EGAS 2009 Conference – public lecture, Wednesday, July 8

Quantum information – why it is fascinating

Abstract

Quantum information is a branch of modern science which is a highly nontrivial composition of quantum mechanics and information theory that originates from Shannon and Turing works. Historically the first discoveries that founded that field were the idea of quantum money that are impossibility to counterfeit (S. Wiesner, 1970) and quantum cryptography with polarized photons (C. H. Bennett and G. Brassard , 1984). Elementary analysis of the two phenomena suggests that they are possible because … quantum sheep, if existed, could never be cloned. In fact, this is true, the no-cloning rule of quantum state (realized by Wigner 1969, Dieks, Wooters and Zurek 1983) is one of fundamental rules that govern all information processing. Another phenomenon that lies in heart of the theory was realized first by Schrödinger and – independently - Einstein, Rosen and Podolsky. This is so called quantum entanglement. Schrödinger analysis (which he found highly unsatisfactory, though consistent) of that phenomenon can be easily translated into very surprising conclusion about how much disorder you may have in your office if you know the amount of disorder (entropy) in the whole building your office is located in (provided that the whole building is driven by quantum mechanical rules, of course). Recently (2005) it turned out that the latter issue, which bothered Schrödinger so much, provides even more striking implications in term of missing information. What it means if the information we miss is quantum and … negative? What role is played in this context by quantum teleportation and what the latter is? And finally – what quantum computer is expected to be? These questions will be answered in possible elementary way with some references to quantum-optical set-ups. In particular, Alice and Bob, the two intelligent ,,celebrities'' in quantum information field, will help us in understanding how quantum computing algorithm can help in fixing the date of two busy persons meeting quickly. Note that we have already quantum cryptography in the market and one can already buy (fully quantum) random generator compatible with PC computer. On the other hand still there are open problems, including some experimental challenges, that make quantum information field very dynamical and intellectually fascinating.