operation to the state.

gated in the context of geometry of separability (Baumgartner *et al.*, 2006). It turns out that the analog of the octahedron is no longer a polytope.

One can naturally ask about a reasonable set of the parameters or in general functions of the state that are invariants of product unitary operations. Properly chosen invariants allow for characterization of local *orbits*, i.e., classes of states that are equivalent under local unitaries. (Note that any given orbit contains either only separable or only entangled states since entanglement property is preserved under local unitary product transformations.) The problem of characterizing local orbits was analyzed in general in terms of polynomial invariants by Grassl *et al.* (1998), and Schlienz and Mahler (1995). In the case of two qubits this task was completed explicitly with 18 invariants in which 9 are functionally independent (Makhlin, 2002; cf. Grassl *et al.*, 1998). Further, this result has been generalized up to four qubits (Briand *et al.*, 2003, Luque and Thibon, 2003). Another way of characterizing entanglement in terms of local invariants was initiated by Linden and Popescu (1998), and Linden, Popescu, and Sudbery (1999) by analysis of dimensionality of the local orbit. The full solution of this problem for mixed two-qubit states and general bipartite pure states has been provided by Kuś and Życzkowski (2001) and Sinołęcka *et al.* (2002), respectively. For further development in this direction see Grabowski *et al.* (2005), and references therein. There are many other results concerning geometry or multiqubit states; we mention only Miyake (2003); Heydari (2006); Levay (2006).

There is another way to ask about geometrical properties of entanglement; namely, to ask about the volume of a set of separable states, its shape, and the boundary of this set. The question about the volume of separable states was first considered by Życzkowski *et al.* (1998) and extended by Życzkowski (1999). Życzkowski *et al.* (1998) proved with the help of entanglement witnesses theory that for any finite dimensional system (bipartite or multipartite) the volume of separable states is nonzero. In particular there always exists a ball of separable states around the maximally mixed state.[44] An explicit bound on the ratio of volumes of the set of all states $\mathcal{S}$ and that of the separable states $\mathcal{S}_{\text{sep}}$,

$$\text{vol}(\mathcal{S})/\text{vol}(\mathcal{S}_{\text{sep}}) \geqslant [1/(1+d/2)]^{(d-1)(N-1)}, \tag{80}$$

for N-partite systems each of dimension d was provided by Vidal and Tarrach (1999). This has inspired further discussion which has shown that experiments in NMR quantum computing may not correspond to real quantum computing since they are performed on pseudopure states which are in fact separable (Braunstein *et al.*, 1999). Interestingly, one can show (Życzkowski *et al.*, 1998; Kendon *et al.*, 2002) that for any quantum system on some Hilbert space $\mathcal{H}$ a maximal ball inscribed into a set of mixed states is located around maximally mixed states and is given by $\text{Tr}(\varrho^2) \leqslant (\dim \mathcal{H}^2 - 1)^{-1}$. Since this condition guarantees also the positivity of any unit trace operator, and since for bipartite states $\text{Tr}(\varrho_{AB}^2) = \text{Tr}[(\varrho_{AB}^{\Gamma})^2]$ this means that the maximal ball contains only PPT states [the same argument works also for multipartite states (Kendon *et al.*, 2002)]. In the case of $2 \otimes 2$ or $2 \otimes 3$ this implies also separability giving a way to estimate the volume of separable states from below.

These estimates have been generalized to multipartite states (Braunstein *et al.*, 1999) and further improved providing strong upper and lower bounds with the help of a subtle technique exploiting among others entanglement witnesses theory (Gurvits and Barnum, 2002, 2003, 2005). In particular for bipartite states the exact size of the largest separable ball around maximally mixed states was found. One of the applications of the largest separable ball results is the proof of NP hardness in deciding whether or not a state is separable (Gurvits, 2003) (see Sec. IX).

There is yet another related question: one can define the state (bipartite or multipartite) ϱ that remains separable under the action of any unitary operation U. Such states are called absolutely separable (Kuś and Życzkowski, 2001). In full analogy one can define what we call here absolute PPT property (i.e., PPT property that is preserved under any unitary transformation). The question of which states are absolutely PPT has been fully solved (Hildebrand, 2005). For example, for $2 \otimes n$ systems those are all states satisfying $\lambda_1 \leqslant \lambda_{2n-1} + \sqrt{\lambda_{2n-2}\lambda_{2n}}$ where $\{\lambda_i\}_{i=1}^{2n}$ are eigenvalues of ϱ in decreasing order. This provides the characterization of absolutely separable states in $d_A \otimes d_B$ systems with $d_A d_B \leqslant 6$ since PPT is equivalent to separability in those cases. Note that for $2 \otimes 2$ states this characterization was proven much earlier by different methods (Verstraete, Audenaert, and De Moor, 2001). In particular it follows that for those low dimensional cases the set of absolutely separable states is strictly larger than that of the maximal ball inscribed into the set of all states. Whether it is true in higher dimensions remains an open problem.

Speaking about the geometry of separable states one can not avoid a question about what is the boundary $\partial\mathcal{S}$ of the set of states. This not easy in general, question, can be answered analytically in the case of the two qubit where it can be shown to be smooth (Djokovic, 2006) relative to the set of all two-qubit states which is closely related to the separability characterization (Horodecki, Augusiak, *et al.*, 2006) $\det(\varrho_{AB}^{\Gamma}) \geqslant 0$. Interestingly, it has been shown that the set of separable states is not a polytope (Ioannou and Travaglione, 2006); it has no faces (Gühne and Lütkenhaus, 2007).

There are many other interesting geometrical issues that can be addressed in the case of separable states. One of them is how the probability of finding a separable state (when the probability is measured with an *a priori* probability measure μ) is related to the probability (calculated by an induced measure) of finding a ran-

[44]The radius of the ball provides a *sufficient* condition for separability. A different sufficient condition which is not based solely on eigenvalues was provided by Pittenger and Rubin (2002, 2002).

dom boundary state to be separable. The answer, of course, will depend on a choice of the probability measure, which is by no means unique. Numerical analysis suggested (Slater, 2005a, 2005b) that in the two-qubit case the ratio of those two probabilities is equal to 2 if one assumes a measure based on the Hilbert-Schmidt distance. Recently it has been proven that for any $d_A \otimes d_B$ system this rate is indeed 2 if we ask about the set of PPT states rather than the separable ones (Szarek *et al.*, 2006). For the $2\otimes 2$ and $2\otimes 3$ cases this reproduces the previous conjecture since the PPT condition characterizes separability there (see Sec. VI.B.2).

XI. THE PARADIGM OF LOCAL OPERATIONS AND CLASSICAL COMMUNCIATION (LOCC)

A. Quantum channel: The main notion

Here we recall that the most general quantum operation that transforms one quantum state into the other is a probabilistic or stochastic physical operation of the type

$$\varrho \to \Lambda(\varrho)/\mathrm{Tr}[\Lambda(\varrho)], \tag{81}$$

with a trace-nonincreasing CP map, i.e., a map satisfying $\mathrm{Tr}[\Lambda(\varrho)]\leqslant 1$ for any state ϱ, which can be expressed in the form

$$\Lambda(\varrho) = \sum_i V_i(\varrho)V_i^\dagger, \tag{82}$$

with $\Sigma_i V_i^\dagger V_i \leqslant I$ [domain and codomain of operators V_i called Kraus operators (Kraus, 1983) are in general different]. The operation above takes place with the probability $\mathrm{Tr}[\Lambda(\varrho)]$ which depends on the argument ϱ. The probability is equal to 1 if an only if the CP map Λ is trace preserving, which corresponds to $\Sigma_i V_i^\dagger V_i = I$ in Eq. (82); in such a case Λ is called deterministic or a quantum channel.

B. LOCC operations

We already know that in the quantum teleportation process Alice performs a local measurement with maximally entangled projectors $P^i_{AA'}$ on her particles AA' and then sends classical information to Bob (see Sec. III.C). Bob performs accordingly a local operation U^i_B on his particle B. Note that the total operation acts on ρ as $\Lambda_{AA'B}(\rho) = \Sigma_i P^i_{AA'} \otimes U^i_B(\rho) P^i_{AA'} \otimes (U^i_B)^\dagger$. This operation belongs to the so-called one-way LOCC class which is important in quantum communication theory. The general LOCC paradigm was formulated by Bennett, Di Vincenzo, *et al.* (1996).

In this paradigm all that the distant parties (Alice and Bob) are allowed is to perform arbitrary local quantum operations and sending classical information. No transfer of quantum systems between the labs is allowed. It is a natural class for considering entanglement processing because classical bits cannot convey quantum information and cannot create entanglement so that entanglement remains a resource that can be only manipulated. Moreover, one can easily imagine that sending classical bits is much cheaper than sending quantum bits, because it is easy to amplify classical information. Sometimes it is convenient to put some restrictions also onto classical information. One then distinguishes in general the following subclasses of operations described below. Below we define classes of trace preserving, i.e., deterministic (channel-type) maps. The analogous list (except for C1 below) of trace nonincreasing, i.e., stochastic, maps can be defined [see description of Eq. (81)].

C1: class of local operations. In this case no communication between Alice and Bob is allowed. The mathematical structure of the map is elementary $\Lambda^{\varnothing}_{AB} = \Lambda_A \otimes \Lambda_B$ with Λ_A, Λ_B being both quantum channels. As already stated this operation is always deterministic.

C2a: class of "one-way" forward LOCC operations. Here classical communication from Alice to Bob is allowed. The form of the map is $\Lambda^{\rightarrow}_{AB}(\varrho) = \Sigma_i V^i_A \otimes I_B[[I_A \otimes \Lambda^i_B](\varrho)](V^i_A)^\dagger \otimes I_B$ with deterministic maps Λ^i_B which reflect the fact that Bob is not allowed to perform a "truly stochastic" operation since he cannot tell Alice whether it has taken place or not (which would happen only with some probability in general).

C2b: class of one-way backward LOCC operations. Here one has $\Lambda^{\leftarrow}_{AB}(\varrho) = \Sigma_i I_A \otimes V^i_B[\Lambda^i_A \otimes I_B](\varrho) I_A \otimes (V^i_B)^\dagger$. The situation is the same as in class C2a but with the roles of Alice and Bob interchanged.

C3: class of "two-way" LOCC operations. Here both parties are allowed to send classical communication to each other. Mathematically, these are all, in general, complicated operations that can be composed out of local operations (class C1) and the following maps:

$$\Lambda_1(\rho_{AB}) = \sum_i (A_i \otimes I \rho_{AB} A_i^\dagger \otimes I) \otimes |i\rangle\langle i|_{B'},$$

$$\Lambda_2(\rho_{AB}) = \sum_i (I \otimes B_i \rho_{AB} I \otimes B_i^\dagger) \otimes |i\rangle\langle i|_{A'}, \tag{83}$$

where $\Sigma_i A_i^\dagger A_i = I_A$, $\Sigma_i B_i^\dagger B_i = I_B$; cf. Grudka *et al.* (2007). Fortunately, there are two other larger (in a sense of inclusion) classes, that are much easier to deal with: the classes of separable and PPT operations.

C4: class of separable operations. This class was considered by Rains (1997) and Vedral and Plenio (1998). These are operations with product Kraus operators:

$$\Lambda^{\mathrm{sep}}_{AB}(\varrho) = \sum_i A_i \otimes B_i \varrho A_i^\dagger \otimes B_i^\dagger, \tag{84}$$

which satisfy $\Sigma_i A_i^\dagger A_i \otimes B_i^\dagger B_i = I \otimes I$.

C5: PPT operations. These are operations (Rains, 1999, 2000) Λ^{PPT} such that $(\Lambda^{PPT}[(\cdot)^\Gamma])^\Gamma$ is completely positive. We show that the simplest example of such an operation is $\varrho \to \varrho \otimes \varrho_{PPT}$, i.e., the process of adding some PPT state.

There is an order of inclusions $C1 \subset C2a$, $C2b \subset C3 \subset C4 \subset C5$, where all inclusions are strict, i.e., are not equalities. [The *stochastic* analogs of C3 and C4 are equivalent up to probability of transformation (81),

the analogs of C4 and C5 are still not since only the latter can create (PPT-type) entanglement.] The most intriguing is nonequivalence $C3 \neq C4$ which follows from the so-called nonlocality without entanglement (Bennett, DiVinenzo, Fuchs, *et al.*, 1999): there is an example of product basis which is orthonormal (and hence perfectly distinguishable by suitable von Neumann measurement) but is not a product of two orthonormal local ones which represent vectors that cannot be perfectly distinguished by parties that are far apart and can use only LOCC operations. The inclusion $C3 \subset C4$ is extensively used in the context of LOCC operations. This is because they are hard to deal with, as characterized in a difficult way. If instead one deals with separable or PPT operations, thanks to the inclusion, one can still draw conclusions about the LOCC ones.

Subsequently, if it is not specified, the term LOCC will refer to the most general class of operations with the help of local operations and classical communication, namely, the class C3 above.

Below we provide examples of some LOCC operations.

Example. The (deterministic) $U \otimes U$, $U \otimes U^*$ twirling operations:

$$\tau(\varrho) = \int dU U \otimes U \varrho (U \otimes U)^\dagger,$$

$$\tau'(\varrho) = \int dU U \otimes U^* \varrho (U \otimes U^*)^\dagger. \tag{85}$$

Here dU is a uniform probabilistic distribution on a set of unitary matrices. They are of one-way type and can be performed in the following manner: Alice picks up randomly the operation U, rotates her subsystem with it, and sends the information to Bob which U she had chosen. Bob performs on his side either U or U^* (depending on which of the two operations they wanted to perform). The integration above can be made discrete (see Gross *et al.*, 2007) which follows from Caratheodory's theorem.

An important issue is that any state can be depolarized with the help of τ, τ' to Werner [Eq. (64)] and isotropic [Eq. (65)] states respectively. This element is crucial for the entanglement distillation recurrence protocol (Bennett, Brassard, *et al.*, 1996) (see Sec. XII.B).

XII. DISTILLATION AND BOUND ENTANGLEMENT

Many basic effects in quantum information theory exploit the pure maximally entangled state $|\psi^+\rangle$. However, in laboratories we usually have mixed states due to imperfection of operations and decoherence. A natural question arises: How should one deal with a noise so that one can take advantage of the interesting features of pure entangled states. This problem was first considered by Bennett, Brassard, Popescu, Schumacher, Smolin, and Wootters in 1996 (Bennett, Brassard, *et al.* 1996). In their seminal paper, they established a paradigm for purification (or distillation) of entanglement. When two distant parties share n copies of a bipartite mixed state ρ, which contain noisy entanglement, they can perform some LOCC and obtain in turn some (less) number of k copies of systems in a state close to a singlet state which contains pure entanglement. A sequence of LOCC operations achieving this task is called entanglement purification or entanglement distillation protocol. We are interested in optimal entanglement distillation protocols, i.e., those which result in a maximal ratio k/n in limit of a large number n of input copies. This optimal ratio is called distillable entanglement and denoted as E_D (see Sec. XV for the formal definition). Having performed entanglement distillation, the parties can use the obtained nearly singlet states to perform quantum teleportation, entanglement-based quantum cryptography, and other useful pure entanglement-based protocols. Therefore entanglement distillation is one of the fundamental concepts in dealing with quantum information and entanglement in general. Here we present important entanglement distillation protocols. We then discuss the possibility of entanglement distillation in general and report the bound entangled states which being entangled cannot be distilled.

A. One-way hashing distillation protocol

If only one party can tell the other party her or his result during the protocol of distillation, the protocol is called one-way, and two-way otherwise. One-way protocols are closely connected to error correction, as shown below. Bennett, DiVincenzo, *et al.* (1996) (see also Bennett, Brassard, *et al.* 1996) presented a protocol for two-qubit states which originates from the cryptographic privacy amplification protocol, called hashing. Following this work we consider here the so-called Bell diagonal states which are mixtures of two-qubit Bell basis states (3). Bell diagonal states $\rho_{B\text{diag}}$ are naturally parametrized by the probability distribution of mixing $\{p\}$. For these states, the one-way hashing protocol yields singlets at a rate $1-H(\{p\})$, thus proving[45] $E_D(\rho_{B\text{diag}}) \geqslant 1-H(\{p\})$, where $H(\{p\})$ is Shannon entropy of $\{p\}$. In the two-qubit case there are four Bell states (3). The n copies of the two-qubit Bell diagonal state $\rho_{B\text{diag}}$ can be viewed as a classical mixture of strings of n Bell states. Typically, there are only about $2^{nH(\{p\})}$ such strings that are likely to occur (Cover and Thomas, 1991). Since the distillation procedure yields some (shorter) string of singlets solely, there is a straightforward "classical" idea, that to distill one needs to know what string of Bell states occurred. This knowledge is sufficient as one can then rotate each nonsinglet Bell state into a singlet state easily as in a dense coding protocol (see Sec III).

We note that sharing ϕ^- instead of ϕ^+ can be viewed as sharing ϕ^+ with a phase error. Similarly ψ^+ means bit error and ψ^--both bit and phase error. Identification of

[45]It is known that if there are only two Bell states in a mixture, then one-way hashing is optimal so that distillable entanglement is equal to $1-H(\{p\})$ in this case.

the string of all Bell states that have occurred is then equivalent to learning which types of errors occurred in which places. Thus the above method can be viewed as an error correction procedure.[46]

Now, as is well known, to distinguish between $2^{nH(\{p\})}$ strings one needs $\log_2 2^{nH(\{p\})}=nH(\{p\})$ binary questions. Such a binary question can be the following: What is the sum of the bit values of the string at certain $i_1,\ldots,i_k$ positions, taken modulo 2? In other words: What is the parity of the given subset of positions in the string? From probabilistic considerations it follows that after r such questions about a random subset of positions (i.e., taking each time random k with $1\leqslant k\leqslant 2n$) the probability of distinguishing two distinct strings is no less than $1-2^{-r}$, hence the procedure is efficient.

The trick of the "hashing" protocol is that it can be done in a quantum setting. There are certain local unitary operations for the two parties, so that they are able to collect the parity of the subset of Bell states onto a single Bell state and then get to know it locally measuring this Bell state and comparing the results. Each answer to the binary question consumes one Bell state, and there are $nH(\{p\})$ questions to be asked. Therefore, if $H(\{p\})<1$, then, after the protocol, there are $n-nH(\{p\})$ unmeasured Bell states in a known state. The parties can then rotate them all to a singlet form (that is, correct the bit and phase errors), and hence distill singlets at an announced rate $1-H(\{p\})$.

This protocol can be applied even if Alice and Bob share a non-Bell-diagonal state, as they can twirl the state by applying at random one of the four operations $\sigma_x\otimes\sigma_x$, $\sigma_y\otimes\sigma_y$, $\sigma_z\otimes\sigma_z$, $I\otimes I$. The resulting state is a Bell diagonal state. Of course, this operation often will kill entanglement. We show how to improve this in Secs. XII.B and XII.D.

The above idea has been further generalized, leading to the general one-way hashing protocol which is discussed in Sec. XII.F.

B. Two-way recurrence distillation protocol

The hashing protocol cannot distill all entangled Bell diagonal states (one easily find this, knowing that those states are entangled if and only if some eigenvalue is greater than 1/2). To cover all entangled Bell diagonal states one can first launch a two-way distillation protocol to enter the regime where the one-way hashing protocol works. The first such protocol, called recurrence, was announced already in the first paper on distillation (Bennett, Brassard, *et al.* 1996), and developed by Bennett, DiVincenzo, *et al.* (1996). It works for two-qubit states satisfying $F=\mathrm{Tr}\,\rho|\phi^+\rangle\langle\phi^+|>\frac{1}{2}$ with $|\phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$.

The protocol is based on iteration of the following two-step procedure. In the first step Alice and Bob take two pairs, and apply locally a controlled NOT (CNOT) gate. Then they measure the target pair in a bit basis. If the outcomes are different they discard the source pair (failure), otherwise they keep it. In the latter case, a second step can be applied: they twirl the source pair to the Werner state. In the two-qubit case, Werner states are equivalent to isotropic states and hence are parametrized only by the singlet fraction F (see Sec. VI.B.9). If Alice and Bob succeed, the parameter improves with respect to the preceding one according to the rule

$$F'(F)=\frac{F^2+\frac{1}{9}(1-F)^2}{F^2+\frac{2}{3}F(1-F)+\frac{5}{9}(1-F)^2}. \tag{86}$$

Now, if only $F>\frac{1}{2}$, then the above recursive map converges to 1 for a sufficiently large initial number of copies.

The idea behind the protocol is the following. The first step decreases the bit error (i.e., in the mixture the weight of correlated states $|\phi^\pm\rangle$ increases). At the same time, the phase error increases, i.e., the bias between states of type + and those of type − gets smaller. Then there is a twirling step, which equalizes bit and phase error. Provided that the bit error went down more than the phase error went up, the net effect is positive. The protocol consumes a lot of resources (as it is probabilistic, and each iteration decreases the number of pairs by half), one usually applies it until F is so high that the hashing protocol is applicable. Instead of twirling one can apply a deterministic transformation (Deutsch *et al.*, 1996), switching between phase and bit errors, which is much more efficient.

C. Development of distillation protocols: Bipartite and multipartite cases

The idea of recurrence protocol was developed in different ways. The CNOT operation, which is done in the first step of the above original protocol, can be viewed as a permutation of standard basis. If one applies some other permutation acting locally on $k\geqslant 2$ qubits and performs measurement on a group of m of these pairs one obtains a natural generalization of this scheme, developed by Dehaene *et al.* (2003) for the case of two-qubit states. It follows that in the case of $k=4$, $m=1$, and a special permutation of this protocol yields a higher distillation rate. This paradigm has been further analyzed in the context of so-called code based entanglement distillation protocols (Matsumoto, 2003; Ambainis and Gottesman, 2006) by Hostens *et al.* (2004). The original idea of Bennett, Brassard, *et al.* (1996) linking entanglement distillation protocols and error correction procedures (Gottesman, 1997) have been also developed in the context of quantum key distribution; see Ambainis *et al.* (2002), Gottesman and Lo (2003), and the discussion in Sec. XIX.A.

The original recurrence protocol was generalized to higher-dimensional systems in two ways by Horodecki

[46]Actually this reflects a remarkable relation developed by Bennett, DiVincenzo, *et al.* (1996) between entanglement distillation and the large domain of quantum error correction designed for quantum computation in the presence of noise.

and Horodecki (1999) and Alber, Delgado, *et al.* (2001). An interesting improvement of distillation techniques is due to Vollbrecht and Verstraete (2005), where a protocol that interpolates between the hashing and recurrence one was provided. This idea has been developed by Hostens *et al.* (2006a). Also, distillation was considered in the context of topological quantum memory (Bombin and Martin-Delgado, 2006).

The above protocols for distillation of bipartite entanglement can be used for distillation of a multipartite entanglement, when n parties are provided many copies of a multipartite state; namely, any pair of the parties can distill some EPR pairs and then, using teleportation, the whole group can distribute a desired multipartite state. An advantage of such an approach is that it is independent from the target state. Dür, Cirac, *et al.* (1999) and Dür and Cirac (2000b) provided a sufficient condition for the distillability of an arbitrary entangled state from an n-qubit multipartite state, based on this idea.

However, as found by Murao *et al.* (1998) in the first paper on multipartite entanglement distillation, the efficiency of a protocol which uses bipartite entanglement distillation is in general less than that of direct distillation. The direct procedure is presented there which is a generalization of the bipartite recurrence protocol of the n-partite GHZ state from its "noisy" version (mixed with identity). Maneva and Smolin (2002) generalized the bipartite hashing protocol for distillation of the n-partite GHZ state.

In the multipartite scenario, there is no distinguished state like a singlet state that can be a universal target state in entanglement distillation procedures. There are, however, some natural classes of interesting target states, including the commonly studied GHZ state. An example is the class of the graph states (see Sec. VII.A), related to the one-way quantum computation model. A class of multiparticle entanglement purification protocols that allow for distillation of these states was first studied by Dür *et al.* (2003) where it was shown again to outperform bipartite entanglement purification protocols. It was further developed by Aschauer *et al.* (2005) for the subclass of graph states called two-colorable graph states. The recurrence and breeding protocol which distills all graph states has also been found (Kruszyńska *et al.*, 2006) [for a distillation of graph states subject to local noise see Kay *et al.* (2006)].

The class of two-colorable graph states is locally equivalent to the class of so-called Calderbank-Shor-Steane states (CSS states) that stems from quantum error correction (Calderbank and Shor, 1996; Steane, 1996a, 1996b). The distillation of CSS states has been studied in the context of multipartite quantum cryptographic protocols by Chen and Lo (2004). Recently, the protocol which is a direct generalization of the original hashing method (see Sec. XII.A) has been found that distills CSS states (Hostens *et al.*, 2006b). This protocol outperforms all previous versions of hashing of CSS states (or their subclasses such as Bell diagonal states) (Maneva and Smolin, 2002; Dür *et al.*, 2003; Chen and Lo, 2004; Aschauer *et al.*, 2005). Distillation of the state W which is not a CSS state has been studied by Miyake and Briegel (2005). Glancy *et al.* (2006) proposed a protocol of distillation of all stabilizer states (a class which includes CSS states) based on stabilizer codes (Gottesman, 1997; Nielsen and Chuang, 2000). Based on this, a breeding protocol for stabilizer states was provided by Hostens *et al.* (2006c).

D. All two-qubit entangled states are distillable

The recurrence protocol followed by hashing can distill entanglement only from states satisfying $F>\frac{1}{2}$. One can then ask what is known in the general case. Here we present a protocol which allows us to overcome this limitation in the case of two qubits. The idea is that with certain (perhaps small) probability, one can conclusively transform a given state into a more desired one (i.e., so that one knows if the transformation succeeded). This step can increase the parameter F, so that one can then perform the recurrence and hashing protocol. Selecting successful cases in the probabilistic transformation is called local filtering (Gisin, 1996), which gives the name of the protocol. The composition of filtering, recurrence, and hashing proves the following result (Horodecki *et al.*, 1997): *Any two-qubit state is distillable if and only if it is entangled*.

There is a generalization of two-qubit distillability to the case of NPT states acting on $\mathcal{C}^2\otimes\mathcal{C}^N$ Hilbert space (Dür and Cirac, 2000a; Dür, Cirac, *et al.*, 2000). It follows also that for $N=3$ all states are distillable if and only if they are entangled (since any state on $\mathcal{C}^2\otimes\mathcal{C}^3$ is entangled if and only if it is NPT). The same equivalence has been shown for all rank two bipartite states (Horodecki, Smolin, *et al.*, 2003).

E. Reduction criterion and distillability

It has been shown that any state that violates reduction criterion of separability (see Sec. VI) is distillable (Horodecki and Horodecki, 1999). Namely, for states which violate this criterion, there exists a filter such that the output state has fidelity $F>\frac{1}{d}$, where F is the overlap with a maximally entangled state $|\Phi^+\rangle=(1/\sqrt{d})\Sigma_{i=0}^{d-1}|ii\rangle$. Such states are distillable, similarly, as for two-qubit states with $F>\frac{1}{2}$. The simplest protocol (Braunstein *et al.*, 1999) is the following: one projects such a state using local rank 2 projectors $P=|0\rangle\langle 0|+|1\rangle\langle 1|$, and finds that the obtained two-qubit state has $F>\frac{1}{2}$ hence is distillable.

The importance of this property of reduction criterion lies in the fact that its generalization to continuous variables allowed one to show that all two-mode Gaussian states which violate the PPT criterion are distillable (Giedke, *et al.*, 2000).

F. General one-way hashing

In Sec. XII.A we learned a protocol called one-way hashing which for Bell diagonal states with a spectrum given by distribution $\{p\}$ gives $1-H(\{p\})$ of distillable entanglement. Since in the case of these states the von Neumann entropy of the subsystem reads $S(\rho^B_{B\,\mathrm{diag}})=1$ and the total entropy of the state $S(\rho^{AB}_{B\,\mathrm{diag}})$ is equal to $H(\{p\})$, there has been a common belief that in general there should be a one-way protocol that yields the rate $S(\rho_B)-S(\rho_{AB})$ so that

$$E_D(\rho_{AB}) \geqslant S(\rho_B) - S(\rho_{AB}). \tag{87}$$

The above inequality, called the hashing inequality, states that distillable entanglement is lower bounded by coherent information defined as $I^{\mathrm{coh}}_{A>B}=S(\rho_B)-S(\rho_{AB})\equiv -S(A|B)$. This conjecture has been proven by Devetak and Winter (2005). The proof was based on cryptographic techniques, where one first performs an error correction (corresponding to the correcting bit) and then privacy amplification (corresponding to the correcting phase), both procedures by means of random codes (discussed in Sec. XIX).

Another protocol that distills the amount $I^{\mathrm{coh}}_{A>B}$ of singlets from a given state is the following (Horodecki, Oppenheim, *et al.*, 2005, 2007): given many copies of the state, Alice projects her system onto so-called typical subspace (Schumacher, 1995) (the probability of failure is exponentially small with the number of copies). Subsequently, she performs incomplete measurement $\{P_i\}$ where the projectors P_i project onto blocks of size $2^{n(S_B-S_{AB})}$. If the measurement is chosen at random according to uniform measure (Haar measure), it turns out that for any given outcome Alice and Bob share almost a maximally entangled state, hence equivalent to $n(S_B-S_{AB})$ e-bits. Of course, for each particular outcome i the state is different, therefore one-way communication is needed (Bob has to know the outcome i).

The above bound is often too rough (because one can distill states with negative coherent information using the recurrence protocol). Coherent information $I^{\mathrm{coh}}_{A>B}$ is not an entanglement monotone. It is then known that in general the optimal protocol of distillation of entanglement is some two-way protocol which increases I^{coh}, followed by the general hashing protocol; that is, we have (Horodecki *et al.*, 2000c)

$$E_D(\rho) = \sup_{\Lambda\in \mathrm{LOCC}} I^{\mathrm{coh}}(\Lambda(\rho)). \tag{88}$$

It is, however, not known how to attain the highest coherent information via the two-way distillation protocol. Interestingly, the rate (87) can be improved even by one-way protocol (Shor and Smolin, 1996).

G. Bound entanglement: When distillability fails

Since the seminal paper on distillation (Bennett, Brassard, *et al.*, 1996), there was a common expectation that all entangled bipartite states are distillable. Surprisingly it is not the case. It was shown by M. Horodecki *et al.* (1998) that the PPT states cannot be distilled. It is rather obvious that one cannot distill from separable states. Interestingly, the first example of the entangled PPT state had been already known from Horodecki (1997). Generally the states that are entangled yet not distillable are called bound entangled. It is not known if there are other bound entangled states than PPT entangled states. There are many quite interesting formal approaches allowing us to obtain families of the PPT entangled state. There is, however, no operational, intuitive "reason" for the existence of this mysterious type of entanglement.

We first comment on the nondistillability of separable states. The intuition for this is straightforward: separable states can be created via LOCC from scratch. If one could distill singlets from them, it would be creating something out of nothing. This reasoning of course does not hold for entangled PPT states. However, one can look from a different angle to find relevant formal similarities between PPT and separable states. Namely, concerning separable states one can observe that the fidelity $F=\mathrm{Tr}\,\sigma_{\mathrm{sep}}|\Phi^+\rangle\langle\Phi^+|$ is no greater than $1/d$ for σ_{sep} acting on $\mathcal{C}^d\otimes\mathcal{C}^d$. Since LOCC operations can only transform a separable state into another separable state (i.e., the set of separable states is closed under LOCC operations), one cannot distill singlet from separable states since one cannot increase the singlet fraction.

It turns out that also PPT states do not admit a higher fidelity than $1/d$ as well as are closed under LOCC operations (Rains, 1999, 2000). Indeed we have $\mathrm{Tr}\,\rho_{AB}|\Phi^+\rangle\langle\Phi^+|=(1/d)\mathrm{Tr}\,\rho^{\Gamma}_{AB}V$ which can not exceed $1/d$ [here V is the swap operator (42)]. This is because $\rho^{\Gamma}_{AB}\geqslant 0$, so that $\mathrm{Tr}\,\rho^{\Gamma}_{AB}V$ can be viewed as an average value of a random variable which cannot exceed 1 since V has eigenvalues ± 1. To see the second feature, note that any LOCC operation Λ acts on a state ρ_{AB} as follows:

$$\rho_{\mathrm{out}} = \Lambda(\rho_{AB}) = \sum_i A_i\otimes B_i(\rho_{AB})A_i^\dagger\otimes B_i^\dagger, \tag{89}$$

which after partial transpose on subsystem B gives

$$\rho^{\Gamma}_{\mathrm{out}} = \sum_i A_i\otimes (B_i^\dagger)^T(\rho^{\Gamma}_{AB})A_i^\dagger\otimes B_i^T. \tag{90}$$

The resulting operator is positive, only if ρ^{Γ}_{AB} was positive.

Since the discovery of the first bound entangled states many further examples of such states were found, only a few of which we have discussed (see Sec. VI.B.7). The comprehensive list of achievements in this field, as well as the introduction to the subject, can be found in Clarisse (2006b). There has been also an extensive research devoted to multipartite bound entanglement; see Horodecki *et al.* (2007).

H. The problem of NPT bound entanglement

Although it is already known that there exist entangled nondistillable states, still we do not have a characterization of the set of such states. The question which

remains open since the discovery of bound entanglement properties of PPT states is, are all NPT states distillable? For two main attempts[47] to solve the problem see DiVincenzo, Shor, *et al.*, (2000) and Dür, Cirac, (2000). Horodecki and Horodecki (1999) showed that this holds if and only if all NPT Werner states (64) (equivalently entangled Werner states) are distillable. It simply follows from the fact that as in the case of two qubits any entangled state can be filtered, to such a state, that after proper twirling one obtains an entangled Werner state. The question is hard to answer because of its asymptotic nature. A necessary and sufficient condition for entanglement distillation (M. Horodecki *et al.*, 1998) can be stated as follows: The bipartite state ρ is distillable if and only if there exists n such that ρ is n-copy distillable (i.e., $\rho^{\otimes n}$ can be filtered to a two-qubit entangled state)[48] for some n. It is, however, known that there are states that are not n-copy distillable but are $(n+1)$-copy distillable (Watrous, 2004) (see also Bandyopadhyay and Roychowdhury, 2003); for this reason, the numerical search concerning distillability based on a few copies may be misleading. There is an interesting characterization of n-copy distillable states in terms of entanglement witnesses found in Kraus *et al.* (2002). Namely, a state is distillable if the operator

$$W_n = P^+_{A'B'} \otimes [\rho^{\otimes n}_{AB}]^\Gamma \tag{91}$$

is not an entanglement witness (here $A'B'$ is a two-qubit system, P^+ is a maximally entangled state).

One may also think that the problem could be solved by the use of a simpler class of maps, namely, PPT operations. However, Eggeling *et al.* (2001) showed that any NPT state can be distilled by PPT operations. Recently the problem was attacked by means of positive maps, and associated "distillability witnesses" by Clarisse (2005) (see also Clarisse, 2006a).

The problem of the existence of NPT bound entangled (BE) states has important consequences. If they indeed exist, then distillable entanglement is nonadditive and nonconvex (Shor, Smolin, and Terhal, 2001). Two states of zero E_D will together give nonzero E_D. The set of bipartite BE states will not be closed under tensor product, and under mixing. For an extensive review of the problem of existence of NPT BE states see Clarisse (2006b).

Schematic representation of the set of all states including hypothetical set of NPT bound entangled states is shown in Fig. 3.

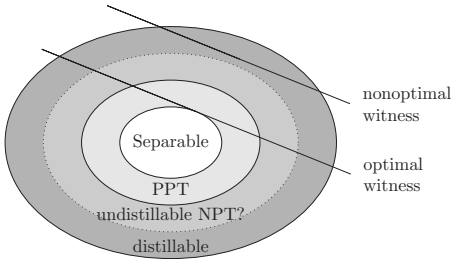

FIG. 3. Schematic representation of the set of all states with an example of entanglement witness and its optimization.

I. Activation of bound entanglement

Entanglement is always considered as a resource useful for a certain task. It is clear that pure entanglement can be useful for many tasks, as considered in Sec. III. Since the discovery of bound entanglement much effort was devoted to find some nontrivial tasks that this type of entanglement allows us to achieve.

The first phenomenon which proves the usefulness of bound entanglement, called activation of bound entanglement, was discovered by R. Horodecki *et al.* (1999). A parameter which is improved after activation is the so-called probabilistic maximal singlet fraction, that is, $F^{(p)}_{\max}(\rho) = \max_\Lambda \mathrm{Tr}[\Lambda(\rho)|\Phi^+\rangle\langle\Phi^+|]\mathrm{Tr}[\Lambda(\rho)]$ for ρ acting on $\mathcal{C}^d \otimes \mathcal{C}^d$, where Λ are local filtering operations.[49]

Consider a state σ with $F^{(p)}_{\max}$ bounded away from 1, such that no LOCC protocol can go beyond this bound. Then a protocol was found, involving k pairs of some BE state ρ_{be}, which takes as an input a state σ, and outputs a state σ' with singlet fraction arbitrarily close to 1 (which depends on k). That is,

$$\rho^{\otimes k}_{\mathrm{be}} \otimes \sigma \to \sigma', \quad \lim_k F^{(p)}_{\max}(\sigma') = 1. \tag{92}$$

The protocol is actually closely related to the recurrence distillation protocol (see Sec. XII.B), generalized to higher dimension and with the twirling step removed. In the above scenario the state ρ_{be} is an activator for a state σ. The probability of success in this protocol decreases as the output fidelity increases. To understand the activation, recall that the probabilistic maximal singlet fraction of every bound entangled state is by definition bounded by $1/d$, as discussed in Sec. XII.G. It implies that $\rho^{\otimes k}_{\mathrm{be}}$ also have $F^{(p)}_{\max}$ bounded away from 1. We have then two states with probabilistic maximal fidelity bounded away from 1, which, however, changes if they are put together. For this reason, the effect of activation demonstrates a sort of *nonadditivity* of maximal singlet fraction.

The effect of activation was further developed in various directions. It was shown by Vollbrecht and Wolf (2002a) that any NPT state can be made one-copy

[47]Two recent attempts are unfortunately incorrect (Chattopadhyay and Sarkar, 2006; Simon, 2006).

[48]Equivalently, there exists a pure state $|\psi\rangle$ of Schmidt rank 2 such that $\langle\psi|(\rho^{\otimes n})^\Gamma|\psi\rangle < 0$ (DiVincenzo, Shor, *et al.*, 2000; Dür, Cirac, *et al.*, 2000).

[49]The superscript (p) emphasizes a "probabilistic" nature of this maximal singlet fraction so that it would not be confused with a different parameter defined analogously as $F_{\max}(\rho) = \max_\Lambda \mathrm{Tr}[\Lambda(\rho)|\Phi^+\rangle\langle\Phi^+|]$ with Λ a trace preserving LOCC operation, that is called a maximal singlet fraction.

distillable[50] by use of BE states. Moreover, to this end one can use BE states which are arbitrarily close to separable states.

A remarkable result showing the power of LOCC operations supported with an arbitrarily small amount of BE states was established by Ishizaka (2004). Namely, the interconversion of pure bipartite states is ruled by entanglement measures. In particular, a pure state with a smaller measure called Schmidt rank (see Sec. XV) cannot be turned by LOCC, even probabilistically, into a state with higher Schmidt rank. However, any transition between pure states is possible with some probability, if assisted by arbitrarily weakly bound entangled states. This works also for multipartite states. Interestingly, the fact that one can increase Schmidt rank by PPT operations (i.e., also with some probability by assistance of a PPT state) was implicit already by Audenaert *et al.* (2003).

Although specific examples of *activators* has been found, the general question if any (bound) entangled state can be an activator has waited until the discovery of Masanes (2005, 2006a). He showed that every entangled state (even a bound entangled one) can enhance a maximal singlet fraction and in turn a fidelity of teleportation of some other entangled state, i.e., for any state ρ there exists state σ such that

$$F_{\max}^{(p)}(\sigma) < F_{\max}^{(p)}(\rho \otimes \sigma). \tag{93}$$

This result[51] for the first time shows that every entangled state can be used to some nonclassical task. Masanes provides an existence proof via *reductio ad absurdum*. It is then still a challenge to construct for a given state some activator, even though one has a promise that it can be found. This result indicates the first useful task that can be performed by all bound entangled states.

The idea of activation for the bipartite case was developed in the multipartite case by Dür and Cirac (2000a) and Bandyopadhyay, Chattopadhyay, *et al.* (2005) where specific families of multipartite bound entangled states were found. Interestingly, those states were then used to find an analogous phenomenon in the classical key agreement scenario (see Sec. XIX). It was recently generalized by Masanes (2005).

The activation considered above is a result which concerns one copy of the state. An analogous result which holds in the asymptotic regime, called superactivation, was found by Shor *et al.* (2003); namely, there are four-partite states constructed by Smolin (2001), such that no two parties even with the help of other parties can distill pure entanglement from them:

$$\rho_{ABCD}^{\mathrm{BE}} = \tfrac{1}{4}\sum_{i=1}^{4} |\Psi_{AB}^{i}\rangle\langle\Psi_{AB}^{i}| \otimes |\Psi_{CD}^{i}\rangle\langle\Psi_{CD}^{i}|. \tag{94}$$

However, the following state, consisting of five copies of the same state, but each distributed into different parties, is no longer bound entangled,

$$\rho_{\mathrm{free}} = \rho_{ABCD}^{\mathrm{BE}} \otimes \rho_{ABCE}^{\mathrm{BE}} \otimes \rho_{ABDE}^{\mathrm{BE}} \otimes \rho_{ACDE}^{\mathrm{BE}} \otimes \rho_{BCDE}^{\mathrm{BE}}. \tag{95}$$

This result is stronger than activation in two ways. First, it turns two totally nonuseful states (bound entangled ones) into a useful state (distillable one), and second, the result does not concern one copy but it has an asymptotically nonvanishing rate. In other words, it shows that there are states ρ_1 and ρ_2 such that $E(\rho_1 \otimes \rho_2) > E(\rho_1) + E(\rho_2)$, despite the fact that $E(\rho_1) = E(\rho_2) = 0$ where E is a suitable measure describing the effect of distillation (see Sec. XV).

Apart from superactivation, the Smolin states (94) have another interesting application, namely, remote quantum information concentration (Murao and Vedral, 2001). This works as follows: consider the three-qubit state $\psi_{ABC}(\phi)$ being an output of a quantum cloning machine that is shared by three parties Alice, Bob, and Charlie. Suppose that they want to recreate the initial ϕ in some other distant place. This is clearly impossible by LOCC. If, however, each of them is given in addition one particle of the four-particles in a Smolin state $\varrho_{ABCD}^{\mathrm{unlock}}$ [Eq. (72)] with the remaining fourth D particle handed to another party (David) then a simple LOCC action of the three parties can "concentrate" the state ϕ back remotely at David's site.

XIII. MANIPULATIONS OF ENTANGLEMENT AND IRREVERSIBILITY

A. LOCC manipulations on pure entangled states: Exact case

The study of exact transformations between pure states by LOCC was initiated by Lo and Popescu (2001). A seminal result in this area is due to Nielsen (1999). It turns out that the possible transitions can be classified in terms of squares of Schmidt coefficients λ_i (i.e., eigenvalues of a local density matrix). That is, a pure state $|\psi\rangle = \sum_{j=1}^{d} \sqrt{\lambda_j^{(\psi)}}|jj\rangle$ can be transformed into another pure state $|\phi\rangle = \sum_{j=1}^{d} \sqrt{\lambda_j^{(\phi)}}|jj\rangle$ if and only if for each $k \in \{1, \ldots, d\}$, holds that

$$\sum_{j=1}^{k} \lambda_j^{(\psi)\downarrow} \leqslant \sum_{j=1}^{k} \lambda_j^{(\phi)\downarrow}, \tag{96}$$

where $\lambda_j^{(\psi,\phi)\downarrow}$ are eigenvalues of a subsystem of ψ (ϕ) in descending order. The above condition states that ϕ majorizes ψ (see also Sec. V.C). Thus one can transform ψ into ϕ only when subsystems of ψ are more mixed than those of ϕ. This is compatible with the Schrödinger approach: the more mixed the subsystem, the more entangled the state (see Sec. V).

[50] A state ρ is called one-copy distillable if there exist projectors P, Q of rank 2 such that $P \otimes Q \rho P \otimes Q$ is NPT. In other words, from ρ one can then obtain by LOCC a two-qubit state with F greater than 1/2.

[51] Actually, the result is even stronger: it holds also for $F_{\max}$ (i.e., a singlet fraction achievable with probability 1).

Since majorization constitutes a partial order, reversible conversion $\psi \leftrightarrow \phi$ is possible if and only if the Schmidt coefficients of both states are equal. Moreover, there exist states either of which cannot be converted into each other. Thus generically, LOCC transformations between pure states are irreversible. However, as shown it can be lifted in the asymptotic limit (see Sec. XIII.B.1).

Further results in this area have been provided by Vidal (2003) who obtained the optimal probability of success for transitions between pure states (see Sec. XV.D.1), and Jonathan and Plenio (1999), who considered transitions state→ensemble.

1. Entanglement catalysis

The most surprising consequence of Nielsen's laws of pure state transitions have been discovered by Jonathan and Plenio (1999); namely, for some states ψ_1 and ψ_2 for which the transition $\psi_1 \to \psi_2$ is impossible, the following process is possible:

$$\psi_1 \otimes \phi \to \psi_2 \otimes \phi. \tag{97}$$

Thus we borrow state ϕ, run the transition, and obtain the untouched ϕ back. The latter state plays exactly the role of a catalyst which though not used up in the reaction, its presence is necessary to run it. Interestingly, it is not hard to see that the catalyst cannot be maximally entangled. The catalysis effect was extended to the case of mixed states by Eisert and Wilkens (2000).

2. SLOCC classification

For multipartite pure states Schmidt decomposition does not exist. Therefore the Nielsen result cannot be easily generalized. Moreover, analysis of LOCC manipulations does not allow us to classify states into some coarse grained classes, that would give a rough, but more transparent picture. Indeed, two pure states can be transformed into each other by LOCC if and only if they can be transformed by local unitary transformations so that to parametrize classes one needs continuous labels, even in the bipartite case.

To obtain a simpler, "coarse grained" classification, which would be helpful to grasp important qualitative features of entanglement, it was proposed (Dür, Vidal, *et al.*, 2000) to treat states as equivalent, if with some nonzero probability they can be transformed into each other by LOCC. This is called *stochastic* LOCC (SLOCC). It is equivalent to say that there exist reversible operators A_i such that

$$|\psi\rangle = A_1 \otimes \cdots \otimes A_N |\phi\rangle. \tag{98}$$

For bipartite pure states of a $d \otimes d$ system we obtain d entangled classes of states, determined by a number of nonzero Schmidt coefficients (the so-called Schmidt rank). Here is an example of SLOCC equivalence: the state

$$|\psi\rangle = a|00\rangle + b|11\rangle \tag{99}$$

with $a > b > 0$ can be converted (up to an irrelevant phase) into $|\phi^+\rangle$ by the filter $A \otimes I$, with

$$A = \begin{bmatrix} \frac{b}{a} & 0 \\ 0 & 1 \end{bmatrix}$$

with probability $p = 2b^2$. So we have two classes: that of $|\phi^+\rangle$ and that of $|00\rangle$.

A surprising result is due to Ishizaka (2004) who considered SLOCC assisted by bound entangled PPT states. He then showed that every state can be converted into any other (see Sec. XII.I). This works for both bipartite and multipartite pure states. For multipartite states SLOCC classification was done in the case of three (Dür, Vidal, *et al.*, 2001) and four qubits (Verstraete *et al.*, 2002), and also two qubits and a qudit (Miyake and Verstraete, 2004). For three qubits there are five classes plus a fully product state, three of them being Bell states between two qubits (i.e., states of type $\mathrm{EPR}_{AB} \otimes |0\rangle_C$). Two others are the GHZ state,

$$|\mathrm{GHZ}\rangle = (1/\sqrt{2})(|000\rangle + |111\rangle), \tag{100}$$

and the so-called W state,

$$|W\rangle = (1/\sqrt{3})(|100\rangle + |010\rangle + |001\rangle). \tag{101}$$

They are inequivalent, in a sense, that none of them can be converted into the other one with nonzero probability (unlike in bipartite state case, where one can go from any class to any lower class, i.e., having lower Schmidt rank).

In the $2 \otimes 2 \otimes d$ case (Miyake, 2004; Miyake and Verstraete, 2004), there is still a discrete family of inequivalent classes, where there is a maximally entangled state—two EPR states $\phi^+_{AB_1} \otimes \phi^+_{B_2C}$ (where the system B is four dimensional). Any state can be produced from it simply via teleportation (Bob prepares the needed state, and teleports its parts to Alice and to Charlie).

In the four-qubit case the situation is not so simple: the inequivalent classes constitute a continuous family, which one can divide into nine qualitatively different subfamilies.

The SLOCC classification is a quite elegant generalization of local unitary classification. In the latter case the basic role is played by invariants of group $\mathrm{SU}_{d_1} \otimes \cdots \otimes \mathrm{SU}_{d_N}$ for the $d_1 \otimes \cdots \otimes d_N$ system, while in SLOCC, the relevant group is $\mathrm{SL}_{d_1,C} \otimes \cdots \otimes \mathrm{SL}_{d_N,C}$ (one restricts to filters of determinant 1, because the normalization of states does not play a role in the SLOCC approach).

Finally, the SLOCC classification of pure states can be used to obtain some classification of mixed states (see Acín *et al.*, 2001; Miyake and Verstraete, 2004).

B. Asymptotic entanglement manipulations and irreversibility

Classifications based on exact transformations suffer from some lack of continuity: for example, in the

SLOCC approach ψ with squares of Schmidt coefficients (0.5,0.49,0.01) is in the same class as the state (1/3, 1/3, 1/3), but in a different class than (0.5,0.5,0), while we clearly see that the first and the last have much more in common than the middle one. In order to neglect small differences, one can employ some asymptotic limit. This is in the spirit of Shannon's communication theory, where one allows for some inaccuracies of information transmission, provided they vanish in the asymptotic limit of the many uses of the channel. Interestingly, the first results on the quantitative approach to entanglement (Bennett, Bernstein, *et al.*, 1996; Bennett, Brassard, *et al.*, 1996, Bennett, DiVincenzo, *et al.*, 1996) were just based on LOCC transformations in the asymptotic limit.

In asymptotic manipulations, the main question is what is the rate of transition between two states ρ and σ? One defines the rate as follows. We assume that Alice and Bob have initially n copies in state ρ. They apply LOCC operations, and obtain m pairs[52] in some joint state σ_m. If for large n the latter state approaches state $\sigma^{\otimes m}$, i.e.,

$$\|\sigma_m - \sigma^{\otimes m}\|_1 \to 0, \tag{102}$$

and the ratio m/n does not vanish, then we say that ρ can be transformed into σ with rate $R=\lim m/n$. The largest rate of transition we denote by $R(\rho\to\sigma)$. In particular, distillation of entanglement described in Sec. XII is the rate of transition to the EPR state,

$$E_D(\rho) = R(\rho \to \psi^+). \tag{103}$$

The cost of creating a state out of EPR states is given by

$$E_C(\rho) = 1/R(\psi^+ \to \rho) \tag{104}$$

and it is the other basic important measure (see Sec. XV.A for a description of those measures).

1. Unit of bipartite entanglement

The fundamental result in the asymptotic regime is that any bipartite pure state can be transformed into a two-qubit singlet with a rate given by the entropy of entanglement $S_A=S_B$, i.e., the entropy of the subsystem (either A or B, since for pure states they are equal). And, to create any state from a two-qubit singlet, one needs an S_A singlets pair two-qubit state. Thus any pure bipartite state can be reversibly transformed into any other state. As a result, in the asymptotic limit entanglement of these states can be described by a single parameter—the von Neumann entropy of a subsystem. This simplification is due to the fact, that many transitions that are not allowed in an exact regime become possible in an asymptotic limit. Thus the irreversibility implied by the Nielsen result is lifted in this regime, and the EPR state becomes a universal unit of entanglement.

2. Bound entanglement and irreversibility

However, even in the asymptotic limit one cannot get rid of irreversibility for bipartite states, due to the existence of bound entangled states; namely, to create such a state from pure states by LOCC one needs entangled states, while no pure entanglement can be drawn back from it. Thus the bound entangled state can be viewed as a sort of black hole of entanglement theory (Terhal *et al.*, 2003). One can also use a thermodynamical analogy (P. Horodecki *et al.*, 1998; Horodecki *et al.*, 2002). Namely, a bound entangled state is like a single heat bath: to create the heat bath, one needs to dissipate energy, but no energy useful to perform mechanical work can be drawn in a cyclic process (the counterpart of the work is quantum communication via teleportation). We note here that the interrelations between entanglement and energy were considered also in different contexts (see, e.g., R. Horodecki *et al.*, 2001; Osborne and Nielsen, 2002; McHugh, Zuman, *et al.*, 2006).

It was a formidable task to determine if we have irreversibility in an asymptotic setting, as it was related to the fundamental problem of whether the entanglement cost is equal to the entanglement of formation (see Sec. XV). The first example of states with asymptotic irreversibility was provided by Vidal and Cirac (2001). Subsequently more examples have been revealed. Vollbrecht *et al.* (2004) analyzed mixtures of maximally entangled states by use of the uncertainty principle. It turns out that irreversibility for this class of states is generic: the reversible states happen to be those which minimize the uncertainty principle, and they all turn out to be so-called pseudopure states (see P. Horodecki *et al.*, 1998), for which reversibility holds for trivial reasons. An example of such a state is

$$\tfrac{1}{2}|\psi^+_{AB}\rangle\langle\psi^+_{AB}| \otimes |0\rangle_{A'}\langle 0| + \tfrac{1}{2}|\psi^-_{AB}\rangle\langle\psi^-_{AB}| \otimes |1\rangle_{A'}\langle 1|. \tag{105}$$

The states $|0\rangle$, $|1\rangle$ are local orthogonal "flags," which allow us to return to the pure state ψ_+ on system AB. This shows that, within mixtures of maximally entangled states, irreversibility is a generic phenomenon.

In the above cases, the states were not bound entangled. The irreversibility was quantitative: more pure entanglement was needed to create states than can be obtained from them. For bound entangled states, one might hope to regain reversibility as follows: perhaps for many copies of bound entangled state, a sublinear (in number of copies) amount of pure entanglement would be enough to create them. In other words, it might be that for bound entangled states E_C vanishes. This would mean, that asymptotically, the irreversibility is lifted. However, it was shown that irreversibility is exhibited

[52]Here m depends on n, which we do note write explicitly for brevity.

by all bound entangled states (Yang, Horodecki, *et al.*, 2005).

An open general question is the following: for what mixed states we have reversibility, so that distillable entanglement is equal to entanglement cost. Already in the original papers on entanglement distillation (Bennett, Brassard, *et al.*, 1996; Bennett, DiVincenzo, *et al.*, 1996) there was an indication that generically we would have a gap between those quantities,[53] even though for some trivial cases we can have $E_C=E_D$ for mixed states (P. Horodecki *et al.*, 1998). Continuing the thermodynamical analogy, a generic mixed state would be like a system of two heat baths of different temperature, from which part of the energy but not the whole can be transferred into a mechanical work.

Surprisingly, Brandão and Plenio (2008) showed that irreversibility is lifted when one applies a larger class of operations than LOCC—namely, the ones that preserve separability (supplemented by a sublinear amount of entanglement). Under this new class, entanglement of distillation and entanglement cost coincide with being equal to the relative entropy of entanglement. It can be interpreted as follows (cf. M. Horodecki, 2008): as said, physically, the second law forbids changing full energy into work in the cyclic process. However, a hypothetical process, which obeys only energy conservation, but not the second law, can do this, hence it removes the difference between heat and useful energy. Now, the separable maps—ones that cannot be done in a distant lab without quantum communication—would then correspond to this latter process, and they remove the difference between bound entanglement and the pure one.

3. Asymptotic transition rates in multipartite states

In the multipartite case there is no such universal unit of entanglement as the singlet state. Even for three particles, we can have three different types of EPR states: the one shared by Alice and Bob, by Alice and Charlie, and by Bob and Charlie. By LOCC it is impossible to create any of them from the others.

It turns out, however, that not only are EPR states "independent" units, but also GHZ state cannot be (even asymptotically) created from them, for any number of parties, hence it constitutes another independent unit (Linden, Popescu, Schumacher, *et al.*, 1999). This shows that there is true N-partite entanglement in the asymptotic limit.

The general open problem is to find a minimal reversible entanglement generating set (Bennett *et al.*, 2000), i.e., a minimal set of states from which any other state can be reversibly obtained by LOCC. For a more detailed discussion, see Horodecki *et al.* (2007).

[53]Although in their operational approach the authors meant what we now call entanglement cost, to quantify it they used nonregularized measure entanglement of formation.

XIV. ENTANGLEMENT AND QUANTUM COMMUNICATION

In classical communication theory, the most important notion is that of correlations. To send a message means in fact to correlate the sender and the receiver. Also the famous Shannon formula for channel capacity involves mutual information, a function describing correlations. Thus the ability to faithfully transmit a bit is equivalent to the ability to faithfully share maximally correlated bits. It was early recognized that in quantum communication theory it is entanglement which will play the role of correlations. For this reason entanglement is the cornerstone of quantum communication theory.

In classical communication theory, a central task is to send some signals. For a fixed distribution of signals emitted by a source, there is only one ensemble of messages. In the quantum case, a source is represented by a density matrix ρ, and there are many ensembles realizing the same density matrix. What does it then mean to send quantum information? According to Bennett *et al.* (1993) it is the ability of transmitting an unknown quantum state. For a fixed source, this would mean that all possible ensembles are properly transmitted. For example, consider a density matrix $\rho=(1/d)\Sigma_i|i\rangle\langle i|$. Suppose that a channel decoheres its input in basis $\{|i\rangle\}$. We see that the set of states $\{|i\rangle\}$ goes through the channel without any disturbance. However, a complementary set consisting of states $U|i\rangle$, where U is the discrete Fourier transform, is completely destroyed by a channel, because the channel destroys superpositions. [For $d=2$, an example of such a complementary ensemble is $|+\rangle$, $|-\rangle$ where $|\pm\rangle=\frac{1}{2}(|0\rangle\pm|1\rangle)$]. As a matter of fact, each member of the complementary ensemble is turned into maximally mixed state.

How does one recognize whether all ensembles can go through? Schumacher (1995) noted that instead of checking all ensembles we can check whether an *entangled* state ψ_{AB} is preserved, if we send half of it (the system B) down the channel. The state should be chosen to be a *purification* of ρ, i.e., $\mathrm{Tr}_A(|\psi\rangle\langle\psi|_{AB})=\rho$. Thus sending an unknown state is equivalent to faithfully sending entanglement.

Coming back to our example, the state can be chosen as $|\Phi^+\rangle=(1/\sqrt{d})\Sigma_i|i\rangle|i\rangle$. One can see that after applying our channel to one subsystem, the state becomes a classical (incoherent) mixture of states $|i\rangle|i\rangle$. This shows that the channel cannot convey quantum information at all. It is a reflection of a mathematical fact that if we send half of the purification of a full rank density matrix down the channel, then the resulting state will encode all the parameters of the channel. This heuristic statement has its mathematical form in terms of Choi-Jamiołkowski isomorphism between states and channels. Its most standard form links the channel Λ with a state ϱ_{AB}^{Λ} having maximally mixed left subsystem $\mathrm{Tr}_B(\varrho_{AB}^{\Lambda})=I/d_A$ as follows:

$$\varrho_{AB}^{\Lambda} = [I_A \otimes \Lambda_{A' \to B}] P_{AA'}^{+}, \tag{106}$$

where the projector onto maximally entangled state $P_{AA'}^{+}$ is defined on a product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_{A'}$, with $\mathcal{H}_A \simeq \mathcal{H}_{A'}$.[54]

A. Capacity of quantum channel and entanglement

The idea of quantum capacity $Q(\Lambda)$ of quantum channel Λ was introduced by Bennett, DiVincenzo, *et al.* (1996) where milestone achievements connecting quantum entanglement and quantum data transfer were provided. The capacity Q measures the largest rate of quantum information sent asymptotically faithfully down the channel:

$$Q = \sup \frac{\text{no. transmitted faithful qubits}}{\text{no. uses of channel}}, \tag{107}$$

where the fidelity of the transmission is measured by minimal subspace fidelity $f(\Lambda) = \min_{\psi} \langle \psi | \Lambda(|\psi\rangle\langle\psi|) | \psi \rangle$ (Bennett *et al.*, 1997). Also, the average fidelity transmission can be used, which is a direct analog of the average fidelity in the quantum teleportation process $\bar{f}(\Lambda) = \int \langle \psi | \Lambda(|\psi\rangle\langle\psi|) | \psi \rangle d\psi$ with uniform measure $d\psi$ on the unit sphere. We may have different scenarios: (i) a quantum channel without the help of a classical channel (capacity denoted by $Q^{\varnothing}$), (ii) with the help of a classical channel: one-way forward[55] ($Q^{\rightarrow}$), backward ($Q^{\leftarrow}$), and two-way ($Q^{\leftrightarrow}$). There is also entanglement assisted capacity Q_{ass} originating from a dense coding scheme, where entanglement is a free supplementary resource (Bennett, Shor, *et al.*, 1999).

An other approach based on the idea described above was formalized in terms of entanglement transmission. In particular, the quality of transmission was quantified by entanglement fidelity,

$$F(\Lambda, \Psi_{AB}) = \langle \Psi_{AB} | [I_A \otimes \Lambda_B] \, (|\Psi_{AB}\rangle\langle\Psi_{AB}|) | \Psi_{AB} \rangle, \tag{108}$$

with respect to a given state Ψ_{AB}.[56] The alternative definition of quantum capacity [which has been worked out by Schumacher (1996), Schumacher and Nielsen (1996), and Barnum *et al.* (1998) and shown to be equivalent to Bennett *et al.* (Bennett, DiVincenzo, *et al.*, 1996; Bennett *et al.*, 1997) in Barnum *et al.* (2000)] was based on counting the optimal pure entanglement transmission under the condition of high entanglement fidelity defined above.

A variation of the entanglement fidelity (Reimpell and Werner, 2005) is when the input is equal to the output $d_A = d_B = d$ and we send half of the maximally entangled state Φ_d^{+} down the channel. It is measured by the maximal entanglement fidelity of the channel:

$$F(\Lambda) := F(\Lambda, \Phi_d^{+}), \tag{109}$$

which is equal to the overlap of the state ϱ^{Λ} with a maximally entangled state, namely, $F(\Lambda) = F(\varrho^{\Lambda}) := \mathrm{Tr}(|\Phi_d^{+}\rangle\langle\Phi_d^{+}| \varrho^{\Lambda})$. It is interesting that one has (M. Horodecki *et al.*, 1999; Nielsen, 2002)

$$\bar{f}(\Lambda) = [dF(\Lambda) + 1]/(d+1). \tag{110}$$

This formula says that the possibility of sending on average faithfully quantum information happens if and only if it is possible to create maximal entanglement of Φ_d^{+} with the help of the channel. The above relation is used in the proof that the definition of zero-way (or, alternatively, one-way forward) version of quantum capacity Q (see below) remains the same if we apply any of the fidelities recalled above [for details of the proof, see Kretschmann and Werner (2004)].

The LHS of the above equality can be interpreted as an average teleportation fidelity of the channel that results from teleporting a given state through the mixed bipartite state ϱ_{Λ}.

An impressive connection between entanglement and quantum channel theory has been worked out by Bennett, Brassard, *et al.* (1996) and Bennett, DiVincenzo, *et al.* (1996) using teleportation. They have shown how to achieve a nonzero transmission rate by combining three elements: (i) creating many copies of ϱ^{Λ} by sending halves of singlets down the channel Λ, (ii) distilling maximal entanglement from many copies of the created state, and (iii) teleporting quantum information down the (distilled) maximal entanglement. Since the last process corresponds to ideal transmission the rate of the quantum information transmission is equal to the distillation rate in step (ii). In this way one can prove the inequality linking entanglement distillation E_D with quantum channel capacity $Q^{\leftrightarrow}$ as (Bennett, DiVincenzo, *et al.*, 1996)

$$E_D(\varrho^{\Lambda}) \leqslant Q^{\leftrightarrow}(\Lambda), \tag{111}$$

where ϱ^{Λ} is given by Eq. (106). The inequality holds for one-way forward and two-way scenarios of distillation (respectively, coding). The above inequality is one of the central links between quantum channels and quantum

[54]Note that this isomorphism has an operational meaning, in general, only one way: given the channel, Alice and Bob can obtain a bipartite state, but usually not vice versa. However, sometimes if Alice and Bob share a mixed bipartite state, then by use of classical communication they can simulate the channel. An example is the maximally entangled state, which allows us to regain the corresponding channel via teleportation. This was first pointed out by Bennett, DiVincenzo, *et al.* (1996).

[55]Remarkably, we have $Q^{\varnothing} = Q^{\rightarrow}$. It was argued by Bennett, DiVincenzo, *et al.* (1996) and the proof was completed by Barnum *et al.* (2000).

[56]For a typical source all three types of fidelity; average, minimum, and entanglement, are equivalent (Barnum *et al.*, 2000).

entanglement theory (see below). It is not known whether there is a lower bound like $cQ(\Lambda) \leqslant E_D(\varrho^\Lambda)$ for some constant c. However, there is at least qualitative equivalence shown by (Horodecki (2003e)

$$E_D(\varrho^\Lambda) = 0 \Rightarrow Q^{\leftrightarrow}(\Lambda) = 0. \tag{112}$$

An alternative simple proof which also works for multipartite generalization of this problem has been given by Dür *et al.* (2004). It uses teleportation and Choi-Jamiołkowski isomorphism to collective channels (Cirac *et al.*, 2001).

B. Formulas for capacities

For the capacity $Q^\varnothing$, the formula is given by the so-called LSD theorem (Lloyd, 1997; Shor, 2002; Devetak, 2003); namely, one maximizes coherent information over all bipartite states resulting from a pure state, half of it sent down the channel (see Sec. XII.F). However, one should optimize this quantity over many uses of the channel, so that the capacity reads

$$Q^\varnothing(\Lambda) = \lim(1/n) \sup_\psi I^{\mathrm{coh}}_{A>B}[(I \otimes \Lambda^{\otimes n})|\psi\rangle\langle\psi|]. \tag{113}$$

The fact that the formula is not "single letter," in the sense that it involves many uses of the channel, was established by (Shor and Smolin, 1996; see also DiVincenzo *et al.*, 1998).

Coherent information can be nonzero only for entangled states. Indeed, only entangled states can have greater entropy of the subsystem than that of the total system (Horodecki and Horodecki, 1994). In this context, an additional interesting qualitative link between entanglement and channel capacity formula is the hashing inequality stating that $E_D^{\rightarrow} \geqslant I^{\mathrm{coh}}_{A>B}$ (see Sec. XII). Quite remarkably we may have $E_D^{\rightarrow}(\varrho_{AB}) > 0$ even though $I^{\mathrm{coh}}_{A>B}(\varrho_{AB}) = 0$ which is related to the above mentioned Shor-Smolin result. Quite surprisingly, Smith and Yard (2008) discovered that two channels with zero capacity, if used jointly, can have nonzero capacity: $Q_\varnothing(\Lambda_1) = 0$, $Q_\varnothing(\Lambda_2) = 0$, but $Q_\varnothing(\Lambda_1 \otimes \Lambda_2)$. This is a highly nonclassical effect.

Another type of capacity for which the formula is known is entangled assisted capacity. It is given by the following single letter expression (Bennett, Shor, *et al.*, 1999, 2002):

$$Q_{\mathrm{ass}} = \tfrac{1}{2} \sup_{\psi_{AB}} I_{A:B}[(I_A \otimes \Lambda_B)(|\psi\rangle_{AB}\langle\psi|)], \tag{114}$$

where I is the quantum mutual information (for details, see Horodecki *et al.*, 2007).

C. Entanglement breaking and entanglement binding channels

Equations (111) and (112) naturally provoke the question which channels have capacity zero?

If the state ϱ^Λ is separable, then the corresponding channel is called entanglement breaking (Horodecki, Shor, *et al.*, 2003) and one cannot create entanglement at all by means of such a channel.[57] Now since it is impossible to distill entanglement from a separable state we see from Eq. (112) that the capacity of the entanglement breaking channel is zero, i.e., no quantum faithful quantum transmission is possible with the entanglement breaking channel. However, the converse is not true: the possibility to create entanglement with the help of the channel is not equivalent to quantum communication and it is the bound entanglement phenomenon which is responsible for that. To see it we observe that if the corresponding state ϱ^Λ is bound entangled, then the channel Λ, called in this case the binding entanglement channel (introduced by P. Horodecki, M. Horodecki, *et al.*, 2000; DiVincenzo *et al.*, 2003), allows for creation of entanglement. However, it cannot convey quantum information at all—it has capacity zero (Horodecki, 2003e).

Note that binding entanglement channels are not completely useless from a general communication point of view. First of all, some of them can be used to generate a secure cryptographic key; see Sec. XIX. Second, just these channels if composed with erasure channels (Bennett *et al.*, 1997), give rise the "0+0=1" effect discovered by Smith and Yard, described in the previous subsection.

D. Additivity questions

There is one type of capacity, where we do not send half of the entangled state, but restrict ourselves just to separable states. This is the classical capacity of the quantum channel, $C(\Lambda)$ (without any further support such as shared entanglement or so). However, even here entanglement comes in. Namely, it is still not resolved whether the sending of signals entangled between distinct uses of a channel can increase the transmission rate. A closely related problem is the following: Can we decrease the production of entropy by operations Λ_1 and Λ_2 by sending a joint state through the combined operation $\Lambda \otimes \Lambda$, i.e.,

$$\inf_\rho S[\Lambda_1(\rho)] + \inf_\rho S[\Lambda_2(\rho)] > \inf_\sigma S[(\Lambda_1 \otimes \Lambda_2)(\sigma)]. \tag{115}$$

One finds that this sharp equality can hold only via entangled input state σ. Interestingly, this problem has further connection with entanglement. It is equivalent to additivity of important measure of entanglement, the so-called entanglement of formation E_F [Shor (2003), see also Audenaert and Braunstein (2004), Koashi and Winter (2004), Matsumoto (2005), and references therein].

[57] Simply, its Kraus operators (in some decomposition) are of rank 1. Impossibility of creating entanglement follows from the fact that action of any channel of that kind can be simulated by a classical channel: for any input state, one measures it via some positive-operator-valued measure (POVM), and sends the classical outcome to the receiver. Based on this, the receiver prepares some state.

We have the following equivalent statements: additivity of entanglement of formation, superadditivity of entanglement of formation, additivity of minimum output entropy, additivity of so-called Holevo capacity, and additivity of Henderson-Vedral classical correlation measure C_{HV} (see Secs. XV and XIII for definitions of E_F and C_{HV}). To prove or disprove them for a long time was one of the fundamental problems of quantum information theory. The breakthrough has been done by Hastings (2008) (who built upon Hayden and Winter, 2008). He showed existence of two channels which satisfy inequality (115). Thus all the above quantities are nonadditive. Moreover, by Fukuda and Wolf (2007),[58] this implies that there is nonadditivity also if the channels are the same, which, in turn, implies, e.g., that entanglement of formation is not equal to the so-called entanglement cost (see Sec. XV). Another question which remains open is additivity classical capacity $C(\Lambda)$. A step forward was made by Czekaj and Horodecki (2008) who showed nonadditivity of classical capacity for multiply access channels, the effect impossible for classical channels. One of their channels is based on dense coding.

In discussing the links between entanglement and communication, one has to mention one more additivity problem inspired by entanglement behavior. This is the problem of the additivity of quantum capacities Q touched on already by Bennett, Divincenzo, *et al.* (1996). Due to a nonadditivity phenomenon called activation of bound entanglement (see Sec. XII.I) it has even been conjectured (P. Horodecki *et al.* (1999) that for some channels $Q^{\leftrightarrow}(\Lambda_1 \otimes \Lambda_2) > 0$, even if both channels have vanishing capacities, i.e., $Q^{\leftrightarrow}(\Lambda_1) = Q^{\leftrightarrow}(\Lambda_2) = 0$. Here again, as in the question of additivity of the classical capacity $C(\Lambda)$, a possible role of entanglement in inputs of the channel $\Lambda_1 \otimes \Lambda_2$ comes into play. Though we know that such strange nonadditivity can hold for $Q^{\varnothing}$ (Smith and Yard, 2008), the question is open for $Q^{\leftrightarrow}$.

Though this problem is still open, there is a multipartite version where nonadditivity was found (Dür *et al.*, 2004). In fact, the multiparty communication scenario can be formulated and the analog of Eqs. (111) and (112) can be proven (Dür *et al.*, 2004), together with the notion and construction of binding entanglement channels. Remarkably, in this case the application of multipartite BE channels isomorphic to multipartite bound entangled states and application of the multipartite activation effect leads to nonadditivity of two-way capacity regions for a quantum broadcast (equivalently multiply access) channel (Dür *et al.*, 2004). A tensor product of three binding channels Λ_i which automatically have zero capacity leads to the channel $\Lambda: \otimes_{i=1}^{3} \Lambda_i$ with nonzero capacity. In this case bound entanglement activation (see the section on activation) leads to the proof of nonadditivity effect in quantum information transmission.

[58] We are grateful to Francesco Buscemi for pointing out this reference.

XV. QUANTIFYING ENTANGLEMENT

A. Distillable entanglement and entanglement cost

The initial idea to quantify entanglement was connected with its usefulness in terms of *communication* (Bennett, Brassard, *et al.*, 1996; Bennett, DiVincenzo, *et al.*, 1996). As one knows via a two-qubit maximally entangled state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ one can teleport one qubit. If a state is not maximally entangled, then it does not allow for faithful teleportation. However, in analogy to Shannon communication theory, it turns out that when having many copies in such a state, one can obtain asymptotically faithful teleportation at some rate (see Sec. XII). To find how many qubits per copy we can teleport it is enough to determine how many *e*-bits we can obtain per copy, since every $|\phi^+\rangle$ can then be used for teleportation. In this way we arrive at transition rates as described in Sec. XIII, and two basic measures of entanglement E_D and E_C.

Distillable entanglement. Alice and Bob start from n copies of state ρ, and apply an LOCC operation, that ends up with a state σ_n. We now require that for large n the final state approaches the desired state $|\phi^+\rangle^{\otimes m_n}$. If it is impossible, then $E_D = 0$. Otherwise we say that the LOCC operations constitute a distillation protocol $\mathcal{P}$ and the rate of distillation is $R_{\mathcal{P}} = \lim_n m_n/n$. The distillable entanglement is the supremum of such rates over all possible distillation protocols. It can be defined concisely (cf. Plenio and Virmani, 2006) as follows:

$$E_D(\rho) = \sup\{r: \lim_{n\to\infty} [\inf_{\Lambda} \|\Lambda(\rho^{\otimes n}) - \Phi_{2^{rn}}^{+}\|_1] = 0\}, \tag{116}$$

where $\Phi_{2^{rn}}^{+} = (|\phi_+\rangle\langle\phi_+|)^{\otimes rn}$ and $\|\cdot\|_1$ is the trace norm [see Rains (1998) for showing that other possible definitions are equivalent].[59]

Entanglement cost. It is a measure dual to E_D, and it reports how many qubits we have to communicate in order to create a state. This, again, can be translated to *e*-bits, so that $E_C(\rho)$ is the number of *e*-bits one can obtain from ρ per input copy by LOCC operations. The definition is

$$E_C(\rho) = \inf\{r: \lim_{n\to\infty} [\inf_{\Lambda} \|\rho^{\otimes n} - \Lambda(\Phi_{2^{rn}}^{+})\|_1] = 0\}. \tag{117}$$

Hayden *et al.* (2001) showed that E_C is equal to regularized entanglement of formation E_F—a prototype of entanglement cost; see Sec. XV.C.2. The two quantities are, in general, not equal (see Sec. XIV.D). As mentioned, for pure states $E_D = E_C$.

Distillable key. There is yet another distinguished operational measure of entanglement for bipartite states, designed in similar spirit as E_D and E_C. It is distillable

[59] In place of the trace norm one can use Uhlmann fidelity $F(\rho,\sigma) = (\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})^2$, thanks to the inequality proven by Fuchs and van de Graaf (1997), $1 - \sqrt{F(\rho,\sigma)} \leq \frac{1}{2}\|\rho - \sigma\|_1 \leq \sqrt{1 - F(\rho,\sigma)}$.

private key K_D: The maximum rate of a bits of private key that Alice and Bob can obtain by LOCC from state ρ_{AB} where it is assumed that the rest E of the total pure state ψ_{ABE} is given to adversary Eve. The distillable key satisfies obviously $E_D \leqslant K_D$: indeed, a possible protocol of the distilling key is to distill EPR states and then from each pair obtain one bit of key by measuring in the standard basis. A crucial property of K_D is that it is equal to the rate of transition to a special class of states: so-called private states, which are a generalization of EPR states. We elaborate more on the distillable key and the structure of private states in Sec. XIX.

B. Entanglement measures: Axiomatic approach

The measures such as E_D or E_C are built to describe entanglement in terms of some tasks. Thus they arise from optimization of some protocols performed on quantum states. However, one can apply an axiomatic point of view, by allowing any function of state to be a measure, provided it satisfies some postulates. We now go through basic postulates.

1. Monotonicity axiom

The most important postulate for entanglement measures was proposed by Bennett, DiVincenzo, *et al.* (1996) still in the context of operationally defined measures.

Monotonicity under LOCC: Entanglement cannot increase under local operations and classical communication.

Vedral, Plenio, Rippin, *et al.* (1997) introduced the idea of axiomatic definition of entanglement measures and proposed that an entanglement measure is any function that satisfies the above condition plus some other postulates. Then Vidal (2000) proposed that monotonicity under LOCC should be the only postulate necessarily required from entanglement measures. Other postulates would then either follow from this basic axiom or should be treated as optional [see Popescu and Rohrlich (1997)]. The montonicity axiom can be written as follows. For any LOCC operation Λ we have

$$E(\Lambda(\rho)) \leqslant E(\rho). \tag{118}$$

Note that the output state $\Lambda(\rho)$ may include some registers with stored results of measurements of Alice and Bob (or more parties, in a multipartite setting), performed in the course of the LOCC operation Λ. The mathematical form of Λ is in general quite ugly (see, e.g., Donald *et al.*, 2002). A better mathematical expression is known as the so-called "separable operations" (Vedral, Plenio, Rippin, *et al.*, 1997; Rains, 2001)

$$\Lambda(\rho) = \sum_i A_i \otimes B_i(\rho) A_i^\dagger \otimes B_i^\dagger, \tag{119}$$

with obvious generalization to a multipartite setting. Every LOCC operation can be written in the above form, but not vice versa, as proved by Bennett, DiVincenzo, Fuch, *et al.* (1999). (For a more extensive treatment of various classes of operations, see Sec. XI.B.)

The known entanglement measures usually satisfy a stronger condition, namely, they do not increase on average,

$$\sum_i p_i E(\sigma_i) \leqslant E(\rho), \tag{120}$$

where $\{p_i, \sigma_i\}$ is ensemble obtained from the state ρ by means of LOCC operations. This condition was earlier considered as mandatory, see, e.g., M. Horodecki (2001); Plenio (2005), but there is now common agreement that the condition (118) should be considered as the only necessary requirement.[60] However, it is often easier to prove the stronger condition. In patricular, for convex measures, it can be expressed in terms of several simple conditions Vidal (2000) (see Horodecki *et al.*, 2007 for more details).

Interestingly, for bipartite measures monotonicity also implies that there is maximal entanglement in bipartite systems. More precisely, if we fix the Hilbert space $C^d \otimes C^{d'}$, then there exist states from which any other state can be created: these are states $U_A \otimes U_B$ equivalent to a singlet. Indeed, by teleportation, Alice and Bob can create from a singlet any pure bipartite state. Namely, Alice prepares locally two systems in a joint state ψ, and one of the systems teleports through a singlet. In this way Alice and Bob share the state ψ. Then they can also prepare any mixed state. Thus E must take the greatest value to the state ϕ^+.

Sometimes, one considers monotonicity under LOCC operations for which the output system has the same local dimension as the input system. For example, for n-qubit states, we may be interested only in output n-qubit states. Measures that satisfy such monotonicity can be useful in many contexts, and sometimes it is easier to prove such monotonicity (Verstraete *et al.*, 2003) (see Sec. XV.H.1).

2. Vanishing on separable states

If a function E satisfies the monotonicity axiom, it turns out that it is constant on separable states. It follows from the fact that every separable state can be converted to any other separable state by LOCC (Vidal, 2000). Even more, E must be *minimal* on separable states, because any separable state can be obtained by LOCC from any other state. It is reasonable to set this constant to zero. In this way we arrive at an even more basic axiom, which can be formulated already on the qualitative level: Entanglement vanishes on separable states.

[60] Indeed, the condition (118) is more fundamental, as it tells about entanglement of state, while Eq. (120) tells about average entanglement of an ensemble (family $\{p_i, \rho_i\}$), which is a less operational notion than the notion of state. Indeed it is not clear what it does mean to "have an ensemble." An ensemble can always be treated as a state, $\Sigma_i p_i |i\rangle\langle i| \otimes \rho_i$, where $|i\rangle$ are local orthogonal flags. However, it is not clear at all why one should require *a priori* that $E(\Sigma_i p_i |i\rangle\langle i| \otimes \rho_i) = \Sigma_i p_i E(\rho_i)$.

It is interesting that the LOCC monotonicity axiom almost imposes the latter axiom. Note also that those two axioms impose E to be a non-negative function.

3. Other possible postulates

The above two axioms are essentially the only ones that should be necessarily required from entanglement measures. However, there are other properties that may be useful and are natural in some contexts.

Normalization. One can require that the entanglement measure behaves in an "information theoretic way" on maximally entangled states, i.e., it counts e-bits:

$$E((\Phi_2^+)^{\otimes n}) = n. \tag{121}$$

A slightly stronger condition would be $E(\Phi_d^+)=\log_2 d$. For multipartite entanglement, there is no such natural condition, due to the nonexistence of a maximally entangled state.

Asymptotic continuity. One can also require some type of *continuity*. The asymptotic manipulations paradigm suggests continuity of the form (Donald *et al.*, 2000; Horodecki *et al.*, 2000; Vidal, 2002)

$$\|\rho_n - \sigma_n\|_1 \to 0 \Rightarrow |E(\rho_n) - E(\sigma_n)|/\log_2 d_n \to 0, \tag{122}$$

for states σ_n, ρ_n acting on Hilbert space $\mathcal{H}_n$ of dimension d_n. This is called asymptotic continuity. Measures which satisfy this postulate are useful in estimating E_D, and other transition rates, via inequality (146) (Sec. XV.E.2). The most prominent example of the importance of asymptotic continuity is that together with the above normalization an additivity is enough to obtain a *unique* measure of entanglement for pure states (see Sec. XV.E.1).

Convexity. Finally, entanglement measures are often convex. Convexity used to be considered a mandatory ingredient of the mathematical formulation of monotonicity. At present we consider convexity as merely a convenient mathematical property. Most known measures are convex, including relative entropy of entanglement, entanglement of formation, robustness of entanglement, negativity, and all measures constructed by means of a convex roof (see Sec. XV.C). It is an open question whether distillable entanglement is convex (Shor *et al.*, 2001). In the multipartite setting it is known that a version of distillable entanglement[61] is not convex (Shor *et al.*, 2003).

C. Axiomatic measures: A survey

Here we review bipartite entanglement measures built on an axiomatic basis. Some of them immediately generalize to the multipartite case. Multipartite entanglement measures will be presented in Sec. XV.H.

[61]For example a maximal amount of EPR pairs between two chosen parties, that can be distilled with the help of all parties.

1. Entanglement measures based on distance

A class of entanglement measures (Vedral, Plenio, Rippin, and Knight, 1997; Vedral and Plenio, 1998) are based on the natural intuition, that the closer the state is to the set of separable states, the less entangled it is. The measure is minimum distance, $\mathcal{D}$,[62] between the given state and the states in $\mathcal{S}$:

$$E_{\mathcal{D},\mathcal{S}}(\varrho) = \inf_{\sigma\in\mathcal{S}} \mathcal{D}(\varrho,\sigma). \tag{123}$$

The set $\mathcal{S}$ is chosen to be closed under LOCC operations. Originally it was just the set of separable states S. It turns out that such a function is monotonous under LOCC, if the distance measure is monotonous under all operations. It is then possible to use known, but so far unrelated, results on monotonicity under completely positive maps. Moreover, it proves that it is not only a technical assumption to generate entanglement measures: monotonicity is a condition for a distance to be a measure of *distinguishability* of quantum states (Fuchs and van de Graaf, 1997; Vedral, Plenio, Jacobs, *et al.*, 1997).

We thus require that

$$\mathcal{D}(\rho,\sigma) \geqslant \mathcal{D}(\Lambda(\rho),\Lambda(\sigma)) \tag{124}$$

and obviously $\mathcal{D}(\rho,\sigma)=0$ for $\rho=\sigma$. This implies nonnegativity of $\mathcal{D}$ (similarly as it was in the case of the vanishing of entanglement on separable states). More importantly, the above condition immediately implies monotonicity (118) of the measure $E_{\mathcal{D},\mathcal{S}}$. To obtain stronger monotonicity, one requires $\Sigma_i p_i \mathcal{D}(\varrho_i,\sigma_i) \leqslant \mathcal{D}(\varrho,\sigma)$ for ensembles $\{p_i,\varrho_i\}$ and $\{q_i,\sigma_i\}$ obtained from ρ and σ by applying an operation.

Once a good distance was chosen, one can consider different measures by changing the sets closed under LOCC operations. In this way we obtain $E_{\mathcal{D},\mathrm{PPT}}$ (Rains, 2001) or $E_{\mathcal{D},\mathrm{ND}}$ (the distance from nondistillable states). The measure involving set PPT is much easier to evaluate. The greater the set (see Fig. 3), the smaller the measure is, so that if we consider the set of separable states, those with positive partial transpose and the set of nondistillable states, we have

$$E_{\mathcal{D},\mathrm{ND}} \leqslant E_{\mathcal{D},\mathrm{PPT}} \leqslant E_{\mathcal{D},S}. \tag{125}$$

Vedral and Plenio (1998) showed two distances to satisfy Eq. (124) and convexity: the square of Bures metric $B^2 = 2-2\sqrt{F(\varrho,\sigma)}$ where $F(\varrho,\sigma)=[\mathrm{Tr}(\sqrt{\varrho}\sigma\sqrt{\varrho})^{1/2}]^2$ is fidelity (Uhlmann, 1976; Jozsa, 1994) and relative entropy $S(\varrho\|\sigma)=\mathrm{Tr}\,\varrho(\log_2\varrho-\log_2\sigma)$. Originally, the set of separable states was used and the resulting measure

$$E_R = \inf_{\sigma\in\mathrm{SEP}} \mathrm{Tr}\varrho(\log_2\varrho - \log_2\sigma) \tag{126}$$

is called the relative entropy of entanglement. It is a fundamental entanglement measure, as the relative entropy is an important function in quantum information theory (see Schumacher and Westmoreland, 2000; Ve-

[62]We do not require the distance to be a metric.

dral, 2002). Its other versions—the relative entropy distance from PPT states (Rains, 2001) and from nondistillable states (Vedral, 1999)—will be denoted as E_R^{PPT} and E_R^{ND} respectively. Relative entropy of entanglement turned out to be a powerful upper bound for entanglement of distillation (Rains, 2001). Plenio and Brandão (2008) have recently shown that it uniquely describes entanglement (both in a bipartite as well as a multipartite state) in a paradigm, where LOCC operations are replaced with nonentangling operations (strictly speaking, operations, that create an amount of entanglement vanishing in the appropriate limit). The distance based on fidelity received interpretation in terms of the Grover algorithm (Shapira *et al.*, 2006).

2. Convex roof measures

Here we consider the following method of obtaining entanglement measures: one starts by imposing a measure E on pure states, and then extends it to mixed ones by convex roof (Uhlmann, 1998),

$$E(\varrho) = \inf \sum_i p_i E(\psi_i), \quad \sum_i p_i = 1, \quad p_i \geqslant 0, \tag{127}$$

where the infimum is taken over all ensembles $\{p_i, \psi_i\}$ for which $\varrho = \Sigma_i p_i |\psi_i\rangle\langle\psi_i|$. The infimum is reached on a particular ensemble (Uhlmann, 1998). We call such an ensemble *optimal*. Thus E is equal to the average under the optimal ensemble.

The first entanglement measure built in this way was entanglement of formation E_F introduced by Bennett, DiVincenzo, *et al.* (1996), where $E(\psi)$ is the von Neumann entropy of the reduced density matrix of ψ. It constituted the first upper bound for distillable entanglement. Bennett, DiVincenzo, *et al.* (1996) showed the monotonicity of E_F. Vidal (2000) exhibited a general proof for monotonicity of all possible convex-roof measures. We consider measures for pure bipartite states in more detail in Sec. XV.D, and multipartite states in Sec. XV.H.1.

a. Schmidt number

The Schmidt rank can be extended to mixed states by means of a convex roof. A different extension was considered by Terhal and Horodecki (2000) and Sanpera *et al.* (2001) (called the Schmidt number) as follows:

$$r_S(\varrho) = \min\{\max_i [r_S(\psi_i)]\}, \tag{128}$$

where the minimum is taken over all decompositions $\varrho = \Sigma_i p_i |\psi_i\rangle\langle\psi_i|$ and $r_S(\psi_i)$ are the Schmidt ranks of the corresponding pure states. Thus instead of the average Schmidt rank, the supremum is taken. An interesting feature of this measure is that its logarithm is strongly nonadditive. Namely, there exists a state ρ such that $r_S(\rho) = r_S(\rho \otimes \rho)$.

b. Concurrence

For two qubits the measure called *concurrence* was introduced for pure states by Hill and Wootters (1997). Wootters (1998) provided a closed expression for its convex roof extension and based on it derived a computable formula for E_F in the two-qubit case. For pure states concurrence is $C = \sqrt{2(1 - \mathrm{Tr}\rho^2)}$, where ρ is a reduced state. For two qubits this gives $C(\psi) = 2a_1 a_2$, where a_1, a_2 are Schmidt coefficients. Another way of representing C for two qubits is the following:

$$C = \langle\psi|\theta|\psi\rangle, \tag{129}$$

where θ is the antiunitary transformation $\theta\psi = \sigma_y \otimes \sigma_y \psi^*$, with $*$ being the complex conjugation in the standard basis, and σ_y is the Pauli matrix. It turns out that the latter expression for C is useful in the context of mixed states, for which the convex roof of C can be then computed as follows. We denote $\tilde{\rho} = \theta\rho\theta$, and consider the operator

$$\omega = \sqrt{\rho}\sqrt{\tilde{\rho}}. \tag{130}$$

Let $\lambda_1, \ldots, \lambda_4$ be singular values of ω in decreasing order. Then we have

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}. \tag{131}$$

Interestingly, Uhlmann (2000) has shown that for any conjugation Θ, i.e., antiunitary operator satisfying $\Theta = \Theta^{-1}$, the convex roof of the function Θ concurrence $C_\Theta(\psi) = \langle\psi|\Theta|\psi\rangle$ is given by the generalization of Wootters' formula:

$$C_\Theta(\rho) = \max\left\{0, \lambda_1 - \sum_{i=2}^{d} \lambda_i\right\}, \tag{132}$$

where λ_i are eigenvalues of operator $\sqrt{\rho}\sqrt{\Theta\rho\Theta}$ in decreasing order.

The importance of the measure stems from the fact that it allows us to compute entanglement of formation for two qubits according to (Wootters, 1998)

$$E_F(\rho) = H\left(\frac{1 + \sqrt{1 - C^2(\rho)}}{2}\right), \tag{133}$$

where H is the binary entropy $H(x) = -x \log_2 x - (1 - x)\log_2(1 - x)$. One can extend concurrence to higher dimensions (Audenaert, Verstraete, *et al.*, 2001; Rungta *et al.*, 2001; see also Badziag *et al.*, 2002) as follows:

$$C(\psi) = \sqrt{\sum_\alpha C_\alpha(\psi)^2} = \sqrt{\langle\psi|\psi\rangle - \mathrm{Tr}\,\rho^2}, \tag{134}$$

where ρ is the density matrix of the subsystem. A strong algebraic lower bound for its convex roof was obtained by Mintert *et al.* (2004) allowing us to detect states which are bound entangled (see also Mintert, Carvalha, *et al.*, 2005; Bae *et al.*, 2009).

There are other interesting measures introduced by Sinołęcka *et al.* (2002) and Fan *et al.* (2003) and developed by Gour (2005), which are built by means of polynomials of the squares of the Schmidt coefficients λ's:

$$\tau_1 = \sum_{i=1}^{d} \lambda_i = 1, \quad \tau_2 = \sum_{i>j}^{d} \lambda_i \lambda_j, \quad \tau_3 = \sum_{i>j>k}^{d} \lambda_i \lambda_j \lambda_k, \text{ etc.}$$

The above measures τ_p are well defined if the dimension of the Hilbert space d is no smaller than the degree p. For convenience, one can also set $\tau_p = 0$ for $p < d$, so that each of the above measures is well defined for all pure states. The functions are generalizations of concurrence and can be thought of as higher rank concurrences. In particular τ_2 is the square of concurrence. The measures are Schur concave (i.e., they preserve majorization order), so that by the Nielsen theorem (see Sec. XIII.A) they satisfy monotonicity.

3. Other entanglement measures

a. Robustness measures

Robustness of entanglement was introduced by Vidal and Tarrach (1999). For a state ρ consider a separable state σ_{sep}. Then $R(\rho|\sigma_{\text{sep}})$ is defined as minimal t such that the state

$$\frac{(\rho + t\sigma_{\text{sep}})}{(1+t)} \tag{135}$$

is separable. Now robustness of entanglement is defined as

$$R(\rho) = \inf_{\sigma_{\text{sep}}} R(\rho|\sigma_{\text{sep}}). \tag{136}$$

It is related to the quantity $P(\rho)$ given by minimal p such that the state

$$(1-p)\rho + p\sigma_{\text{sep}} \tag{137}$$

is separable. We then have $P = R/(1+R)$. Though P is more intuitive, it turns out that R has better mathematical properties, being convex. R satisfies monotonicity (120). Harrow and Nielsen (2003) and Steiner (2003) considered generalized robustness R_g, where the infimum is taken over all states rather than just the separable ones. Interestingly, it was shown that for pure states it does not make a difference. R_g is a monotone too. Brandão (2005) showed that the generalized robustness R_g has operational interpretation: it is equal to the measure $E^{(d)}$ quantifying the activation power.

b. Negativity

A simple computable measure was introduced by Życzkowski *et al.* (1998) and then shown by Vidal and Werner (2002) to be a LOCC monotone. It is negativity,

$$\mathcal{N} = \sum_{\lambda<0} \lambda, \tag{138}$$

where λ are eigenvalues of ρ^Γ (where Γ is a partial transpose). A version of the measure called logarithmic negativity given by

$$E_{\mathcal{N}}(\rho) = \log_2 \|\rho^\Gamma\|_1 \tag{139}$$

is the upper bound for distillable entanglement (Vidal and Werner, 2002). It can be also written as $E_{\mathcal{N}}(\rho) = \log_2 [2\mathcal{N}(\rho)+1]/2$. The measure $E_{\mathcal{N}}(\rho)$ is easily seen to satisfy monotonicity (118), because $\mathcal{N}(\rho)$ does satisfy it, and the logarithm is a monotonic function. However, the logarithm it is not convex, and as such might be expected not to satisfy the stronger monotonicity condition (120). Yet, it was recently shown that it does satisfy it (Plenio, 2005). The measure is, moreover, additive. For states with positive $|\rho^\Gamma|^\Gamma$, $E_{\mathcal{N}}$ has operational interpretation—it is equal to the exact entanglement cost of creating a state by PPT operations from singlets (Audenaert *et al.*, 2003).

It turns out that negativity and robustness can be also obtained from one scheme originating from the base norm (Vidal and Werner, 2002; Plenio and Virmani, 2006).

c. Squashed entanglement

Squashed entanglement was introduced by Tucci (2002) and then independently by Christandl and Winter (2004), who showed that it is a monotone, and proved its additivity. It is the first additive measure with good asymptotic properties. In the latter paper, the definition of squashed entanglement E_{sq} has been inspired by relations between cryptography and entanglement. Namely, E_{sq} was designed on the basis of a quantity called intrinsic information (Maurer and Wolf, 1997; Gisin and Wolf, 2000; Renner and Wolf, 2003), which was monotonic under local operations and public communication. The squashed entanglement is given by

$$E_{\text{sq}}(\rho_{AB}) = \inf_{\rho_{ABE}} \tfrac{1}{2} I(A:B|E), \tag{140}$$

where $I(A:B|E) = S_{AE} + S_{BE} - S_E - S_{ABE}$ and infimum is taken over all density matrices ρ_{ABE} satisfying $\text{Tr}_E \rho_{ABE} = \rho_{AB}$. The measure is additive on the tensor product and superadditive in general, i.e.,

$$E_{\text{sq}}(\rho_{AB} \otimes \rho_{A'B'}) = E_{\text{sq}}(\rho_{AB}) + E_{\text{sq}}(\rho_{A'B'}),$$

$$E_{\text{sq}}(\rho_{AA'BB'}) \geqslant E_{\text{sq}}(\rho_{AB}) + E_{\text{sq}}(\rho_{A'B'}). \tag{141}$$

It is not known whether it vanishes if and only if the state is separable. (It would be true, if infimum could be turned into minimum; this is, however, unknown.) The measure is asymptotically continuous (Alicki and Fannes, 2004), and therefore lies between E_D and E_C. Even though it was computed for just two families of states, a clever guess for ρ_{ABE} can give good estimates for E_D in some cases. There was a question if the optimization in the definition of E_{sq} can be restricted to the subsystem E being a classical register (Tucci, 2002). Brandão (2008) showed that the answer is negative.

D. All measures for pure bipartite states

Vidal (2000) showed that measures for pure states satisfying strong monotonicity (120) are in one-to-one correspondence to functions f of density matrices satisfying (i) f is symmetric, expansible function of eigenvalues of ϱ; (ii) f is concave function of ϱ [by expansibility we

mean $f(x_1,\ldots,x_k,0)=f(x_1,\ldots,x_k)$]. In this way all possible entanglement measures for pure states were characterized.

More precisely, let E_p, defined for pure states, satisfy $E_p(\psi)=f(\varrho_A)$, where ϱ_A is a reduction of ψ, and f satisfies (i) and (ii). Then there exists an entanglement measure E satisfying LOCC monotonicity coinciding with E_p on pure states (E is convex-roof extension of E_p). Also conversely, if we have arbitrary measure E satisfying Eq. (120), then $E(\psi)=f(\varrho_A)$ for some f satisfying (i) and (ii).

We recall the proof of the direct part; namely, we show that convex-roof extension E of E_p satisfies Eq. (120). As Vidal showed, it suffices to show it for pure states. Consider then any operation on, say, Alice's side (for Bob's side, the proof is the same) which produces ensemble $\{p_i,\psi_i\}$ out of state ψ. We show that the final average entanglement $\bar{E}=\Sigma_i p_i E(\psi_i)$ does not exceed the initial entanglement $E(\psi)$. In other words, we show that $\Sigma_i p_i f(\varrho_A^{(i)})\leqslant f(\varrho_A)$, where $\varrho_A^{(i)}$ are reductions of ψ_i on Alice's side. We note that due to the Schmidt decomposition of ψ, reductions ϱ_A and ϱ_B have the same nonzero eigenvalues. Thus $f(\varrho_A)=f(\varrho_B)$, due to (i). Similarly $f(\varrho_A^{(i)})=f(\varrho_B^{(i)})$. Thus it remains to show that $\Sigma_i p_i f(\varrho_B^{(i)})\leqslant f(\varrho_B)$. However, $\varrho_B=\Sigma_i p_i \varrho_B^{(i)}$ (which is an algebraic fact, but can be understood as a no-superluminal-signaling condition—no action on Alice's side can influence the statistics on Bob's side, provided no message was transmitted from Alice to Bob). Thus our question reduces to the inequality $\Sigma_i p_i f(\varrho_B^{(i)})\leqslant f(\Sigma_i p_i \varrho_B^{(i)})$. This is, however, true, due to the concavity of f.

As mentioned, examples of entanglement measures for pure states are quantum Renyi entropies of the subsystem for $0\leqslant\alpha\leqslant 1$. Interestingly, the Renyi entropies for $\alpha>1$ are not concave, but are Schur concave. Thus they satisfy monotonicity (118) for pure states, but do not satisfy the strong one (120). It is not known whether the convex roof construction will work, therefore it is an open question how to extend such measure to mixed states.

Historically the first measure was the von Neumann entropy of the subsystem (i.e., $\alpha=1$) which has operational interpretation—it is equal to distillable entanglement and entanglement cost. It is the unique measure for pure states, if we require some additional postulates, especially asymptotic continuity (see Sec. XV.E).

1. Entanglement measures and transition between states: Exact case

Another family of entanglement measures is the following. Consider squares of Schmidt coefficients of a pure state λ_k in decreasing order so that $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_d$, $\Sigma_{i=1}^d\lambda_i=1$. Then the sum of the $d-k$ smallest λ's,

$$E_k(\psi)=\sum_{i=k}^{d}\lambda_i, \tag{142}$$

is an entanglement monotone (Vidal, 1999). Thus for a state with n nonzero Schmidt coefficients we obtain $n-1$ nontrivial entanglement measures. It turns out that these measures constitute a complete set of entanglement measures for bipartite pure states.

Vidal proved the following inequality relating probability $p(\psi\to\phi)$ of obtaining state ϕ from ψ by LOCC with entanglement measures:

$$p(\psi\to\phi)\leqslant E(\psi)/E(\phi). \tag{143}$$

[If we fix an entangled state ϕ_0, then $p(\psi\to\phi_0)$ is itself a measure of entanglement, as a function of ψ.] It turns out that the measures E_k constitute a full set of constraints. Namely (Vidal, 1999), the optimal probability of transition from state ψ to ϕ is given by

$$p(\psi\to\phi)=\min_k E_k(\psi)/E_k(\phi). \tag{144}$$

This returns, in particular, Nielsen's result (Nielsen, 1999) stating that $p=1$ if for all k, $E_k(\psi)\geqslant E_k(\phi)$, which is precisely the majorization condition (96).

Thus the considered set of abstractly defined measures determines possible transformations between states, as well as optimal probabilities of such transformations. We further show the generalization of such a result to the asymptotic regime, where nonexact transitions are investigated.

E. Entanglement measures and transition between states: Asymptotic case

In the asymptotic regime, where we tolerate small inaccuracies, which disappear in the limit of a large number of copies, the landscape of entanglement looks more "smooth." Of many measures for bipartite pure states only one becomes relevant: entropy of entanglement, i.e., any measure significant for this regime reduces to entropy of entanglement for pure states.[63] Moreover, only the measures with some properties, such as asymptotic continuity, can be related to operational quantities such as E_D, or, more generally, to asymptotic transitions rates. We refer to such measures as good asymptotic measures.

1. E_D and E_C as extremal measures: Unique measure for pure bipartite states

If measures satisfy some properties, it turns out that their regularizations are bounded by E_D from one side and by E_C from the other side. By regularization of any function f we mean $f^\infty(\rho)=\lim_n(1/n)f(\rho^{\otimes n})$ if such a limit exists. It turns out that if a function E is monotonic under LOCC, asymptotically continuous, and satisfies $E(\psi_d^+)=\log_2 d$, then we have

[63] One can consider the half asymptotic regime, where one takes the limit of many copies, but does not allow for inaccuracies. Then other measures can still be of use, such as logarithmic negativity, which is related to the PPT cost of entanglement (Audenaert *et al.*, 2003) in such a regime.

$$E_D \leqslant E^{\infty} \leqslant E_C. \tag{145}$$

In particular, this implies that for pure states there is a unique entanglement measure in the sense that regularization of any possible entanglement measure is equal to the entropy of a subsystem.[64] An exemplary measure that fits this scheme is the relative entropy of entanglement (related either to the set of separable states or to PPT states). Thus whenever we have reversibility, then the transition rate is determined by relative entropy of entanglement. Some versions of the theorem are useful to find upper bounds for E_D—one of the central quantities in entanglement theory. We have, for example, that any function E satisfying the conditions: (i) E is weakly subadditive, i.e., $E(\rho^{\otimes n}) \leqslant nE(\rho)$, (ii) for isotropic states $E(\rho_F^d)/\log d \to 1$ for $F \to 1$, $d \to \infty$, (iii) E is monotonic under LOCC [i.e., it satisfies Eq. (118)] is an upper bound for distillable entanglement. This theorem covers all known bounds for E_D.

There are not many measures which fit the asymptotic regime. Apart from operational measures such as E_C, E_D, and K_D only entanglement of formation, relative entropy of entanglement (together with its PPT version), and squashed entanglement belong here. For a review of properties of those measures see Christandl (2006).

2. Transition rates

One can consider transitions between any two states (Bennett, DiVincenzo, *et al.*, 1996) by means of LOCC: $R(\rho \to \sigma)$ defined analogously to E_D, but with σ in place of a maximally entangled state. Thus we consider n copies of ρ and want to obtain a state σ_n^{out} that will converge m copies of σ for large n. $R(\rho \to \sigma)$ is then defined as the maximum asymptotic rate m/n that can be achieved by LOCC operations. One then can generalize the theorem about extreme measures as follows:

$$R(\rho \to \sigma) \leqslant E^{\infty}(\rho)/E^{\infty}(\sigma) \tag{146}$$

for any E satisfying (i) E is nonincreasing under LOCC, (ii) regularizations exist for states ρ and σ and $E^{\infty}(\sigma) > 0$, (iii) E is asymptotically continuous (see Sec. XV.B.3). This result is an asymptotic counterpart of Vidal's relation between optimal probability of success and entanglement measures (143).

F. Evaluation of measures

It is usually not easy to evaluate measures. The only measure that is easily computable for any state is $E_{\mathcal{N}}$ (logarithmic negativity). Entanglement of formation is efficiently computable for two qubits (Wootters, 1998). Other measures are usually computable for states with high symmetries, such as Werner states, isotropic states, or the family of "iso-Werner" states (see Bennett, DiVincenzo, *et al.*, 1996; Rains, 1999; Terhal and Vollbrecht, 2000; Vollbrecht and Werner, 2001).

An analytical lower bound for concurrence for all states was provided by Mintert *et al.* (2004) (see also Audenaert, Verstraete, *et al.*, 2001). The bound constitutes also a new criterion of separability. A way to bound a convex-roof measure is to provide a computable convex function, that is, greater than or equal to the measure on the pure states. For example, we have

$$\|(|\psi\rangle\langle\psi|)^{\Gamma}\|_1 = \|R(|\psi\rangle\langle\psi|)\|_1 = \left(\sum_i \sqrt{p_i}\right)^2, \tag{147}$$

where p_i are squares of Schmidt coefficients of ψ and R is the realignment map (see Sec. VI.B.8). Comparing this with concurrence one gets a bound obtained by Chen *et al.* (2005a),

$$C(\rho) \geqslant \sqrt{\frac{2}{m(m-1)}}[\max(\|\rho^{\Gamma}\|_1, \|R(\rho)\|_1) - 1]. \tag{148}$$

As far as entanglement of formation is concerned, Terhal and Vollbrecht (2000) introduced a method for which it is enough to optimize over some restricted set rather than the set of pure states. This was further successfully developed by Chen *et al.* (2005b), Fei and Li-Jost (2006), and Datta *et al.* (2007) where lower bounds for E_F were obtained based on known separability criteria such as PPT, realignment, or the recent Breuer's map (see Secs. VI.B.8 and VI.B.6).

Vollbrecht and Werner (2001) obtained a surprising result concerning possible additivity of E_R. They showed that E_R is nonadditive for Werner asymmetric states, and, moreover, for large d, E_R of two copies is almost the same as for one copy. Thus the relative entropy of entanglement can be strongly nonadditive. Therefore regularization of E_R is not equal to E_R. Audenaert, Eisert, *et al.* (2001) computed for the first time E_R^{∞} for some states. Namely, for Werner states we have

$$E_{R,\mathcal{S}}^{\infty} = \begin{cases} 1 - H(p) & \frac{1}{2} < p \leqslant \frac{1}{2} + \frac{1}{d} \\ \log_2\left(\frac{d-2}{d}\right) + p \log_2\left(\frac{d+2}{d-2}\right) & \frac{1}{2} + \frac{1}{d} < p \leqslant 1. \end{cases} \tag{149}$$

Concerning the operational measures, we know that $E_C = E_F^{\infty} \equiv \lim_{n\to\infty} E_F(\varrho^{\otimes n})$ (Hayden *et al.*, 2001). If E_F were additive (which is still an open problem, see Sec. XIV.D) then it would be equal to E_C. E_D is bounded from above by E_F (Bennett, DiVincenzo, *et al.*, 1996). For pure states $E_D = E_F = E_C = E_R = S(\varrho_A)$, where ϱ_A is the reduced density matrix of the given pure state (Bennett, Bernstein, *et al.*, 1996; Vedral and Plenio, 1998). Vidal and Cirac (2001) found that for some bound entangled state (i.e., with $E_D = 0$) $E_C > 0$. In Yang (2006) it was shown that $E_C > 0$ for all entangled states. It seems that we can have $E_D = E_C$ only for states of the form

[64] The uniqueness of the entanglement measure for pure states was put forward by Popescu and Rohrlich (1997). The postulates that lead to uniqueness were further worked out by Vidal (2000), Horodecki *et al.* (2000b), Donald *et al.* (2002).

$$\sum_i p_i |\psi_i\rangle\langle\psi_i|_{AB} \otimes |i\rangle\langle i|_{A'B'}, \tag{150}$$

where $|i\rangle_{A'B'}$ are product states distinguishable by Alice and Bob (P. Horodecki *et al.*, 1998) (or some generalizations in a similar spirit, that Alice and Bob can distinguish states, which satisfy $E_D = E_C$ trivially).

Apart from the above trivial case of locally orthogonal mixtures the value of the measure E_D is known only for maximally correlated states $\Sigma_{ij} a_{ij} |ii\rangle\langle jj|$ for which $E_D = S_A - S_{AB}$. It is the upper bound, since it is equal to E_R (Rains, 1999). That it can be achieved follows from the general result of Devetak and Winter (2005) stating that $E_D \geqslant S_A - S_{AB}$. An example is a mixture of two maximally entangled two qubit states where

$$E_D(\varrho) = 1 - S(\varrho). \tag{151}$$

For higher dimension powerful tools for evaluating E_D were provided by Rains (2001). One knows several upper bounds for E_D (Bennett, DiVincenzo, *et al.*, 1996; Vedral and Plenio, 1998; Rains, 1999; Horodecki *et al.*, 2000a; Vidal and Werner, 2002). The best known bound is $E_{R+\mathcal{N}} = \inf_\sigma [S(\rho|\sigma) + \|\sigma^\Gamma\|_{\mathrm{Tr}}]$ provided by Rains (2001). For Werner states it is equal to regularization of $E_{R,\mathcal{S}}$ [this is true for the more general class of symmetric states (Audenaert *et al.*, 2002)].

G. Entanglement imposes different orderings

One can ask whether different entanglement measures impose the same ordering in the set of all states. The question was first posed by Virmani and Plenio (2000). Namely, suppose that $E(\rho) \geqslant E(\sigma)$. Is it also the case that $E'(\rho) \geqslant E'(\sigma)$? That it is not the case, we can see just on pure states. There exist incomparable states, i.e., such states ψ, ϕ, that neither $\psi \to \phi$ nor $\phi \to \psi$ is possible by LOCC. Since LOCC transitions are governed by entanglement measures (see Sec. XV.D) we see that there are two measures which give opposite ordering on those states.

In the asymptotic regime there is a unique measure for pure states. However, again it is easy to see (Virmani and Plenio, 2000), that a unique order would imply $E_D = E_C$ for all states, while we know that it is not the case.

One can interpret this lack of single ordering as follows: there are many different types of entanglement, and in one state we have more entanglement of one type, while in the other state there is more entanglement of some other type [see Miranowicz (2004b) and Verstraete, Porras, and Cirac (2004)].

H. Multipartite entanglement measures

Many axiomatic measures are immediately extended to the multipartite case. For example, relative entropy of entanglement is generalized by taking a suitable set in place of bipartite separable states. One can take the set of fully separable states (then the measure will not distinguish between "truly multipartite" entanglement and several instances of bipartite entanglement such as $\phi^+_{AB} \otimes \phi^+_{CD}$).[65] To analyze truly multipartite entanglement, one has to consider as done by Vedral, Plenio, Rippin, *et al.* (1997) the set of all states containing no more than k-particle entanglement (see Sec. VII). Similarly one can proceed with robustness of entanglement. It is not easy, however to compute such measures even for pure states (see, e.g., Plenio and Vedral, 2001). Moreover, for multipartite states many more parameters to describe entanglement are needed, therefore many new entanglement measures have been designed, especially for pure states. Then they can be extended to all states by convex roof (which is, however, also hard to compute).

1. Multipartite entanglement measures for pure states

There are measures that are simple functions of sums of bipartite entanglement measures. An example is the "global entanglement" of Meyer and Wallach (2001) which is the sum of concurrences between a single qubit and all other qubits. Their monotonicity under LOCC is simply inherited from bipartite measures.

The first measure that is neither a sum of bipartite measures nor an obvious generalization of such a measure is three-tangle (or residual tangle) introduced by Coffman *et al.* (2000). It is defined as follows:

$$\tau(A{:}B{:}C) = \tau(A{:}BC) - \tau(AB) - \tau(AC), \tag{152}$$

where two-tangles on the right-hand side are squares of concurrence (131). The three-tangle is permutationally invariant, even though the definition does not suggest it. It may be zero for pure states that are three-entangled (i.e., that are not a product with respect to any cut). An example is the so-called W state. The tangle vanishes on any states that are separable under any cut, and is nonzero, for example, on the GHZ state.[66] There are attempts to define a good generalization of tangle for multiqubit systems by means of a hyperdeterminant (Miyake, 2003) (see below). Lohmayer *et al.* (2006) computed a convex roof of the three-tangle for a mixture of a GHZ state and W-type states orthogonal to it.

Shortly after introducing the tangle, a concept of another measure for tripartite states was introduced in the context of the asymptotic rate of transitions (Linden, Popescu, Schumacher, *et al.*, 1999):

$$E(\psi) = E_R(\rho_{AB}) + S(\rho_C), \tag{153}$$

where ρ_{AB}, ρ_C are reductions of ψ_{ABC}. The measure allowed one to detect truly tripartite entanglement in the GHZ state in the asymptotic regime (see Horodecki *et al.*, 2007).

[65] Some inequalities between the so-chosen version of E_R and bipartite entanglement were provided by Plenio and Vedral (2001).

[66] In turns out that if tangles in Eq. (152) are replaced by squares of negativities the obtained quantity (after symmetrizing over system permutation) gives also rise to an entanglement monotone (Ou and Fan, 2007).

One of the first measures designed specifically for multipartite states was the Schmidt measure (Eisert and Briegel, 2001). This is the minimum of $\log r$ where r is the number of terms in an expansion of the state in the product basis. For GHZ this measure is 1, because there are just two terms: $|000\rangle$ and $|111\rangle$. One can show that for the W state it is impossible to write it by means of less than three terms (otherwise it would belong either to the GHZ class or to the EPR class). The measure is zero if and only if the state is a full product. Therefore it cannot distinguish true multipartite entanglement from bipartite entanglement. However, it may be useful in many contexts; see, e.g., Mora and Briegel (2005).

An interesting general class of multipartite entanglement measures was obtained in the context of classification of states via the so-called normal forms (Verstraete *et al.*, 2003). Namely, consider any homogeneous function of the state. Now if it is invariant under determinant one SLOCC, i.e., it satisfies

$$f(A_1 \otimes \cdots \otimes A_n\psi) = f(\psi) \tag{154}$$

for A_i square matrices satisfying $\det A_i = 1$, then it is an entanglement monotone in a strong sense, Eq. (120), but under the restriction that the LOCC operation produces output states on the Hilbert space of the same dimension. The three-tangle is an example of such a measure. Many measures designed for pure multipartite states like those obtained by Wong and Christensen (2001), Miyake (2003), Akhtarshenas (2005), and Osterloh and Siewert (2005), are originally defined only for a fixed dimension, hence it is simply not possible to check the standard monotonicity (118). However, concurrence, though initially defined for qubits, can be written in terms of linear entropy of subsystems, being thus well defined for all systems. Therefore there is hope that one can arrive at a definition independent of dimension for other measures. Then to obtain full monotonicity, one will need to also prove that the measure does not change, if the state is embedded into larger Hilbert spaces of subsystems (equivalently, that the measure does not change under adding local ancilla). However, for four-qubit concurrence of Wong and Christensen (2001) $\langle\psi^*|\sigma_y^4|\psi\rangle$ its natural generalization was shown to be not monotonous (Demkowicz-Dobrzański *et al.*, 2006) (see below). Of course, even the functions that are only monotonous for fixed dimension are useful quantities in many contexts.

Measures based on hyperdeterminant. Miyake noticed that measures of entanglement such as concurrence and tangle are special cases of a hyperdeterminant (Miyake, 2003). Consider, for example, qubits. For two qubits concurrence is simply modulus of a determinant, which is a hyperdeterminant of first order. The tangle is hyperdeterminant of second order—a function of tensor with three indices. Though computing hyperdeterminants of higher order than the tangle is rather complex, based on properties of the hyperdeterminant Miyake proved that hyperdeterminants of a higher degree are also entanglement monotones (Miyake, 2004). They describe truly multipartite entanglement (in a sense, that states such as a product of EPR's have zero entanglement). The proof of monotonicity is based on a geometric-arithmetic mean, and is closely related to the construction of entanglement measures based on homogeneous functions described above. An explicit formula for a hyperdeterminant for four qubits has been given by Levay (2006).

Geometric measure. A family of measures have been defined by Barnum and Linden (2001). In particular, the so-called geometric measure is defined as

$$E_g^{(k)}(\psi) = 1 - \Lambda^k(\psi), \tag{155}$$

where $\Lambda^k(\psi) = \sup_{\phi\in S_k}|\langle\psi|\phi\rangle|^2$, with S_k a set of k-separable states. This is a generalization of a Shimony measure (Shimony, 1995), which for bipartite states was related to Renyi entropy with $\alpha=\infty$. For relations with robustness of entanglement, see Cavalcanti (2006). The measure was also investigated by Wei and Goldbart (2003) and Wei *et al.* (2004) where it was in particular computed for Smolin four-qubit bound entangled states (72).

Concurrence-type measures. There were other attempts to generalize concurrence. Wong and Christensen (2001) obtained a measure for an even number of qubits by exploiting conjugation that appeared in the original definition of concurrence for two qubits. Their concurrence works for an even number of qubits and is given by $\langle\psi^*|\sigma_y^n|\psi\rangle$. The measure is nonzero for four-partite states containing two pairs of EPR states. This approach was generalized by Osterloh and Siewert (2005, 2006) who analyzed systematically possible quantities built out of antilinear operations, also of higher order in ψ than concurrence. For example, they obtained the following representation for a three-tangle:

$$\tau = \langle\psi|\sigma_\mu \otimes \sigma_y \otimes \sigma_y|\psi^*\rangle\langle\psi|\sigma^\mu \otimes \sigma_y \otimes \sigma_y|\psi^*\rangle, \tag{156}$$

where $\mu=0,1,2,3$ and the contraction is described by the tensor $g^{\mu,\nu}=\mathrm{diag}[-1,1,0,1]$. They have also designed measures that distinguish between three different SLOCC classes of states (see Sec. XIII.A.2):

$$|\Phi_1\rangle = \tfrac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle),$$

$$|\Phi_2\rangle = \tfrac{1}{\sqrt{6}}(\sqrt{2}|1111\rangle + |1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle),$$

$$|\Phi_3\rangle = \tfrac{1}{2}(|1111\rangle + |1100\rangle + |0010\rangle + |0001\rangle). \tag{157}$$

An interesting proposal is by Akhtarshenas (2005), which, however, is not proved to be a monotone. Mintert, Kus, *et al.* (2005) and Demkowicz-Dobrzański *et al.* (2006) introduced a family of functions of the form

$$C_{\mathcal{A}}(|\psi\rangle) = 2\sqrt{\langle\psi| \otimes \langle\psi|\mathcal{A}|\psi\rangle \otimes |\psi\rangle}, \tag{158}$$

where $\mathcal{A} = \Sigma_{s_1\cdots s_n} p_{s_1\cdots s_n} P_{s_1} \otimes \cdots \otimes P_{s_n}$, with $s_i = \pm 1$, $P^{(\pm 1)}$ is a projector onto symmetric (antisymmetric) subspace (see Sec. VI.B.3), and the coefficients $p_{s_1\cdots s_n}$ are non-negative. They have given sufficient conditions that must be satisfied by the coefficients to ensure monotonicity of C (now without the restriction of fixed dimension). On the other hand, they have shown that if

$\mathcal{A}=P^{(-)}\otimes P^{(-)}\otimes P^{(-)}\otimes P^{(-)}$ then the function returns concurrence $\langle\psi^*|\sigma_y^4|\psi\rangle$, and it is not monotonic. The main tool was the following condition for monotonicity derived on the basis of the conditions of Horodecki (2005); namely, a function C that is real, non-negative, and invariant under local unitaries, satisfies $C(a|\psi\rangle)=|a|^2C(|\psi\rangle)$, and is defined for mixed states as a convex roof is an entanglement monotone if and only if $C(a|\psi\rangle\otimes|\eta_1\rangle+b|\phi\rangle\otimes|\eta_2\rangle)\leqslant|a|^2C(|\psi\rangle\otimes|\eta_1\rangle)+|b|^2C(|\phi\rangle\otimes|\eta_2\rangle)$ with equality for $a=0$ or $b=0$, where ψ and ϕ are arbitrary multipartite pure states, and η_1, η_2 are local orthogonal flags.

I. How much can entanglement increase under communication of one qubit?

Lo and Popescu (1999) postulated that when n qubits are sent entanglement should not increase by more than n. Chen and Yang (2000) showed this for entanglement of formation. Due to teleportation, the sending of qubits is equivalent to bringing in a singlet. The question can then be recast as follows: Which entanglement measures satisfy

$$E(\rho\otimes|\phi^+\rangle\langle\phi^+|)\leqslant E(\rho)+1\,? \tag{159}$$

(Of course it is meaningful to ask such questions only for those entanglement measures that exhibit a sort of extensive behavior.) If a measure is subadditive, i.e., $E(\rho\otimes\sigma)\leqslant E(\rho)+E(\sigma)$, then the condition is satisfied. This is the case for such measures as E_R, E_F, E_C, E_N, E_{sq}. More problematic are E_D and K_D. As far as E_D is concerned, it is easy to see that Eq. (159) is satisfied for distillable states. Simply, if by adding a singlet, we can increase E_D, then we could design a protocol that would produce more singlets than E_D, using singlets obtained from distilling a first bunch of copies to distillation of the next bunch.[67] A more rigorous argument includes continuity of E_D on isotropic states (singlets with admixture of random noise). It is also not hard to see that for PPT states the condition holds too, by exploiting relation $E_D\leqslant E_N$. It was later shown[68] for all states, by exploiting results of DiVincenzo *et al.* (2003). The question is still open for K_D.

XVI. MONOGAMY OF ENTANGLEMENT

One of the most fundamental properties of entanglement is monogamy (Coffman *et al.*, 2000; Terhal, 2001). In its extremal form it can be expressed as follows: If two qubits A and B are maximally quantumly correlated, they cannot be correlated, at all with third qubit C (Bennett *et al.*, 1996). In general, there is trade-off between the amount of entanglement between qubits A and B and the same qubit A and qubit C. This property is purely quantum: in the classical world if A and B bits are perfectly correlated, then there are no constraints on correlations between bits A and C. For three qubits the trade-off is described by the Coffman-Kundu-Wootters monogamy inequality,

$$C_{A:B}^2+C_{A:C}^2\leqslant C_{A:BC}^2, \tag{160}$$

where $C_{A:B}$ is the concurrence between A and B, $C_{A:C}$ is between A and C, while $C_{A:BC}$ is between system A and BC. There was a conjecture that the above inequality can be extended to n qubits. The conjecture has been proved true only recently (Osborne and Verstraete, 2006). Analog of this is also satisfied for Gaussian states (Adesso and Illuminati, 2006; Hiroshima *et al.*, 2007); see Sec. XVII.E. However, it does not hold anymore in higher dimension (Ou, 2006).

More generally, in terms of entanglement measures monogamy takes the following form: For any tripartite state of systems A, B, C,

$$E(A:B)+E(A:C)\leqslant E(A:BC). \tag{161}$$

Note that if the above inequality holds in general (i.e., not only for qubits), then it already itself implies (by induction) the inequality

$$E(A:B_1)+E(A:B_2)+\cdots+E(A:B_N)\leqslant E(A:B_1\cdots B_N). \tag{162}$$

Koashi and Winter (2004) showed that squashed entanglement satisfies this general monogamy,

$$E_{\mathrm{sq}}(A:B)+E_{\mathrm{sq}}(A:C)\leqslant E_{\mathrm{sq}}(A:BC). \tag{163}$$

This is the only known entanglement measure having this property for all states. E_F and E_C are not monogamous (Coffman *et al.*, 2000; Koashi and Winter, 2004).

A beautiful monogamy was found for Bell inequalities. Namely, based on the earlier results concerning a link between the security of quantum communication protocols and violation of Bell's inequalities (Scarani and Gisin, 2001a) and theory of nonlocal games (Cleve *et al.*, 2004), Toner proved that the CHSH inequality is monogamous (Toner, 2006).

There is a qualitative aspect of monogamy, recognized quite early (Werner, 1989a; Doherty *et al.*, 2005); namely, a state ρ_{AB} is separable if and only if for any N there exists its $N+1$ partite symmetric extension, i.e., state $\rho_{AB_1\cdots B_N}$, such that $\rho_{AB_i}=\rho_{AB}$. D. Yang (2006) recently provided an elegant proof of this result and gave an explicit bound on the number N.

XVII. ENTANGLEMENT IN CONTINUOUS VARIABLE SYSTEMS

A. Pure states

Many properties of entanglement (separability) change when passing to continuous variables since the infinite-dimensional Hilbert space is not compact. The term continuous variables comes from the fact that any infinite-dimensional Hilbert space with countable basis is isomorphic to any of the two spaces: (i) $l^2(\mathcal{C})$ which is

[67] See Gottesman, 2005.
[68] See Harrow, Leung, and Shor, 2007.

space of sequences $\Psi=\{c_i\}$ with $\Sigma_{i=1}^{\infty}|c_i|^2<\infty$ and scalar product $\langle\Psi|\Phi\rangle=\Sigma_{i=1}^{\infty}a_i^*b_i$; and (ii) space $L^2(\mathbb{R})$ of all functions $\Psi:\mathbb{R}\to\mathbb{C}$ with $\int_{\mathbb{R}}|\Psi(x)|^2(x)dx<\infty$ and scalar product defined as $\int_{\mathbb{R}}\Psi(x)^*\Phi(x)dx$. The variable x is a continuous variable (CV) here.

An example of entangled state from such a space is a two-mode squeezed state which has its $l^2\otimes l^2$-like representation (in the so-called Fock basis considered to be a standard one):

$$|\Psi_\lambda\rangle=\sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle|n\rangle, \tag{164}$$

where the index goes from zero for physical reasons (n represents the photon number). Here coefficients $a_n:=(1-\lambda^2)\lambda^n$ are just Schmidt coefficients.

Alternatively the state has its $L^2\otimes L^2$ representation:

$$\Psi_\lambda(q_1,q_2)=\sqrt{\frac{2}{\pi}}\exp[-e^{-2r}(q_1+q_2)^2/2 - e^{2r}(q_1-q_2)^2/2], \tag{165}$$

related to the previous representation by

$$\lambda=\tanh(r). \tag{166}$$

In the case of infinite squeezing $r\to\infty$ the $\Psi(q_1,q_2)$ becomes more similar to the delta function $\delta(q_1-q_2)$ while its Fourier transform representation (changing "positions" q_i into "momenta" p_i) becomes almost $\delta(p_1+p_2)$. This limiting case was originally discussed in the famous EPR paper (Einstein *et al.*, 1935), and perfect correlations in positions as well as momenta resemble perfect correlations of local measurements σ_x and σ_z on the sides of the two-qubit state $\Psi_+=\frac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|1\rangle)$ (Bohm, 1951).

The characterization of bipartite CV pure states separability is the same as in the discrete case, namely,

$$\text{separability}\Leftrightarrow\text{PPT}\Leftrightarrow\text{reduced state pure} \Leftrightarrow\text{Schmidt rank 1}. \tag{167}$$

The entropy of entanglement of pure states remains a good measure of entanglement, exhibiting, however, some oddities. In the case of the state (164) it is given by (Barnett and Phoenix, 1989; Giedke *et al.*, 2003; Wolf *et al.*, 2004)

$$E_F(\Psi_\lambda)=\cosh^2(r)\log_2[\cosh^2(r)] - \sinh^2(r)\log_2[\sinh^2(r)]. \tag{168}$$

However, in the bipartite case with both subsystems of CV type typically the entropy of entanglement is *infinite*. This is a consequence of the fact that generically quantum states on CV spaces have the entropy infinite (Wehrl, 1978) (or alternatively the set of density matrices with finite entropy is nowhere dense, i.e., contains no ball).

As an example of such a state take $\Psi_{AB}=\Sigma_n\sqrt{p_n}|n\rangle_A|n\rangle_B$, with p_n proportional (up to the normalization factor) to $1/(n+2)\log_2(n+2)^4$. Then the entropy of entanglement is infinite, since the series $\Sigma_n p_n\log_2 p_n$ is not convergent.

As one can expect the very important fact connected to it is that there is no maximally entangled state in such spaces. Simply, the state with all Schmidt coefficients equal does not mathematically exist (it would have an infinite norm).

A natural question arises here: What about the usefulness of infinite entanglement which is so common a phenomenon in CV? For example, is it possible to distill an infinite amount of two-qubit entanglement from a single copy of bipartite CV quantum states with infinite entanglement? The answer to this is negative and can be proven formally (Keyl *et al.*, 2002).

B. Mixed states

The definition of mixed separable states has to be changed slightly if compared to discrete variables: the state is separable if it is a limit (in trace norm) of a finite convex combination of, in general mixed and not pure product states:[69]

$$\left\|\varrho_{AB}^{\text{sep}}-\sum_i p_i^{(n)}\varrho_A^{(n),i}\otimes\varrho_B^{(n),i}\right\|_1\to 0. \tag{169}$$

The characterization of entanglement in terms of positive maps and entanglement witnesses is again true since the corresponding proofs are valid for general Banach spaces (see M. Horodecki *et al.*, 1996).

There is a small difference here: Since there is no maximally entangled state, one has to use the original version of the Jamiołkowski isomorphism between positive maps and entanglement witnesses:

$$W_{AB}^{\Lambda}=(I\otimes\Lambda)(V_{AA'}), \tag{170}$$

with $d_A\geqslant d_B$ (remember that it may happen that only one of the subspaces is infinite) where $V_{AA'}$ is a swap operator on $\mathcal{H}_{AA'}=\mathcal{H}_A\otimes\mathcal{H}_{A'}$ ($\mathcal{H}_{A'}$ a copy of $\mathcal{H}_A$) and the map acting from system A' to B. This is because there is no maximally entangled state in infinite dimensional space.

The PPT criterion is well defined and serves as a separability criterion as it was in finite dimension. It has a very nice representation in terms of moments (Shchukin and Vogel, 2005a).

There exist nontrivial PPT states (Horodecki and Lewenstein, 2000) that cannot be constructed as a naive, direct sum of finite dimensional structures. It seems that such states are generic, though the definition of a generic CV state in the case of mixed state is not so natural similarly to the case of a pure state where the infinite Schmidt rank (or the rank of the reduced density matrix) is a natural signature defining the CV property [for discussion on the generic property see Horodecki, Cirac, *et al.* (2003)].

[69]This is actually the original definition of separable states (Werner, 1989b).

The first important observation concerning CV separability is (Clifton and Halvorson, 1999) that in the bipartite case the set of separable states is nowhere dense or, equivalently, any state on this space is a limit (in trace norm) of the sequence of the entangled state. Thus the set of separable states contains no ball of finite radius and in that sense is "of zero volume" unlike it was in finite dimensions (Życzkowski *et al.*, 1998). This result can be extended (Horodecki, Cirac, *et al.*, 2003) to the set of all nondistillable states (in a sense of definition inherited from discrete variables, i.e., equivalent to the impossibility of producing two-qubit singlets) and is also nowhere dense in the set of all states. Thus CV bound entanglement like CV separability is a rare phenomenon.

We now turn to quantitative issues involving entanglement measures. If one tries to extend the definition of entanglement of the formation to mixed states (Eisert, Simon, *et al.*, 2002) then the set of states with finite E_F has the same property as the set of separable states—it is again nowhere dense.[70] Also, E_F is not continuous (as already seen in the case of pure states).

The question was how to avoid, at least partially, the above problems with entanglement that occur when both dimensions are infinite? Eisert, Simon, *et al.* (2002) proposed then to consider the subset $\mathcal{S}_M(H)\subset\mathcal{S}$ [of the set $\mathcal{S}$ of all bipartite states, defined as $\mathcal{S}_M(H) := \{\varrho : \mathrm{Tr}(\varrho H) < M\}$ for some fixed constant M and Hamiltonian H] (some chosen Hermitian operator with spectrum bounded from below). The set is nowhere dense but it is defined by a natural physical requirement of bounded mean energy in a physical system. Remarkably for fixed M and all states from $\mathcal{S}_M$, the entanglement of formation E_F and the relative entropy of entanglement E_R are continuous in trace norm on pure states. Moreover, those measures are asymptotically continuous on pure states of the form $\sigma^{\otimes n}$ with finite-dimensional support of σ.

C. Gaussian entanglement

There is a class of CV states that are well characterized with respect to separability. This is the class of Gaussian states. Formally a Gaussian state of m modes (oscillators) is a mixed state on Hilbert space $\mathcal{L}^2(\mathbb{R})^{\otimes m}$ (of functions of position variables $[q_1,\ldots,q_m]$) which is completely characterized by the vector of its first moments $d_i=\mathrm{Tr}(\varrho R_i)$ (called displacement vector) and second moments covariance matrix $\gamma_{ij}=\mathrm{Tr}(\varrho\{R_i-d_iI),(R_j-d_jI\}_+)$, where we use anticommutator $\{,\}_+$ and the observables R_i are canonical position $Q_k=R_{2k-1}$ and momentum $P_k=R_{2k}$ operators of the kth oscillator which satisfy the usual Heisenberg commutation relations $i[R_k,R_{k'}]=J_{kk'}$ where $J=\oplus_{i=1}^m J_i$, with one mode symplectic matrices

$$J_i=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}.$$

A given matrix S is called symplectic if it satisfies $SJS^T=J$. Such matrices represent all canonical transformations $S:\xi\to\xi'=S\xi$ where $\xi=[q_1,p_1;q_2,p_2;\ldots;q_m,p_m]^T$ is a vector of canonical variables. The corresponding action on the Hilbert space is unitary. There is also a broader set of unitary operations called quasifree or linear Bogoliubov transformations $\xi\to S\xi+d$ where S is symplectic and d is the displacement vector.

The canonical operators Q_i,P_i are Hermitian and anti-Hermitian parts of the creation $a_k^\dagger$ and annihilation a_k operators that provide a natural link to $(l^2)^{\otimes m}$ representation since they define a special $\mathcal{L}^2(\mathbb{R})$ Fock basis $\{|n\rangle\}$ of each mode $[a_k^\dagger=\Sigma_{n=0}^\infty\sqrt{n+1}|n+1\rangle_{kk}\langle n|$ and $a_k=(a_k^\dagger)^\dagger]$ via number operator $N=a_k^\dagger a_k=\Sigma_{n=0}^\infty n|n\rangle\langle n|$ which is diagonal in that basis.

Since the displacement d can be easily removed by quasifree local (i.e., on each mode separately) unitary operations (Duan *et al.*, 2000), only the properties of variance matrix are relevant for entanglement tests. Before recalling them we provide conditions for γ to be physical. We recall that via Williamson theorem γ can be diagonalized with some symplectic matrix $\gamma_{\mathrm{diag}}=S_\gamma\gamma S_\gamma^T=\mathrm{diag}[\kappa_1,\kappa_1;\ldots;\kappa_m,\kappa_m]$, with κ_i real. The physical character of the covariance matrix γ is guaranteed by the condition

$$\gamma - iJ \geqslant 0 \Leftrightarrow \tag{171}$$

$$\gamma \geqslant J^T\gamma^{-1}J \Leftrightarrow \tag{172}$$

$$\gamma \geqslant S^TS \quad \text{for some symplectic } S \Leftrightarrow \tag{173}$$

$$\kappa_i \geqslant 1, \quad i=1,\ldots,m. \tag{174}$$

There is the following fact (Simon, 2000): a Gaussian state is pure if and only if its variance matrix is of the form

$$\gamma = S^TS, \tag{175}$$

for some symplectic matrix S. Generally, m modes can be divided into k groups containing $m_1,\ldots,m_k$ modes $(m=\Sigma_i m_i)$, belonging to different local observers $A_1,\ldots,A_k$. We say that the state is a k-partite Gaussian state of $m_1\times m_2\times\cdots\times m_k$ type. For instance, the bipartite state is of $m_1\times m_2$ type if the first m_1 modes are on Alice's side, and the rest m_2 on Bob's side. All reduced states of the systems A_i are Gaussian. With each site we associate the symplectic matrix J_{A_k} as before. There is a general necessary and sufficient separability condition that can resemble to some extent the range criterion (see Werner and Wolf, 2001c):

$$\varrho(\text{Gaussian separable}) \Leftrightarrow \tag{176}$$

[70] This problem does not occur when one of the local Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$ is finite, i.e., $\min[d_A,d_B]<\infty$ then entanglement of formation is well defined and restricted by the logarithm of the finite space dimension (Majewski, 2002).

$$\gamma_{AB}(\varrho) \geqslant \gamma_A \oplus \gamma_B \tag{177}$$

for some variance matrices γ_A, γ_B [which, as shown (Simon, 2003), can be chosen to be pure, i.e., of the form (175)]. Quite remarkably, the above criterion can be generalized to an arbitrary number of parties (see Eisert and Gross, 2007). In general, if the state is not Gaussian the criterion becomes only a necessary condition of separability. The criterion is rather hard to use [see, however, Werner and Wolf (2001c) and the discussion below].

There is a very important separability characterization: the PPT criterion has been shown to be both necessary and sufficient for 1×1 (Duan *et al.*, 2000; Simon, 2000) and subsequently generalized to $1\times n$ Gaussians (Werner and Wolf, 2001c). Further the same result has been proven for $m\times n$ "bisymmetric" (Serafini *et al.*, 2005; Serafini, 2006) (i.e., symmetric under permutations of Alice and Bob modes, respectively) Gaussian states. The equivalence of the PPT condition to separability is not true, in general, if both Alice and Bob have more than one mode.

Operational necessary and sufficient condition. Giedke, Kraus, *et al.* (2001) presented an operational necessary and sufficient condition for the separability for all bipartite Gaussian states. It is so far the only operational criterion of separability that detects all PPT entangled states within such a broad class of states. Entanglement is detected via a finite algorithm that transforms the initial covariance matrix into a sequence of matrices which after a finite number of steps either (i) becomes not physical (does not represent a covariance matrix) and then the algorithm detects entanglement (ii) or its special affine transformation becomes physical and then the initial state is recognized to be separable.

D. General separability criteria for continuous variables

First, it must be stressed that any Gaussian separability criterion that refers only to well defined variances, and does not use the fact that the variance matrix completely describes the state, is also a separability criterion for general CV states. It follows from the fact that from a large number of copies of a given state, one can obtain by LOCC a state arbitrarily close in trace norm to a Gaussian state with the same covariance matrix (Wolf, Giedke, and Cirac, 2006).

One of the natural separability criteria is local projection or, in general, LOCC transformation of a CV state onto the product of finite dimensional Hilbert spaces and then application of one of the separability criteria for discrete variables. This method was used by Horodecki and Lewenstein (2000) where finally discrete variables range criterion was applied.

Separability criteria that do not refer to discrete quantum states usually are based on some uncertainty type relations. As an example of such a relation, consider the position and momenta operators Q_{A_1}, Q_{A_2}, P_{A_1}, P_{A_2} for a bipartite system A_1A_2, which satisfy the commutation relations $[Q_{A_i},P_{A_j}]=i\delta_{ij}$ and define $U=|a|Q_{A_1}+(1/a)Q_{A_2}$, $V=|a|P_{A_1}+(1/a)P_{A_2}$ for arbitrary nonzero real number a. Then any separable bipartite CV state ϱ satisfies (Duan *et al.*, 2000)

$$\langle(\Delta U)^2\rangle_\varrho + \langle(\Delta V)^2\rangle_\varrho \geqslant \tfrac{1}{2}(a^2+1/a^2). \tag{178}$$

The practical implementation of the PPT criterion in terms of all moments that goes beyond variance properties of CV states is the Shchukin-Vogel criterion (Shchukin and Vogel, 2005a; Miranowicz and Piani, 2006). It turned out that their criterion covers many known separability criteria. The idea is that with any state of two modes one can associate the following matrix of moments:

$$M_{ij} = \mathrm{Tr}(\hat{a}^{\dagger q}\hat{a}^p\hat{a}^{\dagger n}\hat{a}^m \otimes \hat{b}^{\dagger l}\hat{b}^k\hat{b}^{\dagger r}\hat{b}^s\rho_{AB}), \tag{179}$$

where $i=(pqrs)$ and $j=(nmkl)$. The operators a,b act on systems A,B, respectively. It turns out that the above matrix is positive if and only if the state is PPT.[71] Positivity of the matrix can be expressed in terms of nonnegativity of subdeterminants. It then turns out that many known separability criteria are obtained by imposing non-negativity of a suitably chosen subdeterminant.

E. Distillability and entanglement measures of Gaussian states

The question of distillability of Gaussian states has attracted much attention. In analogy to the two-qubit distillability of quantum states in finite dimensions, it was first shown that all two-mode entangled Gaussian states are distillable (Giedke *et al.*, 2000). Subsequently it was shown that all NPT entangled Gaussian states are distillable (Giedke, Duan, *et al.*, 2001). In other words, there is no NPT bound entanglement in Gaussian continuous variables: any NPT Gaussian state can be transformed by LOCC into a NPT two-mode one, and then distilled as described by Giedke *et al.* (2000). However, the protocol which achieves this task involves operations which are not easy to implement nowadays. The operations feasible for present linear-optic based technology are the so-called Gaussian operations. The natural question was raised then whether entangled Gaussian states are distillable by means of this restricted class of operations. Unfortunately, it is not the case: one cannot obtain pure entanglement from Gaussian states using only Gaussian operations (Giedke and Cirac, 2002) [see Eisert, Scheel, *et al.* (2002) and Fiurášek (2002a)]. Although these operations are restrictive enough to effectively "bind" entanglement, they are still useful for processing entanglement: by means of them, one can distill a key from entangled NPT Gaussian states (Navascues *et al.*, 2005). Interestingly, no PPT Gaussian state from which a key can be distilled is known so far (Navascués and Acin, 2005).

Apart from the question of distillability and key distillability of Gaussian states, entanglement measures

[71] See Verch and Werner (2005).

such as entanglement of formation and negativity have been studied. It also led to new measures of entanglement called Gaussian entanglement measures.

Giedke *et al.* (2003) calculated entanglement of formation for symmetric Gaussian states. Interestingly, the optimal ensemble realizing E_F consists solely from Gaussian states. The same was proven for *all* two-mode Gaussian states allowing one to compute their E_F exactly (Marian and Marian, 2008). It is not known to hold in general. One can, however, consider the so-called Gaussian entanglement of formation E_G where infimum is taken over decompositions into Gaussian states only. Gaussian entanglement of formation was introduced and studied by Giedke *et al.* (2003). It is shown there that E_G is monotonous under Gaussian LOCC operations. For two-mode Gaussian states its value can be found analytically. If additionally the state is symmetric with respect to sites, this measure is additive and equal to E_F on a single copy.

The idea of Gaussian entanglement of formation has been extended to other convex-roof based entanglement measures by Adesso and Illuminati (2005). The log negativity of Gaussian states defined already by Vidal and Werner (2002) has also been studied by Adesso and Illuminati (2005). In this case the analytic formula has been found, in terms of symplectic spectrum κ_i of the partially transposed covariance matrix:

$$E_N = -\sum_{i=1}^{n} \log_2[\min(1,\kappa_i)]. \tag{180}$$

The continuous variable analog of tangle (squared concurrence; see Sec. XV), called contangle was introduced by Adesso and Illuminati (2006) as the Gaussian convex roof of the squared negativity. It is shown that for three-mode Gaussian states, contangle exhibits Coffman-Kundu-Wootters monogamy. Recently the general monogamy inequality for all N-mode Gaussian states was established (Hiroshima *et al.*, 2007) [in full analogy with the qubit case (Osborne and Verstraete, 2006)]. For three modes, the three-contangle, the analog of the Coffman-Kundu-Wooters three-tangle, is a monotone under Gaussian operations.

Surprisingly, there is a symmetric Gaussian state which is a counterpart of both the GHZ and the W state (Adesso and Illuminati, 2006). Namely, in finite dimension, when maximizing entanglement of subsystems, one obtains the W state, while maximization of tangle leads to the GHZ state. For Gaussian states, such optimizations (performed for a fixed value of mixedness or of squeezing of subsystems) leads to a *single* family of pure states called the GHZ/W class. Thus to maximize tripartite entanglement one has to also maximize the bipartite one.

An exemplary practical use of Gaussian states apart from the quantum key distribution (see, e.g., Gottesman and Preskill, 2001; Navascués *et al.*, 2005) is the application for continuous quantum Byzantine agreement protocol (Neigovzen and Sanpera, 2005). There are many other theoretical and experimental issues concerning Gaussian states and their entanglement properties that we do not discuss. For a recent review on this topic, see Ferraro *et al.* (2005) and Adesso and Illuminati (2007).

XVIII. MISCELLANEOUS FACTS ABOUT ENTANGLEMENT

A. Entanglement under information loss: Locking entanglement

Manipulation of a quantum state with local operations and classical communication in a nonunitary way usually decreases its entanglement content. Given a quantum bipartite system of $2\times\log_2 d$ qubits in state ρ one can ask how much entanglement can decrease if one traces out a single qubit. Surprisingly, many entanglement measures can decrease by an arbitrary large amount, i.e., from $O(\log_2 d)$ to zero. Generally, if some quantity of ρ can decrease by an arbitrarily large amount (as a function of the number of qubits) after LOCC operation on few qubits, then it is called lockable. This is because a large amount of quantity can be controlled by a person who possesses only a small dimensional system which plays a role of a "key" to this quantity.

The following related question was asked earlier by Eisert, Felbinger, *et al.* (2000): How does entanglement behave under classical information loss? It was quantified by means of entropies and for convex entanglement measures takes the form

$$\Delta E \leqslant \Delta S, \tag{181}$$

where $\Delta E = \Sigma_i p_i E(\rho_i) - E(\Sigma_i p_i \rho_i)$ and $\Delta S = S(\rho) - \Sigma_i p_i S(\rho_i)$. The inequality holds for relative entropy of entanglement (Linden, Popescu, Schumacher, *et al.*, 1999) (see also Synak-Radtke and Horodecki, 2006). It turns out, however, that for other measures this inequality can be drastically violated, due to the above locking effect.[72]

The phenomenon of drastic change after tracing out one qubit was recognized by DiVincenzo *et al.* (2004) for classical correlations of quantum states (maximal mutual information of outcomes of local measurements) [see Koenig *et al.* (2005), Buhrman *et al.* (2006), Smolin and Oppenheim (2006), Ballester and Wehner (2007)]. Another effect of this sort was found in a classical key agreement (Renner and Wolf, 2003) (a theory bearing some analogy to entanglement theory; see Sec. XIX.F).

Various entanglement measures have been shown to be lockable. In paricular, entanglement cost, log negativity, squashed entanglement and measures based on convex roof methods (see Sec. XV.C.2) are shown to be lockable (Christandl and Winter, 2005; Horodecki *et al.*, 2005c). Possible consequences of locking for multipartite entanglement measures have been given by Groisman *et al.* (2005).

[72]Using the fact that a loss of one qubit can be simulated by applying one of four random Pauli matrices to the qubit one arrives at the connection between locking and violation of the inequality (181).

It is an open question whether distillable entanglement can be locked, although it is known that its one-way version is lockable, which follows from monogamy of entanglement. In the case of a distillable key, one can consider two versions of locking: the one after tracing out a qubit from Eve (E locking), and the one after the qubit of Alice's and Bob's system is traced out (AB locking). It has been shown that the distillable key both in classical (see Sec. XIX.F) and quantum setting is not E lockable (Renner and Wolf, 2003; Christandl *et al.*, 2007). It is, however, not known if a distillable key can be AB lockable, i.e., if erasing a qubit from Alice's and Bob's systems may diminish by far their ability to obtain secure correlations.

B. Entanglement and distinguishing states by LOCC

Early fundamental results in distinguishing states by LOCC are the following: there exist sets of orthogonal product states that are not perfectly distinguishable by LOCC (Bennett, DiVincenzo, Fuchs, *et al.*, 1999; see also Walgate and Hardy, 2002) and every two orthogonal states (even multipartite) are distinguishable by LOCC (Walgate *et al.*, 2000). In a qualitative way, entanglement was used in the problem of distinguishability by Terhal *et al.* (2001). To show that a given set of states cannot be distinguished by LOCC, they considered all measurements capable to distinguish them, and applied the measurements to the AB part of the system in state $\psi_{AA'} \otimes \psi_{BB'}$ where the components are maximally entangled states. If the state after measurement is entangled across the $AA':BB'$ cut, then one concludes that the measurement cannot be done by use of LOCC because the state was initially produced across this cut.

An interesting twist was given by Ghosh *et al.* (2001) where distillable entanglement was used. We show how they argued that four Bell states ψ_i (3) cannot be distinguished. Consider the four-partite state $\rho_{ABA'B'} = \frac{1}{4}\Sigma_i |\psi_i\rangle\langle\psi_i|_{AB} \otimes |\psi_i\rangle\langle\psi_i|_{A'B'}$. Suppose that it is possible to distinguish Bell states by LOCC. Then Alice and Bob will distinguish Bell states of system AB (perhaps destroying them). Then they will know which of the Bell states they share on system $A'B'$, obtaining then one e-bit of pure entanglement (hence $E_D \geqslant 1$). However, one can check that the initial state $\rho_{ABA'B'}$ is separable in the cut $AA':BB'$ (Smolin, 2001), so that $E_D=0$ and we get a contradiction. This shows that entanglement measures can be used to prove the impossibility of distinguishing some states. For further development, including the "entanglement correction" to the Holevo bound (Badziag *et al.*, 2003), see Horodecki *et al.* (2007) and Xin and Duan (2007).

XIX. ENTANGLEMENT AND SECURE CORRELATIONS

A fundamental difference between the classical and quantum formalisms is that the quantum formalism allows for states of composite systems to be both pure and correlated. While in the classical world those two features never meet in one state, entangled states can exhibit both of them at the same time.

For this reason, entanglement in an astonishing way incorporates the basic ingredients of the theory of secure communication. Indeed, to achieve the latter, the interested persons (Alice and Bob) need a private key: a string of bits which is (i) perfectly correlated (correlations) and (ii) unknown to any other person (security or privacy) [then they can use it to perform a private conversation by use of the so-called Vernam cipher (Vernam, 1926)]. Now, it is purity which enforces the second condition, because an eavesdropper who wants to gain knowledge about a quantum system will unavoidably disturb it, randomizing phase via quantum backreaction. In modern terminology we would say that if Eve applies a CNOT gate, to gain knowledge about a *bit*, at the same time she introduces a *phase* error into the system, which destroys purity; see Zurek (1981).

We note that all we have said can be phrased in terms of monogamy of entanglement in its strong version: If two quantum systems are maximally quantumly correlated, then they are not correlated with any other system at all (neither quantumly nor classically) [see Koashi and Winter (2004)]. In this section we explore the mutual interaction between entanglement theory and the concept of private correlations.

A. Quantum key distribution schemes and security proofs based on distillation of pure entanglement

Interestingly, the first protocol to obtain a private key,[73] the famous BB84 protocol (Bennett and Brassard, 1984), did not use the concept of entanglement at all. Neither do the other protocols (B92) proposed by Bennett in 1992 (Bennett, 1992) and many variations of BB84 like the six-state protocol (Bruß, 1998) use entanglement. Indeed, these QKD protocols are based on sending randomly chosen nonorthogonal quantum states. Alice prepares a random signal state, measures it, and sends it to Bob who also measures it immediately after reception. Such protocols are called a prepare and measure protocol (P&M).

The first entanglement based protocol was discovered by Ekert (see Sec. III). Interestingly, even Ekert's protocol, though using explicitly entanglement, was still not based solely on the "purity and correlations" concept outlined above. He did exploit correlations, but along with the purity argument used violation of Bell inequalities. It seems that it was Bennett, Brassard, and Mermin (BBM) (Bennett *et al.*, 1992) who tilted the later history of entanglement-based QKD from the "Bell inequalities" direction to "disturbance of entanglement": upon attack of Eve, the initially pure entangled state becomes mixed, and this can be detected by Alice and Bob.

[73] We call such protocol quantum key distribution (QKD).

Namely, they have proposed the following protocol, which is also entanglement based, but is not based on Bell inequality. Simply Alice and Bob, when given some (untrusted) EPR pairs, check their quality by measuring correlations in the $\{|0\rangle, |1\rangle\}$ basis, and the conjugated basis $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. So the simplified Ekert's protocol is formally equivalent to the BB84 protocol. Namely, the total final state between Alice, Bob, and Eve is the same in both cases.[74] Thus entanglement looks here quite superfluous, and, moreover, Bell inequalities appeared rather accidentally: just as indicators of a possible disturbance by Eve, hence in simplified protocol, they are not needed.

Paradoxically, it turned out recently that the Bell inequalities are themselves a good resource for key distribution, and allow us to prove the security of a private key without assuming quantum formalism but based solely on the no-signaling assumption (Barrett *et al.*, 2005; Acín *et al.*, 2006; Masanes and Winter, 2006). There is still an analogy with entanglement: nonlocal correlations are monogamous (Barrett *et al.*, 2006).

Concerning entanglement, Ekert noticed that the equivalence of the entanglement-based protocol and BB84 is not complete:[75] the former has an advantage that Alice and Bob can postpone measuring EPR pairs until they need the key, so that a burglar breaking into their labs trying to get some information would disturb the pairs risking detection, while in BB84, there is no possibility of storing the key in quantum form. Thus entanglement provides a *potential* key, in a similar way, as it provides potential communication in dense coding (see Sec. III). However, this is not the only advantage of entanglement: in fact, its role turned out to be indispensable in further development of the theory of secure correlations. Actually, the interaction is bilateral: also the development of entanglement theory was influenced in an essential way by the ideas of secure correlations, to mention only that first protocols of entanglement distillation (fundamental for the whole quantum communication theory) have been designed using methods of generation of a secure key (Bennett, Brassard, *et al.*, 1996; Bennett, DiVincenzo, *et al.*, 1996).

Another theoretical advantage of the entanglement-based QKD protocol is that with quantum memory at disposal, one can apply a dense coding scheme and obtain a protocol which has a higher capacity than usual QKD as it was applied by Long and Liu (2002); see also Cabello (2000). Moreover, entanglement may help to carry out quantum cryptography over long distances by use of quantum repeaters which exploit entanglement swapping and quantum memory (Dür, Briegel, *et al.*, 1999). We should note that all the above potential advantages of entanglement would need quantum memory.

[74]In BB84, the state consists of preparations of Alice, outcomes of Bob's measurement, and quantum states of Eve. In BBM protocol it is the outcomes of Alice's and Bob's measurement, and quantum states of Eve.

[75]See note added in Bennett *et al.* (1992).

1. Entanglement-distillation-based quantum key distribution protocols

Both Ekert's protocol and its BBM version worked in the situation where the disturbance comes only from the eavesdropper, so if only Alice and Bob detect his presence, they can abort the protocol. Since in reality one usually deals with imperfect sources, hence also with imperfect (noisy) entanglement, it is important to ask if the secure key can be drawn from noisy EPR pairs. The purification of EPR pairs appeared to be a crucial idea in this case. The first scheme of purification (or distillation) of entanglement has been discovered and developed in Bennett, Brassard, *et al.* (1996), and Bennett, DiVincenzo, *et al.* (1996) (see Sec. XII). In this scheme Alice and Bob share n copies of some mixed state, and by means of local quantum operations and classical communication (LOCC) they obtain a smaller amount $k < n$ of states which are very close to the EPR state,

$$\rho^{\otimes n} \xrightarrow{\text{distillation}} |\phi^+\rangle^{\otimes k}. \tag{182}$$

The highest asymptotic ratio k/n in the above diagram is called distillable entanglement and is denoted as $E_D(\rho)$ (see Sec. XV.A). This concept was adopted by Deutsch *et al.* (1996), where the distillation process for the cryptographical purpose was named quantum privacy amplification (QPA). From n systems in a joint state ρ_n (which may be in principle supplied by Eve), Alice and Bob distill singlets, and finally generate a key via measurement on a computational basis:

$$\rho_n \xrightarrow{\text{QPA}} |\phi^+\rangle^{\otimes k}. \tag{183}$$

The protocol of QPA assumes that devices used for distillation are perfect. Moreover, the distillation scheme of Bennett *et al.* works if the initial state is in a tensor product of many copies. The question of verification by Alice and Bob whether they indeed share such state (or whether the final state is indeed the desired $\phi^+ = \frac{1}{\sqrt{2}}|00\rangle + |11\rangle$ state) was not solved by Deutsch *et al.* (1996).

This problem has been tackled by Lo and Chau (1999) who provided the first both unconditionally secure and fully entanglement-based scheme.[76] To cope with imperfections, Alice and Bob use fault tolerant quantum computing. In order to obtain a secure key, they perform the entanglement distillation protocol of Bennett, DiVincenzo, *et al.* (1996) to distill singlets, and check their

[76]The first proof of unconditional security of a quantum key distribution was provided by Mayers who proved the security of BB84 (Mayers, 2001).

quality.[77]

The Lo-Chau proposal has a drawback: one needs a quantum computer to implement it, while the first quantum cryptographic protocol (BB84) does not need a quantum computer. And the BB84 was already proved to be secure by Mayers (2001). Yet, the proof was quite complicated, and therefore not easy to generalize to other protocols.

2. Entanglement-based security proofs

A remarkable step was taken by Shor and Preskill (2000), who showed that one can prove security of the BB84 scheme, which is a P&M protocol, by considering a protocol based on entanglement (a modified Lo-Chau protocol). This was something like the Bennett-Brassard-Mermin consideration, but in a noisy scenario. Namely, while using BB84 in the presence of noise, Alice and Bob first obtain a so-called raw key—a string of bits which is not perfectly correlated (there are some errors), and also not perfectly secure (Eve has some knowledge about the key). By looking at the part of the raw key, they can estimate the level of error and the knowledge of Eve. They then classically process it, applying procedures of error correction and privacy amplification (the latter aims at diminishing knowledge of Eve).

In the related entanglement based scheme, we have coherent analogs of those procedures. Without going into details, we can imagine that in an entanglement based scheme Alice and Bob share pairs in one of four Bell states (3), which may be seen as the state ϕ^+ with two kinds of errors: bit and phase error. The error from the previous scheme translates here into bit error, while knowledge of Eve's translates into phase error. Now the task is simply to correct both errors. Two procedures of a different kind (error correction and privacy amplification) are now both of the same type—they correct errors.

After correcting bit error, Alice and Bob are left with Bell states which are all correlated,

$$|\phi^-\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad |\phi^+\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \qquad (184)$$

Then they apply the phase-error-correcting procedure, i.e., they get to know which systems are in ϕ^- and which are in ϕ^+ so that they can rotate each ϕ^- into ϕ^+ and finally obtain a sequence of soley ϕ^+. What Shor and Preskill noticed is that these two quantum procedures are coherent[78] versions of classical error correction and privacy amplification, respectively. Thus Shor-Preskill proof can be phrased as follows: "The BB84 protocol is secure because its suitable coherent version distills EPR states."

It should be emphasized here that the equivalence between noisy BB84 protocol and its coherent version does not continue to the very end. Namely, in distillation Alice and Bob, after finding which pair is in $|\phi^-\rangle$ and which is in $|\phi^+\rangle$, rotate $|\phi^-\rangle$. The classical procedures performed coherently cannot perform this very last step (rotation) as no classical action can act as a phase gate after embedding into quantum. However, the key is secure, because Alice and Bob could have performed the rotation, but they do not have to. Indeed, note that if Alice and Bob measure the pairs in the basis $\{|0\rangle, |1\rangle\}$ they obtain the same results, independently of whether they have rotated $|\phi^-\rangle$ or not. The very possibility of rotation means that the key will be secure. Thus the coherent version of BB84 does not actually give $|\phi^+\rangle$ itself, but it does if supplemented with rotations.

The concept of proving the security of P&M protocols by showing that at the logical level they are equivalent to distillation of entanglement has become very fruitful. In 2003 Tamaki, Koashi, and Imoto (Tamaki *et al.*, 2003) showed that B92 is unconditionally secure, using the Shor-Preskill method (see also Tamaki and Lütkenhaus, 2004). They showed that B92 is equivalent to the special entanglement distillation protocol known as *filtering* (Gisin, 1996; Horodecki *et al.*, 1997) (see Sec. XII.D). Ardehali *et al.* (1998) proposed the efficient version of BB84, which is still unconditionally secure, though the number of systems that Alice and Bob use to estimate the error rate is much smaller than in BB84. Again security is proved in the Shor-Preskill style. Gottesman and Lo (2003) found a P&M scheme with a two-way classical error correction and privacy amplification protocol. It is shown that a protocol with two-way classical communication can have a substantially higher key rate than the one using one-way classical communication only. Also, security of key distribution using dense coding (Long and Liu, 2002) was proved using Shor-Preskill

[77]Using the concept of another entanglement-based communication scheme, quantum repeaters (Briegel *et al.*, 1998; Dür, Briegel, *et al.*, 1999), Lo and Chau established quantum key distribution over arbitrary long distances.

[78]It is worthwhile to observe that formally any QKD scheme can be made "entanglement based," as according to axioms of quantum mechanics any operation is unitary and the only source of randomness is the subsystem of an entangled state. From this point of view, even when Alice sends to Bob a randomly chosen signal state, as it is in P&M schemes, according to axioms she sends a part of an entangled system. Moreover, any operation that Alice and Bob would perform on signal states in the P&M scheme can be done reversibly, so that the whole system shared by Alice, Bob, and Eve is in a pure state at each step of the protocol. This principle of maintaining purity is usually referred to as coherent processing. We note, however, that not always must the coherent application of a protocol that provides a key result in the distillation of ϕ^+. In Sec. XIX.B we show that there is a more general class of states that gives a private key.

techniques (Zhang *et al.*, 2005) (see Degiovanni *et al.*, 2003, 2004; Wójcik, 2005).

Thus, thanks to the simplicity of the Shor-Preskill approach, pure entanglement is a very useful tool for proving unconditional security of QKD protocols (Gisin and Brunner, 2003). As we show, this approach can be generalized by considering mixed entangled states containing an ideal key.

3. Constraints for security from entanglement

So far we have discussed the role of entanglement in particular protocols of quantum key distribution. Aconnection between entanglement and any QKD protocol has been established by Curty, Lewenstein, and Lütkenhaus (2004). They have proved that entanglement is a necessary precondition of unconditional security. Namely, in the case of any QKD protocol, Alice and Bob perform some measurements and are left with some classical data from which they want to obtain a key. Based on these data and measurements settings, they must be able to construct a so called entanglement witness to ensure that the data could not be generated via measurement on some separable state (see Sec. VI.B.3). We emphasize that this holds not only for entanglement based but also for prepare and measure protocols. In the latter case, a kind of "effective" entanglement is witnessed (i.e., the one which is actually never shared by Alice and Bob). This idea has been studied in the case of high dimensional systems (Nikolopoulos and Alber, 2005; Nikolopoulos *et al.*, 2006) and general upper bounds on key rates for "prepare and measure" schemes have been found (Moroder *et al.*, 2006a, 2006b). It is also connected with optimization of entanglement measures from incomplete experimental data (see Sec. VI.B.4).

4. Secure key beyond distillability of pure entanglement: Prelude

The fact that up to date techniques to prove unconditional security were based on entanglement purification i.e., distilling pure entangled states, has supported the belief that the possibility of distilling pure entanglement (singlet) is the only reason for unconditional security. The first interesting step towards this direction was due to Aschauer and Briegel, who showed that Lo and Chau's protocol provides a key even without the fault tolerant computing, i.e., with realistic noisy apparatuses (Aschauer and Briegel, 2002). However, as we show, it turns out that one can get an unconditionally secure key even if by means of perfect operations no pure entanglement could be obtained.

B. Drawing a private key from distillable and bound entangled states of the form $\rho^{\otimes n}$

A strong interrelation between the theory of a secure key and entanglement can already be seen in the scenario where Alice and Bob share n bipartite systems in the same state ρ_{AB} and Eve holds their purification, so that the joint state of the Alice, Bob, and Eve systems is a pure state $|\psi_{ABE}\rangle$. The task of the honest parties (Alice and Bob) is to obtain by means of local operations and classical communication the highest possible amount of correlated bits that are unknown to Eve (i.e., a secure key). The difficulty of this task is due to the fact that Eve makes a copy of any classical message exchanged by Alice and Bob.

The above paradigm allows us to consider a new measure of entanglement: distillable key K_D, which is similar in spirit to distillable entanglement as discussed in Secs. XV.D.1 and XV.A. It is given by the number of secure bits of a key that can be obtained (per input pair) from a given state.

We discuss briefly two extreme cases. (i) All distillable states are key distillable:

$$K_D(\rho_{AB}) \geqslant E_D(\rho_{AB}). \tag{185}$$

(ii) All separable states are key nondistillable:

$$K_D(\sigma_{\text{sep}}) = 0. \tag{186}$$

To see the first statement, one applies the idea of quantum privacy amplification described in Sec. XIX.A. Simply, Alice and Bob distill singlets and measure them locally. Due to the purity and correlation principle described in the beginning of Sec. XIX, this gives a secure key.

To see that a key cannot be drawn from separable states (Gisin and Wolf, 2000; Curty *et al.*, 2004), note that by the definition of separability there is a measurement on Eve's subsystem such that conditionally upon result (say i) Alice and Bob share a product state $\rho_A^{(i)} \otimes \rho_B^{(i)}$. This means that Alice and Bob conditionally on Eve have initially no correlations. Of course, any further communication between Alice and Bob cannot help, because it is monitored by Eve.

In Sec. XIX.B.3 it will be shown that there are nondistillable states which are key distillable:

$$E_D(\rho_{\text{BE}}) = 0 \quad \text{and} \quad K_D(\rho_{\text{BE}}) > 0. \tag{187}$$

1. Devetak-Winter bound

Here we present a result due to Devetak and Winter, which shows that from any state one can draw at least the amount of key equal to the coherent information. This is compatible with the idea that one can draw a key only from entangled states [states with positive coherent information are entangled, as shown by Horodecki and Horodecki (1994)]. The coherent version of the protocol will in turn distill this amount of singlets from the state. In this way Devetak and Winter have for the first time proved the hashing inequality (see Sec. XII.F) for distillable entanglement. It was also used by Devetak (2003) to prove rigorously the quantum Shannon theorem stating that the capacity of a quantum channel is given by coherent information.

That is, consider a state ρ_{AB}, so that the total state including Eve's system is $|\psi_{ABE}\rangle$. As said, we assume that Alice and Bob have n copies of such a state. Now Alice performs a complete measurement, which turns the total

state into $\rho_{cqq}=\Sigma_i p_i|i\rangle\langle i|_A\otimes\rho^i_{\mathrm{BE}}$ where the subscript cqq reminds us that Alice's system is classically correlated with Bob's and Eve's subsystems. They considered drawing a key from a general cqq state as a starting point, and showed that one can draw at least the amount of key equal to

$$I(A:B)-I(A:E), \tag{188}$$

where $I(X:Y)=S(X)+S(Y)-S(XY)$ is quantum mutual information. Now, we note that in the present case

$$I(A:B)=S(\rho_B)-\sum_i p_i S(\rho^i_B),$$

$$I(A:E)=S(\rho_E)-\sum_i p_i S(\rho^i_E), \tag{189}$$

where $\rho^i_B=\mathrm{Tr}_E\rho^i_{BE}$, $\rho^i_E=\mathrm{Tr}_B\rho^i_{BE}$, $\rho_B=\Sigma_i p_i\rho^B_i=\mathrm{Tr}_A\rho_{AB}$, and $\rho_E=\Sigma_i p_i\rho^E_i=\mathrm{Tr}_{AB}\rho_{AE}$.

Since the measurement of Alice was complete, the states ρ^i_{BE} are pure, hence $S(\rho^i_E)=S(\rho^i_B)$. Also, since the total initial state was pure, we have $S(\rho_E)=S(\rho_{AB})$ where ρ_{AB} is the initial state shared by Alice and Bob. Thus we obtain that the amount of key gained in the protocol is actually equal to coherent information. Let us emphasize that DW protocol can be applied to cqq states which *do not* come from *complete* measurement by Alice, as we have assumed above. Therefore the protocol can be used even for bound entangled states, for which coherent information is not positive (see further text).

2. Distillable key as an operational entanglement measure

The states which contain two qudits—one for Alice, one for Bob—that, after measurement give perfect key are called private states (p-dits). Any p-dit must be of the form of "twisted" maximally entangled state (Horodecki *et al.*, 2005d)

$$\gamma^{(d)}=\frac{1}{d}\sum_{i,j=0}^{d-1}|ii\rangle\langle jj|_{AB}\otimes U_i\rho_{A'B'}U_j^\dagger,$$

where U_i are arbitrary unitary transformations acting on the system $A'B'$. [One may define a private state in a slightly different manner, which leads to a form equivalent up to local isometries (Renes and Smith, 2007).] The whole state resides on two systems with distinguished subsystems AA' and BB', respectively. The concept of private states allows us to represent K_D as a quantity analogous to entanglement distillation:

$$\rho^{\otimes n}_{AB}\xrightarrow{\text{LOCC key distillation}}\gamma^{(d)}_{ABA'B'}, \tag{190}$$

where the highest achievable ratio $\log_2 d/n$ in the asymptotic limit equals the distillable key denoted as $K_D(\rho_{AB})$. Instead of singlets we distill private states. Since the class of private states is broader than the class of maximally entangled states, one can expect that a distillable key can be greater than distillable entanglement. Indeed, this is the case, and an example is the private state of Eq. (193) [see Eq. (194)].

Thus a distillable key is an operational measure of entanglement, which is distinct from E_D. It is also distinct from E_C and satisfies

$$E_D\leqslant K_D\leqslant E_C. \tag{191}$$

Moreover, it is upper bounded by relative entropy of entanglement (Horodecki *et al.*, 2005d) and squashed entanglement (Christandl, 2006). In general, an entanglement monotone satisfying some natural axioms in the context of private states is an upper bound on the distillable key (see Christandl *et al.*, 2007). There is also a bound involving the best separable approximation (Moroder *et al.*, 2006b) which exploits the fact that admixing a separable state can only decrease K_D. Moroder *et al.* (2006a) presented a bound for a one-way distillable key, based on the fact that for a state which has a symmetric extension, its one-way distillable key must vanish. Indeed, then Bob and Eve share with Alice the same state, so that any final key which Alice shares with Bob she also share with Eve.

3. Drawing a secure key from bound entanglement

Bound entanglement is a weak resource, especially in the bipartite case. For a long time the only useful task that bipartite BE states were known to perform was activation, where they acted together with some distillable state. Obtaining a private key from bound entanglement, a process which we present now, is the first useful task which bipartite BE states can do themselves.

Since distillable entanglement of some private states can be low, it was tempting to admix with small probability some noise in order to obtain a state which is nondistillable while still entangled:

$$\rho_{\mathrm{total}}=(1-p)\gamma+p\rho_{\mathrm{noise}}. \tag{192}$$

It happens that for certain private states γ the state ρ_{noise} can be adjusted in such a way that the state ρ_{total} is PPT (hence $E_D=0$), and despite this, from many copies of ρ_{total} one can distill a key of arbitrarily good quality. That is, one can distill private state γ' with an arbitrary small admixture of noise.

The first examples of states with a positive distillable key and zero distillable entanglement were found by Horodecki *et al.* (2005a, 2005d). We present here a simple one which has been given by Horodecki, Pankowski, *et al.* (2005). It is actually a mixture of two private bits (correlated and anticorrelated). The total state has a matrix form

$$\rho_{ABA'B'}=\frac{1}{2}\begin{bmatrix}p_1\sqrt{X_1X_1^\dagger} & 0 & 0 & p_1X_1\\ 0 & p_2\sqrt{X_2X_2^\dagger} & p_2X_2 & 0\\ 0 & p_2X_2^\dagger & p_2\sqrt{X_2^\dagger X_2} & 0\\ p_1X_1^\dagger & 0 & 0 & p_1\sqrt{X_1^\dagger X_1}\end{bmatrix}, \tag{193}$$

with $X_1=\Sigma_{i,j=0}^{1}u_{ij}|ij\rangle\langle ji|_{A'B'}$ and $X_2=\Sigma_{i,j=0}^{1}u_{ij}|ii\rangle\langle jj|_{A'B'}$ where u_{ij} are the elements of the one-qubit Hadamard transform and $p_1=\sqrt{2}/(1+\sqrt{2})$ ($p_2=1-p_1$). This state is invariant under partial transposition over Bob's subsystem. If we, however, project its key part (AB subsystem) onto a computational basis it turns out that the joint state of the systems A, B, and Eve system is fully classical and of simple form: with probability p_1 Eve knows that Alice and Bob are correlated, while with probability p_2 that they are anticorrelated. Thus the mutual information $I(A:E)=0$, and $I(A:B)=1-H(p_1)$. Thus applying Devetak-Winter protocol[79] [see Eq. (188)] we obtain a key rate

$$K_D(\rho)\geqslant 1-h(p_1)=0.021\,339\,9>E_D(\rho)=0. \qquad (194)$$

Based on this example it was argued (Horodecki, Pankowski, *et al.*, 2005) that the volume of bound entangled key distillable states is nonzero in the set of states occupying more then four qubits. It is, however, a nontrivial task to provide new examples. Interestingly, no previously known bound entangled state has been shown to be key distillable.

C. Private states: New insight into entanglement theory of mixed states

Investigations concerning a distillable key were fruitful to the entanglement theory itself. A new operational measure of entanglement was obtained, and also a new source of examples of irreversibility in entanglement distillation was provided. The private states, and some PPT states with a nonzero key, constitute a new collection of states which are easy to deal with and have nontrivial properties, in addition to such canonical classes as Werner, isotropic, Bell diagonal, or maximally correlated states. While the simplicity of the latter classes comes from symmetries (e.g., invariance under twirling), the simplicity of the class of private states is based on special asymmetry between the systems AB and $A'B'$.

Some private bits, called flower states, are the ones for which the squashed entanglement has been computed (Christandl and Winter, 2005). Moreover, they exhibit locking of entanglement (see Sec. XVIII.A). There is actually a general link between the locking effect and the problem of drawing a key from bound entanglement. Last but not least, the description of this class of states yields a natural generalization of pure maximally entangled states to the case of mixed states with coefficients becoming operators.

[79]Since in this particular case the state is fully classical, it would be enough to use the classical predecessor of the Devetak-Winter protocol, called the Csiszar-Körner-Maurer protocol.

D. Quantum key distribution schemes and security proofs based on distillation of private states: Private key beyond pure entanglement

The key distillation described in Sec. XIX.B relies upon an important assumption. The initial state shared by Alice and Bob should be a tensor product of the same state ρ_{AB}. This assumption is unreal in almost all security applications, since the eavesdropper can interrupt the communication and entangle copies of the state. It was then unclear whether one can obtain a gap between a distillable key and distillable entanglement (as reported in Sec. XIX.B.2) in the general scenario, where Alice and Bob do not know *a priori* anything about their states. It has not been noticed that a positive answer to this question follows from the results on the finite quantum de Finetti theorem by Renner, Gisin, and Kraus (Kraus *et al.*, 2005; Renner *et al.*, 2005) [see especially Koenig and Renner (2005) and Renner (2005)] and the results of Horodecki *et al.* (2005d) on bound entangled key distillable states. In the meantime, a more entanglement-based approach has been developed (Horodecki, Leung, *et al.*, 2006; Horodecki *et al.*, 2008), which can be seen as a generalization of the Lo and Chau entanglement purification based approach to the private state distillation one. It has been shown there that an unconditionally secure key can be distributed even when no pure entanglement can be obtained. This important result can be rephrased as follows: There are situations in which one can not send faithfully any qubit, but one can send arbitrarily many unconditionally secure bits.

Note that security proof of the Shor-Preskill type as such cannot be used here, as its core from Eve's point of view is that the given protocol is indistinguishable from the one that produces singlets. This cannot work in the present situation. Instead, the protocol is viewed by Eve as producing private states, i.e., "twisted" singlets. It then turns out that one can also suitably "twist" the security proof [see Horodecki *et al.* (2007) for more details].

A general principle that connects entanglement and key distribution in an ultimate way, is that a protocol produces a secure key if and only if its coherent version produces private states. It was recently applied by Renes and Smith (2007) who have found an entanglement based proof of the P&M protocol with the noisy preprocessing of Kraus *et al.* (2005) and Renner *et al.* (2005). They have demonstrated its coherent version, which distills private states, and hence must be secure [cf. Renes and Boileau (2008)].

E. Entanglement in other cryptographic scenarios

There are many other quantum cryptographic scenarios than quantum key distribution where entanglement enters. These include, e.g., third man quantum cryptography (Żukowski *et al.*, 1998) together with intimately related quantum secret sharing (Hillery *et al.*, 1999), and conference key agreement (Chen and Lo,

2004; Horodecki and Augusiak, 2006). Interestingly, entanglement may be important not only because it makes some protocols possible but because it disallows certain schemes as it happens in quantum bit commitment.

Historically, it was claimed that quantum information theory can ensure not only unconditionally secure key distribution but also an important ingredient of classical cryptographic protocols—a bit commitment protocol (Brassard *et al.*, 1993). If so, Alice could commit some decision (a bit value) to Bob, so that after committing she could not change her mind (change the bit value) but Bob also could not infer her decision before she lets him open it. Such a protocol would be an important ingredient in secure transaction protocols. Unfortunately, it is not the case: Mayers (1996, 1997) and independently Lo and Chau (1997, 1998) have proved, under assumptions plausible in cryptographic context, that quantum bit commitment is not possible. Paradoxically, it is exactly entanglement that, even though assuring the security of QKD, is the main reason for which the quantum bit commitment is not possible. It shows the following important fact: When the two parties do not trust each other, entanglement between them may sometimes become the most unwanted property.

There were many attempts to perform quantum bit commitment; some of them invalid as covered by the proof given by Lo and Chau and some of them being approximated versions of impossible quantum bit commitment.

While the proof of Lo and Chau is valid, as pointed out by Yuen (2005) one could weaken assumptions, so that the Lo-Chau theorem does not apply. This caveat was considered by D'Ariano *et al.* (2007). The latter work also provides the most recent and wide review of this topic.

F. Interrelations between entanglement and classical key agreement

So far we have discussed the role of entanglement in quantum cryptography. It is interesting that entanglement, which is originally a quantum concept, corresponds to privacy in general—not only in the context of quantum protocols. Here the interaction between entanglement theory and the domain of classical cryptography, called classical key agreement (CKA), is presented.

The problem of distilling a secret key from correlations shared by Alice and Bob with the presence of an eavesdropper, Eve, was first studied by Wyner (1975) and Csiszár and Körner (1978). It was introduced as a classical key agreement scenario and studied in full generality by Maurer (1993). According to this scenario, Alice and Bob have access to n independent realizations of variables A and B, respectively, while the malicious Eve holds n independent realizations of a variable E. The variables under consideration have joint probability distribution $P(A,B,E)$. The task of Alice and Bob is to obtain via local (classical) operations and public communication (LOPC) the longest bit string which is almost perfectly correlated and about which Eve (who can listen to the public discussion) knows a negligible amount of information.[80]

Here the probability distribution $P(A,B,E)$ is *a priori* given. That is, it is assumed that Alice and Bob somehow know how Eve is correlated with their data.

1. Classical key agreement: Analogy to distillable entanglement scenario

The classical key agreement scenario is an elder sibling of an entanglement-distillation-like scenario. This relation was first found by Gisin and Wolf (1999, 2000), and subsequently developed by Collins and Popescu (2002). The analogy has been recently explored and proved to be fruitful for establishing new phenomena in classical cryptography, and new links between privacy and entanglement theory. The connections are quite beautiful, however, they still remain not fully understood.

The classical key agreement task is described by the following diagram:

$$[P(A,B,E)]^{\otimes n} \xrightarrow[\text{distillation of key}]{\text{classical}} [P(K,K,E')]^{\otimes k}, \tag{195}$$

where $P(K,K,E')$ is a perfectly secure distribution satisfying

$$P(K,K) \equiv \{P(i,j) = \tfrac{1}{2}\delta_{ij}\},$$

$$P(K,K,E') = P(K,K)P(E'), \tag{196}$$

where Alice and Bob hold variable K and E' is some Eve's variable, i.e., Alice and Bob are perfectly correlated and product with Eve. The optimal ratio k/n in the asymptotic limit is a (classical) distillable key rate denoted here as $K(A;B\|E)$ (Maurer, 1993).

Entanglement between two parties (see Sec. XIX) reports that nobody else is correlated with the parties. In a similar way the privacy of the distribution $P(A,B,E)$ means that nobody knows about (i.e., is classically correlated with) the variables A and B. In other words, any tripartite joint distribution with marginal $P(A,B)$ has a product form $P(A,B)P(E)$.

Following along these lines one can see the correspondence between maximally entangled state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and the private distribution (196), and also the correspondence between the problem of transformation of the state $\rho_{AB}^{\otimes n}$ into maximally entangled states which is the entanglement distillation task and the above described task of classical key agreement. Actually, the first entanglement distillation schemes (Bennett, Brassard, *et al.*, 1996; Bennett, DiVincenzo, *et al.*, 1996) have

[80] We emphasize that on classical ground unlike in quantum cryptography it is in principle not possible to verify that Eve possesses only the information described by $P(A,B,E)$. However, in particular situations, there may be good practical reasons for assuming this.

TABLE I. Relations between basic notions of key agreement and entanglement theory following Collins and Popescu (2002).

Entanglement theory	Key agreement
quantum entanglement	secret classical correlations
quantum communication	secret classical communication
classical communication	public classical communication
local actions	local actions

been designed on the basis of protocols of classical key agreement (see Table I). The feedback from entanglement theory to classical key agreement was initiated by Gisin and Wolf (2000) who asked the question of whether there is an analog of bound entanglement, discussed in the next section. Subsequently, in analogy to entanglement cost which measures how expensive in terms of a singlet state is the creation of a given quantum state ρ_{AB} by means of LOCC operations, Renner and Wolf (2003) defined information of formation denoted as $I_{\text{form}}(A;B|E)$ (sometimes called "key cost"). This function quantifies how many secure key bits (196) the parties have to share so that they could create given distribution $P(A,B,E)$ by means of LOPC operations. The axiomatic approach to privacy, resulting in deriving secrecy monotones (also in the multipartite case), has been studied by Cerf, Massa, and Schneider (2002) and Horodecki *et al.* (2005b).

Criteria analogous to those for pure bipartite states transitions and catalytical transitions known as majorization criteria (see Secs. XIII.A and XIII.A.1) can be found in Collins and Popescu (2002). Also other quantum communication phenomena such as quantum state merging (Horodecki, Oppenheim, *et al.*, 2005) and information exchange (Oppenheim and Winter, 2003) as well as the no-cloning principle are found to have counterparts in classical setup (Oppenheim *et al.*, 2002).

A simple and important connection between tripartite distributions containing privacy and entangled quantum states was established by Acín and Gisin (2005). If a bipartite state ρ_{AB} is entangled then there exists a measurement on subsystems A and B such that for all measurements on subsystem E of its purification $|\psi_{ABE}\rangle$ the resulting probability distribution $P(A,B,E)$ has a nonzero key cost. If a bipartite state ρ_{AB} is separable, then for all measurements on subsystems A and B there exists a measurement on subsystems E of purification $|\psi_{ABE}\rangle$ such that the resulting probability distribution $P(A,B,E)$ has a zero key cost.

2. Is there a bound information?

In the entanglement distillation scenario there are bound entangled states which exhibit the highest irreversibility in the creation-distillation process, as the distillable entanglement is zero although the entanglement cost does not vanish (see Sec. XII). One can ask then if the analogous called bound information phenomenon holds in classical key agreement (Gisin and Wolf, 2000; Renner and Wolf, 2003). This question can be stated as follows: Does there exist a distribution $P(A,B,E)_{\text{bound}}$ for which a secure key is needed to create it by LOPC $[I_{\text{form}}(A;B|E)>0]$, but one cannot distill any key back from it $[K(A;B\|E)=0]$? Gisin and Wolf (2000) considered distributions obtained via measurement from bound entangled states as a possible way of searching for the hypothetical ones with bound information. To get Eve's variable, one has first to purify a bound entangled state, and then find a clever measurement to get tripartite distribution. In this way, distributions $P(A,B,E)$ with a nonzero key cost were obtained. However, the no-key distillability still needs to be proved.

A strong confirmation supporting the hypothesis of bound information is the result presented by Renner and Wolf (2003), where examples of distributions which asymptotically have bound information were found. Namely, there is a family of distributions $P(A_n,B_n,E_n)$ such that $\lim_{n\to\infty}K(A_n;B_n\|E_n)=0$ while $I_{\text{form}}(A_n;B_n|E_n)>\frac{1}{2}$ for all n. Another argument in favor of the existence of bound information in this bipartite scenario is the fact that the multipartite bound information has been already proved to exist, and explicit examples have been constructed (Acín, Cirac, *et al.*, 2004). The distribution exhibiting the multipartite bound information was obtained from the quantum bound entangled state (73).

XX. ENTANGLEMENT AND QUANTUM COMPUTING

A. Entanglement in quantum algorithms

Fast quantum computation is one of the most desired properties of quantum information theory. There are few quantum algorithms which outperform their classical counterparts. These are the celebrated Deutsch-Jozsa, Grover and Shor's algorithm, and their variations. Since entanglement is a cornerstone of quantum information theory it is natural to expect that it should be the main ingredient of quantum algorithms which are better than classical. This was first discussed by Jozsa (1997). His seminal paper opened a debate on the role of entanglement in quantum computing. Actually, after more than a decade from the discovery of the first quantum algorithm, there is no common agreement on the role of entanglement in quantum computation. We discuss major contributions to this debate. It seems that entanglement "assists" quantum speedup, but is not sufficient for this phenomenon.

If quantum computer is in pure state, then certainly quantum computation needs some level of entanglement if it is not to be simulated classically. It was shown by

Jozsa and Linden that if a quantum computer's state at all times is a product of states involving only a constant (independent of number of input qubits n) amount of qubits, then it can be simulated efficiently (Jozsa and Linden, 2002).

Next, Vidal showed, that if at all times, under any bipartite cut, the state of the quantum computer has Schmidt rank polynomial in n, then the computation can be efficiently classically simulated. In other words, to give an exponential speedup the quantum algorithm needs to achieve Schmidt rank of exponential order in n, during computation.

This general result was studied by Orús and Latorre (2004) for different algorithms in terms of entropy of the entanglement (von Neumann entropy of the subsystem). It was shown among others that computation of Shor's algorithm generates highly entangled states (with a linear amount of entropy of entanglement which corresponds to exponential Schmidt rank). Although it is not known if Shor's algorithm provides an exponential speedup over classical factoring, this analysis suggests that Shor's algorithm cannot be simulated classically.

Entanglement in Shor's algorithm has been studied in different contexts (Ekert and Jozsa, 1998; Jozsa and Linden, 2002; Parker and Plenio, 2002; Shimoni *et al.*, 2005). Interestingly, as the presence of entanglement in quantum algorithm is widely confirmed (see also Datta *et al.*, 2005; Datta and Vidal, 2007), its role is still not clear, since it seems that the amount of it depends on the type of input number (Kendon and Munro, 2006).

Note that the above Jozsa-Linden-Vidal "no entanglement implies no quantum advantage on pure states" result shows the need for the presence of entanglement for exponential speedup. Without falling into contradiction, one can then ask if entanglement must be present for polynomial speedup when only pure states are involved during computation (see Kenigsberg *et al.*, 2006, and references therein).

Moreover, it was considered possible that a quantum computer using only *mixed*, separable states during computation may still outperform classical ones (Jozsa and Linden, 2002). It is shown that this phenomenon can hold (Biham *et al.*, 2004), but with a small speedup. It was argued that an isotropic separable state cannot be entangled by an algorithm, yet it can prove useful in quantum computing. Answering the general question of how large the enhancement based on separable states may be needs a more algorithm-dependent approach.

That the presence of entanglement is only necessary but not sufficient for exponential quantum speedup follows from the Knill-Gottesman theorem (Gottesman and Chuang, 1999; Jozsa and Linden, 2002). It states that operations from the so-called Clifford group composed with Pauli measurement in a computational basis can be efficiently simulated on a classical computer. This class of operations can, however, produce highly entangled states. For this reason, and as indicated by others, the role of entanglement is still not clear. As it is pointed out by Jozsa and Linden (2002), it may be that what is essential for quantum computation is not entanglement but the fact that the set of states which can occur during computation cannot be described with a small number of parameters [see also Knill (2001), and references therein].

B. Entanglement in quantum architecture

Although the role of entanglement in algorithms is unclear, its role in the architecture of quantum computers is crucial. First the multipartite cluster states provide a resource for one-way quantum computation (Raussendorf and Briegel, 2001). One prepares such a multipartite state, and the computation is based on subsequent measurements of qubits, which uses up the state.

One can ask what other states can be used to perform universal one-way quantum computation. Van den Nest *et al.* (2006) assumed that universality means the possibility of creating any final state on the part of the lattice that was not subjected to measurements. It was pointed out that by the use of entanglement measures one can rule out some states. Namely, they introduced an entanglement measure, entanglement width, which is defined as the minimization of bipartite entanglement entropy over some specific cuts. It turns out that this measure is unbounded for cluster states (if we increase size of the system). Thus any class of states, for which this measure is bounded, cannot be a resource for universal computation, as it cannot create arbitrary large cluster states. For example, the GHZ state is not universal, since under any cut the entropy of entanglement is just 1. One should note here that more natural is the weaker notion of universality where one requires the possibility of a computed arbitrary classical function. Gross and Eisert (2007) showed that entanglement width is not a necessary condition for this type of universality.

An intermediate quantum computing model, between circuits based on quantum gates and one-way computing, is teleportation-based computing (Gottesman and Chuang, 1999). There two- and three-qubit gates are performed by use of teleportation as a basic primitive. The resource for this model of computation are thus EPR states and GHZ states. Teleportation based computing is of great importance, as it allows for efficient computation by use of linear optics (Knill *et al.*, 2001), where it is impossible to perform two-qubit gates deterministically. Moreover, using it Knill has significantly lowered the threshold for fault-tolerant computation (Knill, 2004).

An interesting connection between entanglement and fault-tolerant quantum computation was obtained by Aharonov (1999). She has shown that a properly defined long-range entanglement[81] vanishes in the thermodynamical limit if the noise is too large. Combining this with the fact that the fault-tolerant scheme allows us to achieve such entanglement, one obtains a sort of phase

[81]Another type of long-range entanglement was defined (Kitaev and Preskill, 2006; Levin and Wen, 2006) in the context of topological order.

transition (the result is obtained within a phenomenological model of noise).

The level of noise under which a quantum computer becomes efficiently simulatable was first studied by Aharonov and Ben-Or (1996). It was shown that a quantum computer which operates (globally) on $O(\log_2 n)$ number of qubits at a time (i.e., with limited entangling capabilities) can be efficiently simulated for any nonzero level of noise. For the circuit model (with local gates), a phase transition depending on the noise level is observed (see also Aharonov *et al.*, 1996).

The same problem was studied further by Harrow and Nielsen (2003), but based directly on the entangling capabilities of the gates used for computation. It was shown that so-called separable gates (gates which cannot entangle any product input) are classically simulatable. The bound on the minimal noise level which allows a quantum computer to deal only with separable gates was provided there. This idea has been developed by Virmani *et al.* (2005). They considered a larger class of gates which can be efficiently classically simulated. In particular, they also allowed gates which break entanglement between the qubits they act on, and all the other qubits. As a consequence, a stronger bound on the tolerable noise level is found.

C. Byzantine agreement: Useful entanglement for quantum and classical distributed computation

As already discussed, the role of entanglement in communication networks is uncompromised. We have already described its role in cryptography (see Sec. XIX) and communication complexity. Here we comment on another application—a quantum solution to a famous problem in classical fault-tolerant distributed computing called the Byzantine agreement. This problem is known to have no solution in classical computer science, yet its slightly modified version can be solved using a quantum entangled multipartite state (Fitzi *et al.*, 2001). One goal in distributed computing is to achieve broadcast in a situation when some of the stations can send faulty signals. It has been proved classically that if there are $t \geqslant n/3$ stations which are out of work and can send unpredictable data, then broadcast cannot be achieved. In quantum terms, a so-called "detectable broadcast," where the stations are allowed to abort, can be achieved for $n=3$ by use of the Aharonov state,

$$\psi = \frac{1}{\sqrt{6}}(|012\rangle + |201\rangle + |120\rangle - |021\rangle - |102\rangle - |210\rangle). \tag{197}$$

The subject was further developed, including continuous variable version (Neigovzen *et al.*, 2008) and an alternative solution provided and implemented experimentally by Gaertner *et al.* (2008).

ACKNOWLEDGMENTS

We thank Jadwiga Horodecka for help in the editing of this paper. Many thanks are due to Andrzej Grudka, Łukasz Pankowski, Marco Piani, and Marek Żukowski for their help in editing and useful discussions. We also thank many other colleagues in the field of quantum information for discussions and useful feedback. We wish also to acknowledge the referees for their fruitful criticism. This work was supported by EU SCALA FP6-2004-IST i.d. No. 015714. K.H. acknowledges support of Foundation for Polish Science. P.H. was supported by Polish Ministry of Science and Education, Contract No. 1 P03B 095 29. K.H., M.H., and R.H. were supported by Polish Ministry of Science and Education under the (solicited) Grant No. PBZ-MIN-008/P03/2003.

REFERENCES

Abascal, I. S., and G. Björk, 2007, Phys. Rev. A **75**, 062317.
Acín, A., 2001, Phys. Rev. Lett. **88**, 027901.
Acín, A., D. Bruß, M. Lewenstein, and A. Sanpera, 2001, Phys. Rev. Lett. **87**, 040401.
Acín, A., J. L. Chen, N. Gisin, D. Kaszlikowski, L. C. Kwek, C. H. Oh, and M. Żukowski, 2004, Phys. Rev. Lett. **92**, 250404.
Acín, A., J. I. Cirac, and L. Masanes, 2004, Phys. Rev. Lett. **92**, 107903.
Acín, A., and N. Gisin, 2005, Phys. Rev. Lett. **94**, 020501.
Acín, A., N. Gisin, and L. Masanes, 2006, Phys. Rev. Lett. **97**, 120405.
Acin, A., V. Scarani, and M. M. Wolf, 2003, J. Phys. A **36**, L21.
Acín, A., R. Tarrach, and G. Vidal, 2000, Phys. Rev. A **61**, 062307.
Adesso, G., and F. Illuminati, 2005, Phys. Rev. A **72**, 032334.
Adesso, G., and F. Illuminati, 2006, New J. Phys. **8**, 15.
Adesso, G., and F. Illuminati, 2007, J. Phys. A **40**, 7821.
Agarwal, G. S., and A. Biswas, 2005, J. Opt. B: Quantum Semiclassical Opt. **7**, 350.
Aharonov, D., 1999, e-print arXiv:quant-ph/9910081.
Aharonov, D., and M. Ben-Or, 1996, e-print arXiv:quant-ph/9611029.
Aharonov, D., M. Ben-Or, R. Impagliazzo, and N. Nisan, 1996, e-print arXiv:quant-ph/9611028.
Akhtarshenas, S. J., 2005, J. Phys. A **38**, 6777.
Akopian, N., N. H. Lindner, E. Poem, Y. Berlatzky, J. Avron, D. Gershoni, B. D. Gerardot, and P. M. Petroff, 2006, Phys. Rev. Lett. **96**, 130501.
Alber, G., T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. F. Werner, and A. Zeilinger, 2001, *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments* (Springer, New York).
Alber, G., A. Delgado, N. Gisin, and I. Jex, 2001, J. Phys. A **34**, 8821.
Alicki, R., and M. Fannes, 2004, J. Phys. A **37**, L55.
Almeida, M. P., F. de Melo, M. Hor-Meyll, A. Salles, S. P. Walborn, P. H. S. Ribeiro, and L. Davidovich, 2007, e-print arXiv:quant-ph/0701184.
Alsing, P. M., and G. J. Milburn, 2002, Quantum Inf. Comput. **2**, 487.
Altepeter, J. B., E. R. Jeffrey, P. G. Kwiat, S. Tanzilli, N. Gisin, and A. Acín, 2005, Phys. Rev. Lett. **95**, 033601.
Altewischer, E., M. P. van Exter, and J. P. Woerdman, 2002, Nature (London) **418**, 304.
Alves, C. M., P. Horodecki, D. K. L. Oi, L. C. Kwek, and A. K. Ekert, 2003, Phys. Rev. A **68**, 032306.
Ambainis, A., and D. Gottesman, 2006, IEEE Trans. Inf.

Theory **52**, 748.
Ambainis, A., A. Smith, and K. Yang, 2002, in *Proceedings of the 17th Annual IEEE Conference on Computational Complexity, 2002, Montréal, Québec, Canada* (IEEE Computer Society, Baltimore, MD), pp. 103–112.
Amico, L., R. Fazio, A. Osterloh, and V. Vedral, 2008, Rev. Mod. Phys. **80**, 517.
Anders, J., D. Kaszlikowski, C. Lunkes, T. Ohshima, and V. Vedral, 2006, New J. Phys. **8**, 140.
Anders, S., M. B. Plenio, W. Dür, F. Verstraete, and H.-J. Briegel, 2006, Phys. Rev. Lett. **97**, 107206.
Aolita, L., and F. Mintert, 2006, Phys. Rev. Lett. **97**, 050501.
Ardehali, M., 1992, Phys. Rev. A **46**, 5375.
Ardehali, M., H. F. Chau, and H.-K. Lo, 1998, e-print arXiv:quant-ph/9803007.
Aschauer, H., and H. J. Briegel, 2002, Phys. Rev. Lett. **88**, 047902.
Aschauer, H., W. Dür, and H.-J. Briegel, 2005, Phys. Rev. A **71**, 012319.
Aspect, A., J. Dalibard, and G. Roger, 1982, Phys. Rev. Lett. **49**, 1804.
Aspect, A., P. Grangier, and G. Roger, 1981, Phys. Rev. Lett. **47**, 460.
Audenaert, K., B. De Moor, K. G. H. Vollbrecht, and R. F. Werner, 2002, Phys. Rev. A **66**, 032310.
Audenaert, K., J. Eisert, E. Jané, M. B. Plenio, S. Virmani, and B. De Moor, 2001, Phys. Rev. Lett. **87**, 217902.
Audenaert, K., M. B. Plenio, and J. Eisert, 2003, Phys. Rev. Lett. **90**, 027901.
Audenaert, K., F. Verstraete, and B. De Moor, 2001, Phys. Rev. A **64**, 052304.
Audenaert, K. M., and S. L. Braunstein, 2004, Commun. Math. Phys. **246**, 443.
Audenaert, K. M. R., and M. B. Plenio, 2006, New J. Phys. **8**, 266.
Augusiak, R., M. Demianowicz, and P. Horodecki, 2008, Phys. Rev. A **77**, 030301.
Augusiak, R., and P. Horodecki, 2006, Phys. Rev. A **74**, 010305.
Bądziag, P., C. Brukner, W. Laskowski, T. Paterek, and M. Żukowski, 2008, Phys. Rev. Lett. **100**, 140403.
Badziag, P., P. Deuar, M. Horodecki, P. Horodecki, and R. Horodecki, 2002, J. Mod. Opt. **49**, 1289.
Badziag, P., P. Horodecki, R. Horodecki, and R. Augusiak, 2007, e-print arXiv:quant-ph/0703097.
Badziag, P., M. Horodecki, A. Sen(De), and U. Sen, 2003, Phys. Rev. Lett. **91**, 117901.
Bae, J., M. Tiersch, S. Sauer, F. de Melo, F. Mintert, B. Hiesmayr, and A. Buchleitner, 2009, e-print arXiv:0902.4372.
Ballester, M. A., and S. Wehner, 2007, Phys. Rev. A **75**, 022319.
Ban, M., 2006, J. Phys. A **39**, 1927.
Bandyopadhyay, S., I. Chattopadhyay, V. Roychowdhury, and D. Sarkar, 2005, Phys. Rev. A **71**, 062317.
Bandyopadhyay, S., S. Ghosh, and V. Roychowdhury, 2005, Phys. Rev. A **71**, 012316.
Bandyopadhyay, S., and V. Roychowdhury, 2003, Phys. Rev. A **68**, 022319.
Barbieri, M., F. De Martini, G. Di Nepi, P. Mataloni, G. M. D'Ariano, and C. Macchiavello, 2003, Phys. Rev. Lett. **91**, 227901.
Barenco, A., and A. Ekert, 1995, J. Mod. Opt. **42**, 1253.
Barnett, S. M., and S. J. Phoenix, 1989, Phys. Rev. A **40**, 2404.
Barnum, H., E. Knill, and M. A. Nielsen, 2000, IEEE Trans. Inf. Theory **46**, 1317.
Barnum, H., and N. Linden, 2001, J. Phys. A **34**, 6787.
Barnum, H., M. A. Nielsen, and B. Schumacher, 1998, Phys. Rev. A **57**, 4153.
Barrett, J., L. Hardy, and A. Kent, 2005, Phys. Rev. Lett. **95**, 010503.
Barrett, J., A. Kent, and S. Pironio, 2006, Phys. Rev. Lett. **97**, 170409.
Barrett, M. D., J. Chiaverini, T. Schaetz, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, and D. J. Wineland, 2004, Nature (London) **429**, 737.
Baumgartner, B., B. Hiesmayr, and H. Narnhofer, 2006, e-print arXiv:quant-ph/0610100.
Beige, A., S. Bose, D. Braun, S. F. Huelga, P. L. Knight, M. B. Plenio, and V. Vedral, 2000, J. Mod. Opt. **47**, 2583.
Belinskii, A. V., and D. N. Klyshko, 1993, Phys. Usp. **163**, 1.
Bell, J. S., 1964, Physics (Long Island City, N.Y.) **1**, 195.
Benatti, F., R. Floreanini, and M. Piani, 2003, Phys. Rev. Lett. **91**, 070402.
Benatti, F., R. Floreanini, and M. Piani, 2004, Open Syst. Inf. Dyn. **11**, 325.
Bengtsson, I., and K. Życzkowski, 2006, *Geometry of Quantum States. An Introduction to Quantum Entanglement* (Cambridge University Press, Cambridge).
Bennett, C. H., 1992, Phys. Rev. Lett. **68**, 3121.
Bennett, C. H., 1998, Phys. Scr. **T76**, 210.
Bennett, C. H., H. J. Bernstein, S. Popescu, and B. Schumacher, 1996, Phys. Rev. A **53**, 2046.
Bennett, C. H., and G. Brassard, 1984, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Computer Society, New York, 1984), pp. 175–179.
Bennett, C. H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, 1993, Phys. Rev. Lett. **70**, 1895.
Bennett, C. H., G. Brassard, and N. D. Mermin, 1992, Phys. Rev. Lett. **68**, 557.
Bennett, C. H., G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, 1996, Phys. Rev. Lett. **76**, 722.
Bennett, C. H., D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, 1999, Phys. Rev. A **59**, 1070.
Bennett, C. H., D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, 1999, Phys. Rev. Lett. **82**, 5385.
Bennett, C. H., D. P. DiVincenzo, and J. A. Smolin, 1997, Phys. Rev. Lett. **78**, 3217.
Bennett, C. H., D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, 1996, Phys. Rev. A **54**, 3824.
Bennett, C. H., S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, 2000, Phys. Rev. A **63**, 012307.
Bennett, C. H., P. W. Shor, J. A. Smolin, and A. V. Thapliyal, 1999, Phys. Rev. Lett. **83**, 3081.
Bennett, C. H., P. W. Shor, J. A. Smolin, and A. V. Thapliyal, 2002, IEEE Trans. Inf. Theory **48**, 2637.
Bennett, C. H., and S. J. Wiesner, 1992, Phys. Rev. Lett. **69**, 2881.
Biham, E., G. Brassard, D. Kenigsberg, and T. Mor, 2004, Theor. Comput. Sci. **320**, 15.
Blaauboer, M., and D. P. DiVincenzo, 2005, Phys. Rev. Lett. **95**, 160402.
Blinov, B. B., D. L. Moehring, L. M. Duan, and C. Monroe, 2004, Nature (London) **428**, 153.
Bohm, D., 1951, *Quantum Theory* (Prentice Hall, Englewood Cliffs, NJ).
Bombin, H., and M. A. Martin-Delgado, 2006, Phys. Rev. Lett.

97, 180501.
Boschi, D., S. Branca, F. De Martini, L. Hardy, and S. Popescu, 1998, Phys. Rev. Lett. **80**, 1121.
Bose, S., P. L. Knight, M. B. Plenio, and V. Vedral, 1999, Phys. Rev. Lett. **83**, 5158.
Bose, S., M. B. Plenio, and V. Vedral, 2000, J. Mod. Opt. **47**, 291.
Bose, S., V. Vedral, and P. L. Knight, 1998, Phys. Rev. A **57**, 822.
Boto, A. N., P. Kok, D. S. Abrams, S. L. Braunstein, C. P. Williams, and J. P. Dowling, 2000, Phys. Rev. Lett. **85**, 2733.
Bourennane, M., M. Eibl, C. Kurtsiefer, S. Gaertner, O. G. H. Weinfurter, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera, 2004, Phys. Rev. Lett. **92**, 087902.
Bouwmeester, D., A. K. Ekert, and A. Zeilinger, 2000, *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation* (Springer, New York).
Bouwmeester, D., J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, 1997, Nature (London) **390**, 575.
Bovino, F. A., G. Castagnoli, A. Cabello, and A. Lamas-Linares, 2006, Phys. Rev. A **73**, 062110.
Bovino, F. A., G. Castagnoli, A. Ekert, P. Horodecki, C. M. Alves, and A. V. Sergienko, 2005, Phys. Rev. Lett. **95**, 240407.
Bovino, F. A., M. Giardina, K. Svozil, and V. Vedral, 2006, e-print arXiv:quant-ph/0603167.
Brandão, F. G., 2008, Ph.D. thesis, e-print arXiv:0810.0026.
Brandão, F. G. S. L., and M. B. Plenio, 2008, Nat. Phys. **4**, 873.
Brandão, F. G. S. L., 2005, Phys. Rev. A **72**, 022310.
Brandão, F. G. S. L., and R. O. Vianna, 2006, Int. J. Quantum Inf. **4**, 331.
Brassard, G., C. Crépeau, R. Jozsa, and D. Langlois, 1993, *Proceedings of the 34th Annual IEEE Sym-posium on the Foundations of Computer Science* (IEEE Computer Society, Los Alamitos), p. 362.
Braun, D., 2002, Phys. Rev. Lett. **89**, 277901.
Braunstein, S., and C. M. Caves, 1988, Phys. Rev. Lett. **61**, 662.
Braunstein, S. L., C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, 1999, Phys. Rev. Lett. **83**, 1054.
Braunstein, S. L., and H. J. Kimble, 1998, Phys. Rev. Lett. **80**, 869.
Braunstein, S. L., A. Mann, and M. Revzen, 1992, Phys. Rev. Lett. **68**, 3259.
Braunstein, S. L., and A. K. Pati, 2003, *Quantum Information with Continuous Variables* (Kluwer Academic, Dordrecht).
Breuer, H.-P., 2006a, Phys. Rev. Lett. **97**, 080501.
Breuer, H.-P., 2006b, J. Phys. A **39**, 11847.
Briand, E., J.-G. Luque, and J.-Y. Thibon, 2003, J. Phys. A **36**, 9915.
Briegel, H.-J., W. Dür, J. I. Cirac, and P. Zoller, 1998, Phys. Rev. Lett. **81**, 5932.
Briegel, H. J., and R. Raussendorf, 2001, Phys. Rev. Lett. **86**, 910.
Browne, D. E., and H. J. Briegel, 2006, e-print arXiv:quant-ph/0603226.
Brukner, C., N. Paunkovic, T. Rudolph, and V. Vedral, 2005, e-print arXiv:quant-ph/0509123.
Brukner, C., and V. Vedral, 2004, e-print arXiv:quant-ph/0406040.
Brukner, C., V. Vedral, and A. Zeilinger, 2006, Phys. Rev. A **73**, 012110.
Brukner, C., M. Żukowski, J.-W. Pan, and A. Zeilinger, 2004, Phys. Rev. Lett. **92**, 127901.
Brun, T. A., 2004, Quantum Inf. Comput. **4**, 401.
Brunner, N., N. Gisin, V. Scarani, and C. Simon, 2007, Phys. Rev. Lett. **98**, 220403.
Bruß, D., 1998, Phys. Rev. Lett. **81**, 3018.
Bruß, D., 2002, J. Math. Phys. **43**, 4237.
Bruß, D., J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera, 2002, J. Mod. Opt. **49**, 1399.
Bruß, D., G. M. D'Ariano, M. Lewenstein, C. Macchiavello, A. Sen(De), and U. Sen, 2005, e-print arXiv:quant-ph/0507146.
Bruß, D., and G. Leuchs, 2007, *Lectures on Quantum Information* (Wiley-VCH GmbH, Weinheim).
Bruß, D., and A. Peres, 2000, Phys. Rev. A **61**, 030301.
Buhrman, H., M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, 2006, Phys. Rev. Lett. **97**, 250501.
Buhrman, H., R. Cleve, and W. van Dam, 2001, SIAM J. Comput. **30**, 1829.
Buzek, V., V. Vedral, M. B. Plenio, P. L. Knight, and M. Hillery, 1997, Phys. Rev. A **55**, 3327.
Caban, P., and J. Rembieliński, 2005, Phys. Rev. A **72**, 012103.
Cabello, A., 2000, Phys. Rev. Lett. **85**, 5635.
Cabello, A., 2001a, Phys. Rev. Lett. **87**, 010403.
Cabello, A., 2001b, Phys. Rev. Lett. **86**, 1911.
Cabello, A., 2005, Phys. Rev. Lett. **95**, 210401.
Cabrillo, C., J. Cirac, P. García-Fernández, and P. Zoller, 1999, Phys. Rev. A **59**, 1025.
Calderbank, A. R., and P. W. Shor, 1996, Phys. Rev. A **54**, 1098.
Carteret, H. A., 2003, e-print arXiv:quant-ph/0309212.
Carteret, H. A., 2005, Phys. Rev. Lett. **94**, 040502.
Carvalho, A. R. R., F. Mintert, S. Palzer, and A. Buchleitner, 2005, e-print arXiv:quant-ph/0508114.
Cavalcanti, D., 2006, Phys. Rev. A **73**, 044302.
Cavalcanti, D., F. G. S. L. Brandão, and M. O. T. Cunha, 2006, New J. Phys. **8**, 260.
Cerf, N. J., and C. Adami, 1997, Phys. Rev. Lett. **79**, 5194.
Cerf, N. J., C. Adami, and R. M. Gingrich, 1999, Phys. Rev. A **60**, 898.
Cerf, N. J., S. Massar, and S. Pironio, 2002, Phys. Rev. Lett. **89**, 080402.
Cerf, N. J., S. Massar, and S. Schneider, 2002, Phys. Rev. A **66**, 042309.
Chattopadhyay, I., and D. Sarkar, 2006, e-print arXiv:quant-ph/0609050.
Chen, G., M.-M. He, J.-Q. Li, and J.-Q. Liang, 2006, Eur. Phys. J. B **51**, 25.
Chen, J.-L., C. Wu, L. C. Kwek, and C. H. Oh, 2004, Phys. Rev. Lett. **93**, 140407.
Chen, K., S. Albeverio, and S.-M. Fei, 2005a, Phys. Rev. Lett. **95**, 040504.
Chen, K., S. Albeverio, and S.-M. Fei, 2005b, Phys. Rev. Lett. **95**, 210501.
Chen, K., S. Albeverio, and S.-M. Fei, 2006, Phys. Rev. A **74**, 050101.
Chen, K., and H.-K. Lo, 2004, e-print arXiv:quant-ph/0404133.
Chen, K., and L.-A. Wu, 2003, Quantum Inf. Comput. **3**, 193.
Chen, Y.-X., and D. Yang, 2000, e-print arXiv:quant-ph/0006051.
Chen, Z.-B., Y.-A. Chen, and J.-W. Pan, 2005, e-print arXiv:quant-ph/0505178.
Chen, Z.-B., J.-W. Pan, Y.-D. Zhang, C. Brukner, and A. Zeilinger, 2003, Phys. Rev. Lett. **90**, 160408.
Chen, Z.-B., and Y.-D. Zhang, 2002, Phys. Rev. A **65**, 044102.
Choi, M.-D., 1972, Can. J. Math. **3**, 520.
Choi, M.-D., 1982, Proc. Symp. Pure Math. **38**, 583.

Christandl, M., 2006, Ph.D. thesis, University of Cambridge, Cambridge, England.
Christandl, M., A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, 2007, in *Proceedings of the 4th Theory of Cryptography Conference*, Lecture Notes in Computer Science, Vol. 4392, pp. 456–478.
Christandl, M., and A. Winter, 2004, J. Math. Phys. **45**, 829.
Christandl, M., and A. Winter, 2005, IEEE Trans. Inf. Theory **51**, 3159.
Chruściński, D., and A. Kossakowski, 2006, e-print arXiv:quant-ph/0606211.
Cinelli, C., M. Barbieri, R. Perris, P. Mataloni, and F. De Martini, 2005, Phys. Rev. Lett. **95**, 240405.
Cirac, J. I., W. Dür, B. Kraus, and M. Lewenstein, 2001, Phys. Rev. Lett. **86**, 544.
Cirac, J. I., and P. Zoller, 2004, Phys. Today **57** (3), 38.
Cirel'son, B. S., 1980, Lett. Math. Phys. **4**, 93.
Clarisse, L., 2005, Phys. Rev. A **71**, 032332.
Clarisse, L., 2006a, Quantum Inf. Comput. **6**, 539.
Clarisse, L., 2006b, Ph.D. thesis, University of York.
Clarisse, L., and P. Wocjan, 2006, Quantum Inf. Comput. **6**, 277.
Clauser, J. F., M. A. Horne, A. Shimony, and R. A. Holt, 1969, Phys. Rev. Lett. **23**, 880.
Cleve, R., and H. Buhrman, 1997, e-print arXiv:quant-ph/9704026.
Cleve, R., P. Hoyer, B. Toner, and J. Watrous, 2004, e-print arXiv:quant-ph/0404076.
Clifton, R., 2000, Phys. Lett. A **271**, 1.
Clifton, R., and H. Halvorson, 1999, Phys. Rev. A **61**, 012108.
Coffman, V., J. Kundu, and W. K. Wootters, 2000, Phys. Rev. A **61**, 052306.
Collins, D., N. Linden, and S. Popescu, 2001, Phys. Rev. A **64**, 032302.
Collins, D., and S. Popescu, 2002, Phys. Rev. A **65**, 032321.
Cover, T. M., and J. A. Thomas, 1991, *Elements of Information Theory* (Wiley, New York).
Csiszár, I., and J. Körner, 1978, IEEE Trans. Inf. Theory **24**, 339.
Curty, M., O. Gühne, M. Lewenstein, and N. Lütkenhaus, 2005, Phys. Rev. A **71**, 022306.
Curty, M., M. Lewenstein, and N. Lütkenhaus, 2004, Phys. Rev. Lett. **92**, 217903.
Czachor, M., 1997, Phys. Rev. A **55**, 72.
Czekaj, Ł., and P. Horodecki, 2009, Phys. Rev. Lett. **102**, 110505.
D'Ariano, G. M., D. Kretschmann, D. Schlingemann, and R. F. Werner, 2007, Phys. Rev. A **76**, 032328.
Datta, A., S. T. Flammia, and C. M. Caves, 2005, Phys. Rev. A **72**, 042316.
Datta, A., S. T. Flammia, A. Shaji, and C. M. Caves, 2006, e-print arXiv:quant-ph/0608086.
Datta, A., S. T. Flammia, A. Shaji, and C. M. Caves, 2007, Phys. Rev. A **75**, 062117.
Datta, A., and G. Vidal, 2007, Phys. Rev. A **75**, 042310.
Dawson, C. M., and M. A. Nielsen, 2004, Phys. Rev. A **69**, 052316.
Degiovanni, I. P., I. R. Berchera, S. Castelletto, M. L. Rastello, F. A. Bovino, A. M. Colla, and G. Castagnoli, 2003, e-print arXiv:quant-ph/0312128.
Degiovanni, I. P., I. R. Berchera, S. Castelletto, M. L. Rastello, F. A. Bovino, A. M. Colla, and G. Castagnoli, 2004, e-print arXiv:quant-ph/0410221.
Dehaene, J., M. Van den Nest, B. D. Moor, and F. Verstraete, 2003, Phys. Rev. A **67**, 022310.
Demkowicz-Dobrzański, R., A. Buchleitner, M. Kuś, and F. Mintert, 2006, Phys. Rev. A **74**, 052303.
Deutsch, D., 1985, Proc. R. Soc. London, Ser. A **400**, 97.
Deutsch, D., A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, 1996, Phys. Rev. Lett. **77**, 2818.
Devetak, I., 2003, arXiv:quant-ph/0304127.
Devetak, I., and A. Winter, 2004, Phys. Rev. Lett. **93**, 080501.
Devetak, I., and A. Winter, 2005, Proc. R. Soc. London, Ser. A **461**, 207.
Devi, A. R. U., R. Prabhu, and A. K. Rajagopal, 2007, Phys. Rev. Lett. **98**, 060501.
Dieks, D., 1982, Phys. Lett. **92A**, 271.
Diósi, L., 2003, *Lecture Notes in Physics* (Springer, Berlin), Vol. 622, pp. 157–163.
DiVincenzo, D. P., M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, 2004, Phys. Rev. Lett. **92**, 067902.
DiVincenzo, D. P., T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, 2003, Commun. Math. Phys. **238**, 379.
DiVincenzo, D. P., P. W. Shor, and J. A. Smolin, 1998, Phys. Rev. A **57**, 830.
DiVincenzo, D. P., P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, 2000, Phys. Rev. A **61**, 062312.
DiVincenzo, D. P., B. M. Terhal, and A. V. Thapliyal, 2000, J. Mod. Opt. **47**, 377.
Djokovic, D. Z., 2006, e-print arXiv:quant-ph/0604190.
Dodd, P. J., and J. J. Halliwell, 2004, Phys. Rev. A **69**, 052105.
Doherty, A. C., P. A. Parrilo, and F. M. Spedalieri, 2002, Phys. Rev. Lett. **88**, 187904.
Doherty, A. C., P. A. Parrilo, and F. M. Spedalieri, 2004, Phys. Rev. A **69**, 022308.
Doherty, A. C., P. A. Parrilo, and F. M. Spedalieri, 2005, Phys. Rev. A **71**, 032333.
Donald, M. J., M. Horodecki, and O. Rudolph, 2002, J. Math. Phys. **43**, 4252.
Duan, L.-M., G. Giedke, J. I. Cirac, and P. Zoller, 2000, Phys. Rev. Lett. **84**, 2722.
Dür, W., 2001, Phys. Rev. Lett. **87**, 230402.
Dür, W., H. Aschauer, and H.-J. Briegel, 2003, Phys. Rev. Lett. **91**, 107903.
Dür, W., H.-J. Briegel, J. I. Cirac, and P. Zoller, 1999, Phys. Rev. A **59**, 169.
Dür, W., and J. I. Cirac, 2000a, Phys. Rev. A **62**, 022302.
Dür, W., and J. I. Cirac, 2000b, Phys. Rev. A **61**, 042314.
Dür, W., and J. I. Cirac, 2000c, J. Mod. Opt. **47**, 247.
Dür, W., J. I. Cirac, and P. Horodecki, 2004, Phys. Rev. Lett. **93**, 020503.
Dür, W., J. I. Cirac, M. Lewenstein, and D. Bruß, 2000, Phys. Rev. A **61**, 062313.
Dür, W., J. I. Cirac, and R. Tarrach, 1999, Phys. Rev. Lett. **83**, 3562.
Dür, W., L. Hartmann, M. Hein, M. Lewenstein, and H.-J. Briegel, 2005, Phys. Rev. Lett. **94**, 097203.
Dür, W., G. Vidal, and J. I. Cirac, 2000, Phys. Rev. A **62**, 062314.
Durt, T., D. Kaszlikowski, and M. Żukowski, 2001, Phys. Rev. A **64**, 024101.
Eckert, K., O. Gühne, F. Hulpke, P. Hyllus, J. Korbicz, J. Mompart, D. Bruß, M. Lewenstein, and A. Sanpera, 2003, *Entanglement Properties of Composite Quantum Systems*, edited by Gerd Leuchs and Thomas Beth (Wiley-VCH, Weinheim).
Eckert, K., J. Schliemann, D. Bruß, and M. Lewenstein, 2002,

Ann. Phys. (N.Y.) **299**, 88.
Eggeling, T., K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf, 2001, Phys. Rev. Lett. **87**, 257902.
Eggeling, T., and R. F. Werner, 2001, Phys. Rev. A **63**, 042111.
Einstein, A., B. Podolsky, and N. Rosen, 1935, Phys. Rev. **47**, 777.
Eisenberg, H. S., J. F. Hodelin, G. Khoury, and D. Bouwmeester, 2005, Phys. Rev. Lett. **94**, 090502.
Eisert, J., F. G. S. L. Brandão, and K. M. R. Audenaert, 2007, New J. Phys. **9**, 46.
Eisert, J., and H. J. Briegel, 2001, Phys. Rev. A **64**, 022306.
Eisert, J., T. Felbinger, P. Papadopoulos, M. B. Plenio, and M. Wilkens, 2000, Phys. Rev. Lett. **84**, 1611.
Eisert, J., and D. Gross, 2007, in *Lectures on Quantum Information*, edited by D. Bruß and G. Leuchs (Wiley-VCH, Weinheim).
Eisert, J., P. Hyllus, O. Gühne, and M. Curty, 2004, Phys. Rev. A **70**, 062317.
Eisert, J., K. Jacobs, P. Papadopoulos, and M. B. Plenio, 2000, Phys. Rev. A **62**, 052317.
Eisert, J., and M. B. Plenio, 1999, J. Mod. Opt. **46**, 145.
Eisert, J., S. Scheel, and M. B. Plenio, 2002, Phys. Rev. Lett. **89**, 137903.
Eisert, J., C. Simon, and M. B. Plenio, 2002, J. Phys. A **35**, 3911.
Eisert, J., and M. Wilkens, 2000, Phys. Rev. Lett. **85**, 437.
Ekert, A., and R. Jozsa, 1998, e-print arXiv:quant-ph/9803072.
Ekert, A. K., 1991, Phys. Rev. Lett. **67**, 661.
Ekert, A. K., C. M. Alves, D. K. L. Oi, M. Horodecki, P. Horodecki, and L. C. Kwek, 2002, Phys. Rev. Lett. **88**, 217901.
Emary, C., B. Trauzettel, and C. W. J. Beenakker, 2005, Phys. Rev. Lett. **95**, 127401.
Fan, H., K. Matsumoto, and H. Imai, 2003, J. Phys. A **36**, 4151.
Fang, X., X. Zhu, M. Feng, X. Mao, and F. Du, 2000, Phys. Rev. A **61**, 022307.
Fannes, M., J. T. Lewis, and A. Verbeure, 1988, Lett. Math. Phys. **15**, 255.
Fasel, S., F. Robin, E. Moreno, D. Erni, N. Gisin, and H. Zbinden, 2005, Phys. Rev. Lett. **94**, 110501.
Fei, S.-M., and X. Li-Jost, 2006, Phys. Rev. A **73**, 024302.
Ferraro, A., S. Olivares, and M. G. A. Paris, 2005, *Gaussian States in Continuous Variable Quantum Information. Lecture Notes* (Bibliopolis, Napoli).
Feynman, R. P., 1982, Int. J. Theor. Phys. **21**, 467.
Ficek, Z., and R. Tanaś, 2006, Phys. Rev. A **74**, 024304.
Filip, R., 2002, Phys. Rev. A **65**, 062320.
Fine, A., 1982, Phys. Rev. Lett. **48**, 291.
Fitzi, M., N. Gisin, and U. Maurer, 2001, e-print arXiv:quant-ph/0107127.
Fiurásek, J., 2002a, Phys. Rev. Lett. **89**, 137904.
Fiurásek, J., 2002b, Phys. Rev. A **66**, 052315.
Fiurásek, J., and N. J. Cerf, 2004, Phys. Rev. Lett. **93**, 063601.
Freedman, S. J., and J. F. Clauser, 1972, Phys. Rev. Lett. **28**, 938.
Fuchs, C. A., and J. van de Graaf, 1997, e-print arXiv:quant-ph/9712042.
Fukuda, M., and M. M. Wolf, 2007, J. Math. Phys. **48**, 072101.
Furusawa, A., J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, 1998, Science **282**, 706.
Gaertner, S., M. Bourennane, Ch. Kurtsiefer, A. Cabello, and H. Weinfurter, 2008, Phys. Rev. Lett. **100**, 070504.
Ghosh, S., G. Kar, A. Roy, A. Sen(De), and U. Sen, 2001, Phys. Rev. Lett. **87**, 277902.
Giedke, G., and I. J. Cirac, 2002, Phys. Rev. A **66**, 032316.
Giedke, G., L.-M. Duan, J. I. Cirac, and P. Zoller, 2000, e-print arXiv:quant-ph/0007061.
Giedke, G., L.-M. Duan, J. I. Cirac, and P. Zoller, 2001, Quantum Inf. Comput. **1**, 79.
Giedke, G., B. Kraus, M. Lewenstein, and J. I. Cirac, 2001, Phys. Rev. Lett. **87**, 167904.
Giedke, G., M. M. Wolf, O. Krüger, R. F. Werner, and J. I. Cirac, 2003, Phys. Rev. Lett. **91**, 107901.
Gill, R. D., 2003, in *Foundations of Probability and Physics 2 (Växi, 2002)*, Math. Model. Phys. Eng. and Cogn. Sci. (Växiö University Press, Växiö), Vol. 5, pp. 179–206.
Giovannetti, V., S. Lloyd, and L. Maccone, 2004, Science **306**, 1330.
Giovannetti, V., S. Mancini, D. Vitali, and P. Tombesi, 2003, Phys. Rev. A **67**, 022320.
Gisin, N., 1991, Phys. Lett. A **154**, 201.
Gisin, N., 1996, Phys. Lett. A **210**, 151.
Gisin, N., 2005, e-print arXiv:quant-ph/0512168.
Gisin, N., 2007, e-print arXiv:quant-ph/0702021.
Gisin, N., and N. Brunner, 2003, in *Quantum Entanglement and Information Processing: Lecture Notes of the Les Houches Summer School 2003* (Daniel Esteve, Les Houches).
Gisin, N., and A. Peres, 1992, Phys. Lett. A **162**, 15.
Gisin, N., and S. Wolf, 1999, Phys. Rev. Lett. **83**, 4200.
Gisin, N., and S. Wolf, 2000, e-print arXiv:quant-ph/0005042.
Glancy, S., E. Knill, and H. M. Vasconcelos, 2006, Phys. Rev. A **74**, 032319.
Gottesman, D., 1997, Ph.D. thesis, Caltech.
Gottesman, D., 2005, private communication.
Gottesman, D., and I. L. Chuang, 1999, Nature (London) **402**, 390.
Gottesman, D., and H.-K. Lo, 2003, IEEE Trans. Inf. Theory **49**, 457.
Gottesman, D., and J. Preskill, 2001, Phys. Rev. A **63**, 022309.
Gour, G., 2005, Phys. Rev. A **71**, 012318.
Grabowski, J., M. Kuś, and G. Marmo, 2005, J. Phys. A **38**, 10217.
Grassl, M., M. Rötteler, and T. Beth, 1998, Phys. Rev. A **58**, 1833.
Greenberger, D. M., M. A. Horne, and A. Zeilinger, 1989, *Going Beyond Bell's Theorem in Bell's Theorem, Quantum Theory, and Conceptions of the Universe* (Kluwer Academic, Dordrecht).
Greenberger, D., M. Horne, and A. Zeilinger, 2005a, e-print arXiv:quant-ph/0510207.
Greenberger, D. M., M. Horne, and A. Zeilinger, 2005b, e-print arXiv:quant-ph/0510201.
Groeblacher, S., T. Paterek, R. Kaltenbaek, C. Brukner, M. Żukowski, M. Aspelmeyer, and A. Zeilinger, 2007, Nature (London) **446**, 871.
Groisman, B., N. Linden, and S. Popescu, 2005, Phys. Rev. A **72**, 062322.
Gross, D., K. Audenaert, and J. Eisert, 2007, J. Math. Phys. **48**, 052104.
Gross, D., and J. Eisert, 2007, Phys. Rev. Lett. **98**, 220503.
Grover, L. K., 1997, e-print arXiv:quant-ph/9704012.
Grudka, A., M. Horodecki, P. Horodecki, R. Horodecki, and M. Piani, 2007, e-print arXiv:quant-ph/0703095.
Gühne, O., 2004, Phys. Rev. Lett. **92**, 117903.
Gühne, O., P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, 2003, J. Mod. Opt. **50**, 1079.
Gühne, O., P. Hyllus, O. Gittsovich, and J. Eisert, 2007, Phys.

Rev. Lett. **99**, 130504.
Gühne, O., and M. Lewenstein, 2004a, Phys. Rev. A **70**, 022316.
Gühne, O., and M. Lewenstein, 2004b, in *Quantum Communication, Measurement and Computing*, edited by S. M. Barnett, E. Andersson, J. Jeffers, P. Öhberg, and O. Hirota, AIP Conf. Proc. No. 734 (AIP, Melville, NY), p. 230.
Gühne, O., and N. Lütkenhaus, 2006, Phys. Rev. Lett. **96**, 170502.
Gühne, O., and N. Lütkenhaus, 2007, J. Phys.: Conf. Ser. **67**, 012004.
Gühne, O., M. Mechler, G. Tóth, and P. Adam, 2006, Phys. Rev. A **74**, 010301(R).
Gühne, O., M. Reimpell, and R. F. Werner, 2007, Phys. Rev. Lett. **98**, 110502.
Gurvits, L., 2002, e-print arXiv:quant-ph/0201022.
Gurvits, L., 2003, *Proceedings of the Thirty-Fifth ACM Symposium on Theory of Computing* (University of Nevada, Las Vegas, NV), p. 10.
Gurvits, L., 2004, Special issue: STOC 2003 69, 448.
Gurvits, L., and H. Barnum, 2002, Phys. Rev. A **66**, 062311.
Gurvits, L., and H. Barnum, 2003, Phys. Rev. A **68**, 042312.
Gurvits, L., and H. Barnum, 2005, Phys. Rev. A **72**, 032322.
Häffner, H., W. Hänsel, C. F. Roos, J. Benhelm, D. C. al kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt, 2005, Nature (London) **438**, 643.
Häffner, H., F. Schmidt-Kaler, W. Hänsel, C. F. Roos, T. Körber, M. Chwalla, M. Riebe, J. Benhelm, U. D. Rapol, C. Becher, and R. Blatt, 2005, Appl. Phys. B: Lasers Opt. **81**, 151.
Hald, J., J. L. Sørensen, C. Schori, and E. S. Polzik, 1999, Phys. Rev. Lett. **83**, 1319.
Hall, W., 2006, e-print arXiv:quant-ph/0607035.
Hardy, L., 1993, Phys. Rev. Lett. **71**, 1665.
Harrow, A., D. Leung, and P. W. Shor, 2007, private communication.
Harrow, A. W., and M. A. Nielsen, 2003, Phys. Rev. A **68**, 012308.
Harrow, A. W., and P. W. Shor, 2005, e-print arXiv:quant-ph/0511219.
Hasegawa, Y., R. Loidl, G. Badurek, M. Baron, and H. Rauch, 2004, J. Opt. B: Quantum Semiclassical Opt. **6**, S7.
Hastings, M. B., 2008, e-print arXiv:0809.3972.
Hausladen, P., R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, 1996, Phys. Rev. A **54**, 1869.
Hayden, P. M., M. Horodecki, and B. M. Terhal, 2001, J. Phys. A **34**, 6891.
Hayden, P., and A. Winter, 2008, Commun. Math. Phys. **284**, 263.
Hein, M., W. Dür, J. Eisert, R. Raussendorf, M. V. den Nest, and H.-J. Briegel, 2005, in *Quantum Computers, Algorithms and Chaos*, Vol. 162 of Proceedings of the International School of Physics Enrico Fermi, edited by G. Casati, D. L. Shepelyansky, P. Zoller, and G. Benenti (IOS, Amsterdam).
Heydari, H., 2006, J. Phys. A **39**, 15225.
Hildebrand, R., 2005, e-print arXiv:quant-ph/0502170.
Hill, S., and W. K. Wootters, 1997, Phys. Rev. Lett. **78**, 5022.
Hillery, M., V. Buzek, and A. Berthiaume, 1999, Phys. Rev. A **59**, 1829.
Hillery, M., and M. S. Zubairy, 2006, Phys. Rev. Lett. **96**, 050503.
Hiroshima, T., 2001, J. Phys. A **34**, 6907.
Hiroshima, T., 2003, Phys. Rev. Lett. **91**, 057902.
Hiroshima, T., G. Adesso, and F. Illuminati, 2007, Phys. Rev. Lett. **98**, 050503.
Hofmann, H. F., 2003, Phys. Rev. A **68**, 034307.
Hofmann, H. F., and S. Takeuchi, 2003, Phys. Rev. A **68**, 032103.
Holevo, A. S., 1973, Probl. Peredachi Inf. **9**, 3.
Horodecki, K., M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, 2008, Phys. Rev. Lett. **100**, 110502.
Horodecki, K., M. Horodecki, P. Horodecki, and J. Oppenheim, 2005a, Found. Phys. **35**, 2027.
Horodecki, K., M. Horodecki, P. Horodecki, and J. Oppenheim, 2005b, Phys. Rev. Lett. **94**, 200501.
Horodecki, K., M. Horodecki, P. Horodecki, and J. Oppenheim, 2005c, Phys. Rev. Lett. **94**, 160502.
Horodecki, K., M. Horodecki, P. Horodecki, and J. Oppenheim, 2009 IEEE Trans. Inf. Theory **55**, 1898.
Horodecki, K., D. Leung, H.-K. Lo, and J. Oppenheim, 2006, Phys. Rev. Lett. **96**, 070501.
Horodecki, K., L. Pankowski, M. Horodecki, and P. Horodecki, 2008, IEEE Trans. Inf. Theory **54**, 2621.
Horodecki, M., 2001, Quantum Inf. Comput. **1**, 3.
Horodecki, M., 2005, Open Syst. Inf. Dyn. **12**, 231.
Horodecki, M., 2008, Am. J. Chin. Med. **4**, 833.
Horodecki, M., and P. Horodecki, 1999, Phys. Rev. A **59**, 4206.
Horodecki, M., P. Horodecki, and R. Horodecki, 1996, Phys. Lett. A **223**, 1.
Horodecki, M., P. Horodecki, and R. Horodecki, 1997, Phys. Rev. Lett. **78**, 574.
Horodecki, M., P. Horodecki, and R. Horodecki, 1998, Phys. Rev. Lett. **80**, 5239.
Horodecki, M., P. Horodecki, and R. Horodecki, 1999, Phys. Rev. A **60**, 1888.
Horodecki, M., P. Horodecki, and R. Horodecki, 2000a, Phys. Rev. Lett. **84**, 4260.
Horodecki, M., P. Horodecki, and R. Horodecki, 2000b, Phys. Rev. Lett. **84**, 2014.
Horodecki, M., P. Horodecki, and R. Horodecki, 2000c, Phys. Rev. Lett. **85**, 433.
Horodecki, M., P. Horodecki, and R. Horodecki, 2001, Phys. Lett. A **283**, 1.
Horodecki, M., P. Horodecki, and R. Horodecki, 2006, Open Syst. Inf. Dyn. **13**, 103.
Horodecki, M., J. Oppenheim, and R. Horodecki, 2002, Phys. Rev. Lett. **89**, 240403.
Horodecki, M., J. Oppenheim, and A. Winter, 2005, Nature (London) **436**, 673.
Horodecki, M., J. Oppenheim, and A. Winter, 2007, Commun. Math. Phys. **269**, 107.
Horodecki, M., P. W. Shor, and M. B. Ruskai, 2003, Rev. Math. Phys. **15**, 629.
Horodecki, P., 1997, Phys. Lett. A **232**, 333.
Horodecki, P., 2001a, in *Proceedings of NATO ARW: Decoherence and its Implications in Quantum Computation and Information Transfer*, edited by T. Gonis, and P. E. A. Turchi, Series III: Comp., and Sci. Syst. (IOS, Amsterdam), p. 299.
Horodecki, P., 2001b, Phys. Rev. A **63**, 022108.
Horodecki, P., 2003a, Phys. Lett. A **1**, 319.
Horodecki, P., 2003b, Phys. Rev. A **68**, 052101.
Horodecki, P., 2003c, Phys. Rev. A **67**, 060101.
Horodecki, P., 2003d, Phys. Rev. Lett. **90**, 167901.
Horodecki, P., 2003e, Cent. Eur. J. Phys. **1**, 695.
Horodecki, P., and R. Augusiak, 2006, Phys. Rev. A **74**, 010302.

Horodecki, P., R. Augusiak, and M. Demianowicz, 2006, Phys. Rev. A **74**, 052323.
Horodecki, P., J. I. Cirac, and M. Lewenstein, 2003, in *Quantum Information with Continuous Variables*, edited by S. L. Braunstein and A. K. Pati (Kluwer Academic, Dordrecht), p. 211.
Horodecki, P., and A. Ekert, 2002, Phys. Rev. Lett. **89**, 127902.
Horodecki, P., M. Horodecki, and R. Horodecki, 1999, Phys. Rev. Lett. **82**, 1056.
Horodecki, P., M. Horodecki, and R. Horodecki, 2000, J. Mod. Opt. **47**, 347.
Horodecki, P., and R. Horodecki, 1994, Phys. Lett. A **194**, 147.
Horodecki, P., R. Horodecki, and M. Horodecki, 1998, Acta Phys. Slov. **48**, 141.
Horodecki, P., and M. Lewenstein, 2000, Phys. Rev. Lett. **85**, 2657.
Horodecki, P., M. Lewenstein, G. Vidal, and I. Cirac, 2000, Phys. Rev. A **62**, 032310.
Horodecki, P., J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, 2003, Theor. Comput. Sci. **292**, 589.
Horodecki, R., and M. Horodecki, 1996, Phys. Rev. A **54**, 1838.
Horodecki, R., M. Horodecki, and P. Horodecki, 1999, Phys. Rev. A **59**, 1799.
Horodecki, R., M. Horodecki, and P. Horodecki, 2001, Phys. Rev. A **63**, 022310.
Horodecki, R., P. Horodecki, and M. Horodecki, 1995, Phys. Lett. A **200**, 340.
Horodecki, R., P. Horodecki, and M. Horodecki, 1996, Phys. Lett. A **210**, 377.
Horodecki, R., P. Horodecki, M. Horodecki, and K. Horodecki, e-print arXiv:quant-ph/0702225.
Hostens, E., J. Dehaene, and B. De Moor, 2004, e-print arXiv:quant-ph/0406017.
Hostens, E., J. Dehaene, and B. De Moor, 2006a, Phys. Rev. A **73**, 062337.
Hostens, E., J. Dehaene, and B. De Moor, 2006b, Phys. Rev. A **73**, 042316.
Hostens, E., J. Dehaene, and B. De Moor, 2006c, Phys. Rev. A **74**, 062318.
Huelga, S. F., C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac, 1997, Phys. Rev. Lett. **79**, 3865.
Hulpke, F., and D. Bruß, 2005, J. Phys. A **38**, 5573.
Hyllus, P., C. M. Alves, D. Bruß, and C. Macchiavello, 2004, Phys. Rev. A **70**, 032316.
Hyllus, P., and J. Eisert, 2006, New J. Phys. **8**, 51.
Hyllus, P., O. Gühne, D. Bruß, and M. Lewenstein, 2005, Phys. Rev. A **72**, 012321.
Ioannou, L. M., 2007, Quantum Inf. Comput. **7**, 335.
Ioannou, L. M., and B. C. Travaglione, 2006, Phys. Rev. A **73**, 052314.
Ioannou, L. M., B. C. Travaglione, D. Cheung, and A. K. Ekert, 2004, Phys. Rev. A **70**, 060303.
Ishizaka, S., 2004, Phys. Rev. Lett. **93**, 190501.
Jafarizadeh, M. A., G. Najarbashi, and H. Habibian, 2006, e-print arXiv:quant-ph/0611256.
Jakóbczyk, L., and A. Jamróz, 2004, Phys. Lett. A **333**, 35.
Jamiołkowski, A., 1972, Rep. Math. Phys. **3**, 275.
Jennewein, T., C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, 2000, Phys. Rev. Lett. **84**, 4729.
Jennewein, T., G. Weihs, J.-W. Pan, and A. Zeilinger, 2001, Phys. Rev. Lett. **88**, 017903.
Jing, J., Z. Jing, Y. Ying, Z. Fagang, X. Changde, and P. Kunchi, 2003, Phys. Rev. Lett. **90**, 167903.
Jonathan, D., and M. B. Plenio, 1999, Phys. Rev. Lett. **83**, 3566.
Jordan, T. F., A. Shaji, and E. C. G. Sudarshan, 2006, e-print arXiv:quant-ph/0608061.
Jordan, T. F., A. Shaji, and E. C. G. Sudarshan, 2007, e-print arXiv:0704.0461.
Jozsa, R., 1994, J. Mod. Opt. **41**, 2315.
Jozsa, R., 1997, e-print arXiv:quant-ph/9707034.
Jozsa, R., 1999, Chaos, Chaos, Solitons Fractals **10**, 1657.
Jozsa, R., D. S. Abrams, J. P. Dowling, and C. P. Williams, 2000, Phys. Rev. Lett. **85**, 2010.
Jozsa, R., and N. Linden, 2002, e-print arXiv:quant-ph/0201143.
Julsgaard, B., A. Kozhekin, and E. S. Polzik, 2001, Nature (London) **413**, 400.
Julsgaard, B., J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik, 2004, Nature (London) **432**, 482.
Karnas, S., and M. Lewenstein, 2000, e-print arXiv:quant-ph/0011066.
Kaszlikowski, D., P. Gnaciński, M. Żukowski, W. Miklaszewski, and A. Zeilinger, 2000, Phys. Rev. Lett. **85**, 4418.
Kay, A., J. K. Pachos, W. Dür, and H. J. Briegel, 2006, New J. Phys. **8**, 147.
Kendon, V. M., and W. J. Munro, 2006, Quantum Inf. Comput. **6**, 630.
Kendon, V. M., K. Życzkowski, and W. J. Munro, 2002, Phys. Rev. A **66**, 062310.
Kenigsberg, D., T. Mor, and G. Ratsaby, 2006, Quantum Inf. Comput. **6**, 606.
Keyl, M., D. Schlingemann, and R. F. Werner, 2002, e-print arXiv:quant-ph/0212014.
Kiesel, N., C. Schmid, U. Weber, G. Tóth, O. Gühne, R. Ursin, and H. Weinfurter, 2005, Phys. Rev. Lett. **95**, 210502.
Kim, M. S., J. Lee, D. Ahn, and P. L. Knight, 2002, Phys. Rev. A **65**, 040101.
Kitaev, A., and J. Preskill, 2006, Phys. Rev. Lett. **96**, 110404.
Knill, E., 2001, e-print arXiv:quant-ph/0108033.
Knill, E., 2004, e-print arXiv:quant-ph/0410199.
Knill, E., R. Laflamme, and G. J. Milburn, 2001, Nature (London) **409**, 46.
Koashi, M., and A. Winter, 2004, Phys. Rev. A **69**, 022309.
Kocher, C. A., and E. D. Commins, 1967, Phys. Rev. Lett. **18**, 575.
Koenig, R., and R. Renner, 2005, J. Math. Phys. **46**, 122108.
Koenig, R., R. Renner, A. Bariska, and U. Maurer, 2005, e-print arXiv:quant-ph/0512021.
Korbicz, J. K., and M. Lewenstein, 2006, Phys. Rev. A **74**, 022318.
Kossakowski, A., 2003, e-print arXiv:quant-ph/0307132.
Kraus, B., J. I. Cirac, S. Karnas, and M. Lewenstein, 2000, Phys. Rev. A **61**, 062302.
Kraus, B., N. Gisin, and R. Renner, 2005, Phys. Rev. Lett. **95**, 080501.
Kraus, B., M. Lewenstein, and J. I. Cirac, 2002, Phys. Rev. A **65**, 042327.
Kraus, K., 1983, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer-Verlag, Berlin).
Kretschmann, D., and R. F. Werner, 2004, New J. Phys. **6**, 26.
Kruszyńska, C., A. Miyake, H. J. Briegel, and W. Dür, 2006, Phys. Rev. A **74**, 052316.
Kuś, M., and K. Życzkowski, 2001, Phys. Rev. A **63**, 032307.
Kuzmich, A., and E. S. Polzik, 2000, Phys. Rev. Lett. **85**, 5639.
Kwiat, P. G., K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, 1995, Phys. Rev. Lett. **75**, 4337.

Lamata, L., J. J. García-Ripoll, and J. I. Cirac, 2007, Phys. Rev. Lett. **98**, 010502.
Lambert, N., C. Emary, and T. Brandes, 2004, Phys. Rev. Lett. **92**, 073602.
Larsson, D., and H. Johannesson, 2006, Phys. Rev. A **73**, 042320.
Laskowski, W., T. Paterek, M. Żukowski, and C. Brukner, 2004, Phys. Rev. Lett. **93**, 200401.
Lastra, F., G. Romero, C. E. López, M. F. Santos, and J. Retamal, 2007, e-print arXiv:quant-ph/0702246.
Latorre, J. I., E. Rico, and G. Vidal, 2004, Quantum Inf. Comput. **4**, 48.
Leggett, A. J., 2003, Found. Phys. **33**, 1469.
Leibfried, D., *et al.*, 2005, Nature (London) **438**, 639.
Levay, P., 2006, J. Phys. A **39**, 9533.
Levin, M., and X.-G. Wen, 2006, Phys. Rev. Lett. **96**, 110405.
Lewenstein, M., B. Kraus, J. I. Cirac, and P. Horodecki, 2000, Phys. Rev. A **62**, 052310.
Lewenstein, M., B. Kraus, P. Horodecki, and J. I. Cirac, 2001, Phys. Rev. A **63**, 044304.
Lewenstein, M., and A. Sanpera, 1998, Phys. Rev. Lett. **80**, 2261.
Li, Y. S., B. Zeng, X. S. Liu, and G. L. Long, 2001, Phys. Rev. A **64**, 054302.
Linden, N., and S. Popescu, 1998, Fortschr. Phys. **46**, 567.
Linden, N., S. Popescu, B. Schumacher, and M. Westmoreland, 1999, e-print arXiv:quant-ph/9912039.
Linden, N., S. Popescu, and A. Sudbery, 1999, Phys. Rev. Lett. **83**, 243.
Linden, N., J. A. Smolin, and A. Winter, 2005, e-print arXiv:quant-ph/0511217.
Lindner, N. H., J. Avron, N. Akopian, and D. Gershoni, 2006, e-print arXiv:quant-ph/0601200.
Lloyd, S., 1997, Phys. Rev. A **55**, 1613.
Lo, H.-K., and H. F. Chau, 1997, Phys. Rev. Lett. **78**, 3410.
Lo, H.-K., and H. F. Chau, 1998, Physica D **120**, 177.
Lo, H.-K., and H. F. Chau, 1999, Science **283**, 2050.
Lo, H.-K., and S. Popescu, 1999, Phys. Rev. Lett. **83**, 1459.
Lo, H.-K., and S. Popescu, 2001, Phys. Rev. A **63**, 022301.
Lo, H.-K., T. Spiller, and S. Popescu, 1999, *Introduction to Quantum Computation and Information* (World Scientific, Singapore).
Lohmayer, R., A. Osterloh, J. Siewert, and A. Uhlmann, 2006, Phys. Rev. Lett. **97**, 260502.
Long, G. L., and X. S. Liu, 2002, Phys. Rev. A **65**, 032302.
Lu, C.-Y., X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan, 2007, Nat. Phys. **3**, 91.
Luque, J.-G., and J.-Y. Thibon, 2003, Phys. Rev. A **67**, 042303.
Majewski, A. W., 2002, J. Phys. A **35**, 123.
Majewski, W. A., 2004, Open Syst. Inf. Dyn. **11**, 43.
Makhlin, Y., 2002, Quantum Inf. Comput. **1**, 243.
Maloyer, O., and V. Kendon, 2007, New J. Phys. **9**, 87.
Mancini, S., V. Giovannetti, D. Vitali, and P. Tombesi, 2002, Phys. Rev. Lett. **88**, 120401.
Mandilara, A., V. M. Akulin, M. Kolar, and G. Kurizki, 2007, Phys. Rev. A **75**, 022327.
Maneva, E. N., and J. A. Smolin, 2002, in *Quantum Information and Quantum Computation*, edited by S. J. Lomonaco and H. E. Brandt, AMS Contemporary Mathematics Series Vol. 350 (American Mathematical Society, Providence, RI), pp. 203–212.
Marcikic, I., H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, 2004, Phys. Rev. Lett. **93**, 180502.
Marian, P., and T. A. Marian, 2008, Phys. Rev. Lett. **101**, 220403.
Markham, D., J. Anders, V. Vedral, and M. Murao, 2006, e-print arXiv:quant-ph/0606103.
Masanes, L., 2005, e-print arXiv:quant-ph/0510188.
Masanes, L., 2006a, Phys. Rev. Lett. **96**, 150501.
Masanes, L., 2006b, Phys. Rev. Lett. **97**, 050503.
Masanes, L., A. Acin, and N. Gisin, 2006, Phys. Rev. A **73**, 012112.
Masanes, L., Y.-C. Liang, and A. C. Doherty, 2007, e-print arXiv:quant-ph/0703268.
Masanes, L., and A. Winter, 2006, e-print arXiv:quant-ph/0606049.
Massar, S., and S. Pironio, 2001, Phys. Rev. A **64**, 062108.
Matsumoto, K., 2005, e-print arXiv:quant-ph/0506052.
Matsumoto, R., 2003, J. Phys. A **36**, 8113.
Mattle, K., H. Weinfurter, P. G. Kwiat, and A. Zeilinger, 1996, Phys. Rev. Lett. **76**, 4656.
Maurer, U., and S. Wolf, 1997, in *Proceedings of the 1997 IEEE International Symposium on Information Theory* (IEEE, Piscataway, NJ), p. 88.
Maurer, U. M., 1993, IEEE Trans. Inf. Theory **39**, 773.
Mayers, D., 1996, e-print arXiv:quant-ph/9603015.
Mayers, D., 1997, Phys. Rev. Lett. **78**, 3414.
Mayers, D., 2001, J. ACM **48**, 351.
McHugh, D., V. Buzek, and M. Ziman, 2006, e-print arXiv:quant-ph/0611028.
McHugh, D., M. Ziman, and V. Buzek, 2006, e-print arXiv:quant-ph/0607012.
Meekhof, D. M., C. Monroe, B. E. King, W. M. Itano, and D. J. Wineland, 1996, Phys. Rev. Lett. **76**, 1796.
Mermin, N. D., 1985, Phys. Today **38** (4), 38.
Mermin, N. D., 1990a, Phys. Rev. Lett. **65**, 1838.
Mermin, N. D., 1990b, Phys. Today **43** (6), 9.
Meyer, D. A., and N. R. Wallach, 2001, e-print arXiv:quant-ph/0108104.
Mikami, H., L. Yongmin, K. Fukuoka, and T. Kobayashi, 2005, Phys. Rev. Lett. **95**, 150404.
Mintert, F., and A. Buchleitner, 2006, e-print arXiv:quant-ph/0605250.
Mintert, F., A. R. R. Carvalho, M. Kuś, and A. Buchleitner, 2005, Phys. Rep. **415**, 207.
Mintert, F., M. Kuś, and A. Buchleitner, 2004, Phys. Rev. Lett. **92**, 167902.
Mintert, F., M. Kuś, and A. Buchleitner, 2005, Phys. Rev. Lett. **95**, 260502.
Miranowicz, A., 2004a, J. Phys. A **37**, 7909.
Miranowicz, A., 2004b, Phys. Lett. A **327**, 272.
Miranowicz, A., and A. Grudka, 2004, J. Opt. Soc. Am. B **6**, 542.
Miranowicz, A., and M. Piani, 2006, Phys. Rev. Lett. **97**, 058901.
Miyake, A., 2003, Phys. Rev. A **67**, 012108.
Miyake, A., 2004, Int. J. Quantum Inf. **2**, 65.
Miyake, A., and H.-J. Briegel, 2005, Phys. Rev. Lett. **95**, 220501.
Miyake, A., and F. Verstraete, 2004, Phys. Rev. A **69**, 012101.
Mizuno, J., K. Wakui, A. Furusawa, and M. Sasaki, 2005, Phys. Rev. A **71**, 012304.
Monroe, C., D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, 1995, Phys. Rev. Lett. **75**, 4714.
Montangero, S., 2004, Phys. Rev. A **70**, 032311.

Mora, C. E., and H. J. Briegel, 2005, Phys. Rev. Lett. **95**, 200503.
Moroder, T., M. Curty, and N. Lütkenhaus, 2006a, e-print arXiv:quant-ph/0603270.
Moroder, T., M. Curty, and N. Lütkenhaus, 2006b, Phys. Rev. A **73**, 012311.
Mozes, S., J. Oppenheim, and B. Reznik, 2005, Phys. Rev. A **71**, 012311.
Murao, M., D. Jonathan, M. B. Plenio, and V. Vedral, 1999, Phys. Rev. A **59**, 156.
Murao, M., M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, 1998, Phys. Rev. A **57**, R4075.
Murao, M., and V. Vedral, 2001, Phys. Rev. Lett. **86**, 352.
Naik, D. S., C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, 2000, Phys. Rev. Lett. **84**, 4733.
Navascués, M., and A. Acin, 2005, Phys. Rev. A **72**, 012303.
Navascués, M., J. Bae, J. I. Cirac, M. Lewenstein, A. Sanpera, and A. Acin, 2005, Phys. Rev. Lett. **94**, 010502.
Neigovzen, R., C. Rodo, G. Adesso, and A. Sanpera, 2008, Phys. Rev. A **77**, 062307.
Neigovzen, R., and A. Sanpera, 2005, e-print arXiv:quant-ph/0507249.
Nielsen, M. A., 1998, Ph.D. thesis, The University of New Mexico.
Nielsen, M. A., 1999, Phys. Rev. Lett. **83**, 436.
Nielsen, M. A., 2002, Phys. Lett. A **303**, 249.
Nielsen, M. A., and I. L. Chuang, 2000, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England).
Nielsen, M. A., and J. Kempe, 2001, Phys. Rev. Lett. **86**, 5184.
Nielsen, M. A., E. Knill, and R. Laflamme, 1998, Nature (London) **395**, 5.
Nikolopoulos, G. M., and G. Alber, 2005, Phys. Rev. A **72**, 032320.
Nikolopoulos, G. M., A. Khalique, and G. Alber, 2006, Eur. Phys. J. D **37**, 441.
Norsen, T., 2007, Found. Phys. **37**, 311.
Oppenheim, J., R. W. Spekkens, and A. Winter, 2002, e-print arXiv:quant-ph/0511247.
Oppenheim, J., and A. Winter, 2003, e-print arXiv:quant-ph/0511082.
Orús, R., and J. I. Latorre, 2004, Phys. Rev. A **69**, 052308.
Osaka, H., 1991, Linear Algebr. Appl. **153**, 73.
Osborne, T. J., and M. A. Nielsen, 2002, Phys. Rev. A **66**, 032110.
Osborne, T. J., and F. Verstraete, 2006, Phys. Rev. Lett. **96**, 220503.
Osterloh, A., L. Amico, G. Falci, and R. Fazio, 2002, Nature (London) **416**, 608.
Osterloh, A., and J. Siewert, 2005, Phys. Rev. A **72**, 012337.
Osterloh, A., and J. Siewert, 2006, Int. J. Quantum Inf. **4**, 531.
Ou, Y.-C., 2006, e-print arXiv:quant-ph/0612127.
Ou, Y.-C., and H. Fan, 2007, Phys. Rev. A **75**, 062308.
Ou, Z. Y., and L. Mandel, 1988, Phys. Rev. Lett. **61**, 50.
Ourjoumtsev, A., A. Dantan, R. Tualle-Brouri, and P. Grangier, 2007, Phys. Rev. Lett. **98**, 030502.
Pan, J.-W., D. Bouwmeester, H. Weinfurter, and A. Zeilinger, 1998, Phys. Rev. Lett. **80**, 3891.
Pan, J.-W., C. Simon, C. Brukner, and A. Zeilinger, 2001, Nature (London) **410**, 1067.
Parker, S., and M. B. Plenio, 2002, J. Mod. Opt. **49**, 1325.
Paskauskas, R., and L. You, 2001, Phys. Rev. A **64**, 042310.
Paz, J. P., and A. Roncaglia, 2003, Phys. Rev. A **68**, 052316.
Peng, C.-Z., *et al.*, 2005, Phys. Rev. Lett. **94**, 150501.
Peres, A., 1995, Phys. Lett. A **202**, 16.
Peres, A., 1996a, Phys. Rev. A **54**, 2685.
Peres, A., 1996b, Phys. Rev. Lett. **77**, 1413.
Peres, A., 1999, Found. Phys. **29**, 589.
Peres, A., P. F. Scudo, and D. R. Terno, 2005, Phys. Rev. Lett. **94**, 078902.
Peres, A., and D. R. Terno, 2004, Rep. Math. Phys. **76**, 93.
Piani, M., 2006, Phys. Rev. A **73**, 012345.
Piani, M., and C. E. Mora, 2007, Phys. Rev. A **75**, 012305.
Pittenger, A. O., 2003, Linear Algebr. Appl. **359**, 235.
Pittenger, A. O., and M. H. Rubin, 2000, Phys. Rev. A **62**, 042306.
Pittenger, A. O., and M. H. Rubin, 2002, Linear Algebr. Appl. **346**, 47.
Plenio, M. B., 2005, Phys. Rev. Lett. **95**, 090503.
Plenio, M. B., and S. F. Huelga, 2002, Phys. Rev. Lett. **88**, 197901.
Plenio, M. B., S. F. Huelga, A. Beige, and P. L. Knight, 1999, Phys. Rev. A **59**, 2468.
Plenio, M. B., and V. Vedral, 2001, J. Phys. A **34**, 6997.
Plenio, M. B., and S. Virmani, 2006, Quantum Inf. Comput. **7**, 1.
Popescu, S., 1994, Phys. Rev. Lett. **72**, 797.
Popescu, S., 1995, Phys. Rev. Lett. **74**, 2619.
Popescu, S., 2006, e-print arXiv:quant-ph/0610025.
Popescu, S., and D. Rohrlich, 1992, Phys. Lett. A **166**, 293.
Popescu, S., and D. Rohrlich, 1994, Found. Phys. **24**, 379.
Popescu, S., and D. Rohrlich, 1997, Phys. Rev. A **56**, R3319.
Pregnell, K. L., 2006, Phys. Rev. Lett. **96**, 060501.
Prevendel, R., G. Cronenberg, M. S. Tame, M. Paternostro, P. Walther, M. S. Kim, and A. Zeilinger, 2009, e-print arXiv:0903.2212.
Primas, H., 1983, *Chemistry, Quantum Mechanics and Reductionism* (Springer, New York).
Radmark, M., M. Żukowski, and M. Bourennane, 2009, e-print arXiv:0903.3188.
Raggio, G. A., and R. F. Werner, 1989, Helv. Phys. Acta **62**, 980.
Raimond, J. M., M. Brune, and S. Haroche, 2001, Rev. Mod. Phys. **73**, 565.
Rains, E. M., 1997, e-print arXiv:quant-ph/9707002.
Rains, E. M., 1998, e-print arXiv:quant-ph/9809078.
Rains, E. M., 1999, Phys. Rev. A **60**, 179.
Rains, E. M., 2000, Phys. Rev. A **63**, 019902.
Rains, E. M., 2001, IEEE Trans. Inf. Theory **47**, 2921.
Rajagopal, A. K., and R. W. Rendell, 2001, Phys. Rev. A **63**, 022116.
Raussendorf, R., and H. J. Briegel, 2001, Phys. Rev. Lett. **86**, 5188.
Raussendorf, R., D. E. Browne, and H. J. Briegel, 2003, Phys. Rev. A **68**, 022312.
Raymer, M. G., A. C. Funk, B. C. Sanders, and H. de Guise, 2003, Phys. Rev. A **67**, 052104.
Reichle, R., D. Leibfried, E. Knill, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, 2006, Nature (London) **443**, 838.
Reimpell, M., and R. F. Werner, 2005, Phys. Rev. Lett. **94**, 080501.
Renes, J. M. and J.-Ch. Boileau, 2008, Phys. Rev. A **78**, 032335.
Renes, J. M., and G. Smith, 2007, Phys. Rev. Lett. **98**, 020502.
Renner, R., 2005, Ph.D. thesis, ETH, Zurich.
Renner, R., N. Gisin, and B. Kraus, 2005, Phys. Rev. A **72**,

012332.
Renner, R., and S. Wolf, 2003, *Advances in Cryptology—EUROCRYPT'03, Lecture Notes in Computer Science* (Springer-Verlag, Berlin).
Resch, K. J., P. Walther, and A. Zeilinger, 2005, Phys. Rev. Lett. **94**, 070402.
Riebe, M., H. Häffner, C. F. Roos, W. Hänsel, J. Benhelm, G. P. T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James, and R. Blatt, 2004, Nature (London) **429**, 734.
Roos, C. F., M. Riebe, H. Häffner, W. Hänsel, J. B. Benhelm, G. P. T. Lancaster, C. Becher, F. Schmidt-Kaler, and R. Blatt, 2004, Science **304**, 1478.
Rowe, M. A., *et al.*, 2001, Nature (London) **409**, 791.
Rudolph, O., 2000, J. Phys. A **33**, 3951.
Rudolph, O., 2003, J. Phys. A **36**, 5825.
Rungta, P., V. Buzek, C. M. Caves, M. Hillery, and G. J. Milburn, 2001, Phys. Rev. A **64**, 042315.
Samsonowicz, J., M. Kus, and M. Lewenstein, 2007, Phys. Rev. A **76**, 022314.
Sancho, J. M. G., and S. F. Huelga, 2000, Phys. Rev. A **61**, 042303.
Sanpera, A., D. Bruß, and M. Lewenstein, 2001, Phys. Rev. A **63**, 050301.
Sanpera, A., R. Tarrach, and G. Vidal, 1998, Phys. Rev. A **58**, 826.
Santos, M. F., P. Milman, L. Davidovich, and N. Zagury, 2006, Phys. Rev. A **73**, 040305.
Scarani, V., and N. Gisin, 2001a, Phys. Rev. Lett. **87**, 117901.
Scarani, V., and N. Gisin, 2001b, J. Phys. A **34**, 6043.
Schliemann, J., J. I. Cirac, M. Kuś, M. Lewenstein, and D. Loss, 2001, Phys. Rev. A **64**, 022303.
Schlienz, J., and G. Mahler, 1995, Phys. Rev. A **52**, 4396.
Schrödinger, E., 1935, Naturwiss. **23**, 807.
Schumacher, B., 1995, Phys. Rev. A **51**, 2738.
Schumacher, B., 1996, Phys. Rev. A **54**, 2614.
Schumacher, B., and M. A. Nielsen, 1996, Phys. Rev. A **54**, 2629.
Schumacher, B., and M. D. Westmoreland, 2000, e-print arXiv:quant-ph/0004045.
Seevinck, M., and G. Svetlichny, 2002, Phys. Rev. Lett. **89**, 060401.
Sen(De), A., U. Sen, and M. Żukowski, 2002, e-print arXiv:quant-ph/0206165.
Serafini, A., 2006, Phys. Rev. Lett. **96**, 110402.
Serafini, A., G. Adesso, and F. Illuminati, 2005, Phys. Rev. A **71**, 032349.
Shapira, D., Y. Shimoni, and O. Biham, 2006, Phys. Rev. A **73**, 044301.
Shchukin, E., and W. Vogel, 2005a, Phys. Rev. Lett. **95**, 230502.
Shchukin, E. V., and W. Vogel, 2005b, Phys. Rev. A **72**, 043808.
Sherson, J. F., H. Krauter, R. K. Olsson, B. Julsgaard, K. Hammerer, I. Cirac, and E. S. Polzik, 2006, Nature (London) **443**, 557.
Shimoni, Y., D. Shapira, and O. Biham, 2005, Phys. Rev. A **72**, 062308.
Shimony, A., 1995, Ann. N.Y. Acad. Sci. **755**, 675.
Shor, P., 2002, The quantum channel capacity and coherent information, MSRI workshop on quantum computation, http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/
Shor, P. W., 1995, Phys. Rev. A **52**, R2493.
Shor, P. W., 2003, e-print arXiv:quant-ph/0305035.
Shor, P. W., and J. Preskill, 2000, Phys. Rev. Lett. **85**, 441.
Shor, P. W., and J. A. Smolin, 1996, e-print arXiv:quant-ph/9604006.
Shor, P. W., J. A. Smolin, and B. M. Terhal, 2001, Phys. Rev. Lett. **86**, 2681.
Shor, P. W., J. A. Smolin, and A. V. Thapliyal, 2003, Phys. Rev. Lett. **90**, 107901.
Shresta, S., C. Anastopoulos, A. Dragulescu, and B. L. Hu, 2005, Phys. Rev. A **71**, 022109.
Simon, R., 2000, Phys. Rev. Lett. **84**, 2726.
Simon, R., 2003, in *Separability Criterion for Gaussian States*, edited by S. L. Braunstein and A. K. Pati (Kluwer Academic, Dordrecht), p. 155.
Simon, R., 2006, e-print arXiv:quant-ph/0608250.
Sinołęcka, M. M., K. Życzkowski, and M. Kuś, 2002, Acta Phys. Pol. B **33**, 2081.
Slater, P. B., 2005a, e-print arXiv:quant-ph/0505093.
Slater, P. B., 2005b, Phys. Rev. A **71**, 052319.
Slepian, D., and J. Wolf, 1971, IEEE Trans. Inf. Theory **19**, 461.
Smith, G., and J. Yard, 2008, Science **321**, 1812.
Smolin, J. A., 2001, Phys. Rev. A **63**, 032306.
Smolin, J. A., and J. Oppenheim, 2006, Phys. Rev. Lett. **96**, 081302.
Steane, A., 1996a, Proc. R. Soc. London, Ser. A **452**, 2551.
Steane, A. M., 1996b, Phys. Rev. Lett. **77**, 793.
Steiner, M., 2003, Phys. Rev. A **67**, 054305.
Stevenson, R. M., R. J. Young, P. Atkinson, K. Cooper, D. A. Ritchi, and A. J. Shields, 2006, Nature (London) **439**, 179.
Stobińska, M., and K. Wódkiewicz, 2005, Phys. Rev. A **71**, 032304.
Stobińska, M., and K. Wódkiewicz, 2006, Int. J. Mod. Phys. B **20**, 1504.
Størmer, E., 1963, Acta Math. **110**, 233.
Summers, S. J., and R. F. Werner, 1985, Phys. Lett. **110A**, 257.
Synak-Radtke, B., and M. Horodecki, 2006, J. Phys. A **39**, L423.
Szarek, S. J., I. Bengtsson, and K. Życzkowski, 2006, J. Phys. A **39**, L119.
Tamaki, K., M. Koashi, and N. Imoto, 2003, Phys. Rev. Lett. **90**, 167904.
Tamaki, K., and N. Lütkenhaus, 2004, Phys. Rev. A **69**, 032316.
Tanzilli, S., W. Tittel, M. Halder, O. Alibart, P. Baldi, N. Gisin, and H. Zbinden, 2005, Nature (London) **437**, 116.
Terhal, B. M., 2000, Phys. Lett. A **271**, 319.
Terhal, B. M., 2001, Linear Algebr. Appl. **323**, 61.
Terhal, B. M., 2002, Theor. Comput. Sci. **287**, 313.
Terhal, B. M., 2004, IBM J. Res. Dev. **48**, 71.
Terhal, B. M., D. P. DiVincenzo, and D. W. Leung, 2001, Phys. Rev. Lett. **86**, 5807.
Terhal, B. M., and P. Horodecki, 2000, Phys. Rev. A **61**, 040301.
Terhal, B. M., and K. G. H. Vollbrecht, 2000, Phys. Rev. Lett. **85**, 2625.
Terhal, B. M., M. M. Wolf, and A. C. Doherty, 2003, Phys. Today **56** (4), 46.
Terno, D. R., 2004, Phys. Rev. Lett. **93**, 051303.
Thapliyal, A. V., 1999, Phys. Rev. A **59**, 3336.
Tittel, W., J. Brendel, N. Gisin, and H. Zbinden, 1999, Phys. Rev. A **59**, 4150.
Tittel, W., J. Brendel, H. Zbinden, and N. Gisin, 1998, Phys. Rev. Lett. **81**, 3563.
Tittel, W., J. Brendel, H. Zbinden, and N. Gisin, 2000, Phys. Rev. Lett. **84**, 4737.
Tolkunov, D., V. Privman, and P. K. Aravind, 2005, Phys. Rev.

A **71**, 060308.
Toner, B. F., 2006, e-print arXiv:quant-ph/0601172.
Torgerson, J. R., D. Branning, C. H. Monken, and L. Mandel, 1995, Phys. Lett. A **204**, 323.
Toth, G., 2005, Phys. Rev. A **71**, 010301(R).
Tóth, G., and O. Gühne, 2005, Phys. Rev. Lett. **94**, 060501.
Tóth, G., C. Knapp, O. Gühne, and H. J. Briegel, 2007, Phys. Rev. Lett. **99**, 250405.
Tóth, G., C. Simon, and J. I. Cirac, 2003, Phys. Rev. A **68**, 062310.
Tóth, G., W. Wieczorek, R. Krischek, N. Kiesel, P. Michelberger, and H. Weinfurther, 2009, e-print arXiv:0903.3910.
Trojek, P., C. Schmid, M. Bourennane, C. Brukner, M. Żukowski, and H. Weinfurter, 2005, Phys. Rev. A **72**, 050305.
Tucci, R. R., 2002, e-print arXiv:quant-ph/0202144.
Uhlmann, A., 1976, Rep. Math. Phys. **9**, 273.
Uhlmann, A., 1998, Open Syst. Inf. Dyn. **5**, 209.
Uhlmann, A., 2000, Phys. Rev. A **62**, 032307.
Ursin, R., T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger, 2004, Nature (London) **430**, 849.
Ursin, R., *et al.*, 2007, Nat. Phys. **3**, 481.
Vaglica, A., and G. Vetri, 2007, e-print arXiv:quant-ph/0703241.
Vaidman, L., 1994, Phys. Rev. A **49**, 1473.
Vallone, G., E. Pomarico, P. Mataloni, F. De Martini, and V. Berardi, 2007, Phys. Rev. Lett. **98**, 180502.
Van den Nest, M., A. Miyake, W. Dür, and H. J. Briegel, 2006, Phys. Rev. Lett. **97**, 150504.
Vedral, V., 1999, Phys. Lett. A **262**, 121.
Vedral, V., 2002, Rep. Math. Phys. **74**, 197.
Vedral, V., 2004, New J. Phys. **6**, 102.
Vedral, V., and M. B. Plenio, 1998, Phys. Rev. A **57**, 1619.
Vedral, V., M. B. Plenio, K. Jacobs, and P. L. Knight, 1997, Phys. Rev. A **56**, 4452.
Vedral, V., M. B. Plenio, M. A. Rippin, and P. L. Knight, 1997, Phys. Rev. Lett. **78**, 2275.
Venzl, H., and M. Freyberger, 2007, Phys. Rev. A **75**, 042322.
Verch, R., and R. F. Werner, 2005, Rep. Math. Phys. **17**, 545.
Vernam, G. S., 1926, J. AIEE **45**, 109.
Verstraete, F., K. Audenaert, J. Dehaene, and B. D. Moor, 2001, J. Phys. A **34**, 10327.
Verstraete, F., K. Audenaert, and B. De Moor, 2001, Phys. Rev. A **64**, 012316.
Verstraete, F., and J. I. Cirac, 2003, Phys. Rev. Lett. **91**, 010404.
Verstraete, F., J. Dehaene, and B. De Moor, 2003, Phys. Rev. A **68**, 012103.
Verstraete, F., J. Dehaene, B. De Moor, and H. Verschelde, 2002, Phys. Rev. A **65**, 052112.
Verstraete, F., M. Popp, and J. I. Cirac, 2004, Phys. Rev. Lett. **92**, 027901.
Verstraete, F., D. Porras, and J. I. Cirac, 2004, Phys. Rev. Lett. **93**, 227205.
Vidal, G., 1999, Phys. Rev. Lett. **83**, 1046.
Vidal, G., 2000, J. Mod. Opt. **47**, 355.
Vidal, G., 2003, Phys. Rev. Lett. **91**, 147902.
Vidal, G., 2004, Phys. Rev. Lett. **93**, 040502.
Vidal, G., and J. I. Cirac, 2001, Phys. Rev. Lett. **86**, 5803.
Vidal, G., and J. I. Cirac, 2002, Phys. Rev. Lett. **88**, 167903.
Vidal, G., J. I. Latorre, E. Rico, and A. Kitaev, 2003, Phys. Rev. Lett. **90**, 227902.
Vidal, G., and R. Tarrach, 1999, Phys. Rev. A **59**, 141.
Vidal, G., and R. F. Werner, 2002, Phys. Rev. A **65**, 032314.
Virmani, S., S. F. Huelga, and M. B. Plenio, 2005, Phys. Rev. A **71**, 042328.
Virmani, S., and M. B. Plenio, 2000, Phys. Lett. A **268**, 31.
Vollbrecht, K. G. H., and F. Verstraete, 2005, Phys. Rev. A **71**, 062325.
Vollbrecht, K. G. H., and R. F. Werner, 2001, Phys. Rev. A **64**, 062307.
Vollbrecht, K. G. H., R. F. Werner, and M. M. Wolf, 2004, Phys. Rev. A **69**, 062304.
Vollbrecht, K. G. H., and M. M. Wolf, 2002a, Phys. Rev. Lett. **88**, 247901.
Vollbrecht, K. G. H., and M. M. Wolf, 2002b, J. Math. Phys. **43**, 4299.
Volz, J., M. Weber, D. Schlenk, W. Rosenfeld, J. Vrana, K. Saucke, C. Kurtsiefer, and H. Weinfurter, 2006, Phys. Rev. Lett. **96**, 030404.
von Neumann, J., 1932, *Mathematische Grundlagen der Quantenmechanic* (Springer, Berlin).
Walborn, S. P., P. H. Souto Ribeiro, L. Davidovich, F. Mintert, and A. Buchleitner, 2006, Nature (London) **440**, 1022.
Walgate, J., and L. Hardy, 2002, Phys. Rev. Lett. **89**, 147901.
Walgate, J., A. J. Short, L. Hardy, and V. Vedral, 2000, Phys. Rev. Lett. **85**, 4972.
Walther, P., K. J. Resch, C. Brukner, A. M. Steinberg, J.-W. Pan, and A. Zeilinger, 2005, Phys. Rev. Lett. **94**, 040504.
Wang, J., H. Batelaan, J. Podany, and A. F. Starace, 2006, J. Phys. B **39**, 4343.
Watrous, J., 2004, Phys. Rev. Lett. **93**, 010502.
Wehrl, A., 1978, Rep. Math. Phys. **50**, 221.
Wei, T.-C., J. B. Altepeter, P. M. Goldbart, and W. J. Munro, 2004, Phys. Rev. A **70**, 022322.
Wei, T.-C., and P. M. Goldbart, 2003, Phys. Rev. A **68**, 042307.
Weihs, G., T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, 1998, Phys. Rev. Lett. **81**, 5039.
Weinfurter, H., and M. Żukowski, 2001, Phys. Rev. A **64**, 010102.
Wellens, T., and M. Kuś, 2001, Phys. Rev. A **64**, 052302.
Werner, R. F., 1989a, Lett. Math. Phys. **17**, 359.
Werner, R. F., 1989b, Phys. Rev. A **40**, 4277.
Werner, R. F., and M. M. Wolf, 2000, Phys. Rev. A **61**, 062102.
Werner, R. F., and M. M. Wolf, 2001a, Phys. Rev. A **64**, 032112.
Werner, R. F., and M. M. Wolf, 2001b, e-print arXiv:quant-ph/0107093.
Werner, R. F., and M. M. Wolf, 2001c, Phys. Rev. Lett. **86**, 3658.
Wieczorek, W., R. Krischek, N. Kiesel, P. Michelberger, G. Tóth, and H. Weinfurther, 2009, e-print arXiv:0903.2213.
Wieśniak, M., V. Vedral, and C. Brukner, 2005, New J. Phys. **7**, 258.
Wineland, D. J., J. J. Bollinger, W. M. Itano, F. L. Moore, and D. J. Heinzen, 1992, Phys. Rev. A **46**, R6797.
Wiseman, H. M., and J. A. Vaccaro, 2003, Phys. Rev. Lett. **91**, 097902.
Wójcik, A., 2005, Phys. Rev. A **71**, 016301.
Wolf, M. M., G. Giedke, and J. I. Cirac, 2006, Phys. Rev. Lett. **96**, 080502.
Wolf, M. M., G. Giedke, O. Krüger, R. F. Werner, and J. I. Cirac, 2004, Phys. Rev. A **69**, 052320.
Wong, A., and N. Christensen, 2001, Phys. Rev. A **63**, 044301.
Wootters, W. K., 1998, Phys. Rev. Lett. **80**, 2245.
Wootters, W. K., and W. H. Zurek, 1982, Nature (London) **299**, 802.
Woronowicz, S. L., 1976, Rep. Math. Phys. **10**, 165.
Wu, L.-A., S. Bandyopadhyay, M. S. Sarandy, and D. A. Lidar,

2005, Phys. Rev. A **72**, 032309.
Wu, X. H., and H.-S. Zong, 2003, Phys. Lett. A **307**, 262.
Wunderlich, H., and M. Plenio, 2009, e-print arXiv:0902.2093.
Wyner, A. D., 1975, Bell Syst. Tech. J. **54**, 1355.
Xin, Y., and R. Duan, 2007, e-print arXiv:0709.1651.
Yang, D., 2006, Phys. Lett. A **360**, 249.
Yang, D., M. Horodecki, R. Horodecki, and B. Synak-Radtke, 2005, Phys. Rev. Lett. **95**, 190501.
Yang, T., Q. Zhang, J. Zhang, J. Yin, Z. Zhao, M. Żukowski, Z.-B. Chen, and J.-W. Pan, 2005, Phys. Rev. Lett. **95**, 240406.
Yao, A. C., 1979, in *11th Annual ACM Symposium on Theory of Computing* (ACM, New York), pp. 209–213.
Yi, X. X., H. T. Cui, and L. C. Wang, 2006, Phys. Rev. A **74**, 054102.
Yi, X. X., and C. P. Sun, 1999, Phys. Lett. A **262**, 287.
Yi, X. X., C. S. Yu, L. Zhou, and H. S. Song, 2003, Phys. Rev. A **68**, 052304.
Yu, S., and N. le Liu, 2005, Phys. Rev. Lett. **95**, 150504.
Yu, T., and J. H. Eberly, 2004, Phys. Rev. Lett. **93**, 140404.
Yu, T., and J. H. Eberly, 2006, Opt. Commun. **264**, 393.
Yu, T., and J. H. Eberly, 2007a, Quantum Inf. Comput. **7**, 459.
Yu, T., and J. H. Eberly, 2007b, J. Mod. Opt. **54**, 2289.
Yu, T., and J. H. Eberly, 2009, Science **323**, 598.
Yudin, D. B., and A. S. Nemirovskii, 1976, Ekonomica Mat. Metody **12**, 357.
Yuen, H. P., 2005, e-print arXiv:quant-ph/0505132.
Yurke, B., and D. Stoler, 1992a, Phys. Rev. A **46**, 2229.
Yurke, B., and D. Stoler, 1992b, Phys. Rev. Lett. **68**, 1251.
Zanardi, P., 2002, Phys. Rev. A **65**, 042101.
Zanardi, P., and X. Wang, 2002, J. Phys. A **35**, 7947.
Zanardi, P., C. Zalka, and L. Faoro, 2000, Phys. Rev. A **62**, 030301.
Zapatrin, R. R., 2005, e-print arXiv:quant-ph/0504169.
Zhang, X.-W., K. Wen, and G. L. Long, 2005, e-print arXiv:quant-ph/0512231.
Zhao, Z., Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel, and J.-W. Pan, 2004, Nature (London) **430**, 54.
Ziman, M., and V. Buzek, 2003, Phys. Rev. A **67**, 042321.
Żukowski, M., and C. Brukner, 2002, Phys. Rev. Lett. **88**, 210401.
Żukowski, M., C. Brukner, W. Laskowski, and M. Wieśniak, 2002, Phys. Rev. Lett. **88**, 210402.
Żukowski, M., A. Zeilinger, M. A. Horne, and A. Ekert, 1993, Phys. Rev. Lett. **71**, 4287.
Żukowski, M., A. Zeilinger, M. A. Horne, and H. Weinfurter, 1998, Acta Phys. Pol. A **93**, 187.
Zurek, W. H., 1981, Phys. Rev. D **24**, 1516.
Zurek, W. H., 2003, e-print arXiv:quant-ph/0306072.
Zurek, W. H., 2005, Phys. Rev. A **71**, 052105.
Zurek, W. H., 2009, Nat. Phys. **5**, 181.
Życzkowski, K., 1999, Phys. Rev. A **60**, 3496.
Życzkowski, K., P. Horodecki, M. Horodecki, and R. Horodecki, 2002, Phys. Rev. A **65**, 012101.
Życzkowski, K., P. Horodecki, A. Sanpera, and M. Lewenstein, 1998, Phys. Rev. A **58**, 883.