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, 2014 to April 30, 2015**

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 2nd 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 ACM Symposium on the Theory of Computing (STOC), IEEE Conference on Foundations of Computer Science (FOCS), International Conference on Automata, Languages and Programming (ICALP) 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

The query model studies the complexity of computing in terms of the number of accesses to input data (queries). It provides a useful approach to study the power of quantum computation, since many of the known quantum algorithms can be described in this model.

It is known that quantum query complexity is characterized by a semidefinite program (SDP), the Adversary SDP. This means that one can obtain lower bounds for specific problems by solving this semidefinite program and quantum algorithms for these problems by solving its dual. This idea is increasingly used for designing new quantum algorithms. Here are some of our contributions in this direction.

1. **Bounds on parallel quantum walk algorithms.** We studied the complexity of quantum query algorithms that make several queries in parallel in each timestep [1]. We obtained tight bounds for a number of problems, specifically for element distinctness (finding two equal elements in an array) and for the k-SUM problem (determining whether an array of numbers contains k numbers whose sum is equal to a given number; this problem is significant for cryptanalysis). The upper bounds are obtained by parallelizing the known quantum algorithms for those problems which are based on the use of quantum walks (quantum counterparts of random walks), and the lower bounds are based on a relatively small modification of the adversary lower bound method, combined with recent results of Belovs et al. reported last year on learning graphs (a new approach for analyzing the Adversary SDP). This paper connects two research directions of our project: quantum walks and the learning graph model.

2. **New quantum algorithm for monotonicity testing.** While the first SDP-based quantum algorithms were designed using the framework of learning graphs, in our most recent work [2], we have started to design solutions of the dual SDP directly, without any intermediate framework. The result is a new quantum algorithm for monotonicity testing (the problem of testing whether a Boolean function is monotone or far from monotone) which is faster than any classical algorithm for the same problem. This links together two tasks of our project: finding new uses for the learning graph/adversary bound method and finding new quantum algorithms in the area of property testing.

Besides these contributions, we have also made progress in the areas of quantum algorithms for hidden subgroup problems, quantum-walk based algorithms, and adiabatic quantum computation.

2.2 General Properties of Quantum Algorithms

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

1. **Classical simulations of matchgate circuits.** The theory of matchgate computations was introduced by Valiant and used to provide a striking new class of efficient classical algorithms for a variety of computational tasks. We have obtained a complete characterization of 2-input and 2-output matchgates, and we give an efficient simulation for all cases in Valiant's simulation theorem [3]. This extends previous results on efficient classical simulation of non-interacting fermions (because operations on non-interacting fermions can be described in the matchgate formalism).

2. **Separating quantum from classical query complexity.** We have obtained further results on the number of queries to the input data required for performing certain computational tasks classically and quantumly [4]. In particular, we showed that if a property of input data of size n can be computed with k quantum queries, it can be also computed with $O(n^{1-1/2k})$ queries classically. We constructed a candidate problem for which we conjecture that this bound is optimal. As a step towards resolving this conjecture, we were able to establish a somewhat weaker lower bound.

   We have also considered the task of sampling from a probability distribution that depends on the input data and showed that a certain problem of this type can be solved quantumly with just one query but requires $\Omega(n/\log n)$ queries classically. This gap between quantum and classical computation is even bigger than the gaps that we found for the task of computing functions.

3. **Extensions of the adversary method.** The quantum adversary bound is a powerful tool for studying limitations of quantum query algorithms. We have analyzed the extent to which it can be further generalized [5]. We obtained a version of the adversary bound for arbitrary unitary input oracles as well as for the problem of implementing arbitrary unitary transformations. Using this construction, we also obtained lower bounds on the quantum query complexity of functions and relations with general input oracles.

2.3 Algorithms in Quantum Communication

We highlight two results in quantum communication.

1. **Quantum communication complexity advantage implies violation of a Bell inequality.** In a paper by Buhrman et al. [6], we obtained a general connection between a quantum advantage in communication complexity and non-locality. We show that given any protocol offering a (sufficiently large) quantum advantage in communication complexity, there exists a way of obtaining measurement statistics which violate some Bell inequality. The main tool is port-based teleportation. If the gap between quantum and classical communication complexity can grow arbitrarily large, the ratio of the quantum value to the classical value of the Bell quantity becomes unbounded with the increase in the number of inputs and outputs.

2. **Nonlocality and conflicting-interest games.** In a paper by Pappa et al. [7], we studied nonlocality and conflicting-interest games. Nonlocality enables two parties to win specific games with probabilities strictly higher than allowed by any classical theory. Nevertheless, all known such examples consider games where the two parties have a common interest, since they jointly win or lose the game.

   We asked the question: do the nonlocal features of quantum mechanics offer an advantage in a scenario where the two parties have conflicting interests? We answered this question in the

affirmative by presenting a simple conflicting interest game, where quantum strategies outperform classical ones. We also showed that our game has a fair quantum Nash equilibrium with higher payoffs for both players than in any fair classical Nash equilibrium and demonstrated how to play this game using a commercial entangled photon source, demonstrating the quantum advantage experimentally.

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 two such results from our project.

1. **Quantum algorithms with postselection versus rational functions.** Efficient quantum query algorithms induce low-degree polynomials. This well-known connection between algorithmic and algebraic concepts has been very fruitful in the past 15 years in two directions: proving limitations on quantum algorithms using algebraic tools (e.g., degree lower bounds) and constructing low-degree polynomials using efficient quantum algorithms.

   Sometimes, one considers quantum algorithms that have the added power of *postselection*. This allows the algorithm to pick a specific measurement outcome instead of having the usual probabilistic collapse to a random outcome. Nature does not allow us to postselect, but this computational model is still interesting for various reasons. In [8] we obtained a very tight analogue: the optimal complexity of quantum algorithms with postselection that compute a certain function, is essentially *equal* to the minimal degree of a rational function (i.e., ratio of two polynomials) that approximates this function. This connection is much tighter than the one for regular quantum algorithms, and we hope it will be as fruitful.

2. **Preparing ground states of specific Hamiltonians.** We have been studying the underlying structure of a wide range of states of physical systems, with the aim of understanding how these states can be realized on quantum computers. The central tool in that regard has been Projected Entangled Pair States (PEPS), which on the one hand provide a succinct description for general physical states of complex quantum systems, and on the other hand can be used to devise preparation procedures for such states based on the understanding of their underlying algebraic structure.

   In [9] we studied the ability of PEPS to describe physical states of complex quantum system, such as ground states or thermal states. In particular, we showed that thermal states can be approximated efficiently, i.e., with low bond dimension. We also [10] developed a general PEPS-based scheme for preparing arbitrary topologically ordered states on a quantum computer.

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

((*) denotes the joint publications between different project partners):

[1] (*) S. Jeffery, F. Magniez, R. de Wolf. Optimal parallel quantum query algorithms. *22nd European Symposium on Algorithms*, pp. 592-604, 2014.

[2] A. Belovs, E. Blais. Quantum Algorithm for Monotonicity Testing on the Hypercube. arXiv:1503.02868.

[3] R. Jozsa, A. Miyake, S. Strelchuk. Jordan-Wigner formalism for arbitrary 2-input 2-output match-gates and their classical simulation. *Quantum Information and Computation*, 15(7&8), 0541–0556, 2015. arXiv:1311.3046.

[4] S. Aaronson, A. Ambainis. Forrelation: A Problem that Optimally Separates Quantum from Classical Computing. *Proceedings of STOC 2015*, 307–316, 2015. arXiv:1411.5729.

[5] A. Belovs. Variations on Quantum Adversary. arXiv:1504.06943.

[6] (*) H. Buhrman, L. Czekaj, A. Grudka, M. Horodecki, P. Horodecki, M. Markiewicz, F. Speelman, S. Strelchuk. Quantum communication complexity advantage implies violation of a Bell inequality. arXiv:1502.01058.

[7] A. Pappa, N. Kumar, T. Lawson, M. Santha, S. Zhang, E. Diamanti and I. Kerenidis. Nonlocality and conflicting interest games. *Phys. Rev. Lett.* 114, 020401, 2015.

[8] U. Mahadev, R. de Wolf. Rational approximations and quantum algorithms with postselection. *Quantum Information and Computation*, 15(3&4), 295–307, 2014. arXiv:1401.0912.

[9] A. Molnar, N. Schuch, F. Verstraete, J.I. Cirac. Approximating Gibbs states of local Hamiltonians efficiently with PEPS. *Phys. Rev. B* 91, 045138, 2015. arXiv:1406.2973.

[10] M.B. Sahinoglu, D. Williamson, N. Bultinck, M. Marien, J. Haegeman, N. Schuch, F. Verstraete. Characterizing Topological Order with Matrix Product Operators. arXiv:1409.2150.