Rapport final du projet “Réseaux Quantiques” de l’ACI “Sécurité Informatique” numero 03 510

September 7, 2006

1 Summary of Achievements

The aim of this project was 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 54 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 in 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 reposible), 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 and of quantum routing and in particular quantum walks we have been able to even surpass the goals we have set in this project.

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 was shared between INRIA and LRI. In addition to valuable exchange on previous projects we have been working on common research projects. The most notable one is 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.

Some of our efforts have been aimed at the dissemination of our results at large, at organizing a conference (co-sponsored by this ACI) and a workshop and giving public lectures, and will be reported in Section 5.

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. We have described current progress and obstacles in a recent survey in [Kem06a].

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).

In this framework we have also constructed new stabilizer codes obtained by interleaved serial concatenation of two quantum convolutional codes [OT05a]. Our results show that they are the quantum analog of serial turbo-codes.

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 [COT05a, COT05b], 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.

One of our goals in this project was the construction 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 [OT05b]. Trellises play an important theoretical and practical role for classical codes. Their main utility is to devise complexity-efficient error estimation algorithms. This naturally leads to iterative decoding when two convolutional codes are concatenated. Our 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 described trellis representations for quantum stabilizer codes and showed that they share the same properties as their classical analogs. In particular, for any stabilizer code it is possible to find a minimal trellis representation.

In addition to our work on quantum convolutional codes we have studied another aspect of quantum codes in [FKSS06]. We have introduced a dynamical systems approach to study the noise correction behavior of concatenated quantum codes. To this end we have specified a concatentation 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. We have also devised a new encoding in the setting of superconducting qubits that protects against the most predominant errors, coupling errors [SVB$^+$05].

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 aplications 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.

Another surprising application of quantum walks is the problem of testing group commutativity. In [MN05, MN06] we give a quantum walk based algorithm for this problem. We construct a quite optimal quantum algorithm for this problem whose complexity is in $O(k^{2/3})$, where k is the number of generators of the group. The algorithm uses and highlights the power of quantum walks.

In a further application of quantum walks we studied problems in [BDKL06] computational geometry, like problems on polygons. Using the quantum walk search paradigm we get better algorithms for a set of such problems.

Since the introduction of the quantum walk search algorithm (Shenvi, Kempe, Whaley, 2003) several ways have been found to generalize this paradigm, depending on the specifics of the problem to be solved. In a recent work we have generalized and unified these approaches. We have developed a new method for designing quantum search algorithms for finding a “marked” element in the state space of a classical Markov chain, by using a mixture of quantum walk and amplitude amplification [MNRS06].

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.

Next, we have studied quantum algorithms for graph problems in [DHHM04, DHHM06]. 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.

4 Other projects

Self-testing: Apart from building robust quantum architectures, experimentalists have to face another, and possibly as challenging, problem: debugging. Indeed, as experimental prototypes are able to deal with increasing number of qubits (11 for liquid state NMR), it becomes more and more difficult to ensure that gates act properly when they are used inside a computation. Namely, quantum gates are usually tested and calibrated outside the computing environment. Only later are they inserted at their proper location in the computation. It is customary to assume that the behavior of the gate is the same in both situations, but this is obviously an oversimplification. In fact a major task for an experimentalist working on small scale quantum information processing is precisely to assemble different elements that are known to work in separate contexts in order to produce a new experimental scheme that performs well despite the increase of complexity and the change of context. A possible answer to the problem of debugging a quantum computer is to rely on the notion of self-testing. Self-testers are required to treat the program as a black-box. The tester must be independent of the way the program works internally and can only exploit the input-output relationship of the program, not its internal structure.

In [MMMO06] we give a fully consistent and autonomous procedure for ascertaining that a quantum computer is performing a specified computation, by combining some previously presented approaches to self-testing, namely testing of *sources* of quantum states and testing of quantum *circuits*. We achieve this by starting from certified sources of entangled qubits and measurement devices, and using sets of experimental equations to define quantum gates, together with remote state preparation. This gives a consistent procedure to test a full quantum computation.

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 [OPZ04, OPZ05, 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.

Quantum 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 (see [KLM06] for a recent popular science survey and [Kem06b, Kem06c] for an introduction). 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. This has led us to pose a new question in permutation group theory, which we have answered in [KPS06].

On another algorithmic line we have further studied quantum amplitude amplification as an algorithmic tool. We presented several applications of quantum amplitude amplification for deciding whether all elements in the image of a given function are distinct, for finding an intersection of two sorted tables and for finding a triangle in a graph [BDH$^+$05].

Quantum Communication: Nodes in a network communicate over channels and we have studied several aspects of this quantum communication. To begin with, 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 $e = 2.718...$).

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 or relations. We settle this question in [GKW04, GKRdW06a, GKRdW06b] and exhibit a relation for which this is not true, and where in fact the quantum protocol requires exponentially more communication than the classical protocol with public coins. In [GKW04] we first did this in the zero-error setting. In [GKRdW06a, GKRdW06b] we generalized this to the bounded error model. We also show a separation for a different set of resources: the two parties could share quantum entanglement. It was not known whether this shared entanglement can be of any advantage when the two parties do not communicate directly, as is the case in the simultaneous message passing model. In [GKRdW06a, GKRdW06b] we show, that there are relations, which can be computed by the referee efficiently if the two parties share entanglement (but send only classical messages to the referee), whereas without entanglement the messages need to be exponentially longer *even if* the messages can be quantum.

In a more recent work [GKdW06b] we have studied the power of quantum messages in the simultaneous message passing model, more precisely the power of sending a certain message, called fingerprint, several times. Quantum fingerprints have been very successful to decrease the message length exponentially in the simultaneous message passing model for several functions. We give a connection between a well studied problem in computational learning theory, the problem of finding good embeddings of concept classes into half spaces, and finding good fingerprints. This connection allowed us to give several new bounds and to characterize the power of the quantum fingerprinting technique in this model.

Several of the separations mentioned above are only given in terms of a (multi-valued) relation, not a function, and it has been an open question whether similar separations hold for a Boolean function. In a very recent work [GKdW06a] we give a separation for a *function* between one way quantum communication and classical randomized communication.

We have also studied another aspect of quantum communication, namely the capacity of quantum channels. Gaussian quantum channels have recently attracted a growing interest, since they may lead to a tractable approach to the generally hard problem of evaluating quantum channel capacities. However, the analysis performed so far has always been restricted to memoryless channels. In [CCMR05, CCRM06] we considered the case of a bosonic Gaussian channel with memory, and showed that the classical capacity can be significantly enhanced by employing entangled input symbols instead of product symbols.

Another subfield of our study has focused on quantifying the power of an entangled pair of quantum systems (which can be at the two ends of a communication channel). Since John Bell's seminal work it is known that quantum correlations cannot be simulated with local hidden variables. However, it has also been known that quantum correlations exhibited by a maximally entangled qubit pair can be simulated with the help of shared randomness, when supplemented with additional resources, such as communication, post-selection or non-local boxes. Several recent works have attempted to quantify the supplementary resources necessary for this simulation. For instance, in the case of projective measurements, it is possible to solve this problem with protocols using one bit of communication or making one use of a non-local box. We show in [DLR05, DR05] that this problem reduces to a distributed sampling problem. We give a new method to obtain samples from a biased distribution, starting with shared random variables following a uniform distribution, and use it to build distributed sampling protocols. This approach allows us to derive, in a simpler and unified way, many existing protocols for projective measurements, and extend them to positive operator value measurements. Moreover, this approach naturally leads to a local hidden variable model for Werner states. Recently we extended our approach to higher dimensional quantum systems [DLR06].

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 [ADK$^+$04, ADK$^+$06] 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. This result opens the possibility to implement a quantum computation adiabatically, with particles on a grid. There is some evidence, that a computation in this fashion is more robust to noise and decoherence. Unfortunately, very little analytical results are known today about the behavior of these Hamiltonian algorithms in the presence of noise. In [RC05] we performed a fully analytical study of the resistance to noise of these algorithms using perturbation theory combined with a theoretical noise model based on random matrices drawn from the Gaussian orthogonal ensemble, whose elements vary in time and form a stationary random process. Our general result is that the Hamiltonian algorithms are resistant to noise in this model, i.e., the error probability does not increase with increasing problem sizes as long as the cutoff frequency of the noise is either very high or very low with respect to the inverse of the characteristic time scale of the system.

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, KKR06]. 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.

Another complexity class we have studied is the class PPAD. We have focused on one of its most prominent members, and studied the quantum complexity of Sperner's Lemma in [FISV05, FISV06]. Among other things we show that quantum and classical randomized complexity for this problem are quadratically related.

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, also expanded in [Lap06]. Following this we have scrutinized in [LLS05] one of the known quantum lower bound methods, the quantum adversary method, and have shown that the quantities that appear in this method can also be used to derive lower bounds for formulas in classical complexity theory, giving a surprising new link between the two.

5 Outreach within and outside the scientific community

5.1 Organization of QIP'06

In January 2006 the quantum group at LRI organized the ninth annual conference on Quantum Information Processing (QIP'06). The ACI Sécurité Informatique sponsored this conference with 3000 Euros. This conference brought 250 participants, among them the leaders of the field of quantum information, to Paris.

The QIP conference series is the most prestigious conference in quantum computation attended by more than 200 participants from all the prominent research labs around the world, where the top researchers in the field present their most recent and exciting results. The conference is headed by a steering committee consisting of leading names in the field.

The areas covered by the conference include

- Quantum algorithms and complexity
- Quantum communication
- Quantum cryptography
- Quantum information theory
- Error-correcting codes
- Robust and scalable implementation models

It as held with great success from January 16-20, 2006 at the Carré de Sciences and gave a great visibility to the computer science and quantum community in France and at LRI and INRIA in particular, as well as to the ACI Sécurité Informatique.

5.2 Quantum semester at the Poincare Institute

The LRI group, and in particular Miklos Santha, was co-organizing the trimester "Information Quantique" from January 4 to April 7, 2006. This event brought to Paris several of the leading experts in quantum information, who gave long or short lecture series on various subtopics.

5.3 Contributions to books, lecture series, summer schools and popular science

We have succeeded to represent various aspects of quantum information theory and of the work performed in the framework of this ACI outside the specialized community and to a wider audience.

Two articles in *La Recherche:* In particular we have published two articles in *La Recherche.* In 2004 we authored the article *"La décohérence, espoir du calcul quantique"* (H. Ollivier and P. Pajot, *La Recherche* 378, p. 34 [OP04]) describing results on decoherence, and recently we wrote the leading article of the June 2006 volume, *"Comment calculer quantique"* (J. Kempe, S. Laplante and F. Magniez, *La Recherche 398*, pp. 30–37 [KLM06]), describing progress in quantum algorithms.

Book chapters and lecture notes: We have contributed to two books, Whiley's *Lecture Notes in Quantum Information*, a textbook at the graduate level, with the chapter "Quantum Algorithms" (J. Kempe [Kem06b]) and Birkhäuser's *Decoherence*, part of the *Lecture Notes in Mathematical Physics* series with the chapter "Approaches to quantum error correction" (J. Kempe [Kem06a]). We have also contributed with a set of Lecture Notes on "Quantum Algorithms" (J. Kempe [Kem06c]) that where used at the Summer School on Theory and Technology in Quantum Information, Communication, Computation and Cryptography, at the ITP in Trieste in June 2006, where J. Kempe was lecturing on this topic.

Summer Schools and Public Lecture Series: Several of the members of this projects have been invited to lecture in Summer Schools on aspects of quantum information. In particular in 2005 at the 33rd Theoretical Computer Science Spring School on Computational Complexity in Montagnac-les-truffes, Ch. Durr and F. Magniez lectured on ”Basic algorithms in quantum computation”, and S. Laplante talked about ”Lower bounds in quantum computation”. In 2006 at the Summer School on Theory and Technology in Quantum Information, Communication, Computation and Cryptography, at the ITP in Trieste, J. Kempe talked about ”Quantum algorithms”.

In November 2005 J. Kempe was invited to present in the Bourbaphy lecture series at the Institute Poincare on ”Approaches to Quantum Error Correction”. In March, S. Laplante was invited to give the popularization of science lecture for Université Paris-Sud, ”La Science de l’extrème”.

Strategic report: We have contributed to the document Quantum Information Processing and Communication: Strategic report on current status, visions and goals for research in Europe, which has been recently published in electronic form at the website of FET (the Future and Emerging Technologies Unit of the Directorate General Information Society of the European Commission, http://www.cordis.lu/ist/fet/qipc-sr.htm). In an excerpt publication [ZBB$^+$05] we contribute to the assessment of the state of the art in all relevant quantum information processing subfields.

References

[ADK$^+$04] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. 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.

[ADK$^+$06] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Adiabatic quantum computation is equivalent to standard quantum computation. *SIAM Journal of Computing*, 2006. to appear.

[AKR05] A. Ambainis, J. Kempe, and A. Rivosh. Coins make quantum walks faster. In *Proc. 16th ACM-SODA*, pages 1099–1108. ACM, 2005.

[BDH$^+$05] H. Buhrman, C. Dürr, M. Heiligman, P. Høyer, F. Magniez, M. Santha, and R. de Wolf. Quantum algorithms for element distinctness. *SIAM Journal of Computing*, 34(6):1324–1330, 2005.

[BDKL06] A. Bahadur, Ch. Durr, R. Kulkarni, and T. Lafaye. Quantum query complexity in computational geometry. In *Proc. of the Conference on Quantum Information and Computation IV*. The International Society for Optical Engineering (SPIE), 2006.

[CCMR05] N. J. Cerf, J. Clavareau, C. Macchiavello, and J. Roland. Quantum entanglement enhances the capacity of bosonic channels with memory. *Physical Review A*, 72:042330, 2005.

[CCRM06] N. J. Cerf, J. Clavareau, J. Roland, and C. Macchiavello. Information transmission via entangled quantum states in Gaussian channels with memory. *International*

Journal of Quantum Information, 4(3):439–452, 2006. Proceedings of the International Workshop "Quantum Entanglement in Physical and Information Sciences" (December 14–18, 2004, Pisa, Italy). e-print quant-ph/0508197.

[COT05a] T. Camara, H. Ollivier, and J.-P. Tillich. Constructions and performance of classes of quantum ldpc codes, 2005. quant-ph/0502086.

[COT05b] T. Camara, H. Ollivier, and J.-P. Tillich. Constructions of quantum LDPC codes. In *Proc. of EQUIS'05, ERATO conference on quantum information science*, 2005.

[DHHM04] Ch. Durr, M. Heiligman, P. Hoyer, and M. Mhalla. Quantum query complexity of some graph problems. In *Proc. 31st ICALP*, pages 481–493, 2004.

[DHHM06] C. Dürr, M. Heiligman, P. Høyer, and M. Mhalla. Quantum query complexity of some graph problems. *SIAM J. Comput.*, 35(6):1310–1328, 2006.

[DLR05] J. Degorre, S. Laplante, and J. Roland. Simulating quantum correlations as a distributed sampling problem. *Physical Review A*, 72:062314, 2005.

[DLR06] J. Degorre, S. Laplante, and J. Roland. Simulation of bipartite qudit correlations, 2006. e-print quant-ph/0608064.

[DR05] J. Degorre and J. Roland. An intuitive approach for the simulation of quantum correlations. In *26th Symposium on Information Theory in the Benelux*, 2005.

[FISV05] K. Friedl, G. Ivanyos, M. Santha, and Y. F. Verhoeven. On the black-box complexity of sperner's lemma. In *Proc. of FCT*, pages 245–257, 2005.

[FISV06] K. Friedl, G. Ivanyos, M. Santha, and Y. F. Verhoeven. Locally 2-dimensional sperner problems complete for the polynomial parity argument classes. In *Proc. of CIAC*, pages 380–391, 2006.

[FKSS06] J. Fern, J. Kempe, S. Simic, and S. Sastry. Fault-tolerant quantum computation - a dynamical systems approach. *IEEE Transactions on Automated Control*, 51(3):448–459, 2006.

[GKdW06a] D. Gavinsky, J. Kempe, and R. de Wolf. Exponential separation of quantum and classical one-way communication complexity for a boolean function, 2006. quant-ph/0607174, ECCC TR06-086.

[GKdW06b] D. Gavinsky, J. Kempe, and R. de Wolf. Strength and weaknesses of quantum fingerprinting. In *Proc. 21st IEEE CCC*, pages 288–295. IEEE, 2006.

[GKRdW06a] D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf. Bounded-error quantum state identification and exponential separations in communication complexity. In *Proc. 38th STOC*, pages 594–603. ACM, 2006.

[GKRdW06b] D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf. Bounded-error quantum state identification and exponential separations in communication complexity. *SIAM Journal of Computing*, 2006. invited to special issue dedicated to STOC'06 selected papers, submitted.

[GKW04] D. Gavinsky, J. Kempe, and R. de Wolf. Quantum communication cannot simulate a public coin, 2004. quant-ph/0411051.

[HKMW03] M. Hsieh, J. Kempe, S. Myrgren, and K. B. 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*, 133(2):215–235, 2005.

[Kem06a] Julia Kempe. Approaches to quantum error correction, 2006. bookchapter, Decoherence, Progress in Mathematical Physics series, Birhäuser, to appear.

[Kem06b] Julia Kempe. Quantum algorithms, 2006. bookchapter in Lecture Notes on Quantum Information, Whiley-VCH, to appear.

[Kem06c] Julia Kempe. Quantum algorithms, 2006. Lecture Notes, Summer School and Workshop on Theory and Technology in Quantum Information, Communication, Computation and Cryptography, ITP, Trieste.

[KK04] J. von Korff and J. 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.

[KKR06] J. Kempe, A. Kitaev, and O. Regev. The Complexity of the Local Hamiltonian Problem. *SIAM Journal of Computing*, 35(5):1070–1097, 2006.

[KLM06] J. Kempe, S. Laplante, and F. Magniez. Comment calculer quantique. *La Recherche*, 398:30–37, June 2006.

[KPS06] J. Kempe, L. Pyber, and A. Shalev. Permutation groups, minimal degrees and quantum computing, 2006. `quant-ph/0406046`.

[KS05] J. Kempe and A. Shalev. The hidden subgroup problem and permutation group theory. In *Proc. 16th ACM-SODA*, pages 1118–1125. ACM, 2005.

[Lap06] S. Laplante. Lower bounds using Kolmogorov complexity. In *Proceedings of CiE'06*, pages 297–306, 2006.

[LLS05] S. Laplante, T. Lee, and M. Szegedi. The quantum adversary method and formula size lower bounds. In *Proc. of 20th IEEE Conference on Computational Complexity*, pages 76–90. IEEE, 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.

[MMMO06] F. Magniez, D. Mayer, M. Mosca, and H. Ollivier. Self-testing of quantum circuits. In *Proceedings of 33rd ICALP*, Lecture Notes in Computer Science, pages 72–83. Springer Verlag, 2006.

[MN05] F. Magniez and A. Nayak. Quantum complexity of testing group commutativity. In *Proceedings of 32nd International Colloquium on Automata, Languages and Programming*, volume 1770 of *Lecture Notes in Computer Science*, pages 1312–1324. Springer Verlag, 2005.

[MN06] F. Magniez and A. Nayak. Quantum complexity of testing group commutativity. *Algorithmica*, 2006. To appear.

[MNRS06] F. Magniez, A. Nayak, J. Roland, and M. Santha. Search via quantum walk, 2006. quant-ph/0608026.

[MSS05] F. Magniez, M. Santha, and M. Szegedy. Quantum algorithms for the triangle problem. In *Proceedings of 16th ACM-SIAM Symposium on Discrete Algorithms*, pages 1109–1117. ACM, 2005.

[OP04] H. Ollivier and P. Pajot. La décohérence, espoir du calcul quantique. *La Recherche*, 378:34, 2004.

[OPZ04] H. Ollivier, D. Poulin, and W. H. Zurek. Objective properties from subjective quantum states: Environment as a witness. *Phys. Rev. Lett.*, 93:220401, 2004.

[OPZ05] H. Ollivier, D. Poulin, and W. H. Zurek. Environment as a witness: Selective proliferation of information and emergence of objectivity. *Phys. Rev. A*, 72:042113, 2005.

[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.

[OT05a] H. Ollivier and J.-P. Tillich. Interleaved serial concatenation of quantum convolutional codes: gate implementation and iterative error estimation algorithm. In *Proceedings of the 26th Symposium on Information Theory in the Benelux*, page 149, Brussels, Belgium, 2005.

[OT05b] H. Ollivier and J.-P. Tillich. Trellises for stabilizer codes: definition and uses, 2005. quant-ph/0512041.

[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.

[RC05] J. Roland and N. J. Cerf. Noise resistance of adiabatic quantum computation using random matrix theory. *Physical Review A*, 71:032330, 2005.

[SS04] M. Santha and M. Szegedy. Quantum and classical query complexities of local search are polynomially related. In *Proc. of 36th STOC*, pages 494–501, 2004.

[SVB+05] M. Storcz, J. Vala, K. Brown, J. Kempe, F.K. Wilhelm, and K.B. Whaley. Full protection of superconducting qubit systems from coupling errors. *Phys. Rev. B*, 72:064511, 2005.

[ZBB+05] P. Zoller, Th. Beth, D. Binosi, R. Blatt, H. Briegel, D. Bruss, T. Calarco, J.I. Cirac, D. Deutsch, J. Eisert, A. Ekert, C. Fabre, N. Gisin, P. Grangier, M. Grassl, S. Haroche, A. Imamoglu, A. Karlson, J. Kempe, L. Kouwenhoven, S. Kröll, G. Leuchs, M. Lewenstein, D. Loss, N. Lutkenhaus, S. Massar, J.E. Mooij, M.B. Plenio, E. Polzik, S. Popescu, G. Rempe, A. Sergienko, D. Suter, J. Twamley, G. Wendin, R. Werner, A. Winter, J. Wrachtrup, and A. Zeilinger. Quantum information processing and communication. *Eur. Phys. J. D*, 36:203–228, 2005.