Introduction to Quantum Information and Quantum Computation (Lecture of the Quantum Information class of the Master in Quantum Science and Technology)

Géza Tóth

Theoretical Physics, University of the Basque Country (UPV/EHU), Bilbao, Spain
Donostia International Physics Center (DIPC), San Sebastián, Spain
IKERBASQUE, Basque Foundation for Science, Bilbao, Spain
Wigner Research Centre for Physics, Budapest, Hungary

Room 0.8, Science Building, UPV/EHU, Leioa
16:00-17:00,
13 January 2020

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, 1959: 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 not interact with each other.

Question

- 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 $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

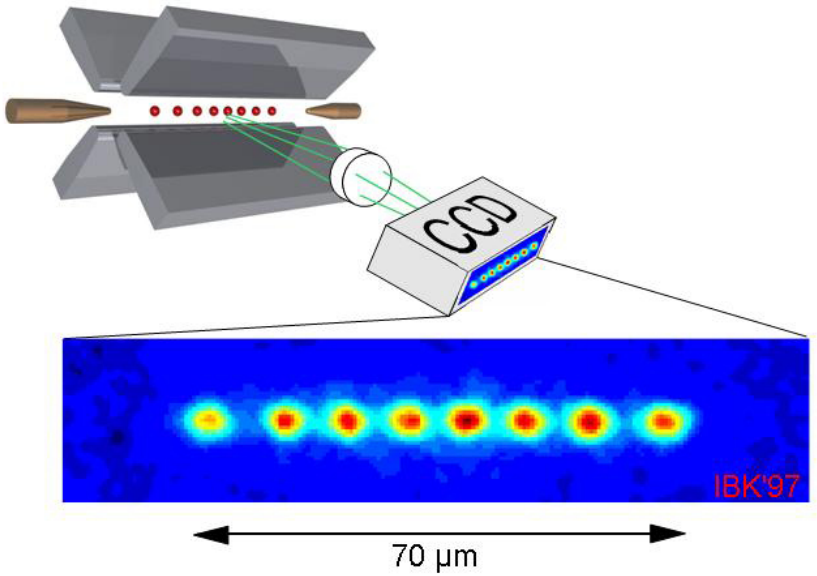
- Two qubits can be in a state

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

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

Trapped cold ions

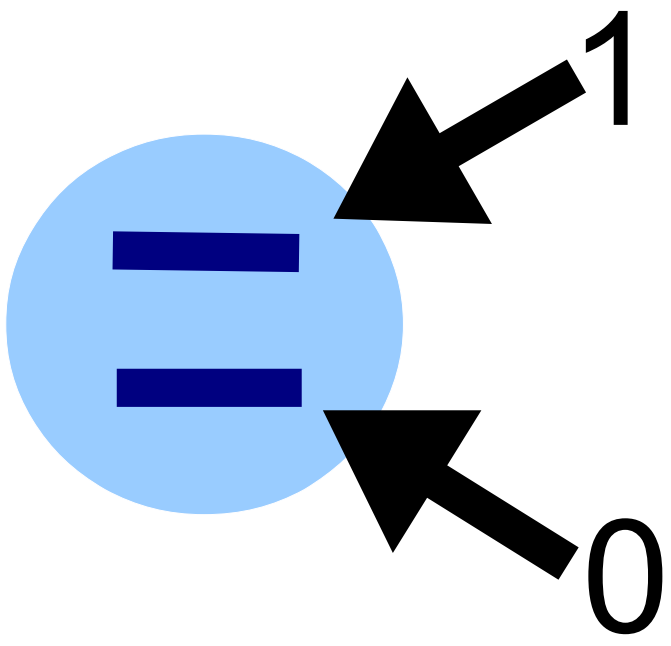
- Manipulating small number of particles, and accessing the particles individually.
- Examples: trapped cold ions



Innsbruck, Austria.

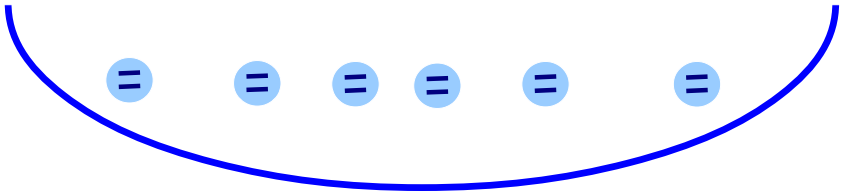
Trapped cold ions II: Qubits

- Ion as a qubit

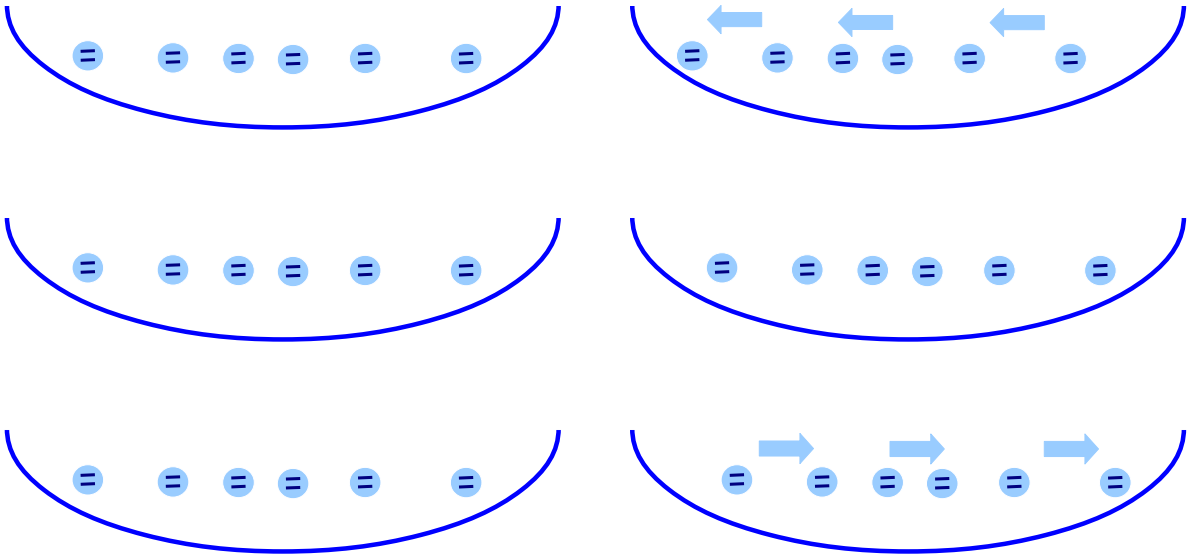


Trapped cold ions III

- Two-state ions trapped in an electromagnetic field



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

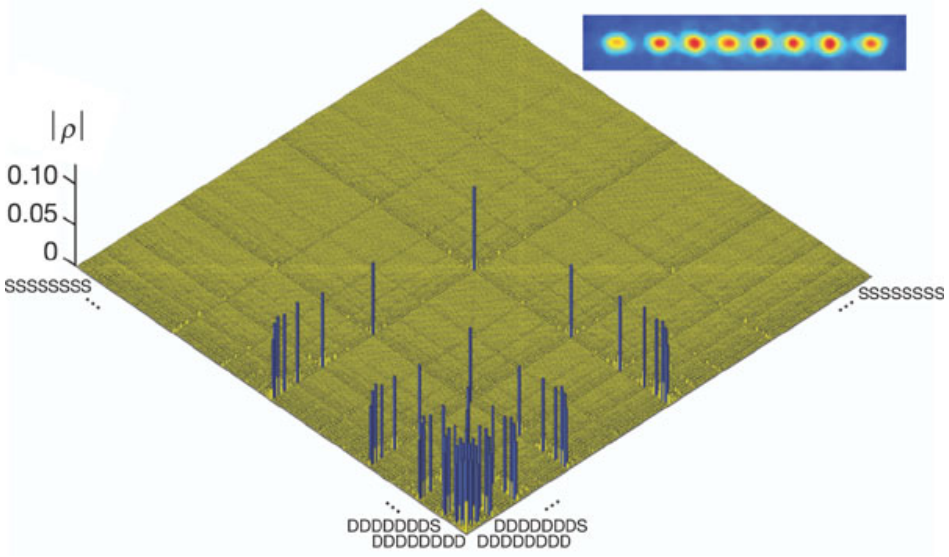


Oscillates

Does not oscillate

Trapped cold ions IV

- Quantum tomography of an eight ion quantum state giving the density matrix (Blatt group, Nature, 2005, Innsbruck, Austria):



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

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

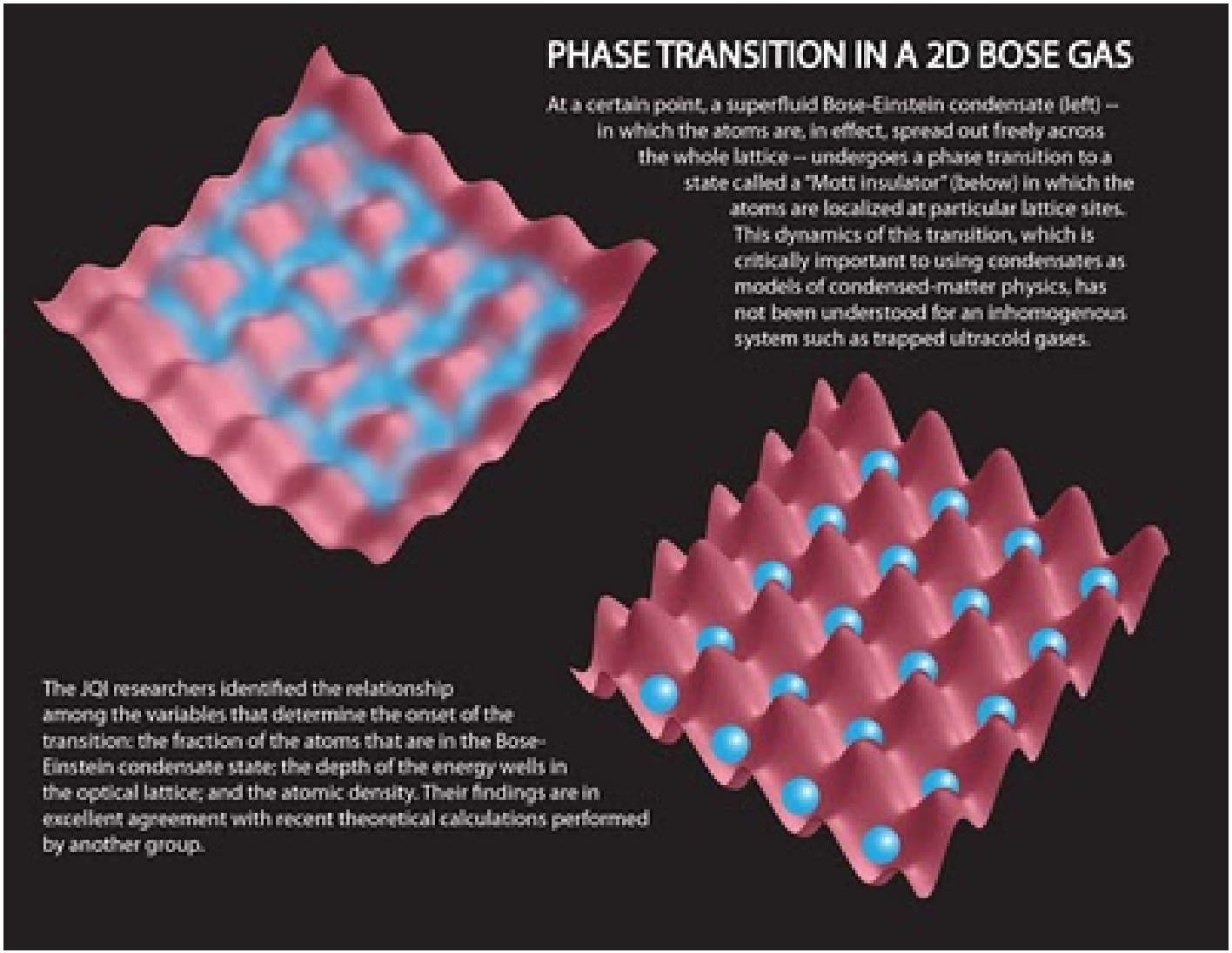
Trapped cold ions V

- Greenberger-Horn-Zeilinger (GHZ) state

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|00...00\rangle + |11..11\rangle\right)$$

- In another context, Schrödinger's cat state.
- Some experiments:
  - 3 particles, Nature 2001. (NIST, Boulder, Colorado)
  - 14 particles, Phys. Rev. Lett 2013. (Innsbruck, Austria)

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

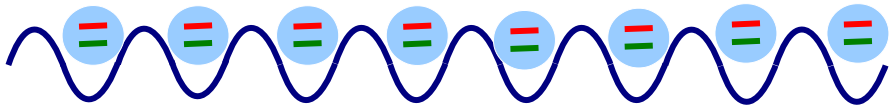
- Hamiltonian: Bose-Hubbard model for two-state atoms:

$$
\begin{aligned}
H = & J_a \sum_k a_k a_{k+1}^\dagger + a_k^\dagger a_{k+1} \\
& + J_b \sum_k b_k b_{k+1}^\dagger + b_k^\dagger b_{k+1} \\
& + \sum_k U_a n_{a,k}(n_{a,k} - 1) \\
& + U_b n_{b,k}(n_{b,k} - 1) + U_{ab} n_{a,k} n_{b,k}.
\end{aligned}
$$

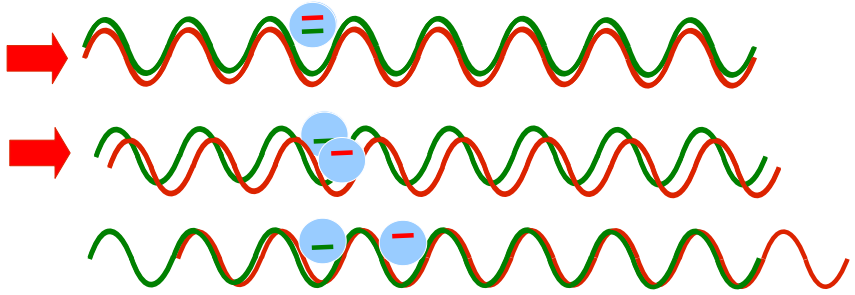
- Tunneling between sites for species a and b, self-interaction for species a and b, and interaction between the two species.

Optical lattices of cold atoms III

- 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.

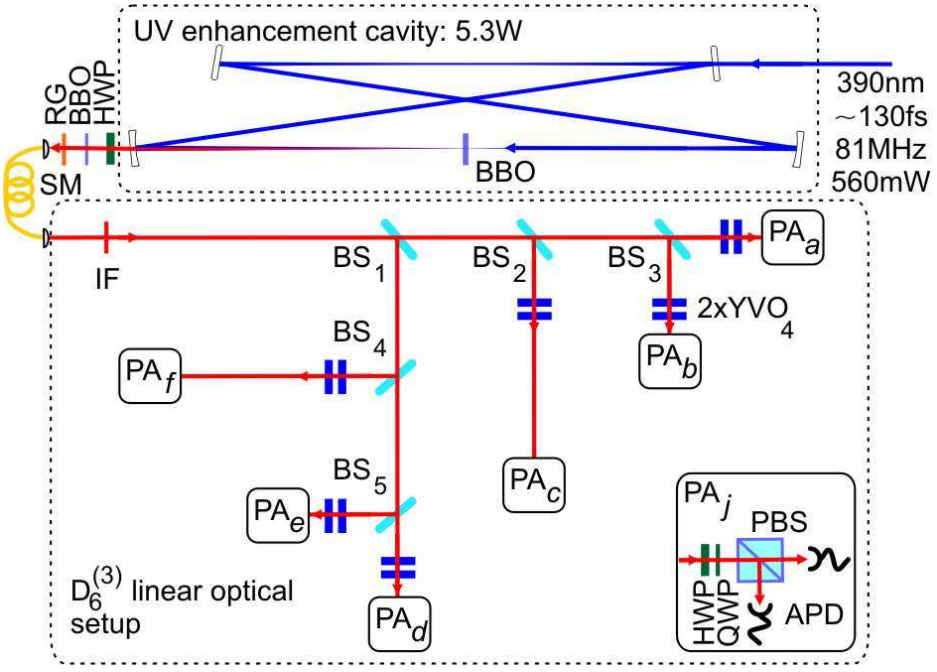
Optical lattices of cold atoms IV

- 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.

Photons II

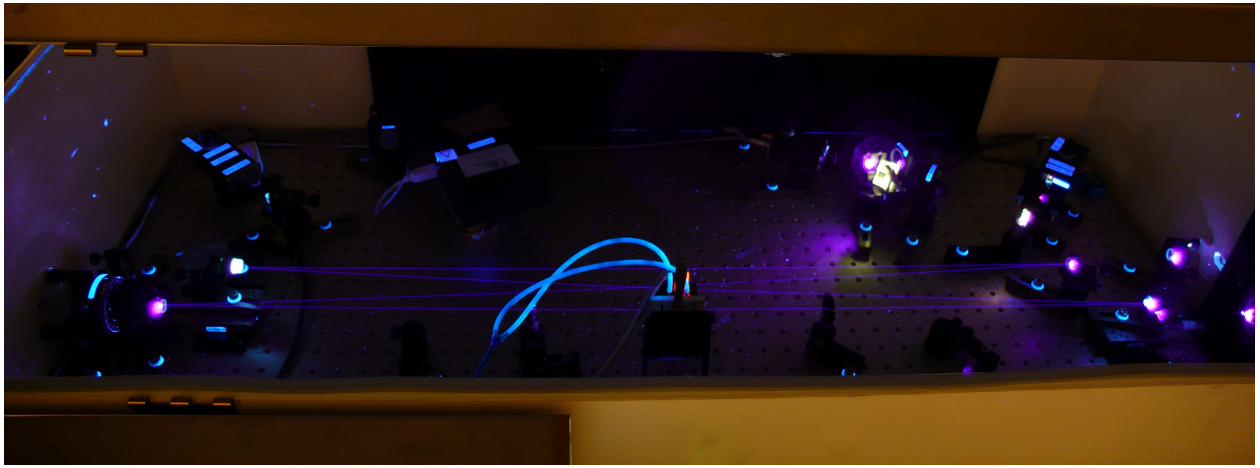


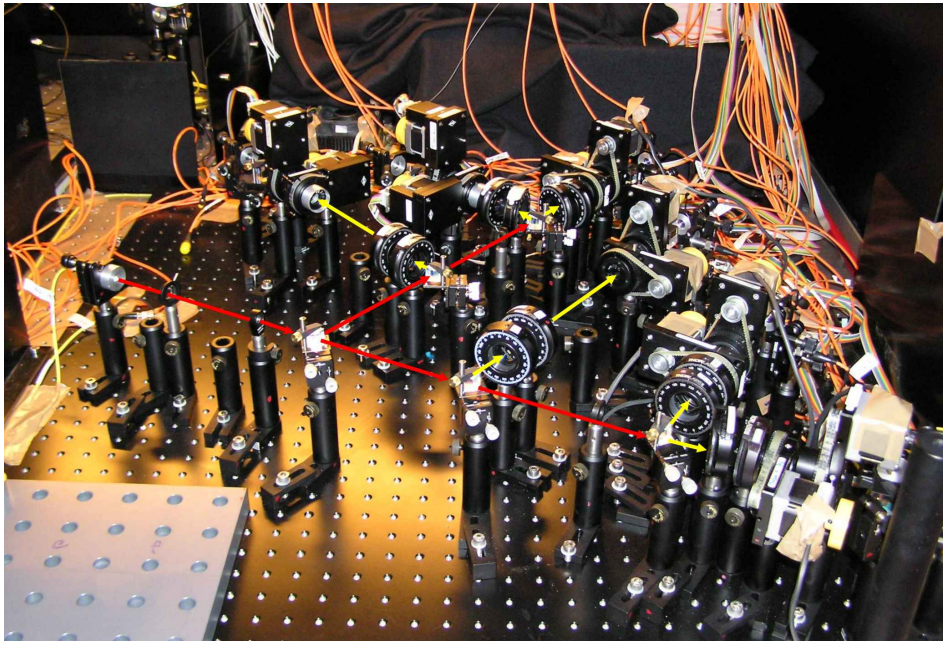
MPQ, Munich. Experiments with 6 photons.

[W. Wieczorek, R. Krischek, N. Kiesel, P. Michelberger, G. Tóth, and H. Weinfurter, Phys. Rev. Lett. 2009.]

$$|D_6^{(3)}\rangle = \frac{1}{\sqrt{20}}\left(|111000\rangle + |110100\rangle + \ldots + |000111\rangle\right).$$

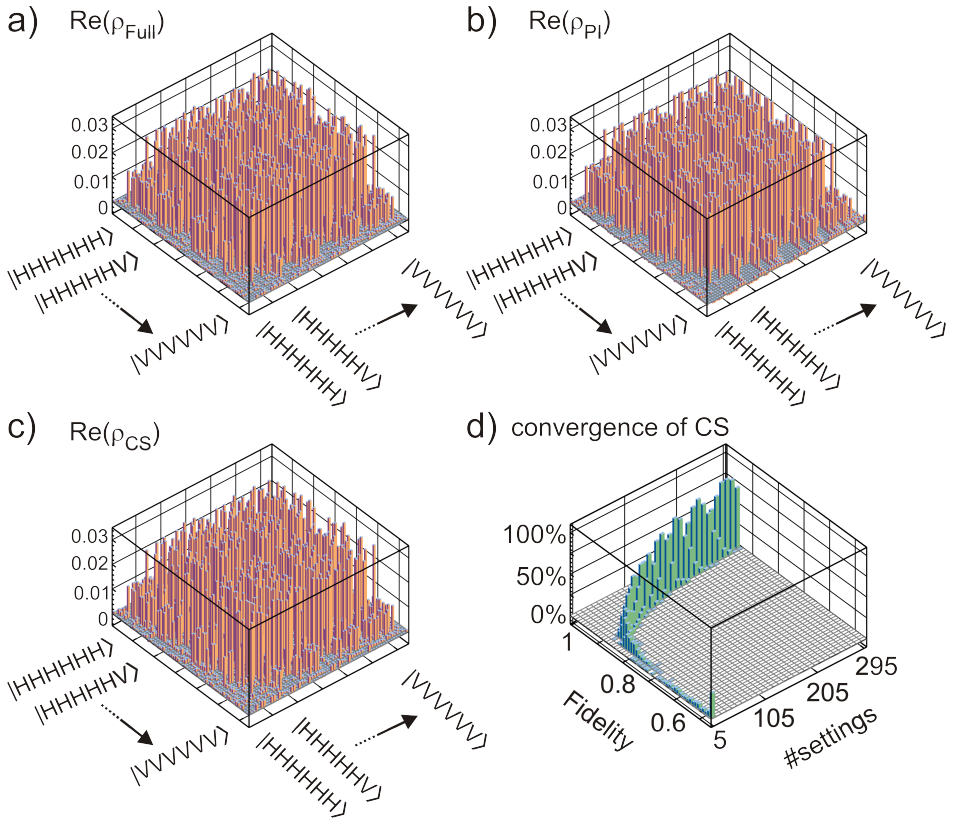
Photons III





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

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 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 III

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

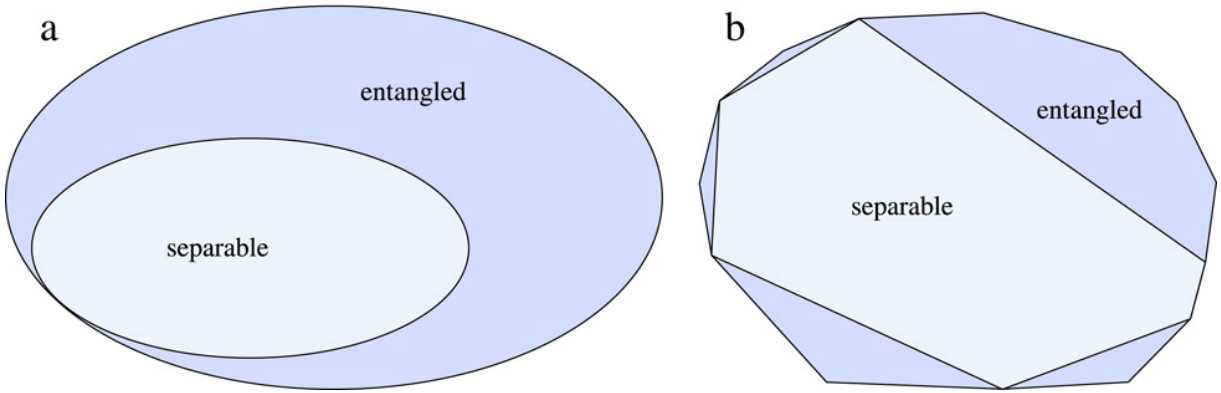


Fig. 1. (a) Schematic picture of the set of all states as a convex set and the set of separable states as a convex subset. (b) Different schematic picture of the same sets. Here, it is stressed that the extremal points of the separable states (the pure product states), are also extremal points of the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

$$\varrho = \sum_i p_i \varrho_i^A \otimes \varrho_i^B \tag{6}$$

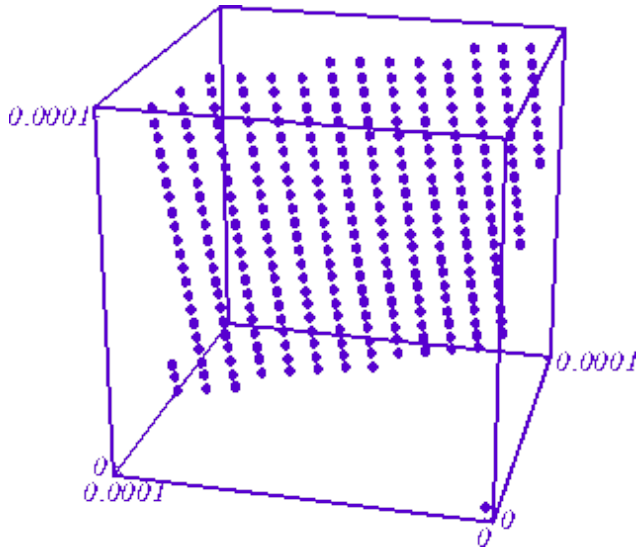
holds. Otherwise the state is called *entangled.*

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.

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

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

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.

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

- Let us code a classical bit $b \in 0, 1$ in a qubit. We can use the $0/1$ basis as before:
$$|q\rangle = (1 - b)|0\rangle + b|1\rangle.$$

- We can also use another basis, the $0 + 1/0 - 1$ basis:
$$|q'\rangle = (1 - b)\frac{|0\rangle + |1\rangle}{\sqrt{2}} + b\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

- If we do not know the basis, we cannot recover the bit b.

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 $0 + 1/0 - 1$ basis, then we get with 50% probability 0, 50% probability 1, independently from b.

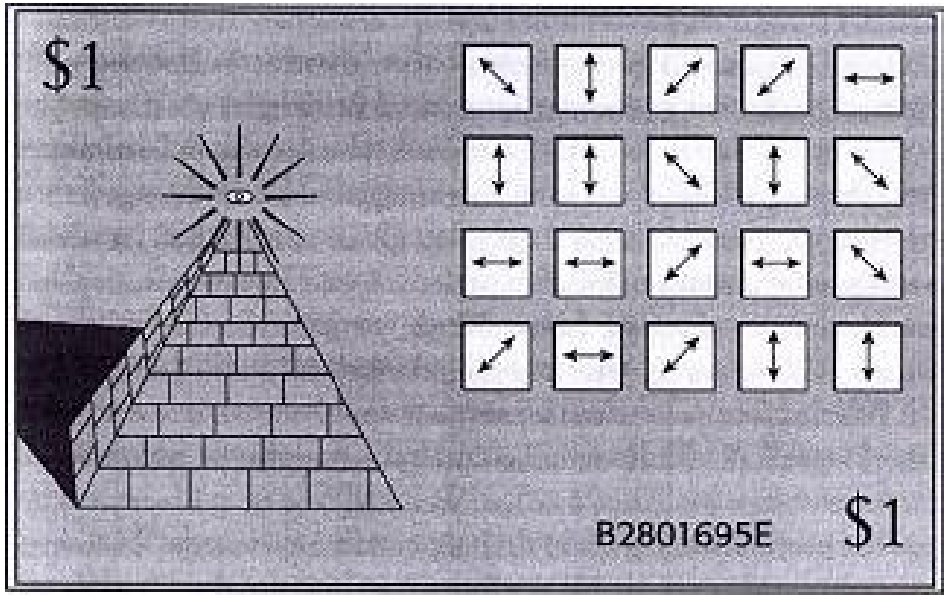
Coding in the 0/1 or on the (0+1)/(0-1) basis III

- 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.

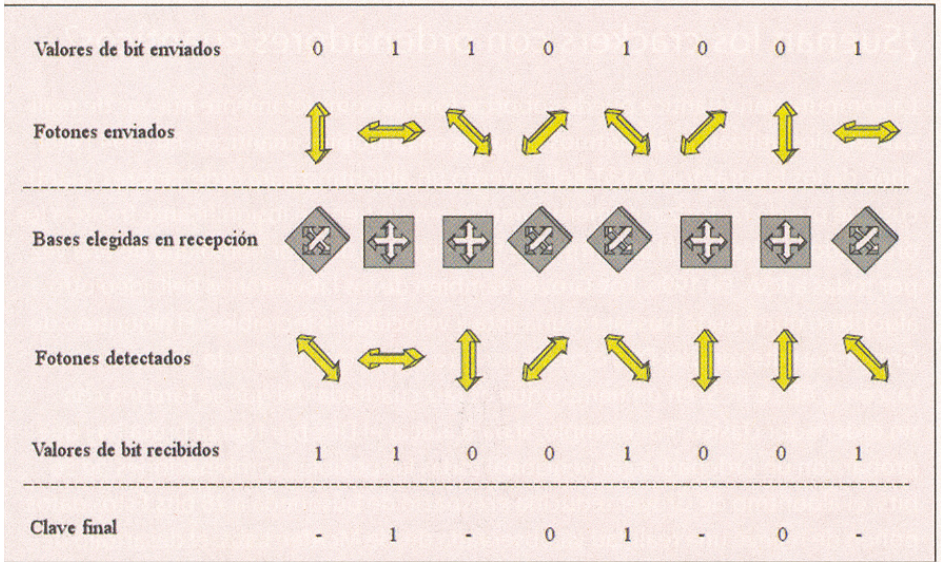
Quantum money

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



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.



Quantum cryptography (BB84) II

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

Outline

Quantum Metrology

- Let us take a GHZ state.

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000..000\rangle + |111..111\rangle\right).$$

- Let us employ the dynamics

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

- The dynamics is

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

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

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
$$(\Delta\theta)^2|_{\theta=0} = \frac{|\partial_\theta \langle M \rangle|^2}{(\Delta M)^2} = \frac{1}{N^2}.$$
- Tested for 3 qubits: Nature 2001. (NIST, Boulder, Colorado).
- One can show that for separable states, for any measurements,
$$(\Delta\theta)^2|_{\theta=0} \geq \frac{1}{N}.$$

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

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: Shor's algorithm

- Usual encryption: difficult to find prime factors for a number.
- Quantum computers can efficiently factor primes: Shor's algorithm, 1994.
- To factor an integer N, the execution time is
  - $O((logN)^3)$ for a quantum computer,
  - $O(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}})$ for the best classical algorithm.
- Thus, for large N the quantum algorithm must be faster.

Search in a database: Grover's algorithm

- Quantum computers can search efficiently in a database: Grover's algorithm, 1996.

- 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.

Conclusions

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

www.gtoth.eu

THANK YOU FOR YOUR ATTENTION!