PROJECT PERIODIC REPORT

Grant Agreement number: 600700

Project acronym: QALGO

Project title: Quantum Algorithmics

Funding Scheme: FET Proactive

Date of latest version of Annex I against which the assessment will be made: October 08, 2012

Periodic report: 1st ☒ 2nd □ 3rd □ 4th □

Period covered: from May 1, 2013 to April 30, 2014

Name, title and organisation of the scientific representative of the project's coordinator[1]:

Andris Ambainis, professor, University of Latvia

Tel: +371 67034517

Fax: +371 67034376

E-mail: ambainis@lu.lv

Project website[2] address: http://qalgo-project.eu/, http://www.lu.lv/qalgo.

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the Grant Agreement .

[2] The home page of the website should contain the generic European flag and the FP7 logo which are available in electronic format at the Europa website (logo of the European flag: http://europa.eu/abc/symbols/emblem/index_en.htm logo of the 7th FP: http://ec.europa.eu/research/fp7/index_en.cfm?pg=logos). The area of activity of the project should also be mentioned.

1 Project objectives for the period

The high level objective of the QALGO project is coming up with new quantum algorithms and quantum communication protocols. This is one of the most important research topics in the theory of quantum information. New quantum algorithms and communication protocols will provide new applications for quantum computers (*when they are built*) and quantum communication devices (*which already exist*).

Coming up with new quantum algorithms is also among the most difficult problems in quantum information. The number of known methods for designing new quantum algorithms is relatively small, and coming up with new ideas requires broad and deep knowledge of both computer science and physics.

The QALGO project aims to address these important scientific challenges. More specifically, the objectives of QALGO are:

- To design new quantum algorithms, by exploring novel approaches and new application areas;
- To achieve better understanding of fundamental questions about the role of various resources in quantum algorithms and the role of structure in quantum speedups;
- To design new quantum communication protocols that are more efficient than the best classical protocols;
- To apply the ideas from quantum algorithms and quantum complexity theory to studying physical problems such as quantum non-locality and the complexity of physical systems;
- To apply the methods from quantum information to solving purely classical problems in computer science.

A key feature of our project is its interdisciplinary nature. While focusing on the computer science side of quantum information, our project involves both computer scientists and physicists, ensuring that each research question gets considered from both computer science and physics perspectives. We expect that this interdisciplinary approach will lead to discovery of new connections between the two fields.

2 The main results of the project during the 1$^{\text{st}}$ year

Our research has been published in leading Physics journals, including Nature Communications, Physical Review Letters, and Physical Review A and in the leading conferences and journals for Theoretical Computer Science, including IEEE Conference on Foundations of Computer Science (FOCS), International Conference on Automata, Languages and Programming (ICALP), IEEE Conference on Computational Complexity (CCC) and SIAM Journal on Computing.

We now provide some highlights for each of the research directions of the project.

2.1 New Ideas for Quantum Algorithms

We have made several important contributions to quantum algorithms:

1. **Learning graphs and quantum walks.** Learning graphs have been a powerful tool for designing new quantum algorithms and have led to new quantum algorithms for a variety of problems. However, some of the learning graph based algorithms (in particular, the quantum algorithm for the k-distinctness problem) are efficient in terms of the number of queries (accesses to input data) but are not efficient with respect to the overall computation time.

   In [4], we have been able to overcome this problem, developing two time-efficient quantum based algorithms for the problem of 3-distinctness (finding 3 equal elements in an array). The first algorithm is based on a new connection with electric networks. We design a form of quantum walk in which the algorithm's quantum state corresponds to an electric flow on a certain network. The second algorithm uses an extension of the quantum walk search framework that facilitates quantum walks with nested updates.

2. **Property testing.** We have completed a survey [7] on a new research area, quantum property testing. Property testing studies very fast algorithms for determining whether the input data have a certain property or are far from having it. Property testing is well studied in conventional computer science and has found many applications there. In contrast, quantum property testing is much less studied.

   We survey the known results on quantum property testing in three broad directions:

(a) *quantum testers for properties of classical objects*, where quantum testers can be much (sometimes exponentially) more efficient than classical testers;

(b) *classical testers of quantum objects*, where the goal is to determine properties of quantum states or operations based on classical input-output behaviour, a scenario that is relevant from experimental perspective;

(c) *quantum testers for properties of quantum objects* such as states or operations, where bounds on testing various natural properties are surveyed.

The survey also highlights connections to other areas of quantum information theory such as complexity theory. We expect that our survey will serve as a systematic guide for future research in this area.

2.2 General Properties of Quantum Algorithms

The three most important achievements of our project in this direction are:

1. **Exact quantum algorithms.** A quantum algorithm is exact if, on any input data, it outputs the correct answer with certainty (probability 1). Designing exact quantum algorithms is substantially more difficult than usual bounded error algorithms which may output an incorrect answer with a small probability. Until recently, the biggest advantage for exact quantum algorithms was just a factor of 2: it was known that parity of N bits can be computed by an exact quantum algorithm using $N/2$ queries to the input bits, whereas classical algorithms require N queries.

   We present the first example [1] of a total Boolean function for which exact quantum algorithms have superlinear advantage over deterministic algorithms. Any deterministic algorithm that computes our function must use N queries but an exact quantum algorithm can compute it with $O(N^{0.8675\ldots})$ queries. This solves an open problem that has been well known in the quantum algorithms community for at least 10 years.

2. **Quantum Attacks on Classical Proof Systems.** For many classically secure protocols it is not clear if they also resist quantum attacks because the classical proof techniques often cannot be applied in the quantum world. This raises the question whether the known proof techniques are insufficient or the protocols themselves are quantum insecure. Quantum zero-knowledge proofs and quantum proofs of knowledge are inherently difficult to analyze because their security analysis uses rewinding. Certain cases of quantum rewinding can be handled by known techniques, yet in general the problem remains elusive.

   We show [2] that this is not only due to a lack of proof techniques: relative to an oracle, we show that classically secure proofs and proofs of knowledge are insecure in the quantum setting. To show these results, we develop a general technique that allows an adversary to find one value satisfying a given predicate but not two.

3. **Adversary lower bounds.** Adversary method is a very powerful mathematical tool that can be used (in principle) to prove tight lower bounds on query complexity of quantum algorithms. In practice, however, it is often hard to construct a solution to this bound that would be close to the optimal. Collision and Set Equality are two problems for which no such solution is known. Furthermore, a weaker (but simpler to use) form of the adversary method with only positive weights is not strong enough for obtaining a solution for these problems. Even though tight bounds are known due to an alternative (polynomial) method, all attempts of reproducing the same bounds with the adversary method have been futile. We have overcome these limitations and proved tight lower bounds on the quantum query complexity of the Collision and Set Equality problems, thus extending the range of applications of the adversary method [3].

2.3 Algorithms in Quantum Communication

We highlight three results in quantum communication.

1. **Optimal device-independent randomness evaluation**. We show [8] how to take into account the full information about the probability distributions characterizing the measurement outcomes of a Bell test in a systematic manner in order to optimally evaluate the randomness that can be certified from non-local correlations. We further determine the optimal Bell inequality for certifying the maximal amount of randomness from a given set of non-local correlations.

2. **Information versus communication via non-local games** In a collaboration between Paris and ULB groups of our project [6], we showed that all known optimal communication protocols can be compressed to their information content. The result uses a new connection between lower bound techniques for communication complexity and the efficiency of non-local games where the players can either output a value or abort.

3. **Experimental implementation of quantum coin flipping** We have experimentally implemented [9] a quantum protocol for performing a coin flip by two parties which do not trust one another.

   The protocol that we implemented performs strictly better than classically possible over a distance suitable for communication over metropolitan area optical networks. The implementation is based on a practical plug and play system, designed for quantum key distribution. We also show how to combine our protocol with coin flipping protocols that are almost perfectly secure against bounded adversaries, hence enhancing them with a level of information-theoretic security.

2.4 Quantum Information in Computer Science and Physical Systems

In recent years, it has been discovered that the ideas of quantum information can be applied to other fields (both classical computer science and the study of quantum physical systems), often in unexpected ways. We highlight one such result from our project.

Circuit-to-Hamiltonian translations. While computer scientists like to think of a quantum computer as a *circuit* of elementary gates, from the physics perspective the primary object is the *Hamiltonian.* Hamiltonian is a matrix that describes the different forces at work in the system, and corresponds to the observable for the total energy in the system.

Translations between the circuit view and the Hamiltonian view are very important. The standard circuit-to-Hamiltonian translation due to Feynman and (subsequently) Kitaev has been a fundamental tool in the study of complexity of physical systems, with many applications: it allows one to construct a universal adiabatic computation, universal quantum random walks, as well as derive results in quantum complexity theory. It crucially involves a quantum register for a clock which counts the steps of the computation.

We have formalized [5] a new circuit-to-Hamiltonian translation which assigns a clock to each interacting qubit, so now there are many local clocks instead of one global one. We have used this to solve a long-standing open problem, namely the mathematical analysis of the spectral gap of the fermionic ground-state computation introduced by Mizel et al. in 2001.

3 Expected final results

To realize the potential of quantum information science, it is crucial to provide a sustained support for theoretical research that will generate more applications for future quantum technologies and study the interdisciplinary connections between quantum information science, quantum mechanics and computer science.

In the QALGO project, we plan to address a major scientific challenge: search for new algorithms and protocols. We expect that our project will have the following impacts:

- New quantum algorithms which would enhance the future impact of quantum computers.
- Better understanding of fundamental questions about quantum algorithms which will help to design new quantum algorithms.
- New protocols for quantum communication achieving more efficient quantum communication.
- Applications of ideas from quantum information to both classical computer science and the study of physical systems.

Our project will also create new collaborations between physicists and computer scientists, with the potential of bringing new insights to both fields.

References

[1] A. Ambainis. Superlinear advantage for exact quantum algorithms. *SIAM Journal on Computing*, accepted for publication.

[2] A. Ambainis, A. Rosmanis, D. Unruh. Quantum Attacks on Classical Proof Systems - The Hardness of Quantum Rewinding. *IEEE Conference on Foundations of Computer Science (FOCS'2014)*, accepted for publication. arXiv:1404.6898.

[3] A. Belovs, A. Rosmanis. Adversary Lower Bounds for the Collision and the Set Equality Problems. arXiv:1310.5185.

[4] A. Belovs, A. Childs, S. Jeffery, R. Kothari, and F. Magniez. Time-efficient quantum walks for 3-distinctness. In *Proceedings of the 40th International Conference on Automata, Languages, and Programming*, ICALP'13, pages 105–122, 2013.

[5] N. Breuckmann, B.M. Terhal. Space-Time Circuit-to-Hamiltonian Construction and Its Applications. J. Phys. A: Math. Theor. **47**, 195304 (2014); arXiv:1311.6101.

[6] I. Kerenidis, S. Laplante, V. Lerays, J. Roland, D. Xiao. Lower bounds on information complexity via zero-communication protocols and applications. SIAM Journal on Computing, to appear.

[7] A. Montanaro and R. de Wolf. A survey of quantum property testing. arXiv:1310.2035, 2013.

[8] O. Nieto-Silleras, S. Pironio, J. Silman. Using complete measurement statistics for optimal device-independent randomness evaluation. *New Journal of Physics*, 16:013035, 2014.

[9] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, E. Diamanti. Experimental plug and play quantum coin flipping, *Nature Communications*, 5, Article Number 3717.