Novel Protocols for Quantum Networks

Résumé du projet de recherche (Langue 1)

The aim of this project is to push the advantages of quantum networks to the limits. Quantum information offers tremendous advantages over its conventional classical counterparts, in particular in security and speed of information processing. Huge effort has gone into the realization of these technologies in the last 20 years, to the point where simple quantum cryptographic devices are now even available commercially. The forefront of current experiments have up to 9 individual quantum systems controlled and manipulated towards this end. However, this current limit in the number of systems we can manipulate is far too small to be useful for quantum computation, yet bigger than necessary for the two-node schemes dominating current quantum cryptography. This background stimulates the need for the development of the theory of what is possible and useful over quantum networks in order to - Make full use of current technological advances - Push to limits the benefits of quantum technologies over networks There is a great need for new approaches to explore how to use quantum networks to their full potential and to develop new protocols. We have come to understand that it is entanglement that is the property of quantum systems that enables quantum networks to perform tasks better than classical networks. Most current quantum network schemes use two-party entanglement, which is well understood. As soon as we have more than three quantum systems, however, entanglement becomes very complicated. We know there are infinitely many different ‘types’ of entanglement – from the perspective of what can be done with a quantum resource in the quantum network setting. There are few schemes using multiparty entanglement, and almost all those use one particular type of entangled state – the graph state. New approaches are needed to explore how to use and exploit all the subtleties that entanglement has to offer for quantum networks. We take two new approaches to look for and develop novel protocols making use of different types of entanglement, that of looking at i) symmetries and ii) causal constraints. We will use symmetry to look for ways entanglement can be used for quantum information, in particular with respect to multiplayer games. Where certain types of entanglement fail in solving some informational or game problem, and others prevail, can often be understood as how the symmetry of problem (or game setting) is reflected by the symmetry of the entanglement of the system. For example, for the problem of leader election, the symmetry of the problem translates to the symmetry of the quantum state which provides a solution. States without this symmetry fail. In turn the symmetry of the quantum state is reflected in the type of entanglement it contains. In fact, this case is one of the only examples where exotic entangled states are used for advantage in quantum information, and they provide a distinct gap from all possible classical solutions (which cannot solve the problem perfectly at all). An additional value to looking from the symmetry point of view is that it will lead to more natural physical implementations also, as they play an important role on describing many physical properties. We will look how symmetries of information problems can be translated to / make use of naturally occurring symmetries (e.g. translational symmetry in condensates) and vice versa. We will also analyse and develop protocols from the viewpoint of causality. The inability to communicate faster than the speed of light implies a causal structure on all possible communication protocols. Recently it has been seen that interpreting correlations in terms of causal constraints is a powerful approach to see the difference between classical and quantum and analyse where quantum advantage may be had. In addition, this method is useful when we do not want to make any assumptions about the physical systems, except causality (the most basic condition implied by nature), allowing for device independent security and verification proofs.