

Scientific Presentation

SubProject 5: Theory

- Subproject leader: Serge Massar
- 20 partners involved (out of 38)
- Administrative Structure:
 - 1 administration workpackage
 - 6 scientific workpackages

Networking

- Informal visits between partners
- Workshops
 - QAP theory meeting
 - Bristol University, U.K. (April 2007)
 - Quantum Algorithms and Applications Workshop 2007 (QAA07)
 - Sydney, Australia (May 2007)
 - Conference on Quantum Information and Many-Body Quantum Systems
 - Scuola Normale Superiore, Pisa, Italy (March 2007)
- Conferences
 - Photons, Atoms and Qubits conference 2007 (PAQ07)
 - London, UK (September 2007)
 - International Conference on Quantum Information Processing and Communication QIPC07
 - Barcelona, Spain (October 2007)

Scientific production

- All Deliverables Achieved
- Publications during Year 2:
 - approximately theory 165 articles reported
 - 1 Nature Physics
 - 24 Phys. Rev. Lett.
 - 3 STOC (*Symposium on Theory of Computing*)
 - 2 FOCS (*Foundations of Computer Science*)
- *Note: Difficult to review all this work in 30 minutes!!*
 - *Focus on a few highlights*
 - *Show that deliverables achieved.*

WP5.1 Algorithms and Complexity

leader: O. Regev

- D 5.1.2 Find more quantum algorithms, improved simulation of quantum systems, new relationships among quantum complexity classes, or new classical results that use quantum arguments

New quantum algorithms

- quantum algorithm for the hidden subgroup problem for nil2 groups (Ivanyos, Sanselme and Santha).
 - Importance: Generalisation of Shor's algorithm. Solving the hidden subgroup problem over the symmetric group would imply an algorithm for graph isomorphism and over the dihedral group would imply an algorithm for lattice problems.

Highlight

- Improving the Quantum Adversary Method
(Hoyer, Lee, Spalek, STOC07)
 - The quantum adversary method is the most important tool to find lower bounds in quantum query complexity
 - Traditional ingredient: if $f(x) \neq f(x')$ then x and x' must map to orthogonal final states of the computer.
 - New ingredient: makes use of the fact that the algorithm actually computes f .

WP5.2 Algorithmic Methods

- D 5.2.2 Further analysis of existing algorithmic techniques for generating new quantum algorithms
- **Quantum Expanders**
(-Ben Aroya, Ta Shma,; -and with O. Schwartz; -D. Gross and J. Eisert; A. Harrow)
 - Quantum expanders arise as a natural quantum analogue of the classical “expander graph”
 - Graph with low degree and high connectivity
 - Intensely over the past three decades and very useful tool in classical algorithmics.
 - These constructions have lead to important improvements of classical expanders (will be reported in year 3)

Other important result

- Hamiltonian with
 - interactions between nearest neighbors
 - in a one-dimensional arrangement of systems
 - with Hilbert space dimension 9

can be used to perform universal adiabatic quantum computation.

Thus:

- One-dimensional systems with nearest neighbor interaction are as powerful as any other system for quantum computation
- (Preliminary result reported last year; now published in FOCS)

WP5.3 Protocols for Quantum Commerce

- D 5.3.2 Security analysis of Quantum Key Distribution (QKD) schemes whose security is independent of the devices in the practically important case when the eavesdropper is limited by quantum mechanics.
- **Use Non Local Correlations to establish a secret key** (Acin, Brunner, Gisin, et al Phys. Rev. Lett.)
 - Security based on “monogamy” of non local correlations
 - Security based on analysis of correlations only. No hypothesis required on dimension of Hilbert space, on state preparation, on quantum measurement.
 - Only technological hypothesis:
 - information remains private=there exist secure laboratories
 - So far results obtained for “collective” attacks.

Highlight

- **Asymmetric Bell-type scenario**: entanglement between
 - Ion (100% efficient detectors)
 - Photon (inefficient detectors)
- What non locality test is best adapted to this scenario?
- Using I3322 inequality and assuming a perfect efficiency for the massive particle, an efficiency of 43% for the photon detection is required.

WP5.4 Toolbox for quantum multi-user protocols

D 5.4.2 Simulation using classical resources of (possibly noisy) maximally entangled states in arbitrary dimension.

- What entangled quantum states can produce non local correlations?
 - Local model for noisy maximally entangled states (noise is $\log(d)$ times larger than amount of noise required for state to become separable)
 - Model Extended to completely arbitrary states and to arbitrary measurements (POVM's)
 - (Almeida, Pironio, Barrett, et al Phys. Rev. Lett.)

WP5.4 Highlight

- **Entanglement percolation**
 - distribution of entanglement through quantum networks
 - networks consist of a series of nodes connected by entangled states.
 - how to create entanglement between two distant nodes in the network.
 - Connected to percolation theory

(A. Acin, J. I. Cirac and M. Lewenstein, Nature Physics)

Quantum Communication

- A. Winter

- The maximum output p -norm of quantum channels is not multiplicative for any $p > 2$

Abstract of the paper: « Four pages only. If you write to me, please don't tell me how simple and obvious it is - I know that myself. I accept suggestions for journals to submit to, though; the obscurer the better :-) V2 has some corrections, and I removed one reference. Don't miss the more recent work [arXiv:0707.3291](https://arxiv.org/abs/0707.3291) »

- P. Hayden

- The maximal p -norm multiplicativity conjecture is false
 - these counterexamples demonstrate that if the additivity conjecture of quantum information theory is true, it cannot be proved as a consequence of maximal p -norm multiplicativity.

WP5.5 Architectures

D.5.5.2 Theoretical analysis of state preparation and execution of quantum information processing protocols in light-matter systems under realistic constraints

- Realistic Analysis of light coupling to solid state quantum memory based on controlled inhomogeneous broadening → **SP1**
(N. Sangouard, C. Simon, M. Afzelius et al Phys. Rev. A)
- How to perform robust quantum computation in QuBus model: matter qubits coupled by coherent state bus mode of light.
(P. van Loock, W. J. Munro, K. Nemoto, et al., archive07)
- Error Correction for quantum information encoded in multimode light undergoing linear losses. Experimentally feasible → **SP2**
(W. Wasilewski and K. Banaszek, Phys. Rev. A)

WP5.5 Highlight

Generating cluster states

If gate success probability $p > 1/2$ then one can efficiently generate cluster states

Detailed computations of overhead and time required for cluster state generation.

Opens the door to realistic cluster state generation.

(S. G. R. Louis, K. Nemoto, W. J. Munro, et al, Phys. Rev. A)

WP5.6 Testing Quantum Systems

D 5.6.2 Characterization of process tomography methods.

Given n uses of a quantum channel:

- what is the most general way of estimating the quantum channel?
- Provide a simple general mathematical formulation of the most general process tomography.
 - (In the same way that POVM's provide the mathematical description of the most general quantum measurements)
- (M. Ziman, submitted to PRA)

- State estimation:
 - distinguishing between two different density matrices in the limit of many copies
 - quantum Chernoff bound (K.M.R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, Ll. Masanes, A. Acín, F. Verstraete)
 - It induces a natural measure of distance between quantum states.

Conclusion

- All Deliverables Achieved
- Important High Quality Scientific Output
- Efficient Networking

Thanks to Workpackage Managers:

O Regev, M. Santha, H. Buhrman, A. Acin, K. Banaszek, M. Ziman.