

Rapport à mi-parcours du projet “Réseaux Quantiques” de l’ACI “Sécurité Informatique”

April 12, 2005

1 Summary of Achievements

The aim of this project is to develop tools and algorithms for use in quantum networks. We have divided our efforts into three broad categories:

- Protection of quantum information and error correcting codes
- Quantum routing and quantum walks
- Other algorithms adapted to quantum networks

We are happy to report that we have been able to contribute to all three of our subgoals. In particular we have published or submitted a total of 21 publications in various collaborations since the start of this project. Details can be found in the following sections.

In the framework of this project one PhD student, Thomas Camara, has been working at INRIA Rocquencourt since October 2003 on various aspects of quantum coding and error protection. And very recently (October 2004) we were able to hire Jeremie Roland as a postdoc at INRIA working both on aspects of quantum noise protection and quantum information transmission through noisy channels.

The other people involved in the project are Harold Ollivier (local responsible) and Jean-Pierre Tillich at INRIA Rocquencourt and Christophe Durr, Julia Kempe (project responsible), Sophie Laplante, Frederic Magniez and Miklos Santha at LRI. We are very glad to note that all of the participants in the project were able to contribute in some form, which is also reflected in our publication list.

In summary we can say that we have been able to follow our schedule very closely. In particular in the area of stabilisation of quantum information and specifically in quantum convolutional coding (5 publications) and of quantum routing and in particular quantum walks (6 publications) we have been able to even surpass the goals we have set for the first 18 months.

Many collaborations have been initiated through the funding provided by the ACI. But most notably, it helped settle INRIA - Codes as new but strong actor in the study of quantum information. This was made possible by focusing on international collaborations and dissemination of our results in international conferences. In parallel to these actions, INRIA and LRI have been working together to define common projects. Our postdoc Jeremie Roland is shared between INRIA and LRI. In addition to valuable exchange on previous projects we are currently working on several common research projects. The most notable one would be quantum testing — a way to ensure quantum computers have no trap doors. This combines previous works of LRI together with tools used at INRIA for the study of decoherence and error correction.

2 Robustness and Quantum Error Correcting Codes

Quantum information is very sensitive to external interactions and noise. It must be stabilized not only for allowing long distance communications, but even inside the registers of quantum computers. The outrageous overhead in physical resources of fault-tolerant architectures makes practical implementations out of reach of our current experimental achievements.

A potential cause for such matter of fact is the absence of efficient codes for quantum communication and computation. To this end, we have introduced quantum convolutional codes as the first step taken to constructing quantum turbo-codes [OT03, OT04]. We have described how to construct such codes, and most importantly how to implement them by a sequence of quantum gates. We showed that the encoding and decoding complexity is linear in the number of protected qubits which fits our demand for classes of codes which can be manipulated with restricted experimental abilities. Our efforts have also been focused on error estimation: we adapted Viterbi's algorithm to take into account the specific nature of quantum information. This modified algorithm achieves maximum likelihood error estimation with linear complexity, while requiring only the value of the syndrome (in contrast to the usual Viterbi algorithm which heavily uses the value of the received bits).

Following the same line of research, we considered a quantum analog of regular Gallager's codes. Previous attempts at constructing quantum low density parity check codes exemplified the difficulty of finding such codes by random constructions. In our approach [COT], we emphasized that this problem can be overcome by enforcing a local rule to the Tanner graph of the code. This allowed us to propose two classes of quantum LDPC codes whose construction uses a generalization of Cayley graphs to satisfy our local constraint. The proposed examples are among the most efficient quantum codes to date.

In addition to our work on quantum convolutional codes we have studied another aspect of quantum codes in [FKSS04]. We have introduced a dynamical systems approach to study the noise correction behavior of concatenated quantum codes. To this end we have specified a concatenation map which acts on the *noise*. We describe the noise acting on qubits as a high-dimensional manifold. Using techniques from iterated maps we were able to give a characterization of the regions of *correctable* noise for a particular code. This approach is general and works for all codes. We have worked out several examples and hope that our techniques will allow to analyze and classify a wide variety of codes.

Another line of work on robustness was pursued in [HKMW03]. Building on previous work on decoherence free subspaces and encoded universality we have determined an explicit gate sequence to implement exchange-only quantum computation on a four-qubit encoding. Exchange-only quantum computation is important in scenarios where one-qubit gates would generate too much noise. It allows to avoid these one qubit gates at the expense of some redundancy in the number of qubits. The four-qubit encoding is one such encoding and we hope that our explicit sequence will be helpful to engineers building quantum computers and quantum communication devices.

Several aspects of our work on quantum error correction are currently under close scrutiny. First in the list are constructions of quantum turbo codes. We have been able to derive a trellis formulation of quantum codes which allows to derive efficient MAP algorithms for quantum codes. This naturally leads to iterative decoding when two convolutional codes are concatenated. Preliminary results show that serial concatenation is preferable and that the iterative algorithm achieves optimal error correction capability when the size of the interleaver is large. We will pursue this study in the remaining time of the ACI funding. Along with the trellis formulation, we hope to

apply some simple equalization techniques to quantum communication in order to reduce defects due to reference frame misalignments. A better understanding of belief propagation algorithms in loopy graphs will be conducted. We believe this topic is crucial for quantum error correction as Tanner graphs of quantum codes have, by construction, many 4-cycles. We propose to analyze this last topic by using results obtained for classical codes, but also with the techniques introduced in [FKSS04]

3 Quantum Routing and Quantum Walks

We have undertaken an extensive study of quantum walks and their various applications. In [Kem05, Kem03] we have studied the hitting times of quantum walks on the hypercube and compared it to the behavior of the classical random walk. We have shown that there is an exponential speed up of quantum walks to reach certain vertices of the hypercube. More precisely the hitting time from one corner to the opposite corner in the quantum case is linear in the dimension (or quadratic with a slightly modified definition), whereas in the classical case it takes the walk exponential time to penetrate the hypercube to its opposite corner. We had to introduce a rigorous definition of hitting time in the quantum case first. Subsequently we have made use of this rapid quantum hitting to propose a quantum routing strategy in a distributed network.

In an effort to study quantum walks and their derived algorithms in various topologies, we have analysed a quantum walk algorithm on the d -dimensional grid. Quantum walk based algorithms can be used to search for a marked item or vertex in a graph in a local manner. They have already found several applications in finding optimal quantum algorithms. In [AKR05] we showed that the quantum walk algorithm on a d dimensional grid of N vertices takes time \sqrt{N} to find a marked vertex for $d \geq 3$ (this is known to be optimal) and $\sqrt{N} \log N$ for $d = 2$. This improved over known search algorithms on the grid.

We found another quantum walk based algorithm to find triangles in a graph in [MSS05]. This algorithm takes time $O(N^{\frac{13}{10}})$ where N is the number of vertices in the graph. This algorithm improves over all other known quantum algorithms for this problem.

Continuing with the theme of local search we have studied the behavior and query complexity of local search both in the classical deterministic, in the classical randomized and in the quantum setting in [SS04]. Let f be an integer valued function on a finite set V . We call an undirected graph $G(V, E)$ a *neighborhood structure* for f . The problem of finding a local minimum for f can be phrased as: for a fixed neighborhood structure $G(V, E)$ find a vertex $x \in V$ such that $f(x)$ is not bigger than any value that f takes on some neighbor of x . The complexity of the algorithm is measured by the number of questions of the form “what is the value of f on x ?” We have shown that the deterministic, randomized and quantum query complexities of the problem are polynomially related.

Finally we have studied quantum algorithms for graph problems in [DHHM04]. These problems, like Connectivity, Strong Connectivity, Minimum Spanning Tree, and Single Source Shortest Paths come up naturally in networks. We have given almost tight lower and upper bounds for the bounded error quantum query complexity for these problems. The upper bounds utilize search procedures for finding minima of functions under various conditions and are polynomially faster than the corresponding classical algorithms. This paper won the Best Paper award at ICALP’s Track A.

In summary we have covered a broad spectrum of quantum walk and network aspects in our work. We hope to continue our study throughout the continuation of this project.

4 Other projects

Decoherence: Quantum information processing uses the superposition principle allowed by quantum mechanics to outperform classical information processing. However, the ability of quantum systems to stay in arbitrary superpositions of states tend to decrease with their size. This effect is known under the name “decoherence”. In a broad meaning it encapsulates all phenomena that tend to enforce a quantum-classical transition as physical systems become macroscopic. In [OPZ04b, OPZ04a, OP04], we argue that interaction with an uncontrolled environment can account for the absence of macroscopic superpositions as well as for the emergence of objective properties of physical systems. This work has tremendous consequences on the field of quantum information. If emergence of objective properties defining the classical world would not have emerged from the quantum substrate, then modifying the quantum theory would have been necessary and such modifications would have probably compromised the future of large scale quantum computing. On the contrary we showed that noise encountered in quantum computers is not of fundamental origin. In particular, its effect can be counteracted by encoding information in protected quantum structures.

Algorithms: Current technology does not allow large scale quantum information processing. However, some prototypes of quantum computers might in the near future be able to manipulate few dozens of qubits. It is then of practical importance to describe simple yet interesting algorithms that use these devices. In [PBKLO04], we propose an algorithm which gives an exponential gain over any known classical algorithm for calculating the fidelity decay of a quantum map. This algorithm has been recently implemented with currently available technology (liquid state NMR quantum information processor). Our result contributed to trigger some interest in small scale networked devices for simulating physical systems.

We also pursued another direction in more standard quantum algorithms. We studied the hidden subgroup problem. Shor’s famous factoring algorithm is an instance of the hidden subgroup problem and since its discovery many other instances of this problem have been studied. In [KS05] we give new upper and lower bounds on the performance of the so called weak standard method for a variety of non-abelian groups. In particular we show that the weak standard method is not stronger than classical search in the context of the symmetric group.

Quantum Communication: We have given a new result in quantum information transmission of a permutation in [KK04] over a quantum channel. The goal is to transmit an ordering of objects by encoding this particular permutation into a quantum state. It turns out that that such a quantum encoding requires less bits than any classical encoding. In particular in order to transmit a permutation of N objects classically, one needs N states per object, whereas in the quantum case only N/e states are required (where $e = 2.718\dots$).

In another line of work we have compared the amount of communication needed in the simultaneous message passing model. In this model two parties send a message to a referee who is supposed to compute some function of the inputs of the parties. It was known that if the two parties are quantum, then there are functions that require exponentially longer messages in the classical setting, even when the players share a public coin, than in the quantum setting. It has been open whether this is true in general for all functions. We settle this question in [GKdW04] and exhibit a function for which this is not true, and where in fact the quantum protocol requires exponentially more communication than the classical protocol with public coins.

Complexity: Several different models of quantum computing have been introduced recently. Some of these models might be easier to implement, in particular in the context of quantum networks. One such model is adiabatic quantum computation. It was not known whether this model

is as strong as standard quantum computation. We have settled this question in [AvDK⁺04] and shown that adiabatic quantum computation is equivalent to quantum computation in the quantum circuit model. We have also given a 2-dimensional implementation of adiabatic computation on a grid with 6-level particles.

Another important aspect of quantum complexity is to introduce complexity classes and find complete problems in each. The quantum analogue of the class NP is the class QMA. We have been able to improve known results and to show that the 2-Local Hamiltonian problem is complete for QMA in [KKR04]. This is in close analogy to the classical fact that MAX-2-SAT is complete for the class NP. We have introduced new perturbation theory techniques to this area and we hope that these techniques will prove very useful in the context of quantum networks, because they allow to implement interactions between parties that are not directly connected by a quantum channel by using intermediate parties.

And finally we have introduced notions of quantum Kolmogorov complexity to the study of quantum query complexity in [LM04]. This has allowed us to prove a very general lower bound technique for quantum query complexity, which generalises several of the known techniques.

References

- [AKR05] Andris Ambainis, Julia Kempe, and Alexander Rivosh. Coins make quantum walks faster. In *Proc. 16th ACM SODA*, pages 1099–1108. ACM, 2005.
- [AvDK⁺04] Dorit Aharonov, Wim van Dam, Julia Kempe, Zeph Landau, Seth Lloyd, and Oded Regev. Adiabatic quantum computation is equivalent to standard quantum computation. In *Proc. 45th Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 42–51. IEEE, 2004.
- [COT] T. Camara, H. Ollivier, and J.-P. Tillich. Constructions and performance of classes of quantum ldpc codes. quant-ph/0502086.
- [DHHM04] Christoph Durr, Mark Heiligman, Peter Hyer, and Medhi Mhalla. Quantum query complexity of some graph problems. In *Proc. 31st ICALP*, pages 481–493, 2004.
- [FKSS04] Jesse Fern, Julia Kempe, Slobodan Simic, and Shankar Sastry. Fault-tolerant quantum computation - a dynamical systems approach, 2004. quant-ph/0409084.
- [GKdW04] Dmitry Gavinsky, Julia Kempe, and Ronald de Wolf. Quantum communication cannot simulate a public coin, 2004. quant-ph/0411051.
- [HKMW03] Michael Hsieh, Julia Kempe, Simon Myrgren, and K. Birgitta Whaley. An explicit universal gate-set for exchange-only quantum computation. *Quantum Information Processing*, 2(4):289–307, 2003.
- [Kem03] J. Kempe. Discrete quantum walks hit exponentially faster. In *RANDOM-APPROX 2003*, Lecture Notes in Computer Science, pages 354–369, Heidelberg, 2003. Springer.
- [Kem05] Julia Kempe. Discrete quantum walks hit exponentially faster. *Probability Theory and Related Fields*, 2005. to appear.

- [KK04] Joshua van Korff and Julia Kempe. Quantum advantage in transmitting a permutation. *Phys. Rev. Lett.*, 93(26):260502, 2004.
- [KKR04] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local hamiltonian problem. In *Proc. of 24th FSTTCS*, pages 372–383, 2004.
- [KS05] Julia Kempe and Aner Shalev. The hidden subgroup problem and permutation group theory. In *Proc. 16th ACM SODA*, pages 1118–1125. ACM, 2005.
- [LM04] S. Laplante and F. Magniez. Lower bounds for randomized and quantum query complexity using Kolmogorov arguments. In *Proceedings of 19th IEEE Conference on Computational Complexity*, pages 214–304, 2004.
- [MSS05] F. Magniez, M. Santha, and M. Szegedy. Quantum algorithms for the triangle problem. In *Proceedings of 16th ACM-SIAM Symposium on Discrete Algorithms*. ACM, 2005.
- [OP04] H. Ollivier and P. Pajot. La décohérence, espoir du calcul quantique, 2004.
- [OPZ04a] H. Ollivier, D. Poulin, and W. H. Zurek. Environment as a witness: Selective proliferation of information and emergence of objectivity, 2004.
- [OPZ04b] H. Ollivier, D. Poulin, and W. H. Zurek. Objective properties from subjective quantum states: Environment as a witness. *Phys. Rev. Lett.*, 93:220401, 2004.
- [OT03] H. Ollivier and J.-P. Tillich. Description of a quantum convolutional code. *Phys. Rev. Lett.*, 91(17):177902, 2003.
- [OT04] H. Ollivier and J.-P. Tillich. Quantum convolutional codes: fundamentals, 2004. quant-ph/0401134.
- [PBKLO04] D. Poulin, R. Blume-Kohout, R. Laflamme, and H. Ollivier. Exponential speed-up with a single bit of quantum information: Measuring the fidelity decay. *Phys. Rev. Lett.*, 2004.
- [SS04] Miklos Santha and Mario Szegedy. Quantum and classical query complexities of local search are polynomially related. In *Proc. of 36th STOC*, pages 494–501, 2004.