ACTA PHYSICA POLONICA A No. 3 Vol. **139** (2021)

INVITED

Special issue, XLVI Extraordinary Congress of Polish Physicists, Warsaw, Poland, October 16–18, 2020

Quantum Information

R. Horodecki[a,b,*]

[a] *International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland*

[b] *Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland*

Dedicated to memory of Roman Stanisław Ingarden on his centennial birthday

"...the quantum information theory is not only scientifically interesting subject, but is a practical need"

R.S. Ingarden

Doi: 10.12693/APhysPolA.139.197 *e-mail: ryszard.horodecki@ug.edu.pl

This article reviews the extraordinary features of quantum information predicted by the quantum formalism, which, combined with the development of modern quantum technologies, have opened new horizons in quantum physics that can potentially affect various areas of our live, leading to new technologies such as quantum cybersecurity, quantum communication, quantum metrology, and quantum computation.

topics: quantum cryptography, quantum entanglement, nonlocality, entanglement witness

1. Introduction

The concept of quantum information was born on the border between quantum mechanics and information theory science. The stunning success of the former has led us to think that the concept of information cannot be separated from the mathematical structure of quantum formalism that imposes fundamental constraints on the form of physical laws.

Already in the 1930s, von Neumann defined entropy [1] for quantum states as an analogue of the classical Boltzmann–Gibbs entropy, which later turned out to be the quantum counterpart of the Shannon entropy [2] — the concept underlying of classical communication theory. At about the same time, Einstein, Podolsky and Rosen pointed out the unusual features of quantum formalism that seemed to lead to the conclusion that quantum mechanics is incomplete [3]. In 1970, two young physicists, Park [4] from the Department of Physics at Washington State University and Wiesner [5] from Columbia University in New York, independently analyzed the physical implications of quantum formalism. While the former discovered a fundamental limitation on copying quantum information, the latter discovered the first application of quantum information to unforgeable quantum money.

Unfortunately, both discoveries were ahead of their time and passed unnoticed. Three years later, Holevo proved [6] that there is a bound for our ability to access classical information from quantum systems which confirmed earlier Gordon's [7] and Levitin's [8] conjectures. This strengthened the conviction that Shannon's communication theory is incomplete, in a sense that it did not consider the transmission of all physical information carriers such as quantum particles. A few years later, Ingarden, a Polish mathematical physicist, published a work entitled *Quantum Information Theory* in which he proposed a quantum generalization of Shannon's theory in terms of the generalized quantum mechanics of open systems [9] (see also [10]). However, it was only a series of seminal papers [11–27] that revealed specific features of the quantum code of nature pointing to the quantum origins of information.

There were various reasons for the relatively late advent of the quantum information era crowned with the building of Shannon's quantum theory (see [28]). In particular, the unusual success of Shannon's theory led to the belief that the laws of physics could be derived from information processing as a purely mathematical concept detached from physical information carriers. On the other hand, the identification of peculiar features of quantum information such as monogamy of entanglement [29–31] required advanced quantum technologies. Additionally, the obstacle was the abstract, mathematical and non-intuitive nature of the standard quantum formalism that looked like an inscription, not all predictions of which were entirely clear even for its fathers.

2. Quantum inscription as paradigm for quantum information

Roughly speaking, quantum inscription is an instruction — a set of prescriptions that determine the way of probabilistic prediction of the results of future measurements in laboratories [32, 33].

Each physical system corresponds to a complex vector space Hilbert H equipped with the linear scalar product $\langle\cdot|\cdot\rangle$ such that the space is complete with respect to the norm

$$||\psi|| = \sqrt{\langle\psi|\psi\rangle}. \tag{1}$$

The space H of system S compound of n subsystems $S_1, S_2, \ldots, S_n$ is a tensor product

$$H = H_1 \otimes H_2, \ldots \otimes H_n \tag{2}$$

of the Hilbert space of subsystems. The subsystems can represent distinguishable particles, various complex objects, e.g., atoms, molecules, or different degrees of freedom of the same object, e.g., photon polarization and propagation modes.

The central object is the wave function (state vector) $|\psi\rangle$ with the unit norm $||\psi|| = 1$, which is an element of a Hilbert space. It contains all probabilistic information about the system and satisfies the Schrödinger equation: $\mathrm{i}\hbar\frac{\partial|\psi\rangle}{\partial t} = H|\psi\rangle$, where H is a linear self-adjoint operator called Hamiltonian. The symbol ϱ denotes the state of the system about which we only have partial information. It can be described by a Hermitian positive semidefinite operator with unit trace: $\varrho = \varrho^\dagger$, $\varrho \geq 0$, $\mathrm{Tr}(\varrho) = 1$, where trace $\mathrm{Tr}(\varrho) = \sum_k \langle\phi_k|\varrho|\phi_k\rangle$ and sum runs over diagonal elements in arbitrary orthonormal basis $\{\phi_k\}$. The symbol U stands for unitary operations that transform states, and in the case of pure states, they keep the scalar product preserved.

Observable quantities correspond to Hermitian linear operators O acting on the state space H. In contrast to classical observables, the quantum ones can be noncommutative: $[O_1, O_2] = O_1O_2 - O_2O_1 \neq 0$. The most familiar example is $[Q, P] = \mathrm{i}$, where Q and P are the position and momentum operators. The structures and mutual interrelations of noncommutative observables bring deep questions concerning the properties of the quantum systems related to the fundamental principles: uncertainty and complementarity. The first one limits the precision of the statistics of the results of two complementary observables, such as position and momentum [34]. The complementarity principle says that two quantum observables cannot be measured simultaneously, and thus provide "independent" information about physical systems [35].

Contrary to classical theories, quantum measurement is active. It creates properties, does it randomly, and can change state if the latter is not specially tailored for a given measurement. The measurement does not always provide information about state but it can be part of a quantum operation. Any state ϱ defines the probability distribution as the mapping assigning to each measurement result i the probability p_i of that measurement result (the Born rule):

$$p_i = \mathrm{Tr}\big(\Pi_i \varrho\big), \tag{3}$$

where $\{\Pi_i\}$, $\sum_i \Pi_i = \boldsymbol{I}$ are the elements of a positive operator-value measure (POVM) and $\boldsymbol{I}$ is the unit operator. In particular, if Π_i is the projector operator, then the generalized measurement corresponds to the von Neumann measurement, which completely determines the post-measurement state. After the measurement with the outcome i, the system goes to the post-measurement state

$$\varrho_i' = p_i^{-1} \Lambda_i\left(\varrho\right), \tag{4}$$

where $\Lambda_i(\varrho) = \Pi_i\varrho\Pi_i$ is the particular positive superoperator which clearly maps positive operators to positive operators and normalization of ϱ_i' requires the condition to be met $\mathrm{Tr}\left(\varrho\Pi_i\right) = \mathrm{Tr}\left(\Lambda_i(\varrho)\right)$, where $\Lambda_i(\varrho) = p_i\varrho_i'$. The most general physically implementable map is a completely positive map Λ which satisfies condition: $\Lambda \otimes \boldsymbol{I}_n \in B(H_1 \otimes C^n, H_2 \otimes C^n)$, where B is the space of positive maps between the Hilbert spaces $H_1 \otimes C^n$ and $H_2 \otimes C^n$, and $\boldsymbol{I}_n$ is the unit operator on n-dimensional Hilbert space C^n. If, in addition, Λ is trace-preserving, it determines the quantum channel which plays a central role in the processing of quantum information [28]. Any completely positive map on a system S in a given state ϱ can be realized via unitary interaction of S with some other system (ancilla) in a pure state followed by a von Neumann measurement and final partial trace. This fact comes from the so called Stinespring's dilation theorem [32].

The crucial difference between the quantum description of physical reality and the classical one is the principle of superposition, i.e., if $|\Psi_1\rangle$, $|\Psi_2\rangle$ are system states, then their superposition

$$|\Psi\rangle = a|\Psi_1\rangle + b|\Psi_2\rangle \tag{5}$$

is also in good state, provided that a and b are chosen so that $|\Psi\rangle$ is normalized.

The prediction power of quantum inscription is astonishing: *All our experience so far using quantum theory seems to say: What is predicted by quantum formalism must come to the laboratory* [36]. In the early 1970s, it seemed that all possible predictions of quantum inscription had already been recognized. The papers of Einstein, Podolsky and Rosen [3] and Schrödinger [37] were initially treated rather as a mathematical artefact detached from its physical implications. Ironically, it was them who drew attention to the extraordinary implications of quantum inscription, which revealed the existence at a fundamental level of a subtle order governed by quantum information. In the classical world, quantum information is "unspeakable". It cannot be written with discrete symbols, e.g., on a tape of a Turing machine. So far, there is no commonly accepted definition of quantum information.

For our purposes, it is convenient to adopt the following interpretation: *Quantum information is what is carried by quantum particles and the wave function ψ is its mathematical image* [38].

Quantum information (QI) can be processed (manipulated) [32, 39], using combinations of unitary operations and measurements. QI is the source of quantum resources [40] such as entanglement [36, 41, 42], steering [43], quantum correlation beyond entanglement [44], quantum coherence [45] and asymmetry [46]. It allows to perform nonclassical tasks such as quantum cryptography [13, 16, 47, 48], teleportation [19, 25–27], quantum computing [14, 15, 18], not feasible with classical resources. QI is a resource for quantum metrology [49] and computational complexity [50–52].

However, this subtle resource has a very unpleasant feature. As one knows, non-diagonal elements of the density matrix ϱ called coherence in the state ϱ provide information about quantum interference. Unfortunately, as a result of the system's interaction with the environment, the process of decoherence [53] occurs, which causes disappearance of non-diagonal elements of density matrix of the state. Reversing the degradation of quantum information still remains a great challenge for effective processing of quantum information.

3. Quantum bit — unit of quantum information

The concept of qubit appeared for the first time in the context of the theory of quantum information transmission [23] as a two-level system, the state of which can be written as a superposition of two base states $|0\rangle$ and $|1\rangle$, namely

$$|\Psi\rangle = a|0\rangle + b|1\rangle, \tag{6}$$

where a and b are complex numbers, $|\Psi\rangle \in \boldsymbol{C}^2$ (two-dimensional Hilbert space).

Contrary to the classical bit, the qubit represents a continuum of possible states defined by its wave function, which can be visualized by the two-dimensional Bloch sphere with two real parameters θ and φ. Then, the complex numbers are expressed as $a = \cos(\theta/2)$, $b = \sin(\theta/2)\exp(\mathrm{i}\varphi)$, where $0 \le \theta \le \pi$, $0 \le \varphi \le 2\pi$. For illustration, consider a photon as a paradigmatic example of a qubit. It requires a Hilbert space H which is a tensor product $H = H_{\mathrm{prop}} \otimes H_{\mathrm{pol}}$, where H_{prop} represents the photon propagation modes while $H_{\mathrm{pol}} = \boldsymbol{C}^2$ describes the photon polarization modes. If one disregards the propagation modes, the photon can be treated as a photonic qubit in a polarization degree of freedom.

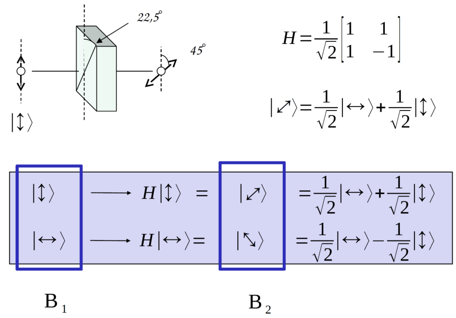

Fig. 1. The photonic realization of the Hadamard H gate. The computation base is denoted by B_1 and the Hadamard base — by B_2.

Consider now a photon in the superposition of the base states $|0\rangle \equiv |\updownarrow\rangle$ and $|1\rangle \equiv |\leftrightarrow\rangle$ corresponding to vertical and horizontal polarization. This photon state is written as $|\Psi\rangle = \sin(\Theta)\,|0\rangle + \cos(\Theta)\,|1\rangle$. If we direct it to a vertical polarizer, it will change to one of the states $|0\rangle$ or $|1\rangle$ with probabilities $p_0 = \mathrm{Tr}\,(\Pi_o \varrho) = \sin^2(\Theta)$, $p_1 = \mathrm{Tr}\,(\Pi_1 \varrho) = \cos^2(\Theta)$, respectively, where $\Pi_0 = |0\rangle, \langle 0|$, $\Pi_1 = |1\rangle, \langle 1|$ are projectors and density matrix of the state $|\Psi\rangle$ is given by

$$\varrho = |\Psi\rangle\langle\Psi| = \begin{bmatrix} \sin^2(\theta) & \sin(\theta)\cos(\theta) \\ \sin(\theta)\cos(\theta) & \cos^2(\theta) \end{bmatrix}, \tag{7}$$

where the diagonal elements are interpreted as the probabilities of the basis state, while the off-diagonal elements represent the coherence of the basis states.

If we now place a specially cut birefringent crystal with the optical axis at an angle of 22.5 degrees on the path of a vertically polarized photon, the photon will be in a state of linear superposition (see Fig. 1). This is nothing but the photonic realization of the Hadamard H gate. It has no classical counterpart and plays a fundamental role in quantum information processing including quantum computing. Note that arbitrary photonic wave plate operations for photonic polarization qubits realizing the Hadamard, Pauli-X, and rotation gates were implemented on the chip [54].

In Fig. 1, B_1 and B_2 denote the computation base and the Hadamard base, respectively, which are mutually unbiased, i.e., they are mutually exclusive. Perfect information about the polarization along the selected axis implies that there is no information about the polarization along the axis rotated by 45°. This is a purely quantum mechanical effect resulting from the fact that the vectors $|0\rangle$, $|1\rangle$, as well as $|+\rangle \equiv |\swarrow\!\!\nearrow\rangle$ and $|-\rangle \equiv |\nwarrow\!\!\searrow\rangle$ are the eigenstates of the Pauli operators σ_z and σ_x, respectively. Importantly, these operators do not commute, i.e., $[\sigma_z, \sigma_x] = \sigma_z\sigma_x - \sigma_x\sigma_z \neq 0$.

There have been many proposals for the physical realization of a qubit on quantum dots [55] electron spins [56], semiconductor spin [57], superconducting charge qubits based on a Josephson junction [58, 59]. Remarkably, it has been demonstrated that linear optics is sufficient for efficient quantum information processing with photonic qubits in two optical modes (such as horizontal or vertical polarization) [60, 61]. There has recently been quite a progress in parallelized quantum information processing which includes tailored quantum memories to simultaneously handle multiple photons [62].

4. Fundamental limitations on quantum information processing

Already in 1961, Wigner pointed out that the existence of self-reproduction in the quantum world is unlikely [63]. In 1970, Park [4] and later Wooters and Żurek [64] and Dieks [65] proved that it is impossible to build a quantum machine that can perfectly copy arbitrary unknown quantum state Ψ:

$$|\Psi\rangle|0\rangle|M\rangle \not\rightarrow |\Psi\rangle|\Psi\rangle|M_\psi\rangle, \quad (8)$$

where $|0\rangle$ means a blank state, while $|M\rangle$, $|M_\psi\rangle$ are the machine state before and after cloning, respectively. The process realized by such a machine would have to be nonunitary and non-linear, which is forbidden by the linearity of quantum formalism. Thus copying destroys the state and it cannot be reconstructed from a single copy. Hence, the quantum signals cannot be noiselessly amplified. Later, the limitation for the unperfect cloning in terms of the so called fidelity function $f(\varrho_{\text{out}}) = \langle\Psi|\varrho_{\text{out}}|\Psi\rangle$ measuring similarity of the state of either of the two outcome registers has been provided within the framework of imperfect quantum cloning machines [66, 67]. There is the dual no-deleting theorem, which states that, in general, given two copies of some arbitrary quantum state, it is impossible to delete one of the copies [68]. In the above mentioned paper, Holevo [6] proved a fundamental theorem that sets an upper limit to the amount of information available about a quantum state. It implies that with the help of one qubit, it is impossible to send more than one bit of classical information.

Quite unexpectedly, it turned out that there is also a restriction on the possibility of generating of quantum superposition. Namely, it has been independently shown [69, 70] that there is no universal probabilistic quantum protocol generating superposition of the two unknown states. Interestingly, a probabilistic protocol generating a superposition of two unknown states having a fixed overlap with a known pure reference state has been proposed [70]. This protocol has been carried out experimentally in a three-quadrant NMR system as well as on unknown photonic quantum states [71, 72].

5. Quantum cryptography based on no-cloning

Parallel to Park's paper on non-cloning, Wiesner, basing on the uncertainty principle, introduced the concept of conjugate coding to make up quantum money [4]. This idea paved the way for the quantum information encryption Bennett's and Brassard's protocol (BB84) [13]. It has the following main three steps:

1. Alice sends randomly polarized photons through the quantum channel in the selected computing bases $\{B_1\}$ $|0\rangle$, $|1\rangle$ and Hadamard $\{B_2\}$ $|+\rangle$, $|-\rangle$; she saves bases and bits.
2. Bob measures photons in randomly selected bases B_1 and B_2; he registers bases and bits.
3. Via the classic public (authenticated) channel, Alice and Bob transmit their choices bases. When their bases match, they retain the appropriate bits.

Thus, they receive a raw key that requires further processing. To check for eavesdropping, they calculate the quantum bit error of a randomly selected data subset that they reveal to each other via the public channel and check if the error (percentage of mismatched bits) is below a certain threshold value. Using classic post-processing protocols, such as error correction and privacy amplification, they generate the final secure key.

Since 1992, when Bennett and Brassard and colleagues demonstrated the first 32 cm quantum distribution of the key in free space [73], there has been tremendous progress in the development of quantum cryptography in free space and in fiber. There is a continuous improvement of cryptographic keys over long distances [74] as well as an increase in a key generation speed using single photon detectors [75]. Quantum key distribution (QKD) networks were established in the US, Austria, Switzerland, China and Japan, and at the European SECOQC network [76]. Due to exponential signal attenuation and decoherence, the effective distribution range of the quantum key of terrestrial networks is limited to 300 km [77]. In cosmic space, both of these factors are many times weaker. In 2016, the first satellite distribution of the BB84 protocol was performed using a one-time key cipher via the Micius satellite at intercontinental distances, thanks to which the photos of Schrödinger and the philosopher Micius were safely transferred between Vienna and Beijing [78].

Despite the enormous advances in quantum cryptography, there are still some problems related to the fact that practical implementations of quantum key decomposition use realistic photonic qubits and imperfect single photon detectors. This creates gaps between the QKD theory and practice enabling quantum hacking, e.g., the "Bright Illumination" attack or photon-number splitting [79]. Therefore, QKD implementations are still in the testing phase and these gaps are identified. Stronger versions of BB84 were developed, such as the BB84 decoy state and protocols resistant to photon-number breaking attacks [47]. As a result, QKD protocols become more and more secure.

6. Quantum entanglement — the most non-classical feature of quantum information

As we have seen, already at the level of simple systems, the properties of quantum information differ substantially from those of classical information that can be amplified and copied. Much earlier, in the 1930s, EPR and Schrödinger revealed a peculiar feature of quantum information in complex quantum systems rooted in the principle of superposition called entanglement. According to the quantum inscription, the state space H_S of the quantum system S compound from distinguishable subsystems $S_1, S_2, \ldots S_n$ is given by $H_{S1} \otimes H_{S2}, \ldots \otimes H_{Sn}$ which is the tensor product of the Hilbert space of the subsystems.

We say that a pure state is entangled if it cannot be written as the product of the states of the individual subsystems

$$|\Psi\rangle_{12\ldots n} \neq |\phi\rangle_1 \otimes |\psi\rangle_2 \ldots \otimes |\chi\rangle_n. \tag{9}$$

In general, a mixed state ϱ of n systems is entangled if it cannot be written as a convex combination of product states

$$\varrho \neq \varrho_{\text{sep}} = \sum_i p_i \varrho_1^i \otimes \cdots \otimes \varrho_n^i. \tag{10}$$

In particular, for any two-part pure entangled state $|\psi\rangle_{12} \in H_1 \otimes H_2$, there exist orthonormal Schmidt bases $\{\phi_i\rangle$, $\{\chi_i\rangle$ in H_1, H_2, respectively, such that

$$|\Psi\rangle_{12} = \sum_i^d c_i |\phi_i\rangle \otimes |\chi_i\rangle, \tag{11}$$

where the summation takes place on the smaller dimensions of the two systems $d = \min(d_1, d_2)$. Specifically, the two-part maximally entangled state in the space $H_1 \otimes H_2$ with the dimension d^2 is defined as:

$$|\Psi_{\max}\rangle = \frac{1}{\sqrt{d}} \sum_i^d |\phi_i\rangle \otimes |\chi_i\rangle. \tag{12}$$

In particular, there is a two-qubit entangled state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} \Big(|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2 \Big), \tag{13}$$

where $\{|0\rangle, |1\rangle\}$ is the computational basis for qubits. Using the von Neumann entropy as a measure of entanglement for pure states, it is easy to check that the above state contains one ebit of entanglement, i.e., the maximum amount of entanglement that a system with dimension $d = 2^2$ allows. In general, for a system consisting of n pairs of entangled qubits and a Hilbert space dimension, $d = 2^n$ contains n ebits of entanglement. Most of the pure state vectors in a pure state two-part Hilbert space are not maximally entangled.

For systems divided into more than two parts, the Schmidt distribution in general does not exist. However, many of the important states in quantum information processing take the form of a multi-part Schmidt distribution. Among them, three-particle states: $|\Psi\rangle_{\text{GHZ}} = \frac{1}{2}(|000\rangle + |111\rangle)$ [80] and $|\Psi\rangle_{\text{W}} = \frac{1}{3}(|001\rangle + |010\rangle + |100\rangle)$ [81], which represent two different types of entanglement that cannot be transformed into each other through local operations and classical communications (LOCC). Interestingly, experimental a W-to-GHZ state conversion was recently demonstrated [82, 83].

Let us emphasize that the above mathematical description of quantum entanglement between various degrees of freedom of complex systems is adequate in a scenario where each subsystem (e.g. qubit) can be individually addressed/manipulated. In a situation when one considers indistinguishable systems in connection with the symmetrization postulate, the complete characterization of entanglement is still a challenge. Many different approaches have been proposed with different entanglement definitions. Recently, Benatti et al. [84] has made an extensive comparative analysis of different approaches to the definition of entanglement of quantum systems composed of indistinguishable particles based on natural physical requirements.

There are many ways to generate quantum entanglement. Entangled states are most often generated in a spontaneous parametric down-conversion and spontaneous four-wave mixing [85–87]. It is intriguing that it is possible to entangle together particles from two independent sources that did not interact with each other in the past [20, 88]. Another peculiar behavior of entanglement, called a sudden entanglement death, was described in a dynamic scenario. Namely, when two entangled qubits interact with natural reservoirs, the entanglement can disappear in a finite time while the coherence disappears asymptotically [89–91]. The source of this phenomenon is due to the fact that in finite-dimensional systems, the set of separable (non-entangled) states has a finite volume [92]. This important result was in particular discussed in the context of quantum computing on NMR which operates on highly mixed, separable states [93].

The discovery of Einstein, Podolsky and Rosen that entangled states could show "ghostly" correlations independent of distance, until the appearance of John Bell's famous work, was not given much interest. On the one hand, they were considered more philosophical than physical, on the other hand, it was believed that such correlations could be simulated classically.

7. Photons entangled in polarization

To illustrate this phenomenon, consider the probabilistic generation of photons entangled in polarization degrees of freedom using a type-II down-conversion [94]. In this process, a high-energy photon in an optical nonlinear medium (BBO crystal) is converted into two lower-energy photons that are emitted along the surface of two anticorrelated intersecting cones with vertical and horizontal polarization (see Fig. 2). Particularly, the photons

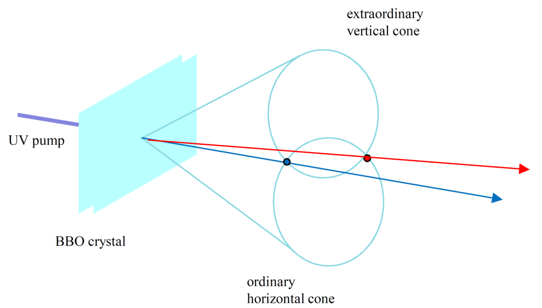

Fig. 2. Generation of photons entangled in polarization using type-II conversion in the Bell state $|\Psi^+\rangle_{AB}$.

emitted along the intersections cannot be assigned a specific polarization because we do not know which cone they come from. We write it down as a quantum alternative

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\Big), \qquad (14)$$

where $|0\rangle$, $|1\rangle$ correspond to vertical and horizontal polarization, respectively. Here, $|\Psi^+\rangle$ is one of four canonical Bell-states (the Bell basis) [95]: $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B\right)$, $|\Phi^\pm\rangle = \frac{1}{2}\left(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B\right)$. Now, if we direct the photons from the entangled pair (EPR pair) in the polarization to distant Alice's and Bob's laboratories, respectively, who independently measure the polarization of the same type, it turns out that they get anticorrelations $0-1$ or $1-0$. What is striking is the fact that individual photons do not carry any bit because their polarization is completely random [16], so local measurement results turn out to be completely random, too. EPR reasoned as follows: If it is possible to "remotely" predict some property of a particle without interacting with it, then this property must have existed before, i.e., before the measurement. They called it the "reality elements", and from there they concluded that quantum inscription offered an incomplete description of physical reality.

8. Nonlocality of quantum correlations. Bell tests

It was a serious objection that no one, including Bohr himself, was able to convincingly refute. The Gordian knot was cut by John Bell [11]. Namely, he formalized the concepts of reality elements by introducing a model of local hidden variables based on the following assumptions: (i) the measurement results are determined by the properties of the particle carried before and independent of the measurement, (ii) the results determined in one place are independent of any actions in the space-like separation, (iii) the settings of local apparatus do not depend on hidden variables that determine the results of local measurements. These assumptions, as Bell showed, impose constraints on correlations, called Bell's inequalities. The key point is that they can be verified in a laboratory regardless of any theory.

Let us briefly illustrate Bell's inequalities by exemplifying the correlation of polarized entangled photons that were sent to distant Alice's and Bob's laboratories along the z axis. The partners measure dichotomous observables, i.e., polarizations that have only two values $+1$ or -1. Each partner measures two such observables. Alice chooses the settings of detectors a, a', Bob — b, b', which are unit vectors showing different angles in the x–y plane along which they can orient polarizing filters. For each pair of settings, correlation functions can be constructed: $\langle a,b\rangle$, $\langle a,b'\rangle$, $\langle a',b\rangle$, $\langle a',b'\rangle$, where $\langle\cdot|\cdot\rangle$ means the average of the product of outputs. On this basis, it is possible to build a new Bell observable $B = a,b + a,b' + a',b + a',b'$. Now, if we accept the assumptions of local realism, in particular that each photon had a certain polarization value ($+1$ or -1) before the measurement, it is easy to check that the absolute value of Bell's observable cannot exceed 2. Hence, we obtain Bell-CHSH inequality [96]:

$$|\langle ab + a'b + ab' - a'b'\rangle_{kl}| \equiv |\langle B\rangle| \le 2. \qquad (15)$$

Quantum mechanics predicts that the mean value of the B observable satisfies the inequality $|\langle B_{\rm QM}\rangle| \le 2\sqrt{2}$ which means that it breaks Bell-CHSH inequality, where $2\sqrt{2}$ is the so-called Tsirelson bound [97].

The verification of Bell's inequality based on the assumptions of local realism proved to be a great challenge for experimentalists, as it required the closure of three loopholes: (i) Locality demands that no signal traveling at the speed of light can inform the distant detector of its settings or the result of a measurement on the local detector before Alice and Bob complete the measurements; (ii) fair-sampling (or detector efficiency) demands that the sample of entangled pairs be a faithful representation of the entire ensemble being broadcast; (iii) freedom of choice requires that the hypothetical local variable should not influence the local choices of measurement setups on the part of Alice and Bob.

The first ground-breaking experiment that convincingly demonstrated breaking the Bell CHSH inequality and good agreement with the predictions of quantum mechanics was performed by Aspect et al. [12]. In their experiment, entangled photon pairs were emitted by the process of atomic calcium cascades. For the first time, the authors used acousto-optical switches, which pseudo-randomly changed the orientation of the analyzers in a short time compared to the photon transit time and detection. They achieved more than 95% of the detection efficiency.

Only in 2015, a series of the Bell tests based on quantum random number generators was performed, which closed both the locality and fair-sampling loophole in the same experiments [98].

Recently, two cosmic Bell tests with photons entangled in polarization have been performed, in which measurement settings were determined by real-time photon wavelength measurements from high red-shift quasars, light emitted billions of years ago. Thus, the authors closed two loopholes at once: locality and freedom of choice [99, 100]. However, these experiments failed to close the fair-sampling loophole. Quite recently, Pan et al. [101] performed an impressive local realism test that closes both locality and fair-sampling loophole and rules out common cause 11.5 years before the experiment, which largely closes the freedom of choice loophole.

The interpretation of violating Bell's inequality is still the subject of discussions [102, 103]. Bell tests show that the quantum correlations cannot be explained using any theoretical model based solely on local variables. This particular feature of quantum information, which has become known as quantum nonlocality (the Bell nonlocality), provides the resource for device-independent quantum key distribution [104–106] (see however [107]).

9. Weaker forms of breaking realism

While I am not going to offer a detailed review of the vast field of difference in Bell's inequality, let me raise two important related concepts. First, it should be mentioned that the violation of local realism by composed quantum systems has its weaker quantum analog, called quantum contextuality, observed with the help of random measurements of specially designed sets of quantum measurements pioneered by [108] which has many further developments (see [109–111]) and can be mathematically quantified [112]. Quite remarkably, it has the so-called state variant fully analogous to the Bell inequalities [113] as well as a state-independent one which is valid for any state, and basically reports the nonclassicality of the set of measurements involved [114].

The fundamental difference is that, roughly speaking, quantum contextuality can contradict classical realism only under the assumption of some bound on the dimension of the Hilbert space, while violation of the Bell inequalities via quantum states is the phenomenon that is independent of that assumption in general. This is why the violation of the inequalities in many cases leads to the powerful concept of quantum *self-testing* [115]. In the case of the inequality (15), self-testing means that independently of the complexity of local systems (for instance one may assume that each of the observables in (15) may concern not polarization but some other or even all of the photon internal degrees of freedom), the saturation of the quantum bound $2\sqrt{2}$ guarantees that up to local isometries and local partial traces the state is in the *unique* qubit form (14). This is an essence of the device independent variant of the Ekert entanglement-based encryption protocol (E91) [16] (see Sect. 11). Quantum self-testing is a cornerstone of device independent quantum cryptography which is based on the idea that only the output statistics of the devices are enough to guarantee cryptographic security without need of knowing the physical structure of the devices (for example see [116]).

Finally, there is a weaker variant of the Bell inequalities on composite systems that is still much stronger than contextuality. This is based on the so called quantum steering [43] in which we assume that for one of the particles the dimension of the Hilbert space is known (much like in contextuality tests) while in the other is not. This leads to the so-called semi-device independent quantum cryptography (see [117] and reference therein), [118].

10. Nonlocality and principle of information causality

The discovery of quantum nonlocality shook our perception of the foundation of quantum physics. Hence, a natural question arose: Is there a nonlocality stronger than that predicted by quantum formalism? Is this the only description that allows for nonlocal phenomena consistent with special relativity?

In the 1994 paper, Popescu and Rohrlich (PR) [119, 120] took nonlocality as the basic axiom and have proposed a model independent approach, consistent with special relativity, based on the conception of input-output black-box devices. In the approach, the experiments of Alice and Bob are space-like separated and each experiment is treated as a black-box. Then all the physical information obtained in the experiment is encapsulated in the joint probability $P(a,b|x,y)$ that Alice obtains a and Bob obtains b when Alice inputs x and Bob inputs y, respectively. In the simplest case where x, y, a, b have only two possible values, they must satisfy the constraints: $a \oplus b = xy$, where $\oplus$ denotes addition modulo 2. It is not difficult to verify that PR nonlocality leads to algebraic breaking of CHSH inequality equal to 4 which drastically breaks Tsirelson's limit $2\sqrt{2}$. Does nature allow information to be processed using such super-quantum correlations? Remarkably the physical principle of information causality was proposed [121], which excludes such a possibility. The information causality principle can be formulated briefly as: *The message cannot contain access to more information than the amount contained in it.* Contrary to its laconic form, this principle has strong implications:

- it strictly determines the maximum value of quantum correlations $\leq 2\sqrt{2}$,
- it is fulfilled by both classical theories and quantum mechanics,
- it excludes the physicality of the super strong Popescu–Rohrlich correlations.

It is significant that although the properties of quantum and classical information are basically different, they both follow the principle of information causality. It should be noted here that nonlocal PR boxes, although nonphysical, provide a conceptual tool in the modeling of nonlocality in the quantum physics and beyond [122–124]. It is remarkable that the PR correlations are under some circumstances a much more powerful resource than quantum entanglement as they lead to trivialising quantum communication complexity [125, 126]. However, they are weaker in another sense since in their language there is no room for nontrivial dynamics and continuous chance of settings of the measurements.

Finally, it is worth noting that in the case of three parties, the concept of relativistic causality that goes beyond the no-signaling paradigm is possible when space-time variables are explicitly involved [127, 128]. Quite recently, the general axiomatic approach to causality of the evolution of the spatial statistic detection has been initiated [129, 130].

11. Entanglement-based cryptography

As mentioned above, quantum correlations, apart from nonlocality, have another feature — they are random. It was intriguing that this randomness ensures a peaceful coexistence of quantum inscription predictions and special relativity, as partners cannot use the correlation to the instant telegraph. This specific "telegraphic no-go" has not yet had clear theoretical foundations, although recently an attempt to explain this phenomenon has been made [131].

As we saw, singlet-state photon pairs entangled generate anti-correlated random numbers at distant locations. Ekert first noticed that the randomness of these correlations could be used to generate a secure cryptographic key and proposed the protocol E91 [16] based on the entangled spin $\frac{1}{2}$ particles in singled state and Bell's theorem, and proposed implementation using nonlocal correlations between maximally entangled photon-pairs. Soon afterwards, Bennett, Brassard and Mermin proposed a simplified protocol based on entanglement without Bell's theorem, and showed that it is equivalent to BB84. The security of E91 is due to the fundamental property called monogamy of entanglement which expresses the fact that entanglement represents correlations that cannot be shared by third parties [29–31]. This peculiar entanglement trait not only provides the security of entanglement-based cryptography, but also sheds new light on physical phenomena in many correlated systems [132].

Experiment implementations of the E91 protocol have been made at ground stations [133, 134]. Both the production and analysis of entangled states have lately been tested with the SpooQy satellite, which is a step towards the realization of a cryptographic key generator based on entanglement in cosmic space [135]. Quite recently, the quantum key distribution has been analyzed with a small block length, which is crucial in entanglement-based quantum communication [136]. It should be emphasized that the original E91 protocol was prophetic as it suggested device-independent cryptography [105, 137], based on the Bell inequality breaking, which ensures that the data produced by quantum devices has a certain degree of secrecy, no matter how exactly the data was generated.

12. Canonical effects based on quantum entanglement

Ekert's work was important for another reason. Namely, it was the first to show that "ghostly" EPR correlations can be harnessed into something useful. Since then, entanglement has been viewed not as a curiosity, but as a real physical resource that can offer completely new unexpected effects. The breakthrough was the discovery of dual effects, i.e., dense coding and quantum teleportation in which the ebit plays a central role — a pair of qubits in a maximally entangled state, distributed between the sender and the receiver. Remarkably, both entanglement-based effects circumvent the non-cloning and Holevo theorem.

12.1. Super dense-coding

Suppose Bob wants to send to Alice two bits of information, using only one noiseless qubit. According to Holevo's theorem, only one bit can be transferred with one qubit. So Bob would need two qubits for this. Bennett and Wiesner showed [17] that if Alice and Bob have one ebit, then it is enough to send only one qubit to transmit one of the four messages (00,01,10,11) to Alice. To do this, Bob encodes messages using local different unitary operations U_{00}, U_{01}, U_{10}, U_{11} on his qubit, generating orthogonal Bell states (the Bell base), and sends the qubit to Alice, which measures the combined two qubits. The four orthogonal Bell states represent the four distinguishable messages.

The first implementation of a super-dense photon encoding protocol was made by Mattle et al. [138] in which Bob performed unitary operations using a combination of half and quarter revolutions of the wavelet. The dense coding protocol was later implemented in particular on atoms [139] and nuclear magnetic resonance [140].

12.2. Quantum teleportation

The most astonishing prediction of quantum inscription is quantum teleportation — a dual effect to dense coding that demonstrates the remarkable power of "exotic" combination of quantum and classical resources (see the fascinating story of the discovery [141]).

This time, Alice wants to send one qubit to Bob in an unknown state, but not by a physical qubit transfer, having two classic bits at her disposal. Obviously, quantum information cannot be transferred with classical bits.

Let us now consider the situation when we provide partners with 1 ebit of entanglement. Alice can now perform a measurement on her two particles, i.e., a qubit in an unknown state ϕ and a particle from the entangled pair. It is not hard to see that this measurement is identical to what Bob did in high-density coding. Alice gets one of four possible outcomes with a $\frac{1}{4}$ probability: 00,01,10,11. Having two bits at her disposal, Alice can send information via the classical channel to Bob which of the results she received. Depending on the result, Bob uses one of the transformations: $U_{00} \cong I$, $U_{01} \cong \sigma_x$, $U_{10} \cong \sigma_y$, $U_{11} \cong \sigma_z$, where σ_x, σ_y, σ_z, are standard Pauli operators. At this point, his particle from the entangled pair will be in state ϕ. Note that Alice's measurement provides no state information (the bits are completely random), but is part of a quantum operation. Thus, the transmission of the qubit had to take place immediately at the moment of Alice's measurement. There is no conflict with special relativity here because quantum inscription predicts that any operation on one subsystem does not cause measurable changes on the other subsystem regardless of the state of the entire system.

Note that there is no contradiction here with the prohibition on cloning, since the initial state of the qubit was completely erased in Alice's laboratory and then recreated, but not known in Bob's laboratory. It should be finally stressed that no information about the unknown state ϕ is transferred here via a classical channel that only conveys the message about the recovery operation at Bob's lab which is completely independent of ϕ.

The original teleportation protocol was extended to continuous variables [142, 143]. Quantum teleportation was demonstrated in pioneering experiments by the Zeilinger [25] and De Martini [26] teams. Furusawa and co-workers [27] independently carried out an unconditional teleportation on continuous variables (see in this context [142–146]). Later, quantum teleportation was demonstrated in many beautiful experiments [147–152]. In 2017, a photon was teleported from a Ngari ground station to the Micius satellite (with an orbit from 500 to 1400) [78, 153].

Quantum teleportation has been continuously researched for more than 20 years (see [154]) due to its central role in the development of quantum information processing including quantum computing [147, 155], the quantum internet and its relationship to the foundations of physics. Various generalizations of the original protocol have been proposed. In particular, the original protocol was generalized including a general teleportation channel [156], multiport teleportation [157–159], teleportation with multiple sender-receiver pairs [160] and telecloning [161].

12.3. Entanglement swapping

The peculiarity of multi-particle entanglement is that one can entangle particles that have never interacted with each other in the past. That such an effect may take place was first suggested by Yurke and Stoler (1992) [88]. This idea was implemented in the pioneering paper: *"Event-ready-detectors" Bell experiment via entanglement swapping.* In this scenario, arbitrarily distant partners Alice and Cecilia, and Bob and David share entangled EPR pairs of photons coming from independent sources

$$|\Phi^+\rangle_{AC} = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big),$$

$$|\Phi^+\rangle_{BD} = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big). \tag{16}$$

The system is then described as

$$|\Phi^+\rangle_{AC} \otimes |\Phi^+\rangle_{BD}. \tag{17}$$

Now Cecilia and Bob make a combined measurement in Bell's basis on B and C particles. As a result, A and D particles become entangled even though they never interacted with each other. Note that this is equivalent to teleporting entanglement of one EPR pair through the other. The entanglement swapping was soon generalized to multi-particle systems [162]. It provided the operational foundations of multi-photon interferometry, in particular the method of interference of photon pairs from independent sources (see review [163]). The entanglement swapping [164–166] has found applications, among others, in the generation of multi-photon entangled states [167], device-independent key distribution [168], construction of quantum repeaters [169–171], quantum photonics [172] and secret sharing [173, 174].

13. Detection of quantum entanglement

All of the above effects and many other non-classical tasks based on quantum information processing require high purity quantum entanglement. Unfortunately, this subtle resource is extremely sensitive to interaction with the environment and it degrades very quickly, i.e., pure states change into mixed (noisy) states with less entanglement. This opened up important issues: how to theoretically check whether a given state is entangled and is it possible to detect noisy entanglement in the laboratory?

In general, characterizing entangled states regardless of the measure of utility for specific tasks is the so-called NP difficult problem [175]. The partial characterization was achieved using criteria that provide necessary but not sufficient conditions for deciding whether a state is entangled or not. The breakthrough was the paper of Peres [176], who proposed an extremely strong separability test based on the partial transposition operation. From mathematical point of view, it is a positive but not completely positive map, thus a non-physical one. Such

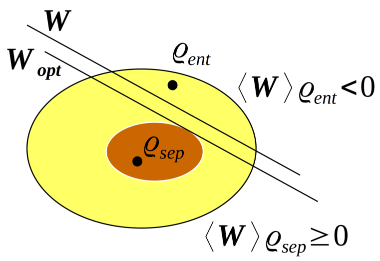

Fig. 3. The line represents a hyperplane corresponding to the entanglement witness W. All states located to the left of the hyperplane or belonging to it (in particular all separable states) provide nonnegative mean value of the witness, i.e., $\mathrm{Tr}(W\varrho_{\mathrm{sep}}) \geq 0$ while those located to the right are entangled states detected by the witness. The optimized entanglement witness is denoted by W_{opt}.

an operation is performed on one S_1 or S_2 of the subsystem on complex state of the system S. If the state subjected to such non-physical surgery does not survive in the sense that it will cease to be positive and lose its probabilistic interpretation, then the state was entangled. Mathematically speaking, this means that its partially transposed density matrix has at least one negative eigenvalue. Based on the complete classification of positive mappings for low dimensions [177], it was proved that the PPT condition is a necessary and sufficient condition for the separability of 2×2 and 2×3 systems [178] which gives a complete characterization for low-dimensional states of systems. In general, a necessary and sufficient, albeit non-operational, separability condition based on positive mappings was provided [36].

The above structural criteria based on positive non-physical mappings of the quantum state, while strong, cannot be implemented in a laboratory. Fortunately, based on the geometric properties of convex sets, it was possible to formulate a linear separability criterion that could be implemented physically. Namely, from the convex set theory and the Hahn–Banach theorem, it follows that for any entangled state ϱ_{ent} there exists a hyperplane in the space of operators separating ϱ_{ent} from the set of separable states S. Such a hyperplane is defined uniquely by the Hermitian operator W (entanglement witness) [179]. Then, the state is entangled if expectation value W on ϱ_{ent} is negative, i.e., $\langle W\rangle\varrho_{\mathrm{ent}} < 0$ whereas its expectation value on all separable states $\langle W\rangle\varrho_{\mathrm{sep}} \geq 0$ (see Fig. 3).

It was shown that such a witness can be optimized by shifting the hyperplane parallel to the set S [180, 181]. Thus, the detection of entanglement consists in measuring the mean value of a properly selected observable. Remarkably, there is a "footbridge" Jamiolkowski isomorphism [182] which allows to go from nonphysical positive maps to the physical measurable quantities to Hermitian operators (entanglement witness), which provides a necessary and sufficient condition separability [178].

The entanglement witness criterion has a number of advantages: (i) it is universal in the sense that for any entangled state there always exists an entanglement witness, (ii) it certifies entanglement in experiments in the presence of noise, (iii) it allows to detect the presence of entanglement even in several measurements in contrast to tomography, where the number of measurements increases exponentially with the number of particles. The disadvantage is that the witness must be precisely selected for the examined state. The quantum entanglement detection based on entanglement witnesses has found wide applications for the certification of two- and multipartite states [183–191] in different physical scenarios. Interestingly, the concept of a measurement-device-independent entanglement witness which allows one to demonstrate entanglement of all entangled quantum states with untrusted measurement apparatuses was introduced [192].

The theory of entanglement detection was developed in different directions [36, 193]. The other separability criteria based on a correlation tensor were proposed [194–196] for a bipartite and multipartite scenario. It has recently been proved that enhanced nonlinear realignment criterion [197] is equivalent to the family of linear separability criteria based on a correlation tensor, i.e., the family of (linear) entanglement witnesses [198]. It was also demonstrated that the separability criteria based on the correlation tensor are weaker than a positive partial transposition criterion [199].

14. Entanglement distillation and bound entanglement

After Peres discovered the entanglement criterion of partial transposition, a problem arose. If the state was untangled, it will remain untangled after a partial transposition operation. It was natural to ask whether there are states in nature that are entangled and have a positive partial transposition? When such states were discovered in 1997 [200], they were treated as a mathematical singularity with no reference to physical reality. At about the same time, Bennett and colleagues were working on the problem of how to reverse the entanglement degradation process. In 1996, they published a paper that played a key role in the theory of entanglement manipulation [201] (see also [202]). Namely, they introduced a natural class of entanglement manipulation operations by experimentalists in distant laboratories: the two partners can perform any local operations on their entangled particles and communicate via the classical channel (LOCC). Consequently, they introduced the entanglement distillation protocol: The two partners share n copies of the ϱ_{AB} state which contains noisy entanglement. With the help of local quantum operations and classical communication, they determine a smaller number of m ($m < n$) of almost maximally entangled pairs — two-qubit singlet states $|\Psi^-\rangle_{AB}$. When the protocol is optimal, the constant $m/n = D$ is a measure of entanglement in a noisy state ϱ (distillable entanglement).

Distillation protocol raised a natural question: Can all noisy states be distilled in this way? It turned out that all noisy entangled two-qubit states can be distilled [203]. It was a big surprise that the distillation protocol does not work for the higher dimension systems [31, 204]. It turned out that the environment can contaminate pure entanglement in such a way that it is no longer possible to recover it by distillation with LOCC. Thus, the entangled states with positive partial transposition are non-distillable. Thus, in nature there are at least two types of noise entanglement: free, that is, distillable entanglement, and bound entanglement that cannot be distilled with LOCC [205]. After 12 years, several centers simultaneously created the bound entanglement in a laboratory on the photons [206, 207], on ions [208], in liquid in NMR [209], with light in continuous variable [210] regime.

It has been shown that the bound entanglement is not a rare phenomenon, since its presence was detected in thermal spin systems [211, 212]. Another surprise was that the bound entanglement can be activated [213] and that a cryptographic key can be extracted from bound entangled states [214]. The latter leads to the general paradigm for distilling classical key from quantum states in terms of the so-called private bits (P-bits) [215] (see experimental implementation [216]). Moreover, bound entangled states can violate the Bell inequalities [217] and can be useful in quantum metrology [218–220]. Another interesting open problem is the use of bound entanglement states in the device-independent quantum key distribution [221–223].

15. Breaking the classical order

When analyzing the structure of entangled states, Schrödinger noticed another peculiarity of quantum correlations that astonished him, as evidenced by the three question marks that appear in his unpublished notes in 1932 (Note in arxiv). In 1935, he makes a laconic conclusion: "Best possible knowledge of a whole does not include best possible knowledge of its parts – and that is what keeps coming back to haunt us." [224]. It was very disturbing because it meant breaking the classical order in complex systems. As is known in the classical world, the measure of the randomness (disorder) of an individual random variable X is the Shannon entropy

$$H(X) = -\sum_i p_i \log\left(p_i\right), \tag{18}$$

where p_i — probabilities of events, and $\sum p_i = 1$.

For two random variables X and Y, the total Shannon entropy is $H(X,Y) = \sum_{ij} p_{ij} \log(p_{ij})$ and conditional entropies $H(X|Y)$, $H(Y|X)$ are always

$$\begin{aligned} &H(X|Y) \equiv H(X,Y) - H(Y) \geq 0, \\ &H(Y|X) \geq 0, \end{aligned} \tag{19}$$

which shows that the entropy of subsystems $H(X)$, $H(Y)$ never exceeds the total entropy of the system $H(X,Y)$.

In the quantum world, the measure of quantum disorder is the von Neumann entropy $S(\varrho)$:

$$S(\varrho) = -\mathrm{Tr}\Big(\varrho\log(\varrho)\Big) = \sum \langle\phi_i|\varrho\log(\varrho)|\phi_i\rangle, \tag{20}$$

defined for the state ϱ, where $\{\phi_i\}$ — any complete orthogonal system in H. When density matrix ϱ is diagonal, it can be regarded as a quantum counterpart of a classical discrete probability distribution as a natural description of quantum information source. The von Neumann entropy can be then written in a form similar to the Shannon entropy

$$S(\varrho) = -\sum_i p_i \log(p_i), \tag{21}$$

where the quantum probabilities p_i are the eigenvalues of the operator ϱ and satisfy $\sum p_i = 1$.

The Schrödinger observation was quantified using the von Neumann entropy [225, 226]. It has been proved that the entropy of the subsystem A or B can be greater than the entropy of the entire system AB only when the system is in an entangled state. This implies that quantum conditional entropies $S(A|B) \equiv S(AB) - S(B)$, $S(B|A)$ can be negative, which means that the disorder in the whole AB system may be smaller than in the subsystems A or B. Recalling our example with photons entangled in polarization, we can see that everything agrees. The polarizations of the photons measured in the laboratories of Alice and Bob are completely random, while the entangled pair is in perfect order. Thus, the entanglement can break the classical order which is the source of the informational "paradox" of Schrödinger.

16. Negative information in quantum communication

Breaking of the classical order was both intriguing and incomprehensible, especially in the context of Shannon's theory, in view of the fact that the negativity of quantum conditional entropy had no operational significance. Let us recall that at the heart of the classical Shannon communication theory is the theorem of noiseless coding, which says that a necessary and sufficient number of bits for faithful transmission is equal to Shannon's entropy H [2]. Schumacher showed that if in Shannon's theory we replace messages by quantum states and bits by qubits, then the necessary and sufficient number of qubits for faithful transmission is equal to the von Neumann entropy $S(\varrho)$ [23]. Soon afterwards, Schumacher and Westmoreland [227] and Holevo [228] generalized Shannon's channel coding theorem. Three kinds of quantum channel capacities were introduced: classical, quantum, and private capacity, which play an important role in quantum communication [29, 229–232]. The essential difference between the last two capacities is the following: the quantum capacity is achieved in the process which guarantees that information in any basis stays uncorrelated from the environment after the transfer (which may be shown to be equivalent to BB84 paradigm). Remarkably in the definition private capacity much more relaxed condition is required: only one base is needed to stay uncorrelated in the above sense. Note that the private capacity while in general higher than the quantum one may have subject to severe restriction in quantum repeater scenario [233] (see more, [28]).

Meanwhile, for a long time there has been no quantum counterpart of the Slepian–Wolf theorem [234]. Namely, in 1973, Slepian and Wolf formulated in the framework of classical communication the following problem: Two partners Alice and Bob have random variables X and Y that are correlated with each other. Bob is given some incomplete information of Y in advance. Alice is in the possession of the missing information of X. Bob's job is to obtain the missing information of X. The question is how much additional information Alice has to send to her partner. Slepian and Wolf proved that the amount of information that Bob needs is expressed by the conditional entropy: $H(X|Y) \equiv H(XY) - H(Y)$ which is a measure of the partial information that Alice must send to Bob. This quantity is always positive.

In 2005, Horodecki et al. [235] proposed a quantum version of the above scenario: Alice and Bob have a system in some unknown quantum state ϱ_{AB} which contains the complete information. Bob has some information about state ϱ_B, while Alice has the missing information ϱ_A. The task is as follows: how much information does Alice have to send to Bob for him to have complete information. The quantum equivalent of the Slepian–Wolf theorem says that this quantity is given by the von Neumann quantum conditional entropy

$$S(A|B) \equiv S(AB) - S(B), \tag{22}$$

where $S(B)$ is the entropy of the Bob state while $S(AB)$ is the entropy of the cumulative ϱ_{AB} state. Contrary to the classical conditional entropy $H(X|Y)$, the conditional entropy can be both positive and negative. The conditional quantum entropy has an operational interpretation of missing information:

- If $S(A|B)$ is positive — this is the missing information that Alice must send to Bob via qubits (classical analogue).
- If $S(A|B)$ is negative, Alice does not need to send the missing information via qubits. Additionally, Bob and Alice get free "quantum impulses" to send a certain number of qubits in the future, for example for teleportation.

Finally, it should be stressed that the above analysis is a strong completion of the previous result [236] which says that for any state with the negative quantity (22), there exists an entanglement distillation protocol with one-way classical communication (from Alice to Bob) that achieves the number of e-bits per an input noisy pair given by (22).

17. Entropy inequalities — nonlinear witnesses of entanglement

The von Neumann entropy can be generalized to the Rényi family α-entropy $S_\alpha(\varrho)$:

$$S_\alpha(\varrho) = \frac{1}{1-\alpha} \ln\Big(\mathrm{Tr}\,(\varrho^\alpha)\Big) \tag{23}$$

for $\alpha > 1$.

It is easy to check that the Rényi entropy in the $\alpha \to 1$ limit turns into the von Neumann entropy $S(\varrho)$. The natural question was whether there are quantum states that satisfy the analog of classical inequalities (19). In 1996 [237], it was proved that all non-entangled (separable) states at a finite dimensional Hilbert space for $\alpha = 1.2$ satisfy α-entropic inequalities

$$S_\alpha(A|B) = S_\alpha(\varrho_{AB}) - S_\alpha(\varrho_B) \geq 0,$$

$$S_\alpha(B|A) = S_\alpha(\varrho_{AB}) - S_\alpha(\varrho_A) \geq 0. \tag{24}$$

It presents entropic nonlinear entanglement criterion which does not require a priori knowledge of the state.

Nonlinear experimentally friendly collective entanglement witnesses were also proposed, which do not require prior knowledge of a given state [238, 239] either. In [240], Bovino et al. demonstrated the first experimental measurement of a non-linear entanglement witness $S_2(\varrho) = -\mathrm{Tr}\left(\ln(\varrho^2)\right)$, using local measurement on two pairs of polarization entangled photons.

At first, it seemed that the entropy criterion based on nonlinear entanglement witnesses, generally weaker than the criterion based on linear ones, will not play a major role. However, it turned out that the feature of non-linearity is its strength. In particular, the nonlinear entanglement witnesses "feel" the subtle features of entanglement in quantum multi-body systems. In the last decade, there has been a renaissance of entropic witnesses opening up the field for wide applications. For pure or nearly pure states, entanglement was detected using the Rényi S_2 entropy via a multi-body quantum interference [241–245] and local random measurements [246–250]. An experimental measurement of nonlinear witnesses of collective entanglement using hyper-entangled two-quart states has been performed [251], see also [252]. Quite recently, an experimental multi-body mixed state detection method has been proposed based on the positive partial transposition of a density matrix condition. This protocol gives the first direct PT measurement of moments in a multi-body system [253].

18. Quantum parallelism as basis for quantum computing

Quantum computing is processing information using a sequence of unitary operations (quantum gates) in order to obtain an answer to a predetermined question, e.g. if a given number factorizable with high probability [254]. As we have seen, a single qubit allows two basic states to be stored and processed simultaneously. The problem is that the decoherence process being a result of disturbance by environment occurs within a short time (decoherence time) and destroys the coherence. Roughly speaking, decoherence time is the characteristic time for a generic qubit state (2) to be transformed into the mixture $\varrho = |a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1|$. One of the basic conditions for effective quantum computing requires long relevant decoherence times, much longer than the gate operation time. This is one of the five basic DiVincenzo criteria required for a physical implementation of quantum computing [255]. If we take a superposition of n qubits, then a pure state will represent a simultaneous superposition of $N = 2^n$ possible distinct basic states

$$|\Psi\rangle = \sum_{i=0}^{N-1} C_i|i\rangle. \tag{25}$$

It is remarkable that one can process simultaneously an exponential number of basic states. This feature (quantum parallelism) underlies the superiority of quantum computing over classical one. To illustrate the latter, suppose that we have access to a quantum oracle that computes a given function $f(i)$ from an input i of n qubits ($i = 0, 1 \ldots 2^n$).

Having a prepared string of qubits in the fiducial state of 0 and applying to each qubit, in parallel, a Hadamard gate, we obtain a register of n qubits in an equal superposition of all bit strings

$$H|0\rangle \otimes H|0\rangle \otimes \cdots \otimes H|0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle, \tag{26}$$

where $|i\rangle$ is the computational basis state indexed by the binary number that would correspond to the number i in base-10 notation.

Now, suppose that the function f is evaluated by unitary transformation $U_f : |x\rangle|0\rangle \to |x\rangle|f(x)\rangle$, then the linearity of quantum formalism implies

$$U_f : \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle|0\rangle \quad \to \quad \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle|f(0)\rangle. \tag{27}$$

This means that all possible evaluations of the function $f(x)$ can be done in a single step.

The idea of quantum computing received a lot of support when it was discovered that certain difficult computational problems, such as number factoring (Shor's algorithm [22]) and searching unstructured data (Grover's algorithm [24]), can be solved far more efficiently than classically. The efficiency of computation is measured by the computation complexity that is the number of steps required to solve a given task as a function of the size of the input. The important discovered algorithms: the Deutsch–Jozsa [18], Shor [22] and Grover [24] demonstrate quantum supremacy over classical computing. All three algorithms have been implemented on primitive quantum computers based on NMR techniques [256], in ions traps [257] and quantum dots [258]. Since then, many other algorithms have been discovered, such as the quantum simulations [259] and variational quantum solvers [260] which demonstrate quantum supremacy (see more [261]).

Any realistic implementation of universal quantum computation is a big challenge. It must meet the DiVincenzo criteria [255]. Apart from the decoherence criterion, there are four more:

1. A scalable physical system with well characterized qubits.
2. The ability to initialize the state of the qubits to a simple fiducial state.
3. A "universal" set of quantum gates.
4. A qubit-specific measurement capability (see details [255]).

Notoriously, the quantum computing process is disturbed by the interaction with the environment, causing the occurrence of errors. Therefore, both the bit (0,1) and phase ("0 + 1", "0 − 1") must be protected. This seems impossible due to the non-cloning theorem. Fortunately, Shor [21] and Steane [262] overcame this difficulty by introducing the error correction codes. The trick is that the information of one logical qubit can be spread onto a highly entangled state of several physical qubits

$$|0\rangle \to |\mathbf{0}\rangle_{\boldsymbol{L}} = [(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \times(|000\rangle + |111\rangle)]/2\sqrt{2}, \tag{28}$$

$$|1\rangle \to |\mathbf{1}\rangle_{\boldsymbol{L}} = [(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \times(|000\rangle - |111\rangle)]/2\sqrt{2}. \tag{29}$$

This code first introduced by Shor [21] corrects both the bit error σ_x and phase error σ_z.

Of course, the error correction procedure itself is not error-free. Fortunately, the possibility of efficient quantum computing is based on the so-called threshold theorem: If error probability of elementary operation is smaller than some threshold value $p < p'$, then efficient quantum computing is possible [263, 264]. In practice, this condition, which is the basis of efficient quantum computing, is extremely demanding. Already in 1995, it was demonstrated that the quantum computing can be implemented with cold ions confined in a linear trap and interacting laser beams [265]. The first 7-qubit quantum computer from IBM and Stanford University based on nuclear magnetic resonance realized Shor's algorithm, decomposition of the number $15 = 3 \times 5$ [256].

The scale of the difficulties is evidenced by the fact that a qualitative breakthrough in this field took place only after 18 years. Namely, researchers at Google's quantum-computing laboratory in Santa Barbara, California, announced the first-ever demonstration of quantum supremacy on the 53 qubit quantum computer Sycomore, made of superconducting circuits that are kept at ultracold temperatures [266]. It executes algorithms quantum with 1500 gates. It is an impressive achievement, however, it was designed for a specific problem — boson sampling [267], which is a simplified non-universal model for quantum computing that may hold the key to implementing the first ever post-classical quantum computer. More specifically, this is the process in which a very nontrivial output statistic is achieved quantumly which requires (under some reasonable assumptions) exponentially longer time to be produced by classical machines. While it is not a quantum algorithm in a standard form, its remarkable practical applications to fast finding of some graph properties are predicted.

In December 2020, Jian-Wei Pan and colleagues at the University of Science and Technology of China in Hefei announced a photon-based quantum computer, which demonstrates quantum supremacy via boson-sampling with 50–70 detected photons [268]. It could find solutions to the boson-sampling problem in 200 seconds, while classical China's Taihu-Light supercomputer needs 2.5 billion years. In contrast to Google's Sycamore, the Chinese team's photonic circuit is not programmable [269].

19. Entanglement — resource in quantum metrology

The discovery that the use of entangled states in quantum metrology can improve the precision of measurements [270, 271] led to a rapid development of quantum enhanced metrology [49] which allows to measure physical quantities by estimating the phase shift θ using interferometric techniques. A basic problem in quantum metrology can be formulated as in the diagram of Fig. 4: A probe state ϱ of N particles is prepared and then is subject to a parameter-dependent quantum channel Λ_θ. The state $\varrho_\theta = \Lambda_\theta(\varrho)$ is finally measured via the POVM measurement $\{\Pi_i\}_I$. It provides conditional probability distribution $p(i|\theta)$, which is used to estimate θ via the estimator function $\widetilde{\Theta}(i)$ for the given measurement outcome i. The estimation of the phase shift is limited by uncertainty

$$\Delta^2\widetilde{\theta} = \left\langle \left(\widetilde{\theta} - \theta\right)^2 \right\rangle, \tag{30}$$

where $\langle\cdot|\cdot\rangle$ means the average over all measurement results. The task is to find the optimal probe

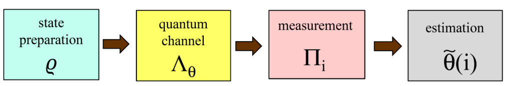

Fig. 4. Phase estimation scheme.

state ϱ, the optimal measurement Π and estimator, which minimize the uncertainty. For unbiased estimators and m independent measurements, the phase uncertainty is limited by the quantum Cramer–Rao bound

$$\Delta\widetilde{\theta} \geq \frac{1}{\sqrt{m F_Q(\varrho_\theta)}} \tag{31}$$

where F_Q is the quantum Fisher information which quantifies the asymptotic usefulness of quantum state and it can be estimated for different quantum channels [49].

For unitary and noiseless quantum channel $\varrho_\theta = \Lambda_\theta(\varrho) = \mathrm{e}^{-\mathrm{i}H\theta}\varrho\mathrm{e}^{+\mathrm{i}H\theta}$, the quantum Fisher information optimized over measurement can be expressed in the form

$$F_Q(\varrho, H) = 2\sum_{k,l} \frac{(\lambda_k - \lambda_l)^2}{\lambda_k + \lambda_l} |\langle k|H|l\rangle|^2, \tag{32}$$

where H is the generator of the phase shift of the system, and $\varrho = \sum_k \lambda_k |k\rangle\langle k|$, $\sum_k \lambda_k = 1$.

For unitary dynamics of the linear two-mode interferometer, the generator of the phase shift is $H \equiv \boldsymbol{J}_{\vec{n}} = \vec{n}\cdot\boldsymbol{J}$, where $\boldsymbol{J}_{\vec{n}}$ is a component of the collective spin operator angular momentum in the direction $\vec{n}$. It has been shown [272, 273] that for the separable input N-particle states, the quantum Fisher information is bounded by $F_Q(\varrho_{\mathrm{sep}}, \boldsymbol{J}_{\vec{n}}) \leq N$. Hence, the phase uncertainty $\Delta\widetilde{\theta}$ is bounded by the standard quantum limit (SQL) $\Delta\theta_{SN} : \Delta\widetilde{\theta} \geq \Delta\theta_{SN}$, where

$$\Delta\theta_{SN} = \frac{1}{\sqrt{mN}}. \tag{33}$$

By using entangled probe states, it is possible to overcome the SQL [49]. Quantum formalism imposes fundamental constraints on measurement precision that scales like $1/N$. It has been shown that for general probe states of N particles, F_Q is bounded by $F_Q(\varrho, \boldsymbol{J}_{\vec{n}}) \leq N^2$, [272, 273] and this inequality can be saturated by certain maximally entangled states. It allows to obtain the optimal Heisenberg bound for the phase uncertainty

$$\Delta\theta_{HN} = \frac{1}{\sqrt{m}}\frac{1}{N}. \tag{34}$$

Note that the genuine multipartite entanglement is needed for reaching the highest sensitivities in some metrological tasks using two-mode linear interferometer [274–276]. Recently, various experiments have demonstrated beating the SQL (see [277] and references therein).

In a realistic scenario, quantum phase estimation requires taking into account the influence effects of losses and decoherence [278–285]. In particular, for N probe particles prepared in state ϱ^N and noisy channel $\Lambda_\Theta^{\otimes N}$, that acts independently on each particle $\varrho_\theta^N = \Lambda_\Theta^{\otimes N}(\varrho^N)$, quantum Fisher information $F_Q(\varrho_\theta^N)$ has asymptotically in N a bound that scales linearly with N: $F_Q(\varrho_\theta^N) \leq N\alpha$ giving bound [281]:

$$\Delta\widetilde{\theta} \geq \frac{1}{\sqrt{\alpha m N}}, \tag{35}$$

where α is constant. Thus, the supremacy over SQL is only limited to constants factor. In particular, in the optical interferometry with losses for a generic two-mode input N-photon state with precisely defined total photon number N, the limit of phase sensitivity is

$$\Delta\widetilde{\theta} \geq \sqrt{\frac{1-\eta}{\eta N}}, \tag{36}$$

where η is the optical transfer coefficient. This bound generalized to states having uncertainty of the photon number, such as coherent states and squeezed states, was used to estimate the fundamental bound on GEO 600 interferometer strain sensitivity [286], where the phase noise decoherence [287], and quantum back-action are negligible [270]. It has been shown that the coherent-state squeezed vacuum strategy is the optimal one for phase estimation with high precision on absolute scale [286].

Recently, a framework for optimization of quantum metrological protocols based on the tensor network approach for the channel with the correlated noise and the phase parameter unitarily encoded has been presented [285]. Note that the multiparameter estimation theory offers a general framework to explore imaging techniques beyond the Rayleigh limit [288].

Generally, the relationship between quantum metrology and the structure of quantum states is still not entirely clear. For example, there are very weakly entangled states (bound entangled states) metrologically useful [218, 219] as well highly entangled states that are not useful for metrology [289]. It leads to the question: Are there any situations where some synergy effects possibly occur with analogy to previous communication protocols such as activation of bound entanglement?

In an attempt to answer this question, the criterion of metrological usefulness has been proposed as follows [290]: The state ϱ is metrologically useful if there exists Hamiltonian H such that Fisher quantum information (32) is sharply greater than Fisher information for separable states $F_Q(\varrho_{\mathrm{sep}}, H)$ maximized over all separable states

$$F_Q(\varrho, H) > \max_{\varrho_{\mathrm{sep}}} = F_Q(\varrho_{\mathrm{sep}}, H) =: F_Q^{(\mathrm{sep})}(H). \tag{37}$$

Then, the metrological gain with respect to the Hamiltonian H defined as $g_H(\varrho) = F_Q(\varrho, H)/F_Q^{(\mathrm{sep})}(H)$ leads to the optimal gain $g(\varrho) = \max_{\mathrm{local} H} g_H(\varrho)$. Having such defined metrological usefulness, it has been shown that the bipartite entangled states that cannot outperform separable states in any linear interferometer, however, can still be more useful than separable ones if several copies of them are considered or an ancilla is added to the quantum system. In particular, it has been proved that all entangled bipartite pure states are metrologically useful.

20. Final remarks

In this article, I have focused only on selected aspects of quantum information. There are many other fascinating phenomena that deserve presentation. These include quantum correlations beyond entanglement [44, 291], nonlocality without entanglement [292], quantum channel super activation effect [44, 293], locking classical correlations in quantum states [294], resources theoretical approach to quantum thermodynamics [40], quantum Darwinism [295–297], objectivity [298–301], quantum based randomness amplification against postquantum attacks [302–304] and others. They all underline the extremely complex nature of quantum information, which is not yet fully understood and provokes many open questions (see for example [305]). Among others there is a long-standing question: Can the quantum formalism be consistently extended to include quantum gravitation effect? If so, how will it impact the quantum information concept?

Acknowledgments

I would like to thank J. Mostowski and A. Wysmołek for encouraging me to write this article based on the lecture given at the Extraordinary Congress of Polish Physicists on the occasion of the centenary of the Polish Physical Society. I would also like to thank J. Horodecka and Ł. Pankowski for their help in editing this paper. I acknowledge the support of the Foundation for Polish Science through the IRAP project co-financed by the EU within the Smart Growth Operational Programme (Contract No. 2018/MAB/5).

References

[1] J. von Neumann, *Mathematische Grundlagen der Quantenmechanic*, Springer, Berlin 1932.

[2] C.E. Shannon, *Bell Syst. Techn. J.* **27**, 379 (1948).

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

[4] J.L. Park, *Foundat. Phys.* **1**, 23 (1970).

[5] S. Wiesner, *ACM SIGACT News* **15**, 78 (1983).

[6] A.S. Holevo, *Probl. Peredachi Inf.* **9**, 3 (1973).

[7] J.P. Gordon, in: *Quantum Electronics and Coherent Light; Proc. Int. School of Physics Enrico Fermi*, Ed. P.A. Miles, Course XXXI, Vol. 156, Academic Press, New York 1964.

[8] L.B. Levitin, in: *Proc. Fourth All-Union Conf. on Information and Coding Theory*, Sect. II, Tashkent, 1969.

[9] R.S. Ingarden, *Rep. Math. Phys.* **10**, 43 (1976).

[10] R. Ingarden, A. Kossakowski, M. Ohya, *Information Dynamics and Open Systems: Classical and Quantum Approach*, Kluwer Academic, 1997.

[11] J.S. Bell, *Physics Physique* **1**, 195 (1964).

[12] A. Aspect, J. Dalibard, G. Roger, *Phys. Rev. Lett.* **49**, 1804 (1982).

[13] C.H. Bennett, G. Brassard, in: *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, IEEE Computer Society Press, New York 1984, p. 175.

[14] D. Deutsch, *Proc. R. Soc. Lond. A Math. Phys. Sci.* **400**, 97 (1985).

[15] R.P. Feynman, *Quant. Mech. Comput. Foundat Phys.* **16**, 507 (1986).

[16] A.K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).

[17] C.H. Bennett, S.J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).

[18] D. Deutsch, R. Jozsa, *Proc. R. Soc. Lond. A Math. Phys. Sci.* **439**, 553 (1992).

[19] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).

[20] M. Żukowski, A. Zeilinger, M.A. Horne, A.K. Ekert, *Phys. Rev. Lett.* **71**, 4287 (1993).

[21] P.W. Shor, *Phys. Rev. A* **52**, R2493 (1995).

[22] P.W. Shor, *SIAM J. Comput.* **26**, 1484 (1997).

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

[24] L.K. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).

[25] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, *Nature* **390**, 575 (1997).

[26] D. Boschi, S. Branca, F.D. Martini, L. Hardy, S. Popescu, *Phys. Rev. Lett.* **80**, 1121 (1998).

[27] A. Furusawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, E.S. Polzika, *Science* **282**, 706 (1998).

[28] M. Wilde, *From Classical to Quantum Shannon Theory*, Cambridge University Press, 2019.

[29] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).

[30] V. Coffman, J. Kundu, W.K. Wootters, *Phys. Rev. A* **61**, 052306 (2000).

[31] B.M. Terhal, M.M. Wolf, A.C. Doherty, *Phys. Today* **56**, 46 (2003).

[32] M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge 2000.

[33] H.-P. Breuer, F. Petruccione, *The Theory of Open Quantum Systems*, Oxford University Press, 2002.

[34] W. Heisenberg, *Z. Phys.* **43**, 172 (1927).

[35] N. Bohr, *Nature* **121**, 579 (1928).

[36] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, *Rev. Mod. Phys.* **81**, 865 (2009).

[37] E. Schrödinger, *Math. Proc. Cambridge Philos. Soc.* **31**, 555 (1935).

[38] R. Horodecki, M. Horodecki, P. Horodecki, *IBM J. Res. Developm.* **48**, 139 (2004).

[39] J.M. Raimond, M. Brune, S. Haroche, *Rev. Mod. Phys.* **73**, 565 (2001).

[40] E. Chitambar, G. Gour, *Rev. Mod. Phys.* **91**, 025001 (2019).

[41] L. Amico, R. Fazio, A. Osterloh, V. Vedral, *Rev. Mod. Phys.* **80**, 517 (2008).

[42] O. Gühne, G. Tóth, *Phys. Rep.* **474**, 1 (2009).

[43] H.M. Wiseman, S.J. Jones, A.C. Doherty, *Phys. Rev. Lett.* **98**, 140402 (2007).

[44] K. Modi, A. Brodutch, H. Cable, T. Paterek, V. Vedral, *Rev. Mod. Phys.* **84**, 1655 (2012).

[45] A. Streltsov, G. Adesso, M.B. Plenio, *Rev. Mod. Phys.* **89**, 041003 (2017).

[46] J. Goold, M. Huber, A. Riera, L. del Rio, P. Skrzypczyk, *J. Phys. A Math. Theoret.* **49**, 143001 (2016).

[47] V. Scarani, A. Acín, G. Ribordy, N. Gisin, *Phys. Rev. Lett.* **92**, 057901 (2004).

[48] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).

[49] L. Pezzé, A. Smerzi, M.K. Oberthaler, R. Schmied, P. Treutlein, *Rev. Mod. Phys.* **90**, 035005 (2018).

[50] H. Buhrman, R. Cleve, S. Massar, R. de Wolf, *Rev. Mod. Phys.* **82**, 665 (2010).

[51] C. Brukner, M. Żukowski, J.-W. Pan, A. Zeilinger, *Phys. Rev. Lett.* **92**, 127901 (2004).

[52] P. Trojek, C. Schmid, M. Bourennane, C. Brukner, M. Żukowski, H. Weinfurter, *Phys. Rev. A* **72**, 050305 (2005).

[53] W.H. Zurek, *Rev. Mod. Phys.* **75**, 715 (2003).

[54] R. Heilmann, M. Gräfe, S. Nolte, A. Szameit, *Sci. Rep.* **4**, 4118 (2014).

[55] V.V. Samartsev, T.G. Mitrofanova, *J. Phys. Conf. Series* **1283**, 012012 (2019).

[56] R. Hanson, J.M. Elzerman, L.H.W. van Beveren, L.M.K. Vandersypen, L.P. Kouwenhoven, in: *IEDM Technical Digest. IEEE Int. Electron Devices Meeting, 2004*, IEEE, 2005, p. 533.

[57] D. Press, T.D. Ladd, B. Zhang, Y. Yamamoto, *Nature* **456**, 218 (2008).

[58] T. Yamamoto, Y.A. Pashkin, O. Astafiev, Y. Nakamura, J.S. Tsai, *Nature* **425**, 941 (2003).

[59] A.F. Kockum, F. Nori, in: *Fundamentals and Frontiers of the Josephson Effect*, Springer Int., 2019, p. 703.

[60] E. Knill, R. Laflamme, G.J. Milburn, *Nature* **409**, 46 (2001).

[61] P. Kok, W.J. Munro, K. Nemoto, T.C. Ralph, J.P. Dowling, G.J. Milburn, *Rev. Mod. Phys.* **79**, 135 (2007).

[62] M. Parniak, M. Dabrowski, M. Mazelanik, A. Leszczynski, M. Lipka, W. Wasilewski, *Nature Commun.* **8**, 2140 (2017).

[63] E.P. Wigner, *The Probability of the Existence of a Self-Reproducing Unit*, London 1961.

[64] W.K. Wootters, W.H. Zurek, *Nature* **299**, 802 (1982).

[65] D. Dieks, *Phys. Lett. A* **92**, 271 (1982).

[66] V. Bužek, M. Hillery, *Phys. Rev. A* **54**, 1844 (1996).

[67] H. Fan, Y.-N. Wang, L. Jing, J.-D. Yue, H.-D. Shi, Y.-L. Zhang, L.-Z. Mu, *Phys. Rep.* **544**, 241 (2014).

[68] A.K. Pati, S.L. Braunstein, *Nature* **404**, 164 (2000).

[69] U. Alvarez-Rodriguez, M. Sanz, L. Lamata, E. Solano, *Sci. Rep.* **5**, 11983 (2015).

[70] M. Oszmaniec, A. Grudka, M. Horodecki, A. Wójcik, *Phys. Rev. Lett.* **116**, 110403 (2016).

[71] K. Li, G. Long, H. Katiyar, T. Xin, G. Feng, D. Lu, R. Laflamme, *Phys. Rev. A* **95**, 022334 (2017).

[72] X.-M. Hu, M.-J. Hu, J.-S. Chen, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, Y.-S. Zhang, *Phys. Rev. A* **94**, 033844 (2016).

[73] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, *J. Cryptol.* **5**, 3 (1992).

[74] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, H. Zbinden, *New J. Phys.* **4**, 41 (2002).

[75] S. Wengerowsky, S.K. Joshi, F. Steinlechner et al., *Proc. Natl. Acad. Sci.* **116**, 6684 (2019).

[76] M. Peev, T. Länger, T. Lorünser, A. Happe, O. Maurhart, A. Poppe, T. Themel, in: *Optical Fiber Communication Conference and National Fiber Optic Engineers Conf.*, OSA, 2009.

[77] B. Korzh, C.C.W. Lim, R. Houlmann, N. Gisin, M.J. Li, D. Nolan, B. Sanguinetti, R. Thew et al., *Nature Photon.* **9**, 163 (2015).

[78] S.-K. Liao, W.-Q. Cai, J. Handsteiner et al., *Phys. Rev. Lett.* **120**, 030501 (2018).

[79] W.O. Krawec, R. Liss, T. Mor, arXiv:2012.02127 (2020).

[80] D.M. Greenberger, M.A. Horne, A. Shimony, A. Zeilinger, *Am. J. Phys.* **58**, 1131 (1990).

[81] W. Dür, G. Vidal, J.I. Cirac, *Phys. Rev. A* **62**, 062314 (2000).

[82] W.-X. Cui, S. Hu, H.-F. Wang, A.-D. Zhu, S. Zhang, *Opt. Expr.* **24**, 15319 (2016).

[83] T. Haase, G. Alber, V.M. Stojanovic, arXiv:2012.15169 (2020).

[84] F. Benatti, R. Floreanini, F. Franchini, U. Marzolino, *Phys. Rep.* **878**, 1 (2020).

[85] R.Y. Chiao, P.G. Kwia, A.M. Steinberg, *Quant. Classic. Opt. J. Europ. Opt. Soc. B* **7**, 259 (1995).

[86] M. Erhard, M. Krenn, A. Zeilinger, *Nature Rev Phys.* **2**, 365 (2020).

[87] N. Akopian, N.H. Lindner, E. Poem, Y. Berlatzky, J. Avron, D. Gershoni, B.D. Gerardot, P.M. Petroff, *Phys. Rev. Lett.* **96**, 130501 (2006).

[88] B. Yurke, D. Stoler, *Phys. Rev. Lett.* **68**, 1251 (1992).

[89] K. Życzkowski, P. Horodecki, M. Horodecki, R. Horodecki, *Phys. Rev. A* **65**, 012101 (2001).

[90] T. Yu, J. Eberly, *Opt. Commun.* **264**, 393 (2006).

[91] T. Yu, J.H. Eberly, *Science* **323**, 598 (2009).

[92] K. Życzkowski, P. Horodecki, A. Sanpera, M. Lewenstein, *Phys. Rev. A* **58**, 883 (1998).

[93] M. Kuś, K. Życzkowski, *Phys. Rev. A* **63**, 032307 (2001).

[94] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, Y. Shih, *Phys. Rev. Lett.* **75**, 4337 (1995).

[95] S.L. Braunstein, A. Mann, M. Revzen, *Phys. Rev. Lett.* **68**, 3259 (1992).

[96] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).

[97] B.S. Cirel'son, *Lett. Math. Phys.* **4**, 93 (1980).

[98] D.I. Kaiser, arXiv:2011.09296 (2020).

[99] T. Scheidl, R. Ursin, J. Kofler et al., *Proc. Natl. Acad. Sci.* **107**, 19708 (2010).

[100] D. Aktas, S. Tanzilli, A. Martin, G. Pütz, R. Thew, N. Gisin, *Phys. Rev. Lett.* **114**, 220404 (2015).

[101] M.-H. Li, C. Wu, Y. Zhang et al., *Phys. Rev. Lett.* **121**, 080404 (2018).

[102] M. Żukowski, C. Brukner, *J. Phys. A Math. Theoret.* **47**, 424009 (2014).

[103] E.G. Cavalcanti, H.M. Wiseman, *Foundat. Phys.* **42**, 1329 (2012).

[104] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, V. Scarani, *New J. Phys.* **11**, 045021 (2009).

[105] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, *Rev. Mod. Phys.* **86**, 419 (2014).

[106] R. Arnon-Friedman, J.-D. Bancal, *New J. Phys.* **21**, 033010 (2019).

[107] M. Farkas, M. Balanzó-Juandó, K. Łukanowski, J. Kołodynski, A. Acín, arXiv:2103.02639v1 (2021).

[108] S. Kochen, E. Specker, *Indiana Univ. Math. J.* **17**, 59 (1967).

[109] A. Cabello, J. Estebaranz, G. García-Alcaine, *Phys. Lett. A* **212**, 183 (1996).

[110] A. Cabello, *Phys. Rev. Lett.* **101**, 210401 (2008).

[111] B. Marques, J. Ahrens, M. Nawareg, A. Cabello, M. Bourennane, *Phys. Rev. Lett.* **113**, 250403 (2014).

[112] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Kłobus, A. Wójcik, *Phys. Rev. Lett.* **112**, 120401 (2014).

[113] A.A. Klyachko, M.A. Can, S. Binicioglu, A.S. Shumovsky, *Phys. Rev. Lett.* **101**, 020403 (2008).

[114] N.D. Mermin, *Phys. Rev. Lett.* **65**, 3373 (1990).

[115] I. Šupic, J. Bowles, *Quantum* **4**, 337 (2020).

[116] S. Pironio, A. Acín, S. Massar et al., *Nature* **464**, 1021 (2010).

[117] N. Miklin, J.J. Borkała, M. Pawłowski, *Phys. Rev. Res.* **2**, 033014 (2020).

[118] R. Ramanathan, D. Goyeneche, S. Muhammad, P. Mironowicz, M. Grünfeld, M. Bourennane, P. Horodecki, *Nature Commun.* **9**, 4244 (2018).

[119] S. Popescu, D. Rohrlich, *Foundat. Phys.* **24**, 379 (1994).

[120] S. Popescu, *Nature Phys.* **10**, 264 (2014).

[121] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Żukowski, *Nature* **461**, 1101 (2009).

[122] M. Piani, M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. A* **74**, 012305 (2006).

[123] K. Horodecki, A. Grudka, P. Joshi, W. Kłobus, J. Łodyga, *Phys. Rev. A* **92**, 032104 (2015).

[124] J.-D. Bancal, N. Gisin, arXiv:2102.03597v1 (2021).

[125] W. van Dam, Ph.D. Thesis, Oxford 2000.

[126] G. Brassard, H. Buhrman, N. Linden, A.A. Méthot, A. Tapp, F. Unger, *Phys. Rev. Lett.* **96**, 250401 (2006).

[127] J. Grunhaus, S. Popescu, D. Rohrlich, *Phys. Rev. A* **53**, 3781 (1996).

[128] P. Horodecki, R. Ramanathan, *Nature Commun.* **10**, 1701 (2019).

[129] M. Eckstein, P. Horodecki, T. Miller, R. Horodecki, *Phys. Rev. A* **101**, 042128 (2020).

[130] T. Miller, M. Eckstein, P. Horodecki, R. Horodecki, *J. Geom. Phys.* **160**, 103990 (2021).

[131] A. Dragan, A. Ekert, *New J. Phys.* **22**, 033038 (2020).

[132] M. Koashi, A. Winter, *Phys. Rev. A* **69**, 022309 (2004).

[133] M.P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, C. Kurtsiefer, *New J. Phys.* **11**, 045007 (2009).

[134] M. Fujiwara, K.-I. Yoshino, Y. Nambu et al., *Opt. Expr.* **22**, 13616 (2014).

[135] H.Y. Lim, T. Vergoossen, R. Bedington et al., arXiv:2006.14442v1 (2020).

[136] C.C.-W. Lim, F. Xu, J.-W. Pan, A. Ekert, arXiv:2009.04882 (2020).

[137] J. Barrett, L. Hardy, A. Kent, *Phys. Rev. Lett.* **95**, 010503 (2005).

[138] K. Mattle, H. Weinfurter, P.G. Kwiat, A. Zeilinger, *Phys. Rev. Lett.* **76**, 4656 (1996).

[139] T. Schaetz, M.D. Barrett, D. Leibfried, J. Chiaverini, J. Britton, W.M. Itano, J.D. Jost, C. Langer, D.J. Wineland, *Phys. Rev. Lett.* **93**, 040505 (2004).

[140] D. Wei, X. Yang, J. Luo, X. Sun, X. Zeng, M. Liu, *Chin. Sci. Bull.* **49**, 423 (2004).

[141] R. Liss, T. Mor, in: *Theory and Practice of Natural Computing*, Vol. 12494, Springer Int., 2020, p. 82.

[142] L. Vaidman, *Phys. Rev. A* **49**, 1473 (1994).

[143] S.L. Braunstein, H.J. Kimble, *Phys. Rev. Lett.* **80**, 869 (1998).

[144] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, N. Gisin, *Nature* **421**, 509 (2003).

[145] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, A. Zeilinger, *Nature* **430**, 849 (2004).

[146] J. Yin, J.-G. Ren, H. Lu et al., *Nature* **488**, 185 (2012).

[147] D. Gottesman, I.L. Chuang, *Nature* **402**, 390 (1999).

[148] X.-S. Ma, T. Herbst, T. Scheidl et al., *Nature* **489**, 269 (2012).

[149] C. Nölleke, A. Neuzner, A. Reiserer, C. Hahn, G. Rempe, S. Ritter, *Phys. Rev. Lett.* **110**, 140403 (2013).

[150] W. Pfaff, B.J. Hensen, H. Bernien et al., *Science* **345**, 532 (2014).

[151] Y.-H. Luo, H.-S. Zhong, M. Erhard et al., *Phys. Rev. Lett.* **123**, 070505 (2019).

[152] X.-M. Hu, C. Zhang, B.-H. Liu et al., *Phys. Rev. Lett.* **125**, 230501 (2020).

[153] J.-G. Ren, P. Xu, H.-L. Yong et al., *Nature* **549**, 70 (2017).

[154] N. Gisin, *Entropy* **21**, 325 (2019).

[155] H. Salih, J.R. Hance, W. McCutcheon, T. Rudolph, J. Rarity, arXiv:2009.05564 (2020).

[156] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. A* **60**, 1888 (1999).

[157] S. Ishizaka, T. Hiroshima, *Phys. Rev. Lett.* **101**, 240501 (2008).

[158] S. Ishizaka, T. Hiroshima, *Phys. Rev. A* **79**, 042306 (2009).

[159] P. Kopszak, M. Mozrzymas, M. Studzinski, M. Horodecki, arXiv:2008.00856v2 (2021).

[160] S. Roy, T. Das, D. Das, A. Sen(De), U. Sen, *Ann. Phys.* **422**, 168281 (2020).

[161] M. Murao, D. Jonathan, M.B. Plenio, V. Vedral, *Phys. Rev. A* **59**, 156 (1999).

[162] S. Bose, V. Vedral, P.L. Knight, *Phys. Rev. A* **57**, 822 (1998).

[163] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, M. Żukowski, *Rev. Mod. Phys.* **84**, 777 (2012).

[164] J.-W. Pan, D. Bouwmeester, H. Weinfurter, A. Zeilinger, *Phys. Rev. Lett.* **80**, 3891 (1998).

[165] R.-B. Jin, M. Takeoka, U. Takagi, R. Shimizu, M. Sasaki, *Sci. Rep.* **5**, 9333 (2015).

[166] F.B. Basset, M.B. Rota, C. Schimpf et al., *Phys. Rev. Lett.* **123**, 160501 (2019).

[167] Y. Zhang, M. Agnew, T. Roger, F.S. Roux, T. Konrad, D. Faccio, J. Leach, A. Forbes, *Nature Commun.* **8**, 632 (2017).

[168] V. Zapatero, M. Curty, *Sci. Rep.* **9**, 17749 (2019).

[169] H.-J. Briegel, W. Dür, J.I. Cirac, P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).

[170] L.-M. Duan, M.D. Lukin, J.I. Cirac, P. Zoller, *Nature* **414**, 413 (2001).

[171] B.K. Behera, S. Seth, A. Das, P.K. Panigrahi, *Quant. Inf. Process.* **18**, 108 (2019).

[172] M. Zopf, R. Keil, Y. Chen, J. Yang, D. Chen, F. Ding, O.G. Schmidt, *Phys. Rev. Lett.* **123**, 160502 (2019).

[173] Z. Zhang, X. Man, *Phys. Rev. A* **72**, 022303 (2004).

[174] N.T.V. Luu, S. Shimamoto, in: *Proc. 2nd Int. Conf. on Information Communication Technologies, 2006, Damascus (Syria)*, Vol. 2, 2006, p. 2051.

[175] L. Gurvits, in: *Proc. Thirty-Fifth ACM Symp. on Theory of Computing — STOC'03*, ACM Press, 2003, p. 10.

[176] A. Peres, *Phys. Rev. Lett.* **77**, 1413 (1996).

[177] S.L. Woronowicz, *Commun. Math. Phys.* **51**, 243 (1976).

[178] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Lett. A* **223**, 1 (1996).

[179] B.M. Terhal, *Phys. Lett. A* **271**, 319 (2000).

[180] M. Lewenstein, B. Kraus, J.I. Cirac, P. Horodecki, *Phys. Rev. A* **62**, 052310 (2000).

[181] M. Lewenstein, B. Kraus, P. Horodecki, J.I. Cirac, *Phys. Rev. A* **63**, 044304 (2001).

[182] A. Jamiołkowski, *Rep. Math. Phys.* **3**, 275 (1972).

[183] M. Barbieri, F.D. Martini, G.D. Nepi, P. Mataloni, G.M. D'Ariano, C. Macchiavello, *Phys. Rev. Lett.* **91**, 227901 (2003).

[184] M. Bourennane, M. Eibl, C. Kurtsiefer et al., *Phys. Rev. Lett.* **92**, 087902 (2004).

[185] C.F. Roos, *Science* **304**, 1478 (2004).

[186] J.B. Altepeter, E.R. Jeffrey, P.G. Kwiat, S. Tanzilli, N. Gisin, A. Acín, *Phys. Rev. Lett.* **95**, 033601 (2005).

[187] H. Häffner, W. Hänsel, C.F. Roos et al., *Nature* **438**, 643 (2005).

[188] H. Mikami, Y. Li, K. Fukuoka, T. Kobayashi, *Phys. Rev. Lett.* **95**, 150404 (2005).

[189] N.K. Langford, T.J. Weinhold, R. Prevedel, K.J. Resch, A. Gilchrist, J.L. O'Brien, G.J. Pryde, A.G. White, *Phys. Rev. Lett.* **95**, 210504 (2005).

[190] W. Laskowski, D. Richart, C. Schwemmer, T. Paterek, H. Weinfurter, *Phys. Rev. Lett.* **108**, 240501 (2012).

[191] B. Dirkse, M. Pompili, R. Hanson, M. Walter, S. Wehner, *Quant. Sci. Technol.* **5**, 035007 (2020).

[192] C. Branciard, D. Rosset, Y.-C. Liang, N. Gisin, *Phys. Rev. Lett.* **110**, 060405 (2013).

[193] M. Oszmaniec, M. Kuś, *Phys. Rev. A* **88**, 052328 (2013).

[194] P. Badziag, C. Brukner, W. Laskowski, T. Paterek, M. Żukowski, *Phys. Rev. Lett.* **100**, 140403 (2008).

[195] W. Laskowski, M. Markiewicz, T. Paterek, M. Żukowski, *Phys. Rev. A* **84**, 062305 (2011).

[196] M. Markiewicz, A. Kołodziejski, Z. Puchała, A. Rutkowski, T. Tylec, W. Laskowski, *Phys. Rev. A* **97**, 042339 (2018).

[197] C.-J. Zhang, Y.-S. Zhang, S. Zhang, G.-C. Guo, *Phys. Rev. A* **77**, 060301(R) (2008).

[198] G. Sarbicki, G. Scala, D. Chruściński, *Phys. Rev. A* **101**, 012341 (2020).

[199] G. Sarbicki, G. Scala, D. Chruściński, arXiv:2011.10159 (2020).

[200] P. Horodecki, *Phys. Lett. A* **232**, 333 (1997).

[201] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).

[202] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).

[203] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **78**, 574 (1997).

[204] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **80**, 5239 (1998).

[205] R. Horodecki, *Europhys. News* **41**, 21 (2010).

[206] E. Amselem, M. Bourennane, *Nature Phys.* **5**, 748 (2009).

[207] J. Lavoie, R. Kaltenbaek, M. Piani, K.J. Resch, *Phys. Rev. Lett.* **105**, 130501 (2010).

[208] J.T. Barreiro, P. Schindler, O. Gühne, T. Monz, M. Chwalla, C.F. Roos, M. Hennrich, *Nature Phys.* **6**, 943 (2010).

[209] H. Kampermann, D. Bruß, X. Peng, D. Suter, *Phys. Rev. A* **81**, 040304(R) (2010).

[210] J. DiGuglielmo, A. Samblowski, B. Hage, C. Pineda, J. Eisert, R. Schnabel, *Phys. Rev. Lett.* **107**, 240503 (2011).

[211] G. Tóth, C. Knapp, O. Gühne, H.J. Briegel, *Phys. Rev. Lett.* **99**, 250405 (2007).

[212] A. Ferraro, D. Cavalcanti, A. García-Saez, A. Acín, *Phys. Rev. Lett.* **100**, 080502 (2008).

[213] P. Horodecki, M. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **82**, 1056 (1999).

[214] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, *Phys. Rev. Lett.* **94**, 160502 (2005).

[215] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, *IEEE Trans. Inform. Theory* **55**, 1898 (2009).

[216] K. Dobek, M. Karpiński, R. Demkowicz-Dobrzański, K. Banaszek, P. Horodecki, *Phys. Rev. Lett.* **106**, 030501 (2011).

[217] T. Vértesi, N. Brunner, *Nature Commun.* **5**, 5297 (2014).

[218] Ł. Czekaj, A. Przysiężna, M. Horodecki, P. Horodecki, *Phys. Rev. A* **92**, 062303 (2015).

[219] G. Tóth, T. Vértesi, *Phys. Rev. Lett.* **120**, 020506 (2018).

[220] K.F. Pál, G. Tóth, E. Bene, T. Vértesi, arXiv:2002.12409 (2020).

[221] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, T. Vidick, *Nature Commun.* **9**, 459 (2018).

[222] R. Arnon-Friedman, F. Leditzky, arXiv:2005.12325 (2020).

[223] M. Christandl, R. Ferrara, K. Horodecki, arXiv:2005.13511v2 (2020).

[224] E. Schrödinger, *Naturwissenschaften* **23**, 807 (1935).

[225] R. Horodecki, P. Horodecki, *Phys. Lett. A* **194**, 147 (1994).

[226] N.J. Cerf, C. Adami, *Phys. Rev. Lett.* **79**, 5194 (1997).

[227] B. Schumacher, M.D. Westmoreland, *Phys. Rev. A* **56**, 131 (1997).

[228] A. Holevo, *IEEE Trans. Inform. Theory* **44**, 269 (1998).

[229] I. Devetak, *IEEE Trans. Inform. Theory* **51**, 44 (2005).

[230] C.H. Bennett, I. Devetak, P.W. Shor, J.A. Smolin, *Phys. Rev. Lett.* **96**, 150502 (2006).

[231] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, J. Oppenheim, *IEEE Trans. Inform. Theory* **54**, 2604 (2008).

[232] K. Li, A. Winter, X. Zou, G. Guo, *Phys. Rev. Lett.* **103**, 120501 (2009).

[233] S. Bäuml, M. Christandl, K. Horodecki, A. Winter, *Nature Commun.* **6**, 6908 (2015).

[234] D. Slepian, J. Wolf, *IEEE Trans. Inform. Theory* **19**, 471 (1973).

[235] M. Horodecki, J. Oppenheim, A. Winter, *Nature* **436**, 673 (2005).

[236] I. Devetak, A. Winter, *Proc. R. Soc. A Math. Phys. Eng. Sci.* **461**, 207 (2005).

[237] R. Horodecki, M. Horodecki, *Phys. Rev. A* **54**, 1838 (1996).

[238] P. Horodecki, A. Ekert, *Phys. Rev. Lett.* **89**, 125003 (2002).

[239] P. Horodecki, *Phys. Rev. Lett.* **90**, 167901 (2003).

[240] F.A. Bovino, G. Castagnoli, A. Ekert, P. Horodecki, C.M. Alves, A.V. Sergienko, *Phys. Rev. Lett.* **95**, 240407 (2005).

[241] R. Islam, R. Ma, P.M. Preiss, M.E. Tai, A. Lukin, M. Rispoli, M. Greiner, *Nature* **528**, 77 (2015).

[242] A.M. Kaufman, M.E. Tai, A. Lukin, M. Rispoli, R. Schittko, P.M. Preiss, M. Greiner, *Science* **353**, 794 (2016).

[243] N.M. Linke, S. Johri, C. Figgatt, K.A. Landsman, A.Y. Matsuura, C. Monroe, *Phys. Rev. A* **98**, 052334 (2018).

[244] C.M. Alves, D. Jaksch, *Phys. Rev. Lett.* **93**, 110501 (2004).

[245] A.J. Daley, H. Pichler, J. Schachenmayer, P. Zoller, *Phys. Rev. Lett.* **109**, 020505 (2012).

[246] T. Brydges, A. Elben, P. Jurcevic, B. Vermersch, C. Maier, B.P. Lanyon, P. Zoller, R. Blatt, C.F. Roos, *Science* **364**, 260 (2019).

[247] S.J. van Enk, C.W.J. Beenakker, *Phys. Rev. Lett.* **108**, 110503 (2012).

[248] A. Elben, B. Vermersch, M. Dalmonte, J. Cirac, P. Zoller, *Phys. Rev. Lett.* **120**, 050406 (2018).

[249] A. Elben, B. Vermersch, C.F. Roos, P. Zoller, *Phys. Rev. A* **99**, 052323 (2019).

[250] H.-Y. Huang, R. Kueng, J. Preskill, *Nature Phys.* **16**, 1050 (2020).

[251] V. Trávnícek, K. Bartkiewicz, A. Cernoch, K. Lemr, *Phys. Rev. A* **98**, 032307 (2018).

[252] K. Bartkiewicz, K. Lemr, A. Cernoch, A. Miranowicz, *Phys. Rev. A* **95**, 030102(R) (2017).

[253] A. Elben, R. Kueng, H.-Y.R. Huang et al., *Phys. Rev. Lett.* **125**, 200501 (2020).

[254] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter, *Phys. Rev. A* **52**, 3457 (1995).

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

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

[257] W.-L. Yang, H. Wei, C.-Y. Chen, M. Feng, *J. Opt.Soc. Am. B* **25**, 1720 (2008).

[258] P. Bianucci, A. Muller, C.K. Shih, Q.Q. Wang, Q.K. Xue, C. Piermarocchi,*Phys. Rev. B* **69**, 161303(R) (2004).

[259] S. Lloyd, *Science* **273**, 1073 (1996).

[260] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P.J. Love, A. Aspuru-Guzik, J.L. O'Brien, *Nature Commun.* **5**, 4213 (2014).

[261] Y. Alexeev, D. Bacon, K.R. Brown et al., arXiv:1912.07577 (2019).

[262] A.M. Steane, *Phys. Rev. A* **54**, 4741 (1996).

[263] D. Aharonov, M. Ben-Or, in: *Proc. Twenty-Ninth Annual ACM Symp. on Theory of Computing, STOC '97*, 1997, p. 176.

[264] E. Knill, R. Laflamme, W.H. Zurek, *Science* **279**, 342 (1998).

[265] J.I. Cirac, P. Zoller, *Phys. Rev. Lett.* **74**, 4091 (1995).

[266] F. Arute, K. Arya, R. Babbush et al., *Nature* **574**, 505 (2019).

[267] S. Aaronson, A. Arkhipov, *Theory Comput.* **9**, 143 (2013).

[268] H.-S. Zhong, H. Wang, Y.-H. Deng et al., *Science* **370**, 1460 (2020).

[269] P. Ball, *Nature* **588**, 380 (2020).

[270] C.M. Caves, *Phys. Rev. D* **23**, 1693 (1981).

[271] V. Giovannetti, *Science* **306**, 1330 (2004).

[272] V. Giovannetti, S. Lloyd, L. Maccone, *Phys. Rev. Lett.* **96**, 010401 (2006).

[273] L. Pezzé, A. Smerzi, *Phys. Rev. Lett.* **102**, 100401 (2009).

[274] G. Tóth, *Phys. Rev. A* **85**, 022322 (2012).

[275] P. Hyllus, W. Laskowski, R. Krischek, C. Schwemmer, W. Wieczorek, H. Weinfurter, L. Pezzé, A. Smerzi, *Phys. Rev. A* **85**, 022321 (2012).

[276] G. Tóth, I. Apellaniz, *J. Phys. A Math. Theoret.* **47**, 424006 (2014).

[277] T. Xie, Z. Zhao, X. Kong et al., arXiv:2101.12048v1 (2021).

[278] S.F. Huelga, C. Macchiavello, T. Pellizzari, A.K. Ekert, M.B. Plenio, J.I. Cirac, *Phys. Rev. Lett.* **79**, 3865 (1997).

[279] R. Demkowicz-Dobrzański, U. Dorner, B.J. Smith, J.S. Lundeen, W. Wasilewski, K. Banaszek, I.A. Walmsley, *Phys. Rev. A* **80**, 013825 (2009).

[280] Y. Matsuzaki, S.C. Benjamin, J. Fitzsimons, *Phys. Rev. A* **84**, 012103 (2011).

[281] R. Demkowicz-Dobrzański, J. Kołodyński, M. Guţă, *Nature Commun.* **3**, 1063 (2012).

[282] A.W. Chin, S.F. Huelga, M.B. Plenio, *Phys. Rev. Lett.* **109**, 233601 (2012).

[283] R. Demkowicz-Dobrzański, J. Czajkowski, P. Sekatski, *Phys. Rev. X* **7**, 041009 (2017).

[284] S. Zhou, M. Zhang, J. Preskill, L. Jiang, *Nature Commun.* **9**, 78 (2018).

[285] K. Chabuda, J. Dziarmaga, T.J. Osborne, R. Demkowicz-Dobrzański, *Nature Commun.* **11**, 250 (2020).

[286] R. Demkowicz-Dobrzański, K. Banaszek, R. Schnabel, *Phys. Rev. A* **88**, 041802(R) (2013).

[287] A. Franzen, B. Hage, J. DiGuglielmo, J. Fiurášek, R. Schnabel, *Phys. Rev. Lett.* **97**, 150505 (2006).

[288] M. Parniak, S. Borówka, K. Boroszko, W. Wasilewski, K. Banaszek, R. Demkowicz-Dobrzański, *Phys. Rev. Lett.* **121**, 250503 (2018).

[289] P. Hyllus, O. Gühne, A. Smerzí, *Phys. Rev. A* **82**, 012337 (2010).

[290] G. Tóth, T. Vértesi, P. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **125**, 020402 (2020).

[291] C.H. Bennett, A. Grudka, M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. A* **83**, 012312 (2011).

[292] C.H. Bennett, D.P. DiVincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin, W.K. Wootters, *Phys. Rev. A* **59**, 1070 (1999).

[293] G. Smith, J. Yard, *Science* **321**, 1812 (2008).

[294] D.P. DiVincenzo, M. Horodecki, D.W. Leung, J.A. Smolin, B.M. Terhal, *Phys. Rev. Lett.* **92**, 067902 (2004).

[295] W.H. Zurek, *Nature Phys.* **5**, 181 (2009).

[296] F.G.S.L. Brandão, M. Piani, P. Horodecki, *Nature Commun.* **6**, 7908 (2015).

[297] T.P. Le, A. Olaya-Castro, *Phys. Rev. Lett.* **122**, 010403 (2019).

[298] J. Korbicz, P. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **112**, 120402 (2014).

[299] R. Horodecki, J.K. Korbicz, P. Horodecki, *Phys. Rev. A* **91**, 032122 (2015).

[300] M.-C. Chen, H.-S. Zhong, Y. Li, D. Wu, X.-L. Wang, L. Li, N.-L. Liu, C.-Y. Lu, J.-W. Pan, *Sci. Bull.* **64**, 580 (2019).

[301] C.M. Scandolo, R. Salazar, J.K. Korbicz, P. Horodecki, arXiv:1805.12126v6 (2020).

[302] R. Colbeck, R. Renner, *Nature Phys.* **8**, 450 (2012).

[303] R. Gallego, L. Masanes, G.D.L. Torre, C. Dhara, L. Aolita, A. Acín, *Nature Commun.* **4**, 2654 (2013).

[304] F.G.S.L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, H. Wojewódka, *Nature Commun.* **7**, 11345 (2016).

[305] P. Horodecki, Ł. Rudnicki, K. Życzkowski, arXiv:2002.03233v2 (2020).