Mandats de retour BELSPO

Rapport final

Jérémie Roland

Titre

Computational aspects of quantum information processing: study of adiabatic quantum computation, quantum algorithms based on quantum walks, and distributed computation with quantum resources

Résumé

The advent of information technologies caused an unprecedented revolution at the end of the twentieth century: indeed, the development of computers and modern communication systems had a huge impact not only on science and technologies, but also on society as a whole. This revolution was made possible by the work of pioneers such as Turing for computer science and Shannon for communication systems, who laid the theoretical foundations on which modern information technologies were built. While these theoretical foundations rely on a description of computers and communication devices as classical systems, the development of quantum physics also revealed that any physical system is at its most fundamental level subject to the laws of quantum mechanics. At first, quantum effects were merely seen as an unwanted disturbance that could only hinder the behavior of computers and communication channels, but it was later realized that, if properly tamed, they could provide an advantage over purely classical devices. Indeed, over the past couple of decades were discovered more and more examples of applications of quantum effects to computation and communication problems. These examples pave the way to a new revolution in information technologies: the advent of quantum computers and quantum communication systems. The goal of this Belspo project was to contribute to this revolution by providing new applications for quantum computation and quantum communication complexity.

When devising new algorithms, an important task is to study their optimality, that is, show that no other algorithm can solve the same problem faster, by proving so-called lower bounds on the complexity of the problem. During this project, we showed that all known lower bounds for quantum query complexity are special cases of a single method, namely the multiplicative adversary method. We also developed a new optimal quantum query algorithm based on an adiabatic evolution.

We studied quantum walk based algorithms in the context of searching and sampling algorithms. In particular, we showed that a quantum walk algorithm we had previously proposed to search for a marked vertex in a graph could

sample from a set of marked vertices in a time given by the square root of the so-called extended hitting time. We also provided new techniques, based on Szegedy-type quantum walks and quantum phase estimation, to mix over the vertices of a graph.

In the context of communication complexity, we have shown that the partition bound, one of the strongest lower bound methods for this model, amounts to finding a Bell inequality that is strongly resistant to the so-called detector loophole in non-locality tests. This new interpretation allowed us to design a new lower bound method for quantum communication complexity, based on the violation of Tsirelson inequalities. Using similar techniques we also showed that almost almost all lower bound methods for communication complexity are also lower bounds for information complexity. This allowed us to prove an exponential separation between classical and quantum information complexities.

keywords Quantum computation, quantum algorithms, quantum communication complexity, quantum non-locality

1 Rappel des objectifs

My original project proposed to study three different subjects related to quantum computation: adiabatic quantum computation, quantum algorithms based on quantum walks, and distributed computation with quantum resources. However, due to the delay incurred in the selection of the grants, I had to postpone my return to Belgium until September 2011, and my project continued to evolve in the meantime as I made progress answering some of the questions I intended to address.

Regarding quantum algorithms, I shifted my interests from adiabatic computation and quantum walks to more general questions about the quantum complexity of computational tasks. In particular, I studied lower bound techniques for quantum query complexity, which allow to show that a quantum algorithm is optimal, or to limit the possible speed-up that quantum computers could provide for a particular problem. This is also useful in cryptography, where the security of a cryptosystem is based on the hardness of some computational task.

As planned in my original project, I also worked on distributed computing, and more precisely on communication complexity. Here, the general problem is to better understand when quantum communication can help distant parties solve a problem together.

2 Méthodologie et résultats

2.1 Adiabatic quantum computation and quantum query complexity

Lower bound methods in quantum query complexity The polynomial method [BBC$^+$01] and the adversary method [Amb02, HLŠ07] are the two main techniques to prove lower bounds on quantum query complexity, and they have so far been considered as unrelated approaches. We have shown an explicit reduction from the polynomial method to the multiplicative adversary

method [Špa08]. The proof goes by extending the polynomial method from Boolean functions to quantum state generation problems. In the process, the bound is even strengthened. We showed that this extended polynomial method is a special case of the multiplicative adversary method with an adversary matrix that is independent of the function. This new result therefore provides insight on the reason why in some cases the adversary method is stronger than the polynomial method. It also reveals a clear picture of the relation between the different lower bound techniques, as it implies that all known techniques reduce to the multiplicative adversary method.

Adiabatic quantum query algorithm It is now known that the (additive) adversary method characterizes the bounded error quantum query complexity of any function, that is, there always exist a quantum algorithm that computes the function with bounded error using at most the number of queries corresponding to the value of the adversary bound. This is shown by constructing an algorithm from the dual of the adversary bound [LMR$^+$11]. The original proof constructs such an algorithm in the usual circuit model of quantum computation. This is a discrete-time model, where the gates in the circuit correspond to successive operations applied on the state of the quantum computer. From the point of view of physics, this is rather unnatural, as physical systems typically evolve continuously in time under the influence of a Hamiltonian.

During the latter part of my grant I started considering the possibility of a continuous-time algorithm that would be optimal for bounded error quantum query complexity. This work later led to a new optimal quantum query algorithm in the adiabatic model, that is, where the the state of the quantum computer evolves under the influence of a very slowly varying Hamiltonian. Compared to the original time-discrete algorithm, this new algorithm is not only more natural from the point of view of physics, but also arguably simpler.

Note that the ultimate goal would be to design an algorithm that would be optimal for any error. One approach would be to consider the multiplicative adversary bound, and this adiabatic algorithm is a first step toward this goal.

2.2 Quantum algorithms based on quantum walks

Hitting time In previous work, my coauthors and I showed that any reversible Markov chain can be turned into a quantum walk that would find a marked vertex quadratically faster, hence showing that the quantum hitting time is quadratically smaller than its classical analogue for any such walk [KMOR10]. This quantum walk search algorithm also succeeds in the presence of multiple marked elements, but in this case its computation time is given by the square root of another quantity which we called the extended hitting time (it generalizes the usual hitting time in the sense that for a single marked vertex, they are equal).

During my return grant, I came back to this problem together with my coauthors in order to better understand the connection between the extended hitting time and the usual hitting time. On the negative side, we could find instances where there is a large separation between theses two hitting times. On the other hand, we also found a good reason why this is the case: our quantum walk search algorithm actually solves a harder result than the corresponding classical algorithm on which the definition of the usual hitting time relies: while the classical

algorithm returns an arbitrary marked vertex, the quantum algorithm samples a marked vertex from the stationary distribution of the walk, hence ensuring a fair sampling within the set of marked vertices. These new discoveries led to a significantly extended article that has been recently accepted for publication.

Mixing time Besides searching, another typical application of random walks is sampling from the vertices of the graph. In particular, for ergodic walks, the mixing time corresponds to the number of steps necessary to approach the stationary distribution of the walk. This raises the question of the efficiency of quantum walks in this context, in particular, can quantum walks provide some generic speed-up for mixing? This question has been considered by Aharonov et al. in [AAKV01], but the quantum hitting time could be characterized only for very specific graphs.

During my return grant, I supervised a Master's Thesis whose goal was to revisit this question using similar tools as the ones we used for the hitting time, in particular Szegedy-type quantum walks and quantum phase estimation. Using these tools, we could reproduce all the results in [AAKV01], but also slightly strengthen them in some cases: in particular, we could remove logarithmic factors in the quantum mixing time of cyclic graphs.

2.3 Communication complexity

Efficiency bound We studied randomized and quantum efficiency lower bounds in communication complexity. These arise from the study of zero-communication protocols in which players are allowed to abort. Our scenario is inspired by the physics setup of Bell experiments, where two players share a predefined entangled state but are not allowed to communicate. Each is given a measurement as input, which they perform on their share of the system. The outcomes of the measurements should follow a distribution predicted by quantum mechanics; however, in practice, the detectors may fail to produce an output in some of the runs. The efficiency of the experiment is the probability that the experiment succeeds (neither of the detectors fails).

When the players share a quantum state, this gives rise to a new bound on quantum communication complexity (eff^*) that subsumes the factorization norm. When players share randomness instead of a quantum state, the efficiency bound (eff), coincides with the partition bound of Jain and Klauck [JK10]. This is one of the strongest lower bounds known for randomized communication complexity, which subsumes all the known combinatorial and algebraic methods including the rectangle (corruption) bound, the factorization norm, and discrepancy.

The lower bound is formulated as a convex optimization problem. In practice, the dual form is more feasible to use, and we showed that it amounts to constructing an explicit Bell inequality (for eff) or Tsirelson inequality (for eff^*).

For one-way communication, we showed that the quantum one-way partition bound is tight for classical communication with shared entanglement up to arbitrarily small error.

Finally, an important goal in physics is to devise robust Bell experiments that are impervious to noise and detector inefficiency. We made further progress towards this by giving a general tradeoff between communication, Bell inequality violation, and detector efficiency.

Information complexity We showed that almost all known lower bound methods for communication complexity are also lower bounds for the information complexity. In particular, we defined a relaxed version of the *partition bound* of Jain and Klauck [JK10] and prove that it lower bounds the information complexity of any function. Our relaxed partition bound subsumes all norm based methods (e.g. the γ_2 method) and rectangle-based methods (e.g. the rectangle/corruption bound, the smooth rectangle bound, and the discrepancy bound), except the partition bound.

Our result uses a new connection between rectangles and *zero-communication* protocols where the players can either output a value or abort. We proved the following compression lemma: given a protocol for a function f with information complexity I, one can construct a zero-communication protocol that has non-abort probability at least $2^{-O(I)}$ and that computes f correctly with high probability conditioned on not aborting. Then, we showed how such a zero-communication protocol relates to the relaxed partition bound.

We used our main theorem to resolve three of the open questions raised by Braverman [Bra12]. First, we showed that the information complexity of the Vector in Subspace Problem [KR11] is $\Omega(n^{1/3})$, which, in turn, implies that there exists an exponential separation between quantum communication complexity and classical information complexity. Moreover, we provided an $\Omega(n)$ lower bound on the information complexity of the Gap Hamming Distance Problem.

References

[AAKV01] Dorit Aharonov, Andris Ambainis, Julia Kempe, and Umesh Vazirani. Quantum walks on graphs. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing - STOC '01*, pages 50–59, New York, New York, USA, 2001. ACM Press.

[Amb02] Andris Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002.

[BBC+01] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48:778–797, 2001.

[Bra12] M. Braverman. Interactive information complexity. In *Proc. 44th STOC*, pages 505–524, 2012.

[HLŠ07] Peter Høyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 526–535. ACM, 2007.

[JK10] R. Jain and H. Klauck. The partition bound for classical complexity and query complexity. In *Proc. 25th CCC*, pages 247–258, 2010.

[KMOR10] Hari Krovi, Frédéric Magniez, Maris Ozols, and Jérémie Roland. Finding is as easy as detecting for quantum walks. In *37th International Colloquium on Automata, Languages and Programming (ICALP'10)*, volume 6198 of *Lecture Notes in Computer Science*, pages 540–551. Springer, 2010.

[KR11] B. Klartag and O. Regev. Quantum one-way communication can be exponentially stronger than classical communication. In *Proc. 43rd STOC*, pages 31–40, 2011.

[LMR+11] Troy Lee, Rajat Mittal, Ben W. Reichardt, Robert Špalek, and Mario Szegedy. Quantum query complexity of state conversion. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*, pages 344–353. IEEE Computer Society, 2011.

[Špa08] Robert Špalek. The multiplicative quantum adversary. In *Proceedings of the 23rd Annual IEEE Conference on Computational Complexity*, pages 237–248. IEEE Computer Society, 2008.

3 Diffusion et valorisation

3.1 Publications

During the first year of my grant, two articles that were the result of previous research appeared in proceedings of conferences:

- Troy Lee and Jérémie Roland. A strong direct product theorem for quantum query complexity. In *27th IEEE Conference on Computational Complexity* (CCC'12), pages 236-246, 2012.
- Maris Ozols, Martin Roetteler, and Jérémie Roland. Quantum rejection sampling. In *3rd Innovations in Theoretical Computer Science Conference* (ITCS'12), pages 290-308. ACM Press, 2012.

Later on, my coauthors and I wrote extended versions of these articles, that were published in international journals:

- Troy Lee and Jérémie Roland. A strong direct product theorem for quantum query complexity. *Computational Complexity*, 22(2):429-462, 2013.
- Maris Ozols, Martin Roetteler, and Jérémie Roland. Quantum rejection sampling. *ACM Transactions on Computation Theory*, 5(3):11:1-11:33, 2013.

Moreover, the work performed during my grant led to the publication of eight other articles:

- Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jérémie Roland, and David Xiao. Lower bounds on information complexity via zero-communication protocols and applications. In *53rd Annual IEEE Symposium on Foundations of Computer Science* (FOCS'12), pages 500-509, 2012.
- Sophie Laplante, Virginie Lerays, and Jérémie Roland. Classical and quantum partition bound and detector inefficiency. In *39th International Colloquium on Automata, Languages and Programming* (ICALP'12), volume 7391 of Lecture Notes in Computer Science, pages 617-628, 2012.

- Loïck Magnin and Jérémie Roland. Explicit relation between all lower bound techniques for quantum query complexity. In *30th International Symposium on Theoretical Aspects of Computer Science* (STACS'13), pages 434-445, 2013.
- Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jérémie Roland, and David Xiao. Lower bounds on information complexity via zero-communication protocols and applications. *SIAM Journal on Computing*, 2014. To appear.
- Loïck Magnin and Jérémie Roland. Explicit relation between all lower bound techniques for quantum query complexity. *International Journal of Quantum Information*, 2014. Online ready.
- Hari Krovi, Frédéric Magniez, Maris Ozols, and Jérémie Roland. Quantum walks can find a marked element on any graph *Algorithmica*, 2014. To appear.

Finally, work started during the last months of the grant later led to the following article:

- Mathieu Brandeho and Jérémie Roland. An optimal adiabatic quantum query algorithm. arXiv preprint arXiv:1409.3558, 2014.

3.2 Participation à des conférences

During the course of this grant, I was invited as a speaker to seven different conferences and workshops, including for one plenary talk:

25/04/2013 *The 3rd Heilbronn Quantum Algorithms Day* in Bristol (UK).
Invited talk: *Quantum query complexity: Adversaries, polynomials and direct product theorems.*

13-14/11/2012 *Quantum Walks in Grenoble* (France).
Invited talk: *Quantum algorithms based on quantum walks.*

04/11-13/2012 *Worskhop on Recent Progress in Quantum Algorithms* in Waterloo (Canada).
Invited talk: *Quantum query complexity: Adversaries, polynomials and direct product theorems*

01/17-21/2012 *First NASA Quantum Future Technologies Conference* in Moffett Field, California (USA).
Invited talk: *Quantum Rejection Sampling*

12/12-16/2011 *Fifteenth Workshop on Quantum Information Processing* (QIP 2012) in Montreal (Canada).
Plenary talk: *Quantum Rejection Sampling*

09/29/2011 *Quantum Information in Paris* (QuPa), France.
Invited talk: *Quantum Rejection Sampling*

09/19-23/2011 *Quantum Cryptanalysis Worskhop* in Dagstuhl, Germany.
Talk: *Quantum adversary lower bounds by polynomials*

4 Bilan et perspectives

The outcome of my return grant is very positive, as it fulfilled all its goals. Indeed, it not only allowed me to move back to Belgium by funding my first two years of research, but it also gave me the opportunity to apply for and obtain a tenure position (*Premier Assistant*) at the *Université Libre de Bruxelles*, which might not have been possible without the support of Belspo. As a consequence, I am now building up a new research group on quantum computation within the *Centre for Quantum Information and Communication* (QuIC) of the *Ecole Polytechnique de Bruxelles*.

In order to obtain the necessary resources to hire new researchers, I coordinated with other researchers at ULB the proposal of an ARC project (COPHYMA), which we successfully obtained in 2012. The project is now well on its way, and I already hired one postdoctoral researcher and one PhD student. Later on, I joined a European consortium in order to write a proposal for a FP7 STREP project (QALGO), where I would act as leader for one of the workpackages. The proposal was successful and the project started in May 2013. I also organized the last annual meeting of this project in May 2014 in Brussels, which gathered around 50 researchers from across Europe. All these initiatives contributed to strengthen the position of ULB and therefore Belgium in the European research landscape.

Besides research, I also heavily invested in teaching following my nomination as a *Premier Assistant* at ULB. In particular, I created two new courses ("Compléments de programmation et d'algorithmique" and "Quantum Information and Computation"), I am titular of the Geometry test for the admission exam in engineering, and I supervised various student projects and two Master's theses.

To conclude, this Belspo return grant gave a new impulse to my career by allowing me to develop my research and finally obtain a tenure position at ULB, and I would like to thank Belspo for this unique opportunity.