An introduction to Quantum Information and Quantum Computation (Temas de Física)

Géza Tóth

[1]Theoretical Physics, University of the Basque Country UPV/EHU, Bilbao, Spain
[2]IKERBASQUE, Basque Foundation for Science, Bilbao, Spain

Leioa,
10:40-11:30, 0.15, 23 February 2014;
10:40-11:30, 0.18, 26 February 2014;
10:40-11:30, 0.18, 2 March 2014;
10:40-11:30, 0.18, 5 March 2014.

Outline

Quantum information science

- Analytic aspects
  - Quantum mechanics
  - Quantum optics

- Constructive aspects
  - Quantum engineering, creating large quantum states, entanglement
  - Quantum cryptography, quantum communication
  - Quantum metrology
  - Quantum computing, quantum simulation

Outline

Quantum mechanics

- Basic tools have been developed in the 1930's:

  - Schrödinger equation,
  - von Neumann equation $i\frac{\partial \varrho}{\partial t} = [H, \varrho]$,
  - state function, state vector $|\Psi\rangle$.
  - density matrix ϱ,
  - Dirac equation.

- However, one thing was missing:

  - it was difficult to test this model since individual particles could not be observed.

Outline

Quantum optics

- LASER: a new system in which quantum mechanics was important.

- They developed a formalism to describe light modes in 1960's

    - annihilation, creation operators (like Ψ and Ψ^+ in field theory)
    - coherent states (light fields we see in practice)
    - Fock states (states with given particle number)
    - Wigner function (even before) $W(x, p)$
    - light-atom interaction, photon detection, superradiance, etc.

- However, one thing was still missing:

    - they could not observe few particles in a correlated quantum state.
    - They could see only many particles interacting with light, where the particles did nothing with each other.

- Do individual particles exist?

- Or they are only a tool for modeling?

Outline

Qubits vs. bits

- A quantum bit (=two-state system, spin-$\frac{1}{2}$ particle) can be in a pure state

$$|q\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle,$$

  where α_0 and α_1 are complex numbers, and the normalization condition $|\alpha_0|^2 + |\alpha_1|^2 = 1$.
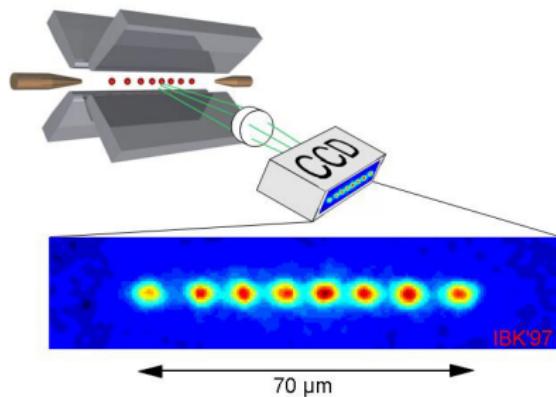
- Two qubits can be in a state

$$|q_1 q_2\rangle = \alpha_{00}|0\rangle \otimes |0\rangle + \alpha_{01}|0\rangle \otimes |1\rangle + \alpha_{10}|1\rangle \otimes |0\rangle + \alpha_{11}|1\rangle \otimes |1\rangle.$$

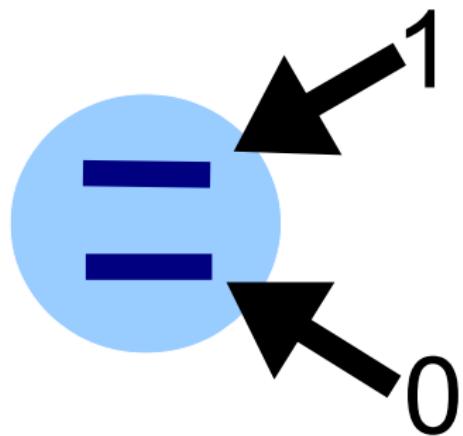- N qubits can be in a state that is the superposition of 2^N basis states $\rightarrow$ exponential scaling.

Trapped cold ions

- Due to the technological development, it became possible to manipulate small number of particles, and accessing the particles individually.

- Examples: trapped cold ions

70 µm

Innsbruck, Austria.
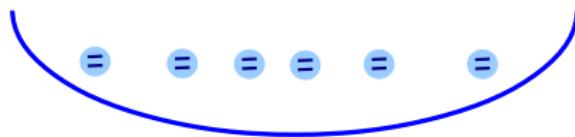
- Ion as a qubit
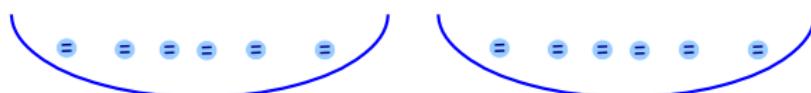
Trapped cold ions III

- Two-state ions trapped in an electromagnetic field

- Coulomb-repulsion keeps them apart from each other.
- Phonon bus: the internal states can be coupled

Oscillates   Does not oscillate

- Q: How can the internal states of the ions interact?
- (The Coulomb interaction is not sensitive to the internal state of the neighbor.)

- A: Through the phonon bus.
  [J. I. Cirac and P. Zoller, Phys. Rev. Lett. 1995]

Trapped cold ions V

- Phonon bus=a bosonic mode$\approx$ extra qubit.

- It can be even in a superposition state
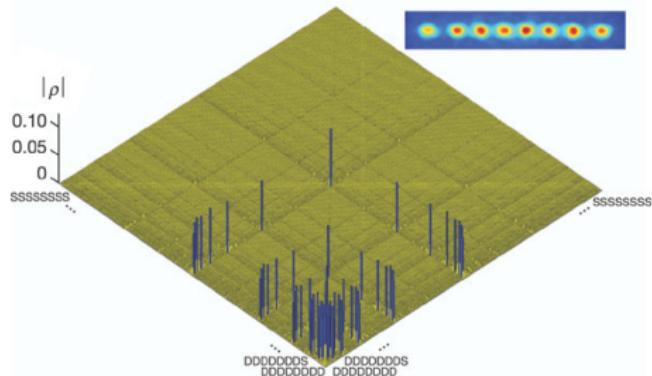
$$\frac{1}{\sqrt{2}}(|\text{Oscillates}\rangle + |\text{Does not oscillate}\rangle).$$

- The Hamiltonian for a single ions is (using RWA)

$$H \propto |0\rangle\langle 1|a + |1\rangle\langle 0|a^{\dagger}.$$

- Quantum tomography of an eight ion quantum state giving the density matrix:

- The state is the state that they wanted to create:

$$|W\rangle = \frac{1}{\sqrt{6}} \left(|10000000\rangle + |01000000\rangle + ... + |00000001\rangle \right).$$

Trapped cold ions VII

- Greenberger-Horn-Zeilinger (GHZ) state

$$|GHZ\rangle = \frac{1}{\sqrt{2}} \left(|00...00\rangle + |11..11\rangle \right)$$
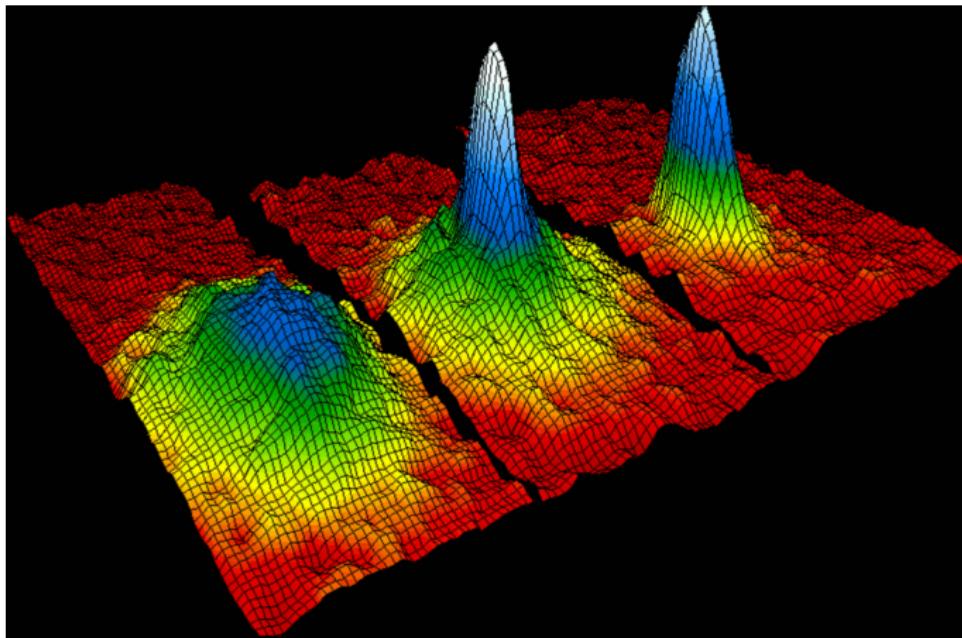
- In another context, Schrödinger's cat state.

- Some experiments:
  - 3 particles, Nature 2001.(NIST, Boulder, Colorado)
  - 14 particles, Phys. Rev. Lett 2013. (Innsbruck, Austria)

Questions

- Experiments are noisy.

- How well quantum systems can be realized in an experiment.
- Is there a fundamental limit that does not allow certain, otherwise not aphysical quantum states? (i.e., Schrödinger cats)

- Is universal quantum computing possible?
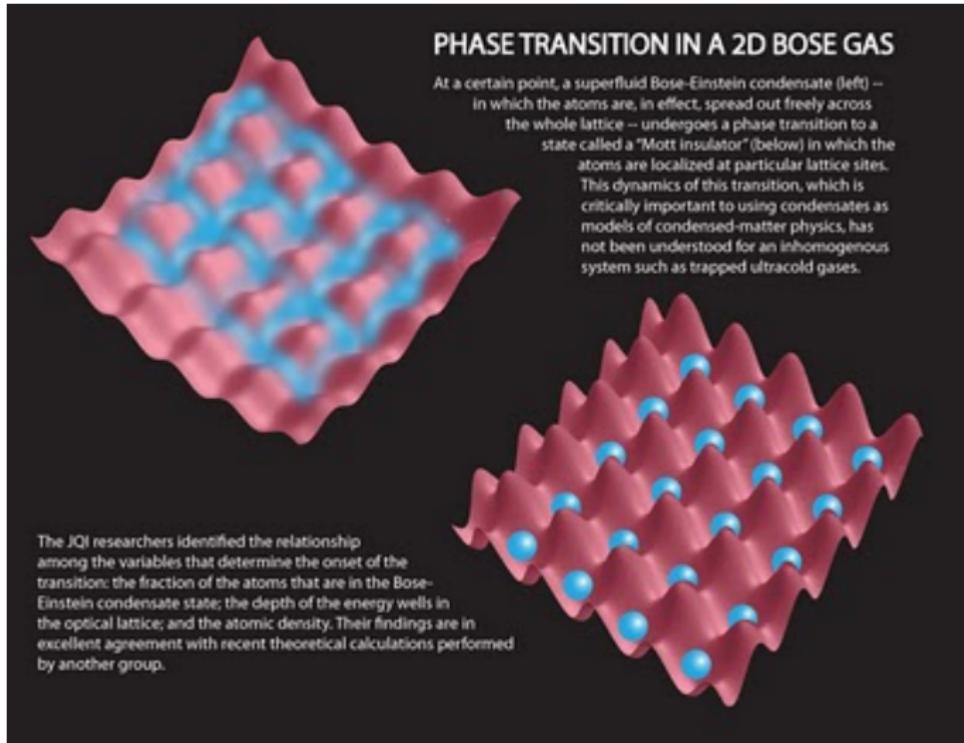
Bose-Einstein condensates

- Bose-Einstein condensation 1995, Nobel prize 2001.

- Velocity distribution before and after condensation.

Optical lattices of cold atoms

Superfluid-Mott insulator phase transition, MPQ, Munich.
[Greiner, Mandel, Esslinger, Hänsch & Bloch, Nature 2002]

Optical lattices of cold atoms II

- Hamiltonian for a Bose-Hubbard model for atoms:

$$H = J \sum_k a_k a_{k+1}^{\dagger} + a_k^{\dagger} a_{k+1}$$
$$+ \sum_k U n_k (n_k - 1).$$

- Tunneling between sites and self-interaction.

- Mott insulator: $U \gg J$, there will be a single atom per site, if possible.

- Superfluid: $U \ll J$, atoms are not localized.

- Observed experimentally in 2002. (See the previous slide.)

Optical lattices of cold atoms III
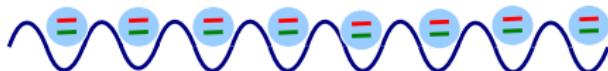
- Hamiltonian for a Bose-Hubbard model for two-state atoms:

$$H = J_a \sum_k a_k a_{k+1}^\dagger + a_k^\dagger a_{k+1}$$
$$+ J_b \sum_k b_k b_{k+1}^\dagger + b_k^\dagger b_{k+1}$$
$$+ \sum_k U_a n_{a,k}(n_{a,k} - 1)$$
$$+ U_b n_{b,k}(n_{b,k} - 1) + U_{ab} n_{a,k} n_{b,k}.$$
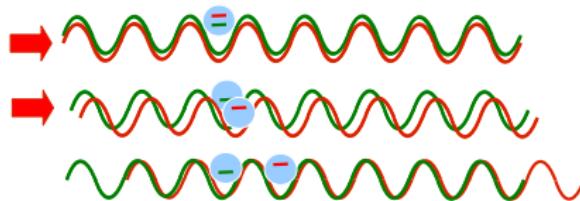
- Tunneling between sites for species *a* and *b*, self-interaction for species *a* and *b*, and interaction between the two species.

Optical lattices of cold atoms IV

- Two species, two potentials

- Atoms in the two basis states can be trapped by different potentials

- An atom can be delocalized by several lattices sites. MPQ, Munich, 2003.
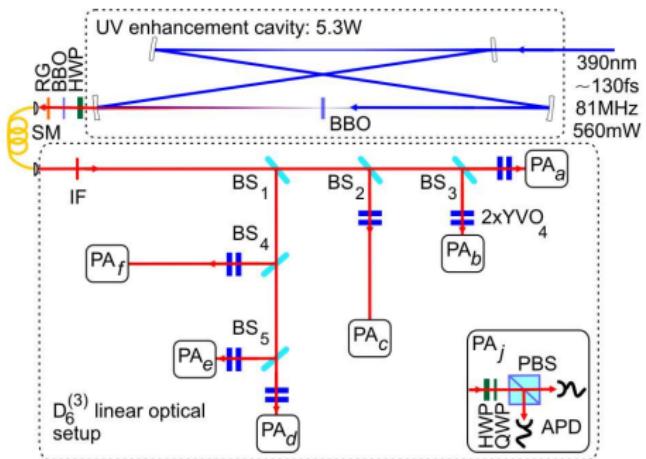
Optical lattices of cold atoms V

- They could realize an Ising spin chain Hamiltonian with this technique. MPQ, Munich, 2003.

Photons

- A photon can have a horizontal and a vertical polarization.

- H/V can take the role of 0 and 1.

- Problem: photons do not interact with each other.
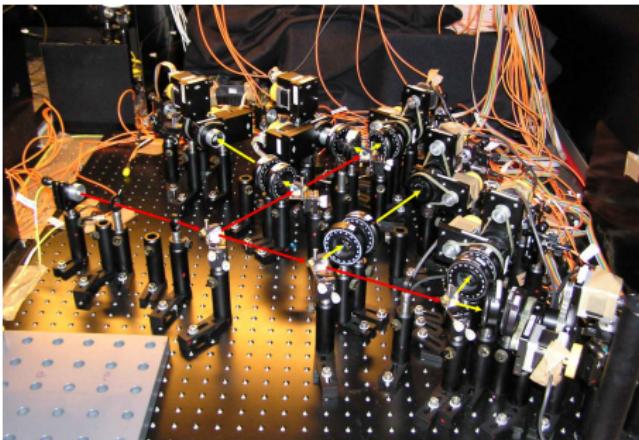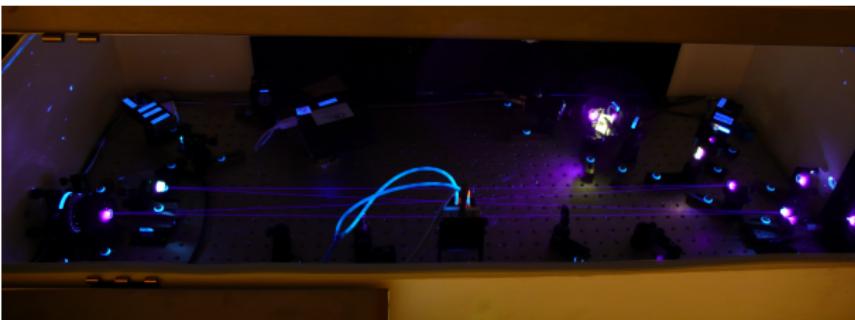
MPQ, Munich. Experiments with 6 photons.
[W. Wieczorek, R. Krischek, N. Kiesel, P. Michelberger, G. Tóth, and H. Weinfurter, Phys. Rev. Lett. 2009.]
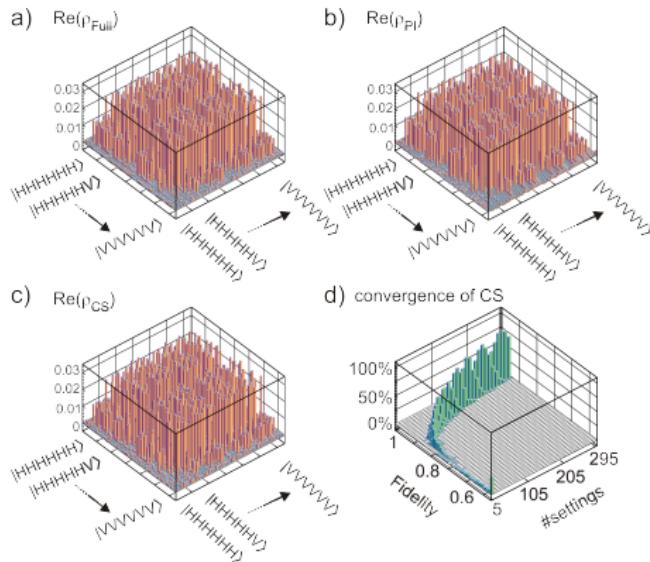
$$|D_6^{(3)}\rangle = \frac{1}{\sqrt{20}} \left(|111000\rangle + |110100\rangle + ... + |000111\rangle \right).$$

Photons IV

6-qubit Quantum state tomography

[C. Schwemmer, G. Tóth, A. Niggebaum, T. Moroder, D. Gross, O. Gühne, and H. Weinfurter, Efficient Tomographic Analysis of a Six Photon State, arxiv:1401.7526.]

Outline
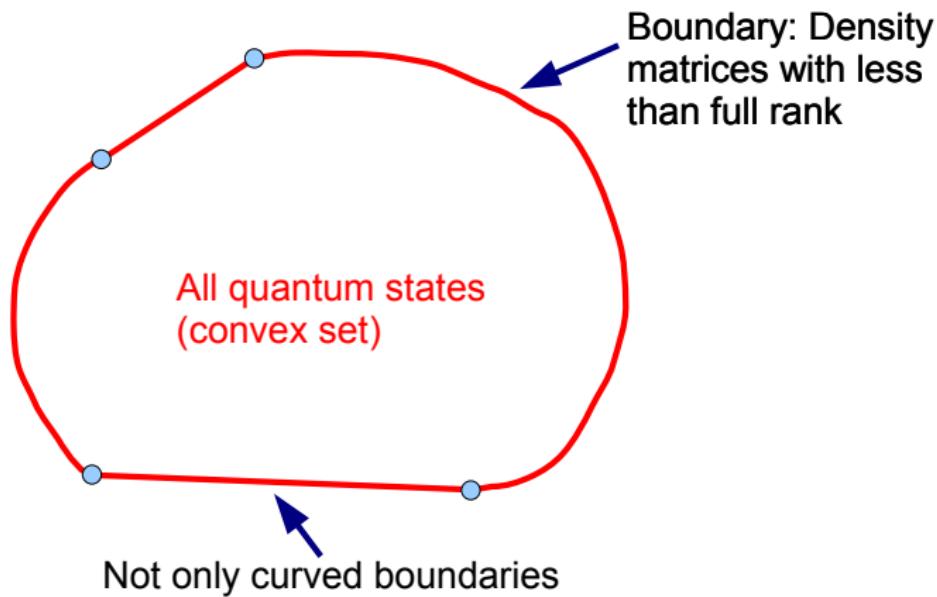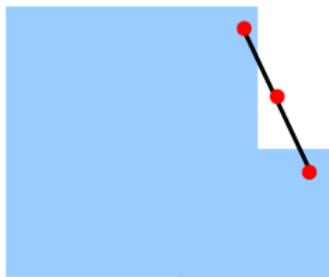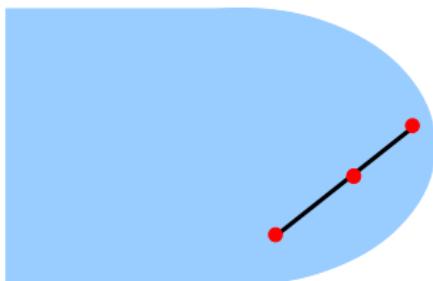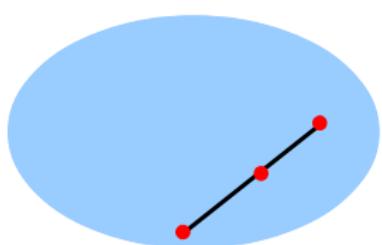
Geometry of quantum states

- Physical quantum states form a convex set

Boundary: Density matrices with less than full rank

All quantum states (convex set)

Not only curved boundaries
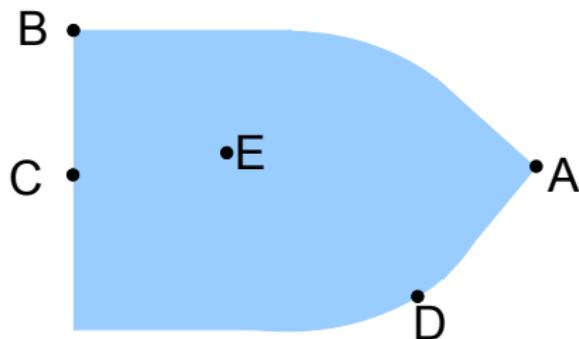
Geometry of quantum states II

- Convex and concave sets

- Boundary points: E - full rank, A,D,B - can be pure, C-not pure, but not full rank

Geometry of quantum states III

- For a single qubit, the density matrix has three real parameters

$$\varrho = \frac{1}{2}(\mathbb{1} + \sum_{l=x,y,z} v_l \sigma_l),$$

where σ_l are the Pauli spin matrices.

- We can write

$$\mathrm{Tr}(\varrho^2) = \frac{1}{2} + \frac{1}{2} \sum_{l=x,y,z} v_l^2.$$

That is, the Bloch vector has a maximal length for pure states.
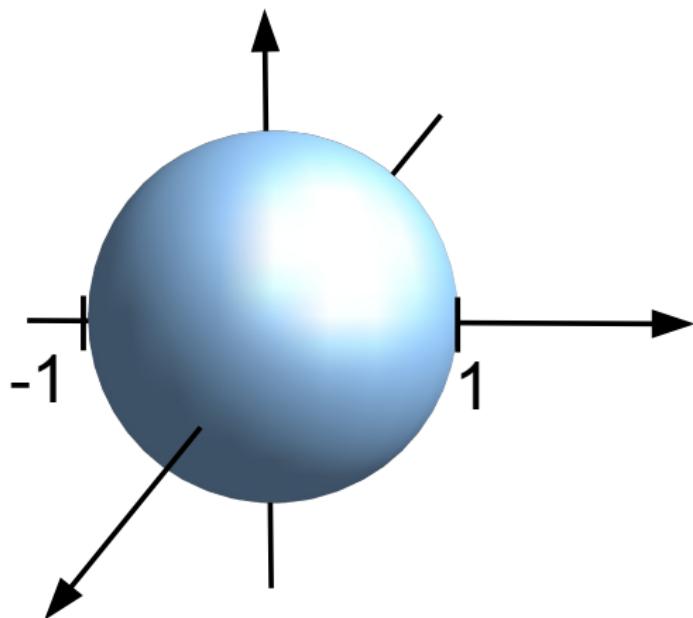
- The condition for being physical is $\mathrm{Tr}(\varrho^2) \le 1$, i.e.,

$$\sum_{l=x,y,z} |v_l|^2 \le 1.$$

The three-element vector is called the Bloch vector.

- Bloch ball:

Geometry of quantum states V

- For higher dimensional systems the picture is much more complicated. Let us consider qudits with dimension d.

- One can write a density matrix as a linear combination of $d^2 - 1$ SU(d) generators as

$$\varrho = \frac{1}{d}\mathbb{1} + \frac{1}{2}\sum_{l=1}^{d^2-1} v_l g_l.$$

Here,

$$\mathrm{Tr}(g_k g_l) = 2\delta_{kl}.$$

(Like for the Pauli matrices. Thus, we have something like the generalized Pauli matrices. $d = 3$: Gell-Mann matrices.) One can check that

$$\mathrm{Tr}(\varrho g_l) = v_l.$$

- With these, we can write

$$\mathrm{Tr}(\varrho^2) = \frac{1}{d} + \frac{1}{2} \sum_{l=1}^{d^2-1} v_l^2.$$

- For physical states the purity is not larger than one. Hence, the Bloch vector still has a length limit

$$\sum_{l=1}^{d^2-1} |v_l|^2 \le L_{\max}^2 = 2(d-1)/d.$$

However, not all values satisfying this length constraint correspond to some physical quantum state.

Theory of quantum entanglement

- Full tomography is not possible for large systems. What can we still say about the state? We can still say entangled/not entangled.
- Pure states
  - A pure product state is separable. All states that are not product states are entangled.
- Mixed states
  - A quantum state is called separable if it can be written as a convex sum of product states as [Werner, 1989]

$$\varrho = \sum_k p_k \varrho_1^{(k)} \otimes \varrho_2^{(k)},$$

where p_k form a probability distribution ($p_k > 0$, $\sum_k p_k = 1$), and $\varrho_n^{(k)}$ are single-qudit density matrices. A state that is not separable is called entangled.

Theory of quantum entanglement II
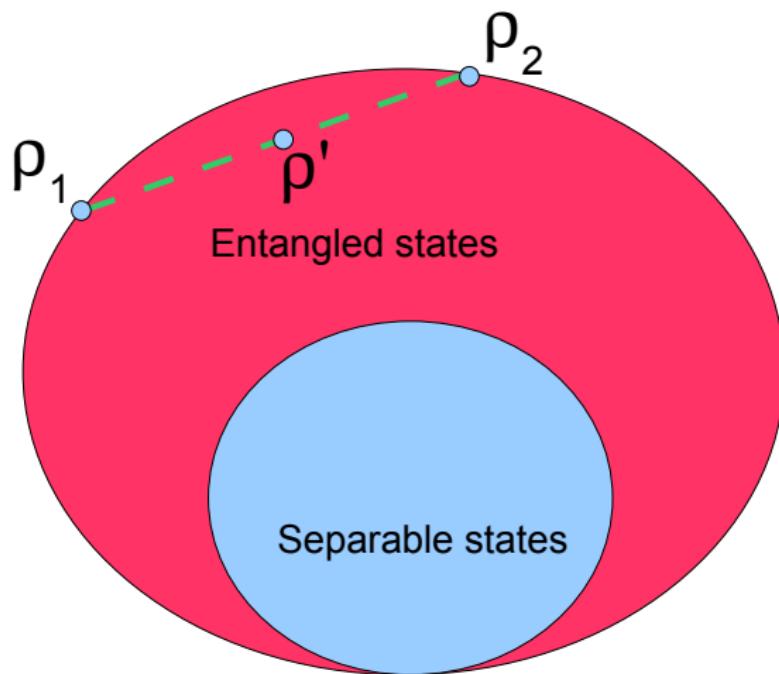
- Entangled states cannot be obtained from separable ones via local operations and classical communication (LOCC).

- Entangled states are more useful than separable ones
  - in certain quantum information processing tasks.
  - in certain metrological tasks.

- It is difficult to decide whether a quantum state is entangled or not.
- For example, Bell inequalities can be used to detect entangled states.

Theory of quantum entanglement IV

- Separable states form a convex set.

ρ_2

ρ_1

ρ'

Entangled states
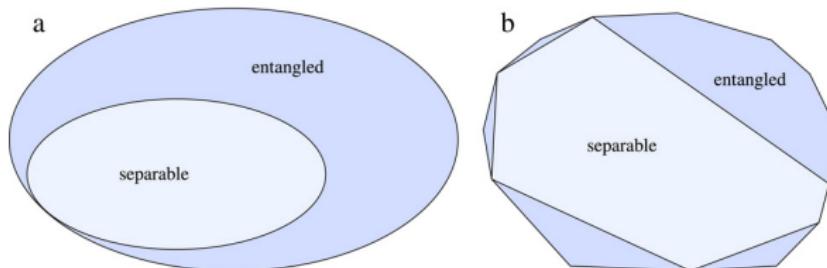
Separable states

Theory of quantum entanglement V

- A more accurate picture (Guhne, Toth, Phys. Rep. 2009):

Fig. 1. (a) Schematic picture of the set of all states as a convex set and the set of separable states as a convex subset. (b) Different schematic picture of the same sets. Here, it is stressed that the extremal points of the separable states (the pure product states), are also extremal points of the set of all states, hence they are located on the border of the total set.

The state is called *separable*, if there are convex weights p_i and product states $\varrho_i^A \otimes \varrho_i^B$ such that

$$\varrho = \sum_i p_i \varrho_i^A \otimes \varrho_i^B \qquad (6)$$

holds. Otherwise the state is called *entangled*.

Physically, this definition discriminates between three scenarios. First, a product state is an uncorrelated state, where Alice and Bob own each a separate state. For non-product states there are two different kinds of correlation. Separable states are classically correlated. This means that for the production of a separable state only local operations and classical communication (LOCC) are necessary. Alice and Bob can, by classical communication, share a random number generator that produces the outcomes i with probabilities p_i. For each of the outcomes, they can agree to produce the state $\varrho_i^A \otimes \varrho_i^B$ locally. By this procedure they produce the state $\varrho = \sum_i p_i \varrho_i^A \otimes \varrho_i^B$. This procedure is not specific for quantum theory, which justifies the notion of *classical* correlations. Otherwise, if a state is entangled, the correlations cannot originate from the classical procedure described above. In this sense entangled states are a typical feature of quantum mechanics.

Theory of quantum entanglement VI

- Concrete example (Verstraete, 2001):

$$\min_t (1-t)\rho^{PT} + \frac{t}{4}I_4 \geq 0 \qquad (8)$$

This problem is readily solved, and the solution is

$$t = \frac{|d_{min}|}{|d_{\min}| + \frac{1}{4}} \qquad (9)$$

where $d_{\min}$ is the minimal negative eigenvalue of ρ^{PT}. The minimal t is therefore only a function of the negative eigenvalues. A geometrical implication of this fact is that all surfaces of constant $d_{\min}$ are similar to the boundary of separable and entangled states: the set of all states with constant $d_{\min}$ can be generated by extrapolating all lines from the identity to the boundary of separable states such that the distance of the extrapolated state to the identity is a constant factor (> 1) of the distance of the separable state to the identity.

Let us now move to the case of two qubits. In this case ρ^{PT} has at most one negative eigenvalue [9]. Numerical investigations indicate that in a vast majority of the states the optimal rank of E^2 is equal to three, and if the rank is equal to two it implies that ρ_s has a negative eigenvalue. For the states for which E^2 is rank 3, it follows that their distance to the set of partially transposed states is given by

$$\|\rho - \rho_s\| = \frac{2}{\sqrt{3}}|d_{\min}| \qquad (10)$$

where $d_{\min}$ is the negative eigenvalue of ρ^{PT}. Surfaces of two-qubit states with constant negativity, defined as $N = 2|d_{\min}|$, have therefore two distinct properties: they are all similar to each other and the Hilbert-Schmidt distance between them is almost everywhere constant.
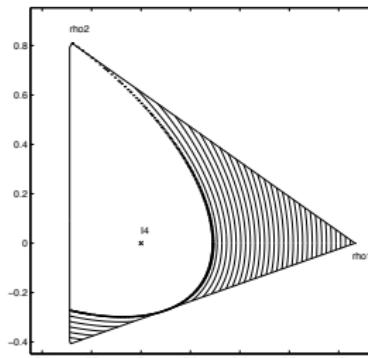
FIG. 2. Intersection of the convex set of all states including states (11) and the maximally mixed state. The contours represent surfaces of constant negativity, the starred line is the boundary between separable and entangled states.
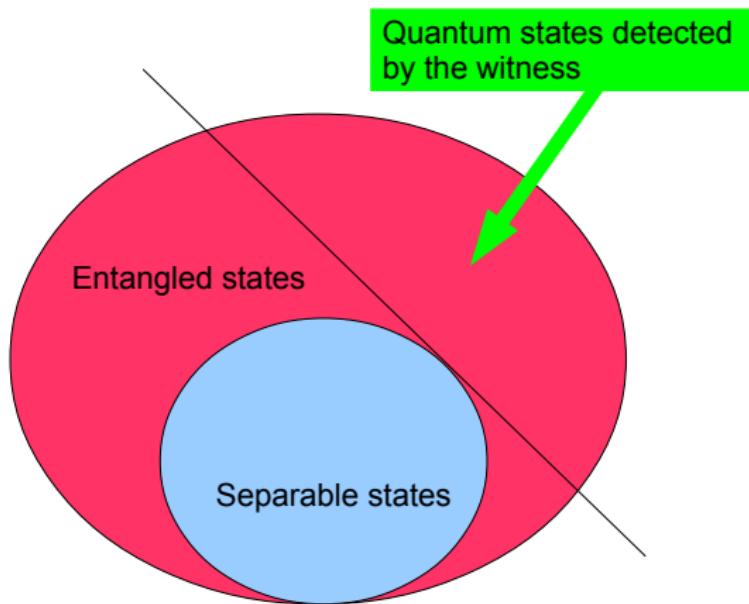
The plane is plotted in figure (2) and the boundary of all (rank-deficient) states is given by the solid enveloppe. The starred line is the boundary between the convex set of separable states and the convex set of all states. The surfaces of constant negativity are indeed all similar to this boundary. The fact that the distance between these surfaces is not constant throughout the picture indicates that the closest separable states lie in other planes. Note that the Werner states lie along the line between the maximally mixed state and the maximally entangled state ρ_1.

How to decide whether a state is entangled?

- The separability problem is generally unsolved. Separability can be decided only for small systems, like 2 qubits.

- For larger systems, we have necessary conditions for separability. If these are violated then the state is entangled.

How to decide whether a state is entangled? II

The convexity of the set of separable states plays an important role:

How to decide whether a state is entangled? III

Example

For separable sates

$$\langle \sigma_x^{(1)} \otimes \sigma_x^{(2)} + \sigma_y^{(1)} \otimes \sigma_y^{(2)} + \sigma_z^{(1)} \otimes \sigma_z^{(2)} \rangle \geq -1.$$

Proof. For product states of the form $|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$, we have

$$\langle \sigma_x \otimes \sigma_x \rangle + \langle \sigma_y \otimes \sigma_y \rangle + \langle \sigma_z \otimes \sigma_z \rangle = \sum_{l=x,y,z} \langle \sigma_l \rangle_{\Psi_1} \langle \sigma_l \rangle_{\Psi_2} \geq -1.$$
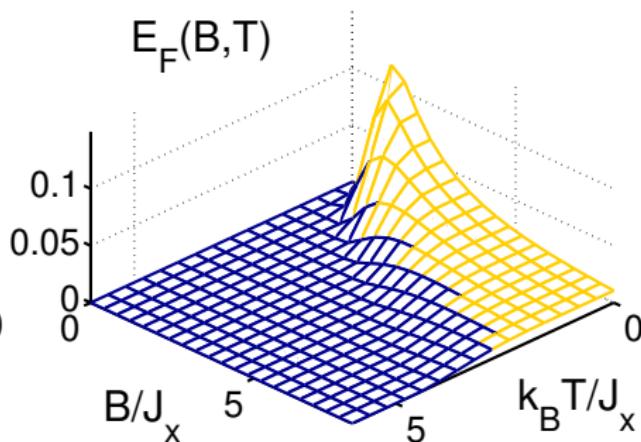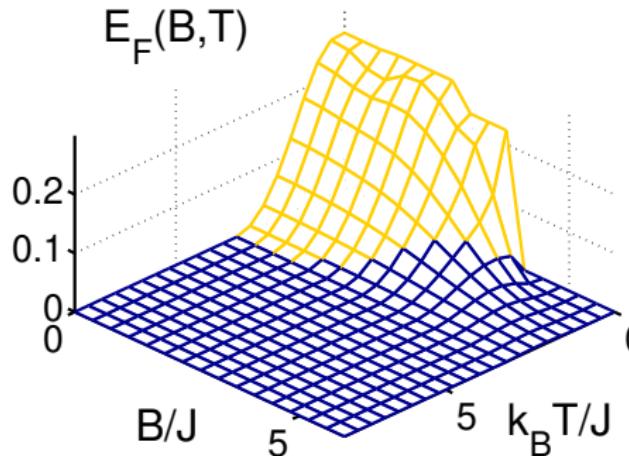
Here, we used the Cauchy-Schwarz inequality. Due to convexity, the inequality is also true for separable states.

The minimum for quantum states is -3. Such a minimum is obtained for the state

$$\frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle \right).$$

How to decide whether a state is entangled? IV

- This can be used in spin chains. If the energy is lower than the minimal energy of the classical model then the ground state is entangled.

Heisenberg chain in an external field / Ising spin chain in a transverse field.

[G. Tóth, Phys. Rev. A 71, 010301(R) (2005); Č. Brukner and V. Vedral, e-print quant-ph/0406040; M. R. Dowling, A. C. Doherty, and S. D. Bartlett, Phys. Rev. A 70, 062113 2004.]

- Any state that violates a Bell inequality is entangled.

- Positivity of the partial transpose

How to decide whether a state is entangled? VII

Detecting Multiparticle Entanglement of Dicke States

Bernd Lücke,[1] Jan Peise,[1] Giuseppe Vitagliano,[2] Jan Arlt,[3] Luis Santos,[4] Géza Tóth[2,5,6] and Carsten Klempt[1]

[1]Institut für Quantenoptik, Leibniz Universität Hannover, Welfengarten 1, D-30167 Hannover, Germany
[2]Department of Theoretical Physics, University of the Basque Country UPV/EHU, P.O. Box 644, E-48080 Bilbao, Spain
[3]QUANTOP, Institut for Fysik og Astronomi, Aarhus Universitet, 8000 Århus C, Denmark
[4]Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstraße 2, D-30167 Hannover, Germany
[5]IKERBASQUE, Basque Foundation for Science, E-48011 Bilbao, Spain
[6]Wigner Research Centre for Physics, Hungarian Academy of Sciences, P.O. Box 49, H-1525 Budapest, Hungary
(Received 27 February 2014; published 17 April 2014)

Recent experiments demonstrate the production of many thousands of neutral atoms entangled in their spin degrees of freedom. We present a criterion for estimating the amount of entanglement based on a measurement of the global spin. It outperforms previous criteria and applies to a wider class of entangled states, including Dicke states. Experimentally, we produce a Dicke-like state using spin dynamics in a Bose-Einstein condensate. Our criterion proves that it contains at least genuine 28-particle entanglement. We infer a generalized squeezing parameter of $-11.4(5)$ dB.

Entanglement, one of the most intriguing features of quantum mechanics, is nowadays a key ingredient for many applications in quantum information science [1,2], quantum simulation [3,4], and quantum-enhanced metrology [5]. Entangled states with a large number of particles cannot be characterized via full state tomography [6], which is routinely used in the case of photons [7,8], trapped ions [9], or superconducting circuits [10,11]. A reconstruction of the full density matrix is hindered and finally prevented by the exponential increase of the required number of measurements. Furthermore, it is technically impossible to address all individual particles or even fundamentally forbidden if the particles occupy the same quantum state. Therefore, the entanglement of many-particle states is best characterized by measuring the expectation values and variances of the components of the collective spin $\mathbf{J} = (J_x, J_y, J_z)^T = \sum_i \mathbf{s}_i$, the sum of all individual spins $\mathbf{s}_i$ in the ensemble.

In particular, the spin-squeezing parameter $\xi^2 = N(\Delta J_z)^2/(\langle J_x \rangle^2 + \langle J_y \rangle^2)$ defines the class of spin-squeezed states for $\xi^2 < 1$. This inequality can be used to verify the presence of entanglement, since all spin-squeezed states are entangled [12]. Large clouds of entangled neutral atoms are typically prepared in such spin-squeezed states, as shown in thermal gas cells [13],

quantified by means of the so-called entanglement depth, defined as the number of particles in the largest nonseparable subset [see Fig. 1(a)]. There have been numerous experiments detecting multiparticle entanglement involving up to 14 qubits in systems, where the particles can be addressed individually [9,20–24]. Large ensembles of neutral atoms
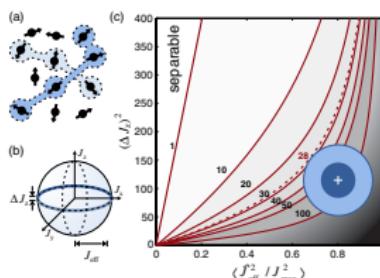
FIG. 1 (color online). Measurement of the entanglement depth for a total number of 8000 atoms. (a) The entanglement depth is given by the number of atoms in the largest nonseparable subset

- We define
$$F_j(X) := \frac{1}{j} \min_{\frac{\langle j_x \rangle}{j} = X} (\Delta j_z)^2.$$

- States for states with at most k-particle entanglement, we have
$$(\Delta J_z)^2 \geqslant \frac{N}{2} F_{\frac{k}{2}} \left(\frac{\sqrt{\langle J_x^2 + J_y^2 \rangle - \frac{N}{2}(\frac{k}{2} + 1)}}{\frac{N}{2}} \right)$$

- Any state that violates this has at least $(k+1)$-particle entanglement.

Outline

True randomness

- Pseudo-random numbers have unexpected correlations. Example from Karl Entacher:

- Solution: measure in the $|0\rangle/|1\rangle$ basis the state

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

- Commercially available random number generators based on this idea.
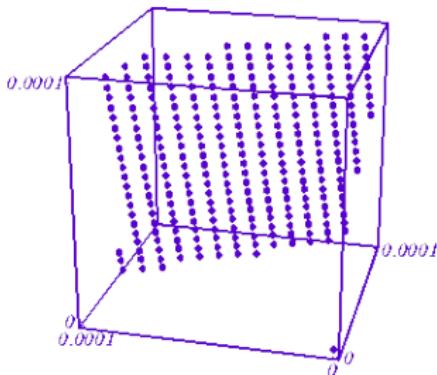
No-cloning theorem

We are looking for a mechanism that clones quantum states

$$U|\Psi\rangle \otimes |0\rangle = |\Psi\rangle \otimes |\Psi\rangle,$$

where U is a unitary dynamics.

Let us see why this is not possible. For the two basis states we have

$$U|0\rangle \otimes |0\rangle = |0\rangle \otimes |0\rangle,$$

$$U|1\rangle \otimes |0\rangle = |1\rangle \otimes |1\rangle.$$

Then, due to the linearity of quantum mechanics

$$U(\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle).$$

However, we would have needed

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Thus, a quantum state cannot be cloned.

Measurement problem

- We have the spin, the measurement device and the environment. The measurement dynamics should be

$$|s = +\frac{1}{2}\rangle \otimes |D_{+1/2}\rangle \otimes |E'\rangle = U|s = +\frac{1}{2}\rangle \otimes |D_0\rangle \otimes |E_0\rangle,$$

and

$$|s = -\frac{1}{2}\rangle \otimes |D_{-1/2}\rangle \otimes |E''\rangle = U|s = -\frac{1}{2}\rangle \otimes |D_0\rangle \otimes |E_0\rangle.$$

Measurement problem II

- If the spin is in a superposition of $s = +1/2$ and $s = -1/2$, then we get

$$\frac{1}{\sqrt{2}}\left(|s = +\frac{1}{2}\rangle \otimes |D_{+1/2}\rangle \otimes |E'\rangle + |s = -\frac{1}{2}\rangle \otimes |D_{-1/2}\rangle \otimes |E''\rangle\right)$$

$$= U\frac{1}{\sqrt{2}}\left(|s = +\frac{1}{2}\rangle + |s = +-\frac{1}{2}\rangle\right) \otimes |D_0\rangle \otimes |E_0\rangle.$$

- We get a superposition of two states, rather than one or the other.

- This is a fundamental problem in quantum mechanics. A possible solution is the many-world interpretation.

Measurement problem III

- A possible solution is the many-world interpretation.

- The idea of MWI originated in Everett's Princeton in 1957; Ph.D. thesis "The Theory of the Universal Wavefunction", developed under his thesis advisor John Archibald Wheeler.

(figure from Wikipedia)

Measurement problem IV

$$\frac{1}{\sqrt{2}}\Big(|s=+\tfrac{1}{2}\rangle \otimes |D_{+1/2}\rangle \otimes |E'\rangle \otimes |MIND_{+1/2}\rangle$$

$$+ |s=-\tfrac{1}{2}\rangle \otimes |D_{-1/2}\rangle \otimes |E''\rangle \otimes |MIND_{-1/2}\rangle\Big)$$

$$= U\frac{1}{\sqrt{2}}\left(|s=+\tfrac{1}{2}\rangle + |s=+-\tfrac{1}{2}\rangle\right) \otimes |D_0\rangle \otimes |E_0\rangle \otimes |MIND_0\rangle.$$

Coding in the 0/1 or on the (0+1)/(0-1) basis II

- Let us assume we used the 0/1 to code the bit

$$|q\rangle = (1 - b)|0\rangle + b|1\rangle.$$

- Then, a *single* measurement of

$$M = 0 \cdot |0\rangle\langle 0| + 1 \cdot |1\rangle\langle 1|$$

will give the bit exactly.
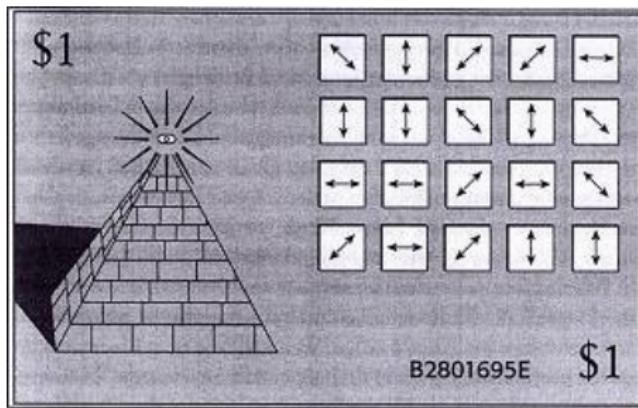
- If the bit was encoded in the 0/1 basis, then we get with 50% probability 0, 50% probability 1, independently from b.

- Note: if the quantum state could be copied, we could just copy the state many times. From many copies, we could guess, which basis was used.

- Thus, it is very important that the quantum states cannot be copied.

Quantum money
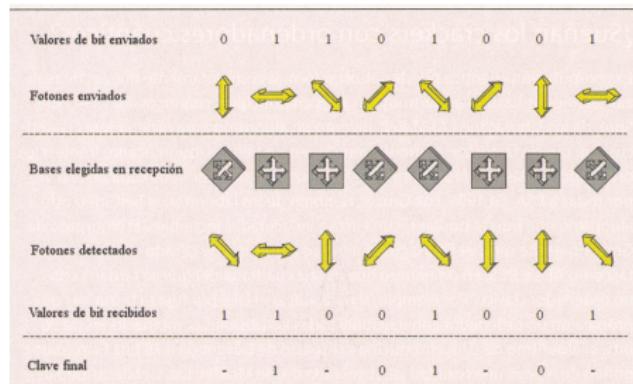
- S. Wiesner 1970, a graduate student at Columbia University, published in 1983.

- Every banknote has a code, a series of bits.
- The bits are encoded either in the 0/1 basis or in the 0+1/0-1 basis.
- The bank has the list of bases.
- The banknote cannot be copied.
- Its validity can be verified by the bank.

Quantum cryptography (BB84)

- Alice sends the secret message in qubits, randomly choosing the bases: 0/1 or (0+1)/(0-1).

- Bob receives the qubits and measures them in randomly chosen bases.

- Alice and Bob decides, using a public classical channel, for which qubits they used the same bases.

(figure from Wikipedia)

Quantum cryptography (BB84) II

- In 2004, the world's first bank transfer using QKD was carried in Vienna, Austria. (Zeilinger group, Vienna)

- Quantum encryption technology provided by the Swiss company Id Quantique was used in the Swiss canton (state) of Geneva to transmit ballot results to the capital in the national election occurring on 21 October 2007. (Gisin group, Geneva)

- In 2013, Battelle Memorial Institute installed a QKD system built by ID Quantique between their main campus in Columbus, Ohio and their manufacturing facility in nearby Dublin.

(Wikipedia)

Quantum teleportation

- A quantum state cannot be copied.

- But, it can be transferred from one particle to another one such that the state of the original particle is destroyed.

Quantum teleportation II

- Initial state:

$$|\Psi\rangle_{AB} \otimes |\Psi\rangle_C = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \otimes (\alpha|0\rangle_C + \beta|1\rangle_C).$$

Alice and Bob want to teleport. Alice has two particles: A and C. She wants to teleport the C particle to the B particle of Bob. Particle A is helping the teleportation.

- Alice makes a measurement on particles A and C in the Bell basis. The Bell basis consists of the states:

$$|\Phi^{\pm}\rangle_{AC} = \frac{1}{\sqrt{2}}(|00\rangle_{AC} \pm |11\rangle_{AC})$$

and

$$|\Psi^{\pm}\rangle_{AC} = \frac{1}{\sqrt{2}}(|01\rangle_{AC} \pm |10\rangle_{AC}).$$

Quantum teleportation III

- To see how this works, one can rewrite

$$|\Psi\rangle_{AB} \otimes |\Psi\rangle_C$$
$$= \tfrac{1}{2}[|\Phi^+\rangle_{AC} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) + |\Phi^-\rangle_{AC} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B)$$
$$+ |\Psi^+\rangle_{AC} \otimes (\beta|0\rangle_B + \alpha|1\rangle_B) + |\Psi^-\rangle_{AC} \otimes (\beta|0\rangle_B - \alpha|1\rangle_B)].$$

- Hence, measurement of AC in the Bell basis results in one of the four possibilities above for particle B. Knowing the result of the measurement, we can obtain

$$(\alpha|0\rangle_B + \beta|1\rangle_B).$$

  Thus, we successfully teleported the state of particle C to particle B.

- Note that this does not make possible faster than light communication, since the result of the Bell measurement has to be sent classically.

Quantum teleportation IV

- Experiment: Experimental quantum teleportation Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter & Anton Zeilinger, Nature 390, 575-579 (11 December 1997).

Quantum teleportation V

- 143 km, employing an optical free-space link between the two Canary Islands of La Palma and Tenerife, Zeilinger's group, 2012.

(figure from www.iqoqi-vienna.at)

Outline

Computing in "parallel"

- Quantum mechanics is linear

$$U|\Psi_1\rangle = |\Phi_1\rangle,$$

$$U|\Psi_2\rangle = |\Phi_2\rangle,$$

hence

$$U(|\Psi_1\rangle + |\Psi_2\rangle) = |\Phi_1\rangle + |\Phi_2\rangle.$$

- Not so simple, since we cannot separate the results.

Factoring of primes I

- RSA (Rivest, Shamir, Adleman) public key cryptography algorithm, 1977.

- Public key is known to everybody. Messages encrypted with the public key can be decoded only with the private key.

- p, q :primes.

- $N = pq$. If N is large, it is difficult to find the prime factors p and q.

Factoring of primes II

- Without all the details.

- Alice sends the public key (n, e) to Bob.

- Bob sends the message to Alice:

$$c \equiv m^e (\mod n),$$

  where e is an integer with specific properties, m is the data we want to send and c is the message we send.

- Alice is decoding the message

$$m \equiv c^d (\mod n),$$

  where d is again some integer with some specific properties, and it is known only to Alice. (d, n) are the private key.

- Important point: it can be shown that if we could find the prime factors p and q for N, we could break the code.

- Quantum computers can efficiently factor primes: Shor's algorithm.

- To factor an integer N, the execution time is
  - $O((logN)^3)$ for a quantum computer,
  - $O(e^{1.9(logN)^{1/3}(loglogN)^{2/3}})$ for the best classical algorithm.
- Thus, for large N the quantum algorithm must be faster.

Search in a database

- Quantum computers can search efficiently in a database: Grover's algorithm.

- Task: find x for which
  $$f(x) = 1,$$
  where x is an N-bit non-negative integer.
  (Assume that $f(x) = -1$ for all other cases.)

- To factor an integer N, the execution time is
  - $O(N^{\frac{1}{2}})$ for a quantum computer,
  - $\frac{N}{2}$ classically.

Thus, again, for large N the quantum algorithm must be faster.

Quantum simulation

- If quantum computing with thousands of qubits is not possible, we can still be interested in specific problems.

- Spin chains of 30-40 particles: already, we cannot simulate them on a classical computer.

Outline

Bell inequalities to detect nonlocality

- We assume that the measurement results can be explained by local hidden variable (LHV) models.

- The Bell inequality violation implies that for the given quantum states and for the given measuements, there is not such a model.

- All states vioalting a Bell inequality are entanged.

Outline

The type of system we consider here

- System of many particles.

- The particles cannot be accessed individually.

- There is no interaction between the particles.

Collective observables

- For spin-$\frac{1}{2}$ particles. The collective quantities are

$$J_l := \sum_{n=1}^{N} j_l^{(n)}$$

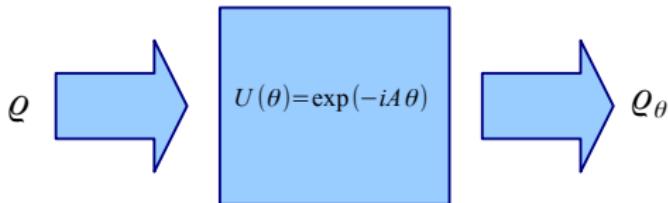for $l = x, y, z$, where $j_l^{(n)}$ are the components of the angular momentum of the nth particle.

- A typical Hamiltonian: describing the action of a magnetic field pointing in the $\vec{b}$-direction

$$H_B = \gamma B J_{\vec{b}},$$

where γ is the gyromagnetic ratio, B is the strength of the magnetic field, $\vec{b}$ is the direction of the field, and $J_{\vec{b}}$ is the angular momentum component parallel with the field.

- No interaction terms, thus starting from a product state we arrive also at a product state.

Basic task of Quantum Metrology

- The Hamiltonian we discussed, with the choice of $\hbar = 1$, generates the dynamics

$$U_\theta = e^{-iJ_{\vec{n}}\theta},$$

where we defined the angle θ that depends on the evolution time t
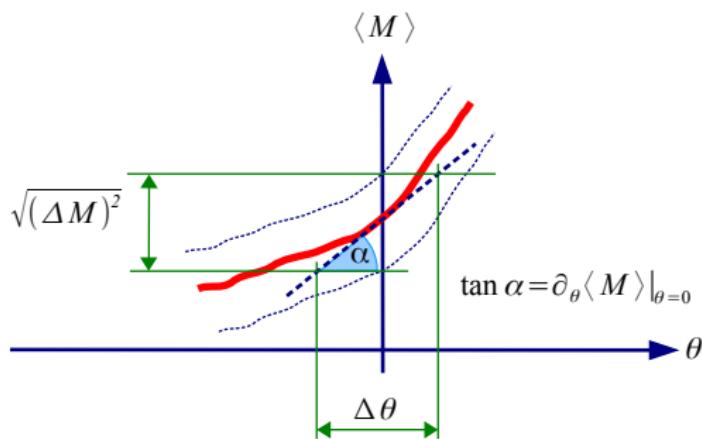
$$\theta = \gamma B t.$$

- A basic task in quantum metrology is to estimate the small parameter θ by measuring the expectation value of by M.
- If the evolution time t is a constant then estimating θ is equivalent to estimating the magnetic field B.
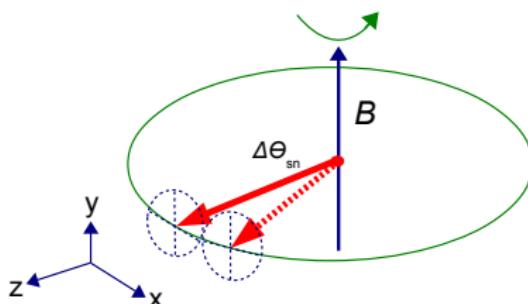
The error propagation formula

- We measure M and estimate the parameter θ.
- The variance of the parameter estimation is

$$(\Delta\theta)^2 = \frac{(\Delta M)^2}{|\partial_\theta\langle M\rangle|^2}.$$

- With fully polarized states, the parameter estimation has a finite variance.

Metrology with a fully polarized ensemble II

- Let us measure

$$M = J_x.$$

- With this,

$$\langle M \rangle = \frac{N}{2} \cos(\theta), \quad (\Delta M)^2 = \frac{N}{4} \sin^2(\theta).$$
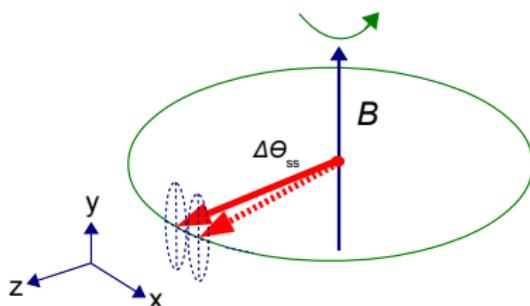
- The precision is

$$(\Delta \theta)^2|_{\theta=0} = \frac{(\Delta M)^2}{|\partial_\theta \langle M \rangle|^2} = \frac{1}{N}.$$

- Note that $(\Delta J_x)^2 = \frac{N}{4}$.

Metrology with spin squeezed states

- Spin squeezing can decrease $(\Delta J_x)^2$. We can reach $(\Delta J_x)^2 < \frac{N}{4}$.

- This also decreases the variance of the parameter estimation.

Metrology with GHZ states

- Let us take a GHZ state.

- Let us employ the dynamics

$$U = e^{-iJ_z\theta}.$$

- The dynamics of the state is

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|000..000\rangle + |111..111\rangle e^{-iN\theta}\right).$$

Metrology with GHZ states II

- Let us measure
$$M = \sigma_x^{\otimes N}.$$

- With this,
$$\langle M \rangle = \cos(N\theta), \quad (\Delta M)^2 = \sin^2(N\theta).$$

- The precision is
$$(\Delta\theta)^2|_{\theta=0} = \frac{(\Delta M)^2}{|\partial_\theta \langle M \rangle|^2} = \frac{1}{N^2}.$$

- Tested for 3 qubits.

[Nature 2001. (NIST, Boulder, Colorado).]

Quantum Metrology

- Let us take a GHZ state.
- Let us employ the dynamics

$$U = e^{-iJ_z\theta}.$$

- Basic task of metrology: we want to estimate θ based on measuring the state after the evolution.
- The dynamics is

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|000..000\rangle + |111..111\rangle e^{-iN\theta}\right).$$

Quantum Metrology II

- Let us measure

$$M = \sigma_x^{\otimes N}.$$

- With this,

$$\langle M \rangle = \cos(N\theta), \quad (\Delta M)^2 = \sin^2(N\theta).$$

- Precision is

$$(\Delta\theta)^{-2}|_{\theta=0} = \frac{(\Delta M)^2}{|\partial_\theta \langle M \rangle|^2} = N^2.$$

- Tested for 3 qubits: Nature 2001.(NIST, Boulder, Colorado).

- One can show that for separable states, for any measurements,

$$(\Delta\theta)^{-2}|_{\theta=0} \leq F_Q[\varrho, J_z] \leq N.$$

[Pezzé, Smerzi, Phys. Rev. Lett. 2007]

The quantum Cramér-Rao bound

- We would like to estimate the parameter θ for the evolution $U = e^{iA\theta}$.

- The variance of the unbiased estimator $\hat{\theta}$ is lower bounded as

$$\mathrm{var}(\hat{\theta}) \geq \frac{1}{F_Q[\varrho, A]},$$

where $F_Q[\varrho, A]$ is the quantum Fisher information for the quantum state ϱ and Hamiltonian A.

Quantum Fisher information

- The quantum Fisher information F_Q can be computed easily with a closed formula. Let us assume that a density matrix is given in its eigenbasis as

$$\varrho = \sum_k \lambda_k |k\rangle\langle k|.$$

- The quantum Fisher information is given as

$$F_Q[\varrho, A] = 2 \sum_{k,l} \frac{(\lambda_k - \lambda_l)^2}{\lambda_k + \lambda_l} |\langle k|A|l\rangle|^2.$$

[C. Helstrom, Quantum Detection and Estimation Theory (1976);
A. Holevo, Probabilistic and Statistical Aspects of Quantum Theory (1982);
S.L. Braunstein and C.M. Caves, Phys. Rev. Lett. 72 3439 (1994);
S.L. Braunstein, C.M. Caves, and G.J. Milburn, Ann. Phys., NY 247 135 (1996)]

- Family of the quantum Fisher informations

[D. Petz, J. Phys. A: Math. Gen 35, 929 (2002);
D. Petz, Quantum Information Theory and Quantum Statistics (Springer: Berlin, 2008).]

Conclusions

- We discussed several aspects of quantum information and quantum computation. For the transparencies, see

www.gtoth.eu

THANK YOU FOR YOUR ATTENTION!