Einstein centennial review article / Article de synthèse commémoratif du centenaire de l'année miraculeuse d'Einstein

A second century of Einstein? Bose–Einstein condensation and quantum information[1]

William Arie van Wijngaarden

Abstract: A century ago Albert Einstein transformed classical physics with his seminal papers on Brownian motion, the Photoelectric effect, and, of course, special and later general relativity. Lesser well-known are his contributions to Bose–Einstein Condensation and the Einstein–Podolsky–Rosen paradox, the latter being a criticism of Quantum Mechanics. These later works were regarded even by physicists for decades as mere Gedanken or thought experiments. In recent years, not only have they been verified experimentally but revolutionary technological applications are emerging including quantum cryptography and possibly quantum computing.

PACS Nos.: 03.65, 03.67, 03.75, 05.30.Jp

Résumé : Il y a un siècle, Albert Einstein a bouleversé la physique classique dans une série de papiers célèbres sur le mouvement Brownien, l'effet photoélectrique et évidemment la relativité, d'abord restreinte et ensuite générale. Certaines de ses contributions sont moins connues, comme celle à la condensation de Bose–Einstein et le paradoxe Einstein–Podolsky–Rosen, ce dernier une critique de la mécanique quantique. Ces derniers travaux ont longtemps été consédérés par les physiciens comme des expériences *en esprit*. Depuis quelques années, non seulement ont-ils été vérifiés expérimentalement, mais sont la source de technologies révolutionnaires, comme la cryptographie quantique et possiblement l'ordinateur quantique.

[Traduit par la Rédaction]

Received 17 January 2005. Accepted 19 May 2005. Published on the NRC Research Press Web site at http://cjp.nrc.ca/ on 13 July 2005.

W.A. van Wijngaarden. Physics Department, Petrie Bldg., York University, 4700 Keele St., Toronto, ON M3J 1P3, Canada (e-mail: wavw@yorku.ca).

[1]This article is one of a series of invited papers that will be published during the year in celebration of the World Year of Physics 2005 — WYP2005.

 doi: 10.1139/P05-042

1. Introduction

In 1905, Albert Einstein [1] transformed physics with his papers on the photoelectric effect [2], Brownian motion [3], and special relativity [4]. In the following decade Einstein completed his work on general relativity [5] and postulated the stimulated emission of radiation [6]. Physicists quickly realized the significance of these revolutionary ideas and tests were carried out. Notably, General Relativity correctly predicted the bending of starlight by the Sun that was verified in a solar eclipse in 1919 [7].

Beginning in the 1920s, Einstein was no longer at the forefront of developments in physics and indeed he became a harsh critic of the probabilistic nature of quantum mechanics theory. He did make two notable contributions that have not been fully appreciated until recently. In 1923, he along with Bose postulated the condensation of bosons at very low temperatures. This is now called Bose–Einstein condensation (BEC) [8, 9]. Later in 1935, he worked with Podolsky and Rosen to question whether quantum mechanics is a complete theory, which became known as the Einstein–Podolsky–Rosen (EPR) paradox [10].

BEC and the EPR paradox were regarded by physicists as "Gedanken" or thought experiments for decades as they were completely unfeasible given the available technology of the time. In 1964, Bell derived conditions that could be tested to show whether or not Quantum Mechanics had so called "hidden variables" [11]. It was not until the early 1980s that definitive experiments were performed testing the EPR paradox [12]. The road to BEC involved the development of laser-cooling and atom-trapping techniques [13, 14]. BEC was finally achieved in dilute alkali vapours cooled to nanoKelvin temperatures in 1995 [15–17]. Today, Einstein's theories have not only been verified but are at the forefront of research that has made exciting contributions to cryptography and may ultimately lead to quantum processing of information or quantum computing.

This paper is organized as follows. First, BEC is defined and some experimental results are given. The EPR paradox is presented next along with its relevance to quantum cryptography. Finally, quantum information processing and a possible scheme describing how quantum computing might be implemented using a two-dimensional array of microtraps to store neutral atoms is discussed.

2. Bose–Einstein condensation

Einstein and Bose considered the population distribution of particles having integral spin angular momentum called bosons. They showed that the average number of such particles occupying a state having energy ε is given by [18]

$$n(\varepsilon) = \left\{ \exp\left[\frac{(\varepsilon - \mu)}{k_{\mathrm{B}} T} \right] - 1 \right\}^{-1} \tag{1}$$

Here, k_{B} is Boltzmann's constant, T is the temperature in Kelvins, and μ is the chemical potential, which is found by summing the particle populations over all of the energy states to give the total particle number N.

$$\sum_{\varepsilon} n(\varepsilon) = N \tag{2}$$

Note that $\mu < \varepsilon_{\mathrm{min}}$ in order for $n(\varepsilon)$ to be well defined. As the temperature increases, states of higher energy become populated and $n(\varepsilon)$ decreases.

The total number of particles that can occupy the excited states is given by

$$N_{\mathrm{ex}} = \int_0^{\infty} g(\varepsilon) n(\varepsilon)\, \mathrm{d}\varepsilon \tag{3}$$

where $g(\varepsilon)$ is the density of states, which depends on the potential experienced by the particle. If the total number of particles N exceeds N_{ex}, then the remaining particles must occupy the ground state and

BEC is said to occur. The transition temperature to BEC denoted by T_c, is the minimum temperature such that all atoms can be accommodated in the excited states, i.e., $N_{ex}(T_c) = N$.

For a free particle in a three-dimensional box, it can be shown that the transition temperature satisfies

$$k_B T_c = \frac{3.31\hbar^2 n^{2/3}}{M} \tag{4}$$

where $\hbar$ is Planck's constant divided by 2π, n is the atomic density, and M is the particle mass [14]. Physical insight into the condition for BEC can be obtained by considering the phase space density ρ, which equals the total number of particles divided by the cube of the de Broglie wavelength $\lambda_{dB} = h/(2\pi M k_B T)^{1/2}$. Equation (4) implies that BEC occurs if

$$\rho = \frac{n}{(\lambda_{dB})^3} > 2.612 \tag{5}$$

In recent years, BEC has been observed by using the vapours of alkali atoms. A major experimental hurdle has been the ability to obtain sufficiently high densities of these atoms at very low temperatures. The atoms are contained in either a magnetic or an optical trap to prevent collisions with the vacuum chamber walls that would heat the atoms. For the case of atoms stored in a harmonic trap whose potential $V = 1/2(K_1 x^2 + K_2 y^2 + K_3 z^2)$ the condition for BEC is given by the expression

$$k_B T_c = 0.94\hbar\omega^* N^{1/3} \tag{6}$$

where $\omega^* = (\omega_1\omega_2\omega_3)^{1/3}$ is the geometric mean of the trap frequencies $\omega_i = (K_i/M)^{1/2}$. The fraction of particles in the condensate is given by

$$f = 1 - \left(\frac{T}{T_c}\right)^{\alpha} \tag{7}$$

where $\alpha = 3/2$ for a free particle in a three-dimensional box and $\alpha = 3$ for a particle experiencing a harmonic oscillator potential.

In 1938, London realized that the superfluid ^{4}He was a BEC when cooled below 2.17 K [19]. Subsequent experiments showed that ^{4}He existed as a mixture of normal and superfluids [20]. Indeed, the BEC fraction was only about 9% due to strong interactions of the liquid helium atoms with each other [21]. It was not until the development of laser-cooling and atom-trapping techniques that pure BECs were created in the mid 1990s [14–17]. These condensates typically consist of up to 10^8 alkali atoms confined in a volume of about 1000 μm^3 cooled to a temperature of less than 100 nK. A number of reviews have been written describing these experimental techniques such as ref. 22.

An example of the transition to BEC in ^{87}Rb obtained by our group is shown in Fig. 1 [22]. Here, the atoms whose magnetic moments are parallel to the magnetic field are trapped by a spatially varying magnetic field [23]. A radio-frequency (RF) signal is applied that flips the spins of the hotter atoms located further from the trap center where the magnetic field has a minimum. The remaining atoms rethermalize as a result of collisions while the radio frequency is swept to progressively lower frequencies over a time of typically 1 min. This is known as evaporative cooling. The temperature distribution is determined by suddenly switching off the magnetic field and passing a low intensity probe laser beam through the atom cloud. The probe laser beam is detected using a CCD camera array.

Fig. 1. Transition to BEC as a function of temperature. (*a*) Thermal cloud with $N = 1.9 \times 10^6$ atoms at temperature $T = 450$ nK, (*b*) Mixed thermal atom cloud and BEC where $N = 1.8 \times 10^6$ atoms and $T = 400$ nK. (*c*) Pure condensate where $N = 4.2 \times 10^5$ atoms and $T < 60$ nK.

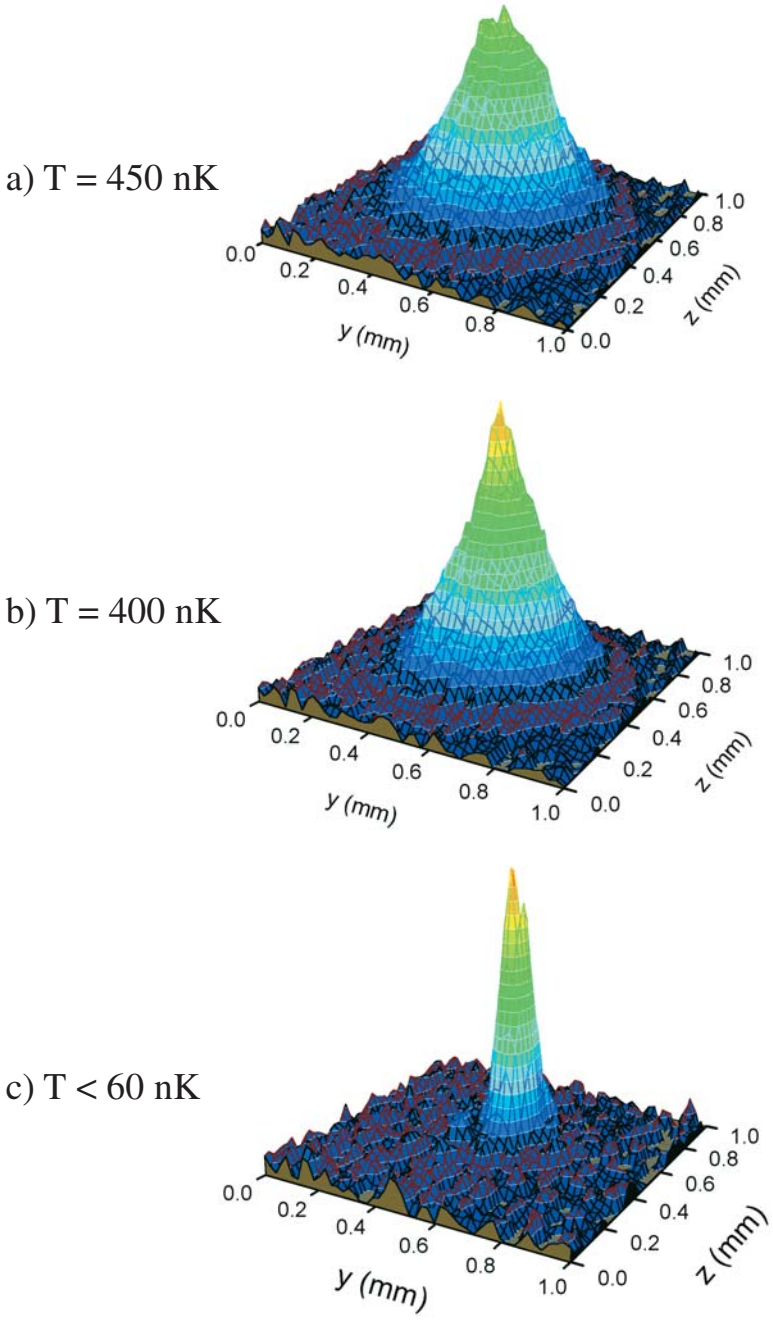


Fig. 2. Condensate fraction as a function of temperature. The data points agree well with the theoretical curve given by $N_{\mathrm{BEC}}/N = 1 - (T/T_{\mathrm{c}})^3$ where T_{c} is the transition temperature.

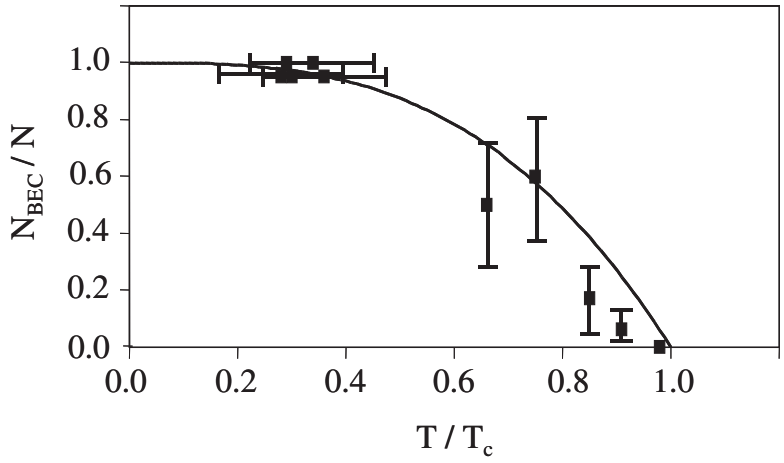


Figure 1*a* shows a thermal atom cloud exhibiting a Gaussian distribution having a temperature of about 0.5 μK. As the temperature decreases below the BEC transition temperature at 400 nK, a sharp spike appears in the atom distribution. Fig. 1*c* shows a pure condensate. The fraction of the atoms in the BEC, shown in Fig. 2, closely follows the theoretical prediction given by (7).

The BEC lifetime is limited by collisions with the background gas even at pressures as low as 1×10^{-11} Torr. Once the RF signal is turned off the BEC disappears in about 200 ms. An order of magnitude increase in the BEC lifetime to over 2 s is achieved if the RF signal is kept on as shown in Fig. 3.

The temporal evolution of the condensate is governed by the Gross Pitaevskii equation [14]

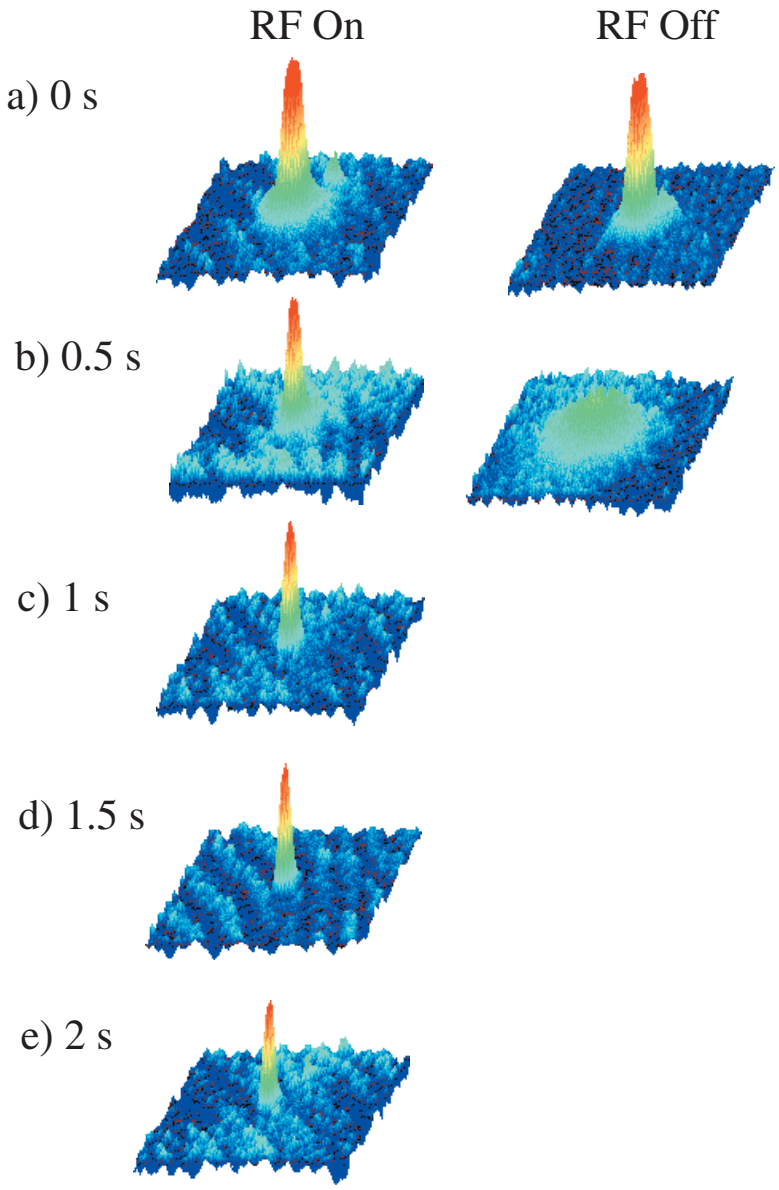
$$\frac{-\hbar^2}{2m}\nabla^2\Psi(r,t) + V(r)\Psi(r,t) + U_0|\Psi(r,t)|^2\Psi(r,t) = i\hbar\frac{\partial\Psi}{\partial t} \tag{8}$$

which is a nonlinear Schrödinger equation that describes the condensate wave function Ψ. Hence, $|\Psi|^2$ is proportional to the number of condensate atoms. V is the trap potential and $U_0 = \boldsymbol{a}h^2/\pi M$ results from the van der Waals interaction between two atoms where $\boldsymbol{a}$ is the scattering length for lowest energy or s wave scattering. In our experiment, the three-dimensional cylindrically symmetric harmonic trap confining the condensate is stronger in the axial (z) direction than in the radial direction (r). Hence, the momentum along the axial direction is greater than along the radial direction causing the cloud to expand anisotropically as a function of the free expansion time as shown in Fig. 4 [24, 25]. The fit of the theoretical curve in Fig. 4 to the data gives a result for the ^{87}Rb scattering length of $(107 \pm 5)a_0$ where a_0 is the Bohr radius. This is in excellent agreement with the result of $(106 \pm 4)a_0$ determined using photoassociative spectroscopy whereby a laser is tuned to excite an atom of an interacting pair of atoms that then forms a molecular state [26]. The latter can decay generating atoms whose kinetic energies exceed the trap depth resulting in enhanced loss of atoms from the trap [27].

3. Einstein–Podolsky–Rosen paradox

The EPR paradox is most easily understood by considering the decay of a spin-zero particle into two spin-1/2 particles as was first formulated by Bohm [28]. Each spin-1/2 particle may have its spin pointing either up or down relative to the z axis denoted by $|1\rangle$ and $|0\rangle$, respectively. The original particle had zero spin and, therefore, angular momentum conservation requires the two spin-1/2 particles to be

Fig. 3. BEC lifetime. The final stage in creating a BEC is to use evaporative cooling. A RF signal is scanned from an initial frequency to a lower final frequency as explained in the text. A BEC is observed after the RF signal is turned off and lasts for about 200 ms before collisions with the background gas heat the atoms above the transition temperature as shown in (*a*). In contrast, if the RF is kept on after the completion of the scan at its final frequency, lifetime can be extended by an order of magnitude.



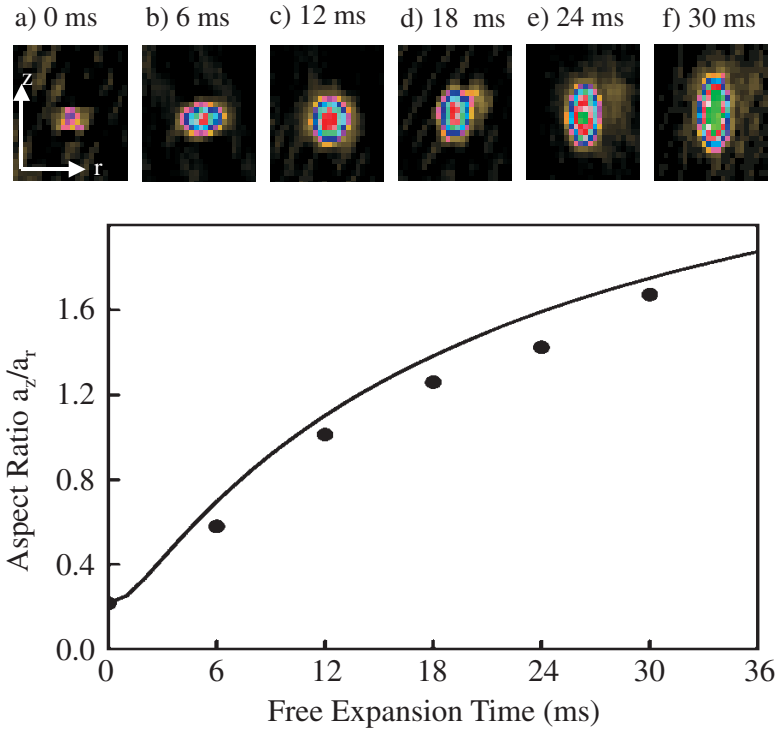
in a spin singlet state given by

$$\psi = \frac{\{|1\rangle|0\rangle - |0\rangle|1\rangle\}}{2^{1/2}} \tag{9}$$

This is an example of an entangled state as it is not possible to assign separate individual spin states to the two particles.

The decay of the original particle produces two spin-1/2 particles traveling in opposite directions.

Fig. 4. Condensate evolution during free expansion for the times indicated. α is the ratio of the condensate diameters in the r and z directions. It is a function of the free expansion time. (*a*) shows the atoms in the trap before the expansion and has a smaller scale than is used in (*b*)–(*f*). The observed data are fitted reasonably well by the theoretical prediction as discussed in the text. The theoretical curve was constrained to fit the data at time $t = 0$.



These particles can be detected by observers A and B. If observer A measures the spin of the first particle relative to the z axis to be $+1/2$, then the wave function collapses to $|1\rangle\,|0\rangle$. Observer B then automatically measures particle two to have spin $-1/2$. Einstein found it troubling that if the two observers were sufficiently far apart, a signal leaving A after A's measurement and traveling at the speed of light would not reach B until after B's measurement. He, therefore, concluded that the particles were in definite spin states prior to the spin measurement, not as a result of the measurement as is assumed by the Copenhagen interpretation of quantum mechanics. The two spin-1/2 particles would then be described by a statistical distribution of $|1\rangle\,|0\rangle$ and $|0\rangle\,|1\rangle$ states depending on some as yet unknown or "hidden" variables rather than the wave function given by (9).

It should be noted that the EPR paradox does not contradict special relativity by allowing for communication faster than the speed of light. The determination by observer B that the spin of particle 2 is down could result from the collapse of the wave function due to the measurement of observer A on particle 1. Alternatively, the same result occurs with a probability of 50% if B makes his measurement before A. B can only distinguish between the two possibilities if he were notified of A's measurement by a classical signal traveling at the speed of light.

An apparent flaw in the preceding argument exists if B can make copies or clone the wave function before making any measurements. B could then distinguish between the two possibilities by determining whether a spin down result occurred with probability of 50% or 100%. Hence, one must conclude that a wave function cannot be cloned for superluminal transmission of information to not be possible.

For several decades it remained an open question whether Quantum Mechanics was a complete theory. However in 1964, Bell derived inequalities that could be experimentally tested to address this

question [11, 28]. He considered the decay of a spin-0 particle into two particles 1 and 2. Observer A measures the spin of particle 1 along direction $\boldsymbol{a}$ while observer B measures the spin of particle 2 along direction $\boldsymbol{b}$. One then evaluates the correlation coefficient defined by

$$C(\boldsymbol{a}, \boldsymbol{b}) = \{(\boldsymbol{\sigma} \cdot \boldsymbol{b})(\boldsymbol{\sigma} \cdot \boldsymbol{a})\}_{\text{av}} \tag{10}$$

where av denotes the average of a large number of repeated measurements and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector composed of the Pauli spin matrices. The correlation coefficient has values between -1, which occurs when $\boldsymbol{a} = \boldsymbol{b}$ and $+1$ when $\boldsymbol{a} = -\boldsymbol{b}$. Bell showed that in any hidden variable theory, the correlation coefficients must satisfy

$$|C(\boldsymbol{a}, \boldsymbol{b}) - C(\boldsymbol{a}, \boldsymbol{c})| - C(\boldsymbol{b}, \boldsymbol{c}) \leq 1 \tag{11}$$

Quantum mechanics, however predicts a violation of this inequality. For example, if $\boldsymbol{a} = (0, 0, 1)$, $\boldsymbol{b} = (\sin\theta, 0, \cos\theta)$ and $\boldsymbol{c} = (\sin 2\theta, 0, \cos 2\theta)$ it can be shown that the left side of (11) equals $|-\cos\theta + \cos 2\theta| + \cos\theta$. Setting $\theta = 45°$ yields a value of $2^{1/2}$ violating (11).

A definitive experimental test of Bell's inequalities was carried out by the group of Aspect in the early 1980s [12] and more recently by other groups [29]. The Aspect experiment used two photons acting as a pair of EPR particles that were generated by stepwise radiative decay of a calcium atom via the $(4p)^2\ ^1S_0 \rightarrow 4s4p\ ^1P_1 \rightarrow (4s)^2\ ^1S_0$ transitions. Two photomultipliers measured photons propagating in opposite directions. The detector signals were then carefully analyzed using fast-photon counting electronics to realize the "EPR Gedanken" experiment. The transmission axes of linear polarizers in front of the detectors were rotated to vary $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$. The experiment found a result consistent with quantum mechanics violating Bell's inequality by an amount greater than 10 standard deviations times the experimental uncertainty.

4. Quantum cryptography

Sending information that can only be deciphered by the intended recipient has been a challenge for thousands of years. Typically, letters are converted to numbers that are then scrambled. Hopefully, only the recipient is aware of how to decrypt the message. A popular method to encrypt messages is the RSA algorithm developed in 1977 by Rivest et al. [30]. It relies on the difficulty of factoring large numbers N having in excess of 100 digits into two prime numbers p and q, i.e., $N = pq$. The number e used to encrypt the message number is selected such that it has no prime factors in common with $(p-1)(q-1)$. The decryption number d is found such that the remainder of the product ed divided by $(p-1)(q-1)$ is 1. Mathematically, this is denoted as follows:

$$(ed) \text{ modulo } [(p-1)(q-1)] = 1 \tag{12}$$

For example, the number $N = 3233$ is factored by prime numbers $p = 61$ and $q = 53$. Selecting $e = 17$, one finds $d = 2753$ using (12). The sender encrypts message number M into M' using

$$M' = M^e \text{ modulo } N \tag{13}$$

while the receiver deciphers M' using

$$M = M'^d \text{ modulo } N \tag{14}$$

The numbers e and N are publicly available and called the key while number d as well as p and q are known only by the intended receiver.

The fastest conventional computers using known algorithms are far too slow to determine p and q by factoring N. It is estimated that it would take a computer operating at 200 million instructions

per second 10 million years to factor a number 250 digits long [31]. However, an algorithm has been developed for a quantum computer that can solve the problem in a reasonable time as is discussed in Sect. 5 thereby rendering conventional encryption methods such as the RSA algorithm obsolete.

In 1984, Bennett and Brassard developed an encryption method that uses a single photon at a time to transfer information [32, 33]. Quantum mechanics shows an eavesdropper would perturb the message in such a way that is readily detectable by the intended receiver and sender [34–39]. The sender passes an unpolarized light beam propagating in the y direction through a linear polarizer. The polarizer is oriented at angle θ such that the transmitted light is linearly polarized along the $(\cos\theta, 0, \sin\theta)$ direction. The angle θ is varied in increments of $\pm 45°$. The resulting light is linearly polarized either vertically or horizontally denoted by states $|1\rangle$ and $|0\rangle$, respectively, or along the directions specified by $\theta = 45°$ and 135°, which are denoted by states $|+\rangle$ and $|-\rangle$, respectively.

The sender sends the encryption key information to the receiver as a series of single photons. A binary bit 1 is represented by either states $|1\rangle$ or $|+\rangle$ while a bit 0 is represented by either states $|0\rangle$ or $|-\rangle$. The sender records whether the vertical, horizontal, or diagonal basis was used to transmit each bit. The receiver has a linear polarizer in front of a detector whose transmission axis is randomly aligned along either the vertical or $\theta = 45°$ axes. The receiver assigns bit 1 if a photon is detected and 0 otherwise. Hence, 50% of the time the receiver filter is aligned such that the intended bit is correctly communicated. For the other 50% of the time, the bit recorded by the receiver agrees with the sent bit only half of the time. For example, if the sender transmits bit 0 using their polarizer in the horizontal direction and the receiver's polarizer is aligned such that $\theta = 45°$ then the receiver detects a photon with 50% probability. The next stage is for the sender to inform the receiver of the orientation of their polarizer for each bit that was sent. The receiver then discards all results for which the sender and receiver polarizer orientations differed by 45°.

The preceding discussion does not consider the effect of errors arising due to either imperfect equipment or intentional eavesdropping. An eavesdropper could either divert all signals traveling to the intended receiver, which is obvious, or attempt to read each signal. However, once the polarization of a photon is measured, the photon's polarization is irreversibly changed. An alternative suggestion is for the eavesdropper to copy each photon state and determine the message after the sender transmits their polarizer orientation. This latter approach, however, is not possible since the EPR paradox prohibits cloning of a quantum state. Hence, both equipment error and eavesdropping can be detected if the sender and receiver compare part of the message. If the error rate is unacceptably large, the sender and receiver can try communicating again using an alternative key.

Quantum encryption has been demonstrated over distances of up to 150 km in an optical fiber and over 20 km in the atmosphere. Commercial quantum cryptographic systems are now available [40]. Indeed, quantum encrypted communication via satellite is a real possibility over the next few years. Ideally, such signals could be transported around the world using quantum repeaters or "teleportation", which is the transfer of an unknown quantum state from one particle to another. This is not the same as cloning since this process destroys all information about the input quantum state. Recently, researchers demonstrated teleportation by transferring the polarization of an input photon to another photon using parametric down conversion in a BBO crystal [41]. Teleportation research involving atoms and ions is also underway [42–44].

5. Quantum information processing

In classical computing, information is recorded as a series of bits having the binary values of either 0 or 1. In contrast, two quantum states denoted by $|0\rangle$ and $|1\rangle$, which can, for example, be represented by the up or down orientation of a spin-1/2 particle are represented by the quantum state or "qubit"

$$\psi = \alpha|0\rangle + \beta|1\rangle \tag{15}$$

Here α and β are complex coefficients satisfying the normalization condition $\alpha^2 + \beta^2 = 1$. The wave function describing two qubits is in turn given by the tensor product of two single qubit wave functions, i.e.,

$$\begin{aligned}\psi &= \{\alpha|0\rangle + \beta|1\rangle\} \otimes \{\gamma|0\rangle + \delta|1\rangle\} \\ &= \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle\end{aligned} \tag{16}$$

A wave function describing n qubits is represented by

$$\psi = \Sigma_{i1i2i3\ldots in} c_{i1i2i3\ldots in}|i_1 i_2 i_3 \ldots i_n\rangle \tag{17}$$

where the sum is over each $i_1, i_2, \ldots i_n$ which takes on the values 0 or 1 and the sum of the squares of all the c coefficients equals one. Hence, an n qubit has $2^n - 2$ degrees of freedom where 2 has been subtracted because ψ is normalized and is unaffected by an overall phase factor. This is considerably greater than the information contained by a classical series of n bits.

Quantum computing is done by manipulating the wave function by operating on the wave function using the evolution operator $U = \mathrm{e}^{-iHt}$ where H is the Hamiltonian. This results in the wave function

$$\psi' = \mathrm{e}^{-iHt}\psi = \Sigma_{i1i2i3\ldots in} d_{i1i2i3\ldots in}|i_1 i_2 i_3 \ldots i_n\rangle \tag{18}$$

We note that operator U has affected each of the basis states $|i_1 i_2 i_3 \ldots i_n\rangle$ performing in effect parallel computing. This is known as quantum parallelism and has been shown to enable quantum computing to solve certain problems exponentially faster than classical computers [34–36].

In 1994, Shor showed that a quantum computer could factor a prime number N in a time of order $n^2 \log n \log(\log n)$ where $n = \log N$ as compared to the time required by the fastest known classical algorithm given by $\exp(n^{1/3}(\log n)^{2/3})$ [45]. Number theory shows that a function $f(a) = x^a$ modulo N is a periodic function, where x is an integer coprime to N. Two numbers are said to be coprime if their greatest common divisor is 1. Shor's algorithm determines the period r of the function. We note that $f(0) = 1$ and, therefore, $f(r) = x^r$ modulo N and $f(2r) = x^{2r}$ modulo N also equal 1. $f(r) = 1$ implies

$$\left(x^{r/2}\right)^2 - 1 = 0 \text{ modulo } N \tag{19}$$

For an even number r, this can be rewritten as follows:

$$(x^{r/2} - 1)(x^{r/2} + 1) = 0 \text{ modulo } N \tag{20}$$

The left side of (20) is an integer multiple of N. Assuming that $x^{r/2}$ does not equal ± 1 then we conclude that at least one of either $(x^{r/2} - 1)$ or $(x^{r/2} + 1)$ must have a nontrivial factor in common with N. If r is not even, the algorithm can be repeated using a different x value.

The function period is found using the Fourier transform. Shor's method is illustrated by showing how it determines the period of the function $f(x) = 1/2(\cos(\pi x) + 1)$ [35]. We consider eight values of the input x denoted by quantum register $|x\rangle$, which consists of 3 qubits, i.e., $|0\rangle = |000\rangle$, $|1\rangle = |001\rangle$, $|2\rangle = |010\rangle$ etc. For these x values, $f(x) = 0$ or 1 and the output register is, therefore, represented by a single qubit $|O\rangle$. The quantum computer is prepared in the following initial state:

$$\psi_0 = 8^{-1/2}\{|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle\}|O\rangle \tag{21}$$

Next, the computer evaluates the function yielding

$$\begin{aligned}\psi_1 &= 8^{-1/2}\{|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle + |2\rangle|f(2)\rangle + \ldots + |7\rangle|f(7)\rangle\} \\ &= 8^{-1/2}\{|0\rangle|1\rangle + |1\rangle|0\rangle + |2\rangle|1\rangle + \ldots + |7\rangle|1\rangle\}\end{aligned} \tag{22}$$

The output register is then measured. If a result of 0 is found then wave function (22) reduces to

$$\psi_2 = 1/2\{|1\rangle + |3\rangle + |5\rangle + |7\rangle\} \tag{23}$$

where the output register has been omitted. The quantum Fourier transform operation transforms $|x\rangle$ to $8^{-1/2}\Sigma_k e^{2\pi ikx/8}|k\rangle$ where index k assumes values from 0 to 7. The quantum computer then obtains

$$\begin{aligned}\psi_3 = 32^{-1/2}\{&|0\rangle + e^{i\pi/4}|1\rangle + e^{i2\pi/4}|2\rangle + \ldots + e^{i7\pi/4}|7\rangle \\ &+ |0\rangle + e^{i3\pi/4}|1\rangle + e^{i6\pi/4}|2\rangle + \ldots + e^{i21\pi/4}|7\rangle \\ &+ |0\rangle + e^{i5\pi/4}|1\rangle + e^{i10\pi/4}|2\rangle + \ldots + e^{i35\pi/4}|7\rangle \\ &+ |0\rangle + e^{i7\pi/4}|1\rangle + e^{i14\pi/4}|2\rangle + \ldots + e^{i49\pi/4}|7\rangle\} \\ = 2^{-1/2}\{&|0\rangle - |4\rangle\}\end{aligned} \tag{24}$$

The register is read and either 0 or 4 is measured with 50% probability. In the case of a 0 result, the calculation must be repeated. If 4 is measured, the period is found by dividing by the number of x values and simplifying to an irreducible fraction. In our case $r/N = 4/8 = 1/2$ and we conclude that the period of $f(x)$ is 2.

Quantum computing is different from classical computing in a number of respects. First, as is illustrated in the preceding example, a meaningful final result is not in general found after every calculation. This is not a significant problem as the time spent repeating the calculation is much less than the time saved using a quantum instead of a classical computer. A second problem is controlling the wave function and preventing it from being perturbed or entangling with unknown states in the environment. This is known as decoherence and could induce errors. Recently, so-called fault-tolerant quantum computation has been developed [46]. This is similar to classical error correcting codes where each bit is represented redundantly by several bits, i.e., $|1\rangle$ by $|111\rangle$. The original information can then be retrieved if only a single bit has flipped.

6. Implementation of quantum computing

Classical computing can be broken down into a series of one- and two-bit operations. The same is true for quantum computation. It has been shown that quantum computational algorithms can be implemented as a series of one- and two-qubit operations [35, 36]. One of the standard two-bit logic operations is the so-called controlled-NOT or CNOT gate. This changes the target bit if the first or control bit is 1 and is denoted as

$$\mathrm{CNOT}|ij\rangle = |i\rangle|i \oplus j\rangle \tag{25}$$

where $i \oplus j = i + j$ modulo 2.

Several systems have been proposed for implementing quantum computing [36, 39]. The ion trap has been the most successful. Indeed, a single trapped $^9Be^+$ ion was used to demonstrate a CNOT gate [47, 48]. The target bit is spanned by the $F = 2$ $m_F = 2$ and $F = 1$ $m_F = 1$ hyperfine levels of the $2S_{1/2}$ ground state. The control qubit is spanned by the two lowest quantized harmonic oscillator states of the ion trap. Manipulation between these four basis eigenstates was done using off-resonant laser beams that stimulated Raman transitions between the basis states. Nuclear spins can also be used to represent qubits. Indeed, 7 spin-1/2 nuclei in a perfluorobutadienyl iron were used to demonstrate Shor's algorithm by factoring 15 [49]. The quantum circuit was realized with a sequence of about 300 RF pulses that were implemented in a total time of 720 ms.

Unfortunately, it is difficult to scale the two preceding technologies to involve sufficient numbers of qubits to make a practical quantum computer. It has been estimated that 3500 qubits would be needed

to factor a 200 digit number. This estimate increases to 100 000 qubits if error correction algorithms are implemented [50, 51].

Neutral atom traps offer an interesting possibility for the attainment of a quantum computer as they can be miniaturized and arranged into a two-dimensional array [39]. Indeed, BEC has been achieved using a single microtrap created using microwires that were deposited onto a silicon chip [52]. The wires were arranged in appropriate shapes having dimensions of less than 1 mm. A microtrap is much smaller than a conventional macroscopic magnetic trap and, therefore, requires much smaller currents. The atom density in the trap is also higher, which facilitates evaporative cooling. Atoms are typically loaded into a microtrap from a nearby magneto-optical trap created by reflecting laser beams off the chip surface. Various schemes to guide atoms and load single surface microtraps are discussed in the review paper by Folman et al. [53].

Fabrication of microtraps is achieved using lithographic techniques that can readily create structures with sizes as small as 100 nm. The trap wires typically consist of gold and can be deposited onto a semiconductor wafer. Current densities must be limited to below 10^8 A/cm^2 to avoid excessive heat buildup that would destroy the chip. This problem would be eliminated if superconducting wires were available.

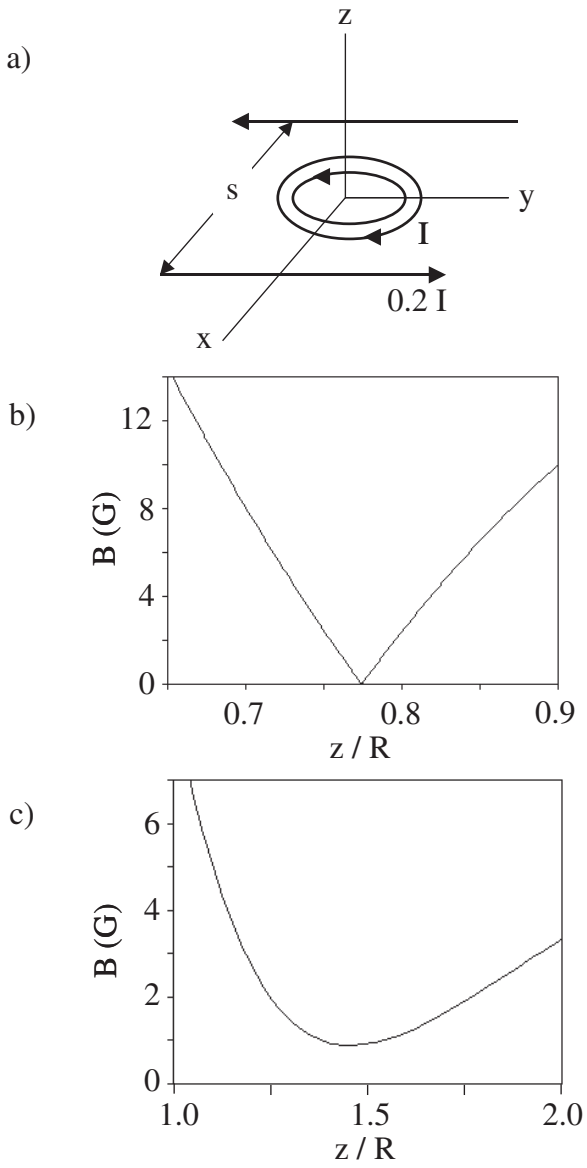
An example of a proposed "unit cell" of a two-dimensional microtrap array is shown in Fig. 5. Figure 5*b* considers the field generated by two circular wire loops of radii R and $1.2R$ carrying oppositely oriented currents I. This creates a three-dimensional magnetic field trap configuration having zero field minimum above the loop. Figure 5*c* shows a trap having a nonzero magnetic field minimum, to prevent atom loss due to Majorana transitions, that is obtained by adding currents traveling along two straight parallel wires.

The qubits would be realized in each microtrap analogously as in the ion trap by using lasers to couple two hyperfine levels of the ground state. The coupling of two qubits would be accomplished using lasers to control the interaction of atoms in neighbouring microtraps. This is analogous to the interaction of cold atoms in so-called optical lattices that are created using counterpropagating laser beams whose frequency is detuned from the atomic transition [54]. These have been used to entangle atoms located at different lattice sites [55]. One recent experiment created a three-dimensional lattice of ^{87}Rb atoms having over 150 000 lattice sites each containing an average of 2.5 atoms [56]. At high laser intensity, the atoms are confined to small regions creating a three-dimensional array of trapped atoms. The tunneling rate of atoms between neighbouring lattice sites increases as the laser power is decreased causing a transition from the Mott insulator state to the superfluid state to occur.

A two-dimensional array of neutral atom microtraps generated by an atom chip has several advantages to be a quantum processor [39]. First, neutral atoms interact much more weakly with each other and with background gas atoms than do ions. Magnetic traps also levitate the atoms above the substrate surface thereby decreasing the rate of decoherence as compared to other proposed solid-state schemes to implement quantum computing [36].

The simplest atom chip would only contain the nanowires to generate the magnetic fields for the traps. We have modeled one- and two-dimensional arrays where each row has up to nine microtraps generated using the unit cell shown in Fig. 5. All of the microtraps in the array have similar magnetic field distributions except for those located along the array boundary. Eventually, it should be possible to incorporate lasers onto the semiconductor substrate. A laser mounted at the center of each microtrap could excite an atomic transition while a photodiode would detect the fluorescence. This is especially convenient in the case of Cs or Rb which have transitions at infrared wavelengths where diode lasers readily operate. Other diode lasers mounted between microtraps could be suitably focused possibly using microlenses to control the coupling between qubits. The entanglement or coupling of qubits at neighbouring microtraps could be controlled by varying the laser frequency and power. The control of the nanowire currents and the temporal switching of an array of diode lasers to manipulate the microtraps to do useful processing would be complex. However, the interface of an atom chip to a

Fig. 5. Magnetic field for an atom chip element. (*a*) An atom chip could consist of individual microtraps as shown. The magnetic field magnitude is plotted along the z direction perpendicular to the chip. (*b*) The field generated by only a pair of concentric wire loops having radii R and $1.2R$ carrying oppositely oriented currents I. Here, we consider $R = 10$ μm and $I = 1$ A. (*c*) The field generated when an additional pair of parallel wires carrying oppositely oriented currents $0.2I$ separated by a distance $s = 6R$. The trap has a nonzero field minimum of 0.88 G that prevents trap loss due to Majorana transitions.



conventional computer would be relatively straight forward. Formidable technological challenges of fabricating such an atom chip exist. Potential limitations include dissipating the heat generated by the high current densities in the nanowires and incorporating a multitude of diode lasers, each having stringent requirements such as narrow linewidth, exact frequency stability, and tunability as well as high beam quality to permit precise focusing.

7. Conclusions

The last 100 years have witnessed unparalleled technological progress largely made possible by advances in theoretical physics. Albert Einstein was the leading theorist during this period. Indeed, he is only rivaled by perhaps Isaac Newton who developed classical mechanics or James Clerk Maxwell who unified electricity, magnetism and optics, as the greatest scientist of all time.

It is interesting that physicists' perception of the relative significance of Einstein's contributions to various fields has changed over time. Einstein received the 1921 Nobel Prize for his explanation of the photoelectric effect not for relativity for which he is today most famous. At the time of his death in 1955, few physicists if any would have thought that BEC and the EPR paradox would be at the forefront of research in 2005. Today commercial quantum cryptographic systems based on the EPR paradox are available at a modest sum and research in quantum computing is a burgeoning field.

The control of quantum information will undoubtedly require systems operating at temperatures below the BEC threshold to facilitate precise control of the atom motion. A quantum computer may allow for the study of problems that today seem intractable such as many body atomic systems. The principal challenge in developing a quantum computer will be increasing the number of qubits while minimizing their unwanted entanglement with the environment. This effort will certainly take many years perhaps even decades but seems especially important as the continued ability to increase the speed of conventional computers is approaching the limit where the integrated chip circuit feature size is comparable to the Bohr radius. In conclusion, Einstein's insights into the true weirdness of quantum mechanics will undoubtedly continue to spur on physicists well into the next century in their efforts to understand and control quantum systems.

Acknowledgements

The author wishes to thank the Natural Science and Engineering Research Council of Canada for financial support. B. Lu helped take the data displayed in Figs. 1–4 while I. Corlett and H. Ming provided invaluable assistance to model the magnetic fields using MAPLE as shown in Fig. 5.

References

1. A. Pais. Subtle is the Lord. Oxford University Press, New York. 1982.
2. A. Einstein. Ann. Phys. (Leipzig), **17**, 132 (1905).
3. A. Einstein. Ann. Phys. (Leipzig), **17**, 549 (1905).
4. A. Einstein. Ann. Phys. (Leipzig), **17**, 891 (1905).
5. A. Einstein. Ann. Phys. (Leipzig), **49**, 769 (1916).
6. A. Einstein. Verh. Deutsch. Phys. Ges. **18**, 318 (1916).
7. A. Eddington. Space, time and gravitation. Cambridge University Press, Cambridge. 1920.
8. S.N. Bose. Z. Phys. **26**, 178 (1924).
9. A. Einstein. Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-mathematische Klasse. 1924.
10. A. Einstein, B. Podolsky, and N. Rosen. Phys. Rev. **47**, 777 (1935).
11. J.S. Bell. Physics, **1**, 195 (1964).
12. A. Aspect, P. Grangier, and G. Roger. Phys. Rev. Lett. **47**, 460 (1981).
13. H.J. Metcalf and P. van der Straten. Laser cooling and trapping. Springer, New York. 1999. pp. 120–126.
14. C.J. Pethick and H. Smith. Bose–Einstein condensation in dilute gases. Cambridge University Press, Cambridge. 2002.
15. K.B. Davis, M.O. Mewes, M. Andrews, M. van Druten, D. Durfee, D. Kurn, and W. Ketterle. Phys. Rev. Lett. **75**, 3969 (1995).
16. M.H. Anderson, J.R. Ensher, M.R. Matthews, C.E. Wieman, and E.A. Cornell. Science, **269**, 198 (1995).
17. C.C. Bradley, C.A. Sackett, J.J. Sackett, J.J. Tollett, and R.G. Hulet. Phys. Rev. Lett. **75**, 1687 (1995).
18. K. Stowe. Introduction to statistical mechanics and thermodynamics J. Wiley, Toronto. 1984.
19. D.R. Tilley and J. Tilley. Superfluidity and superconductivity. Adam Hilger Ltd., Boston. 1986.

20. E.L. Andronikashvili. Zh. Eksp. Theor. Fiz. **16**, 780 (1946).
21. H.N. Robkoff, D.A. Ewen, and R.B. Hallock. Phys. Rev. Lett. **43**, 2006 (1979).
22. W.A. van Wijngaarden and B. Lu. Physics in Canada, **60**, No. 5 (2004).
23. B. Lu and W.A. van Wijngaarden. Can. J. Phys. **82**, 81 (2004).
24. Y. Castin and R. Dum. Phys. Rev. Lett. **77**, 5315 (1996).
25. M.O. Mewes, M.R. Andrews, N.J. van Druten, D.M. Kurn, D.S. Durfee, and W. Ketterle. Phys. Rev. Lett. **77**, 416 (1996).
26. J.L. Roberts, N.R. Claussen, J.P. Burke, C.H. Greene, E.A. Cornell, and C.E. Wieman. Phys. Rev. Lett. **81**, 5109 (1998).
27. J. Weiner, V.S. Bagnato, S. Zilio, and P.S. Julienne. Rev. Mod. Phys. **71**, 1 (1999).
28. H.C. Ohanian. Principles of quantum mechanics. Prentice Hall, Englewood Cliffs. 1990.
29. E.S. Fry and T. Walther. Atom based tests of the Bell inequalities — the legacy of John Bell continues. Quantum [Un]speakables. R.A. Bertlmann and A. Zeilinger (*Editors*.) Springer, New York. 2002. pp. 103–117,
30. R.L. Rivest, A. Shamir, and L. Adleman. CACM Conference Proceedings, 20–26 February (1978).
31. R.J. Hughes. Philos. Trans. R. Soc. London, **A356**, 853 (1998)].
32. C.H. Bennett and G. Brassard. Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, 175, New York. 1984.
33. C.H. Bennett, G. Brassard, and A.K. Ekert. Sci. Am. **267**(4), 50 Oct. (1992).
34. R.P. Feynman. Int. J. Theor. Phys. **21**, 467 (1982).
35. G. Benenti, G. Casati, and G. Strini. Principles of quantum computation and information. World Scientific, London. 2004.
36. M.A. Nielsen and I.L. Chuang. Quantum computation and quantum information. Cambridge University Press, Cambridge. 2000.
37. S.J. Lomonaco. Coding theory and cryptography: From the Geheimschreiber and engima to quantum theory. *Edited by* D. Joyner. Springer-Verlag, Berlin. 1999. p. 144.
38. C.H. Bennett and D.P. DiVincenzo. Nature, **404**, 247 (2000).
39. J.I. Cirac and P. Zoller. Phys. Today, **57**, 38 (2004).
40. G. Stix. Sci. Am. **292**, 79 (2005).
41. R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger. Nature, **430**, 849 (2004).
42. R. Riebe, H. Häffner, C.F. Roos, W. Hänsel, J. Benhelm, G.P.T. Lancaster, T.W.Körber, C. Becher, F. Schmidt-Kaler, D.F.V. James, and R. Blatt. Nature, **429**, 734 (2004).
43. M.D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W.M. Itano, J.D. Jost, E. Knill, C. Langer, D. Leibrief, R. Ozeri, and D.J. Wineland. Nature, **429**, 737 (2004).
44. P. Hommelhoff, W. Hänsel, T. Steinmetz, T.W. Hänsch, and J. Reichel. New J. Phys. **7**, 3 (2005).
45. P.W. Shor. Proc. of 35th Annual Symposium on the Foundations of Computer Science. *Edited by* S. Goldwasser. IEEE Computer Society Press, Los Alamitos, Calif. 1994. p. 124.
46. J. Preskill. Proc. R. Soc. London A, **454**, 385 (1998).
47. J.I. Cirac and P. Zoller. Phys. Rev. Lett. **74**, 4091 (1995).
48. C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano, and D.J. Wineland. Phys. Rev. Lett. **75**, 4714 (1995).
49. L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang. Nature, **414**, 883 (2001).
50. J.L. Cirac and P. Zoller. Nature, **404**, 579 (2000).
51. D. Beckman, A.N. Chari, S. Devabhaktuni, and J. Preskill. Phys. Rev. A, **54**, 1034 (1996).
52. W. Hänsel, P. Hommelhoff, T.W. Hänsch, and J. Reichel. Nature, **413**, 498 (2001).
53. R. Folman, P. Kruger, J. Schmiedmayer, J. Denschlag, and C. Henkel. Adv. At. Mol. Opt. Phys. **48**, 263 (2002).
54. D. Jaksch, C. Bruder, J.I. Cirac, C.W. Gardiner, and P. Zoller. Phys. Rev. Lett. **81**, 3108 (1998).
55. O. Mandel, M. Greiner, A. Widera, T. Rom, T.W. Hänsch, and I. Bloch. Nature, **425**, 937 (2003).
56. M. Greiner, O. Mandel, T. Esslinger, T.W. Hänsch, and I. Bloch. Nature, **415**, 39 (2002).