



2/ Algo

Algorithms and Complexity



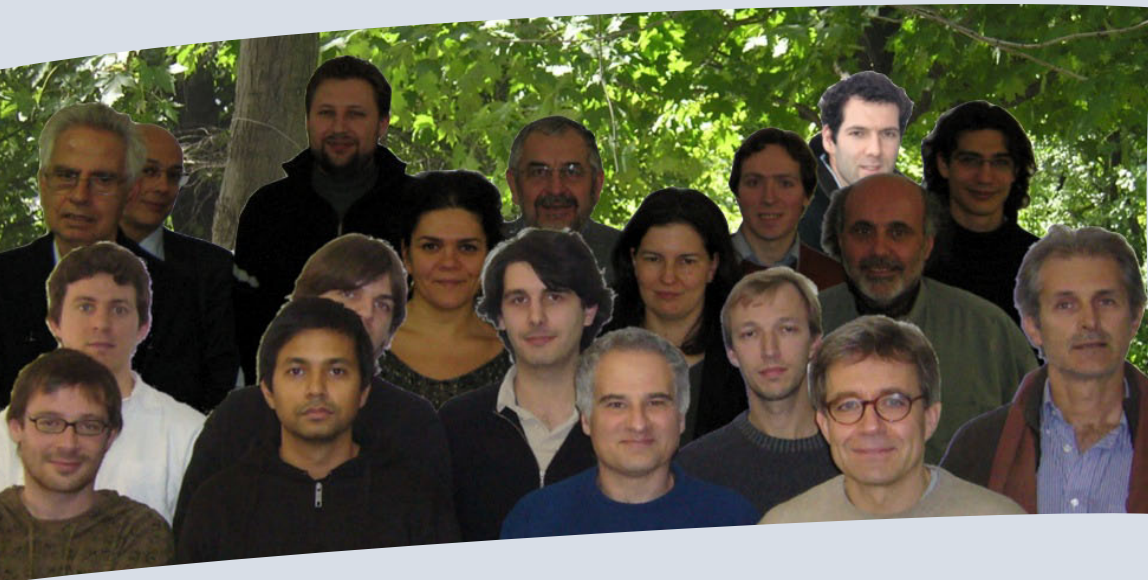
équipe Algorithmique et Complexité

Responsable: Miklos Santha

Les champs des travaux de recherche de notre équipe se concentrent sur des domaines de l'informatique théorique fort compétitifs. La théorie des algorithmes efficaces est la base commune aux axes que nous avons fortement développés : complexité, combinatoire et calcul quantique. L'excellence scientifique est, et restera, l'objectif principal de notre recherche. Les 145 publications, dont nombreuses dans des revues et journaux prestigieux (FOCS, STOC, ICALP, SODA, PODC, FPSAC; SICOMP, Algorithmica, Discrete Mathematics), témoignent que nous avons (au moins en partie) réussi. Nous sommes également fiers des distinctions reçues par les membres de notre équipe (Bourse de réintégration Marie-Curie, Médaille de bronze du CNRS, Prix Irène Joliot-Curie, excellent classement à l'issue de l'appel ERC "Jeunes Chercheurs").

Notre groupe est dynamique : au cours des quatre dernières années six personnes nous ont rejoint, et trois sont parties. Avec treize membres permanents nous sommes actuellement près de notre taille historiquement la plus élevée. Les mouvements ont essentiellement concerné le personnel CNRS. Cinq des six nouveaux membres, Sylvie Corteel, Iordanis Kerenidis, Pascal Ochem, Adi Rosén and Nisheeth Vishnoi sont des chercheurs CNRS, le sixième, Francesca Fiorenzi est enseignante-chercheuse. Christophe Dürr a quitté notre équipe pour devenir chercheur CNRS, et Julia Kempe est en détachement du CNRS à l'Université de Tel Aviv. Nous remercions ici notre collègue et ami, Wenceslas Fernandez de la Vega qui a pris sa retraite du CNRS en 2006. C'était un grand honneur pour nous de travailler avec lui durant toutes ces années. Nous regrettons qu'il n'ait pas pu garder son activité au CNRS plus longtemps, mais nous nous réjouissons, qu'en pratique, il est resté avec nous pour le travail et l'amitié.

La recherche théorique est un mélange subtil d'engagement solitaire et de travail d'équipe coopératif. Nous essayons de créer un environnement scientifique et social qui encourage l'interaction et la communication, afin que chacun puisse exprimer le meilleur de soi.



Algorithms and Complexity

Head: Miklos Santha

Our team's research work is concentrated on several highly competitive fields in theoretical computer science. The theory of efficient algorithms is the common ground that brings together the research directions investigated in depth: complexity, combinatorics and quantum computing. Scientific excellence is, and will remain, our main goal in research. That we (at least partially) succeeded, is witnessed by the 145 publications, including numerous papers in prestigious conferences (FOCS, STOC, ICALP, SODA, PODC, FPSAC) and journals (SICOMP, Journal of Algorithms, Discrete Mathematics). We are also proud of the distinctions (Marie Curie Reintegration Grant, CNRS Bronze Medal, Irène Joliot-Curie Prize, excellent ranking at the ERC Starting Grant) that our team members have received.

Our group is dynamic: in the last four years six persons joined us, and three people left. With thirteen permanent members we are currently almost at our historical peak size. Most moves have concerned the CNRS personnel. Of the six new members Sylvie Corteel, Iordanis Kerenidis, Pascal Ochem, Adi Rosén and Nisheeth Vishnoi belong to the CNRS, and our new University personnel is Francesca Fiorenzi. Christophe Dürr left our team to become CNRS researcher, and Julia Kempe is on long leave from the CNRS at Tel-Aviv University. Our special thanks go here to our colleague and friend Wenceslas Fernandez de la Vega who retired from the CNRS in 2006. It was a great honor to work with him during so many years. We regret that he couldn't stay longer with the CNRS, but we are very happy that in practice he remained with us both for the work and the friendship.

Theoretical investigations are a subtle mixture of individual, solitary involvement and cooperative team work. We try to create a scientific and social environment which fosters interaction and communication so that everyone can realize the best of his or her abilities.

Research Group Members

Permanent faculty (1 october 2008)			
<i>Name</i>	<i>First name</i>	<i>Position *</i>	<i>Institution</i>
ALLOUCHE	Jean-Paul	DR1	CNRS
CORTEEL	Sylvie	CR1	CNRS
DE ROUGEMONT	Michel	PR1	PARIS 2
FIORENZI	Francesca	MCF	PARIS 11
GOUYOU-BEAUCHAMPS	Dominique	PR1	PARIS 11
KERENIDIS	Iordanis	CR2	CNRS
LAPLANTE	Sophie	PR2	PARIS 11
MAGNIEZ	Frédéric	CR1	CNRS
MANOUSSAKIS	Yannis	PR1	PARIS 11
OICHEM	Pascal	CR2	CNRS
ROSEN	Adi	DR2	CNRS
SANTHA	Miklos	DR1	CNRS
VISHNOI	Nisheeth	CR1	CNRS

Doctoral students (1 october 2008)			
<i>Name</i>	<i>First name</i>	<i>Position *</i>	<i>Institution</i>
BOROZAN	Valentin	A	PARIS 11
CHAILLOUX	André	ENS	PARIS 11
HEMON	Sébastien	A	PARIS 11
JOSUAT-VERGES	Matthieu	AC	PARIS 11
KAPLAN	Marc	A	PARIS 11
LE BRETON	Xavier	AC	PARIS 11
MAGNIN	Loïck	ENS	PARIS 11
MENDY	Gervais	Grant	PARIS 11
OULD ABDELLAHI	Sidi Mohamed	Grant	PARIS 11
SANSELMÉ	Luc	AC	PARIS 11
TRACOL	Mathieu	AMX	PARIS 11
VIEILLERIBIERE	Adrien	AM	PARIS 11

Temporary personnel (2005-2008)					
<i>Name</i>	<i>First name</i>	<i>Position *</i>	<i>Institution</i>	<i>Arrival</i>	<i>Departure</i>
DAH	Mohamed Yahya	Post-doc	PARIS 11	10.2006	10.2007
DAS	Kinkar Chan- dra	Post-doc	PARIS 11	10.2005	10.2006
LEE	Troy	Post-doc	Netherlands	07.2006	07.2006
MARTINHON	Carlos	Post-doc	BraziPaul	09.2005	03.2007
MOSHE	Yossi	Post-doc	EGIDE	10.2005	10.2006
RICHTER	Peter	Post-doc	PARIS 11	10.2007	
SADYKOV	Ruslan	Post-doc	CNRS	09.2007	

Visitors for 3 months or more (2005-2008)					
<i>Name</i>	<i>First name</i>	<i>Position *</i>	<i>Institution</i>	<i>Arrival</i>	<i>Departure</i>
SKORDEV	Guentcho	PI	CNRS	10.2007	
HITCZENKO	Pawel	PI		09.2006	09.2007

* See the glossary for the acronyms.

Group evolution

Our team has changed quite substantially in the past 4 years; most moves concerned CNRS personnel. Adi Rosén (DR), Iordanis Kerenidis (CR), Pascal Ochem (CR) and Nisheeth Vishnoi (CR) were respectively hired in October 2005, January 2006, October 2007 and October 2009. Sylvie Corteel (CR) arrived at LRI in January 2006 by "mutation". Wenceslas Fernandez de la Vega (CR), our distinguished colleague, retired in June 2006. We are very grateful to him for the many years he shared with us. Finally, Julia Kempe (CR) is on "détachement" since April 2007 at Tel-Aviv University.

Among the University personnel, Christoph Dürr left our team in October 2005 and became CR CNRS at LIX. Francesca Fiorenzi joined us in October 2006 as a Maître de Conférences, and Sophie Laplante was promoted to Professor in October 2006.

2/ Algo

Highlights

Our research has appeared in the most prestigious conferences (for example FOCS, STOC, ICALP, STACS, SODA, SPAA, PODC, FPSAC) and journals (SICOMP, Algorithmica, Discrete Mathematics) in Computer Science. Furthermore, we have given numerous invited talks at national and international conferences. We have also disseminated our work by writing popular articles for the magazine "La Recherche" and by giving talks to large audiences of non-specialists.

Over the past 4 years, members of the team have served on numerous program committees of international scientific conferences. They have also organized several international scientific events, including the Bertinoro Workshop on Adversarial Modeling and Analysis of Communication Networks in 2006, and the International Combinatorics, Geometry and Computer Science Conference at the CIRM, Luminy in 2007. In January 2006 we organised the 8th Workshop on Quantum Information Processing (QIP) in Paris, the most important annual meeting in the area. Following this conference, in Spring 2006 we organised a special trimester on "Quantum Information, Computation and Complexity", at the Institut Henri Poincaré, with the participation of most of the best researchers in the field. During the trimester, we gave 24 series of lectures (6-12 hours each) on various subjects that were followed by attended 120 participants.

During the past few years our group has solidified and expanded its position as a leading institution at the national and international level in several aspects of algorithmic, combinatorics, and in quantum computation. In France, we serve on the steering committee of the GdR "Information et Communication Quantique", we are responsible for the GT "Informatique Quantique", and member of the GdR "Informatique Mathématique". We have also been awarded several grants by the Agence National de la Recherche and the CNRS on the topics of probabilistic and quantum algorithms, verification, and combinatorics. Moreover, we teach several courses, on probabilistic algorithms, on combinatorics and on quantum computation and information at the Master Parisien de Recherche en Informatique (MPRI). We also teach courses on similar subjects at the Ecole Polytechnique and at the ENSTA. At the European level, we serve in the steering committee of STACS and FCT, and are members of the largest European projects on quantum com-

putation, including Integrated Projects from the 5th and 6th Framework. We are also responsible for bilateral research projects with Canada, Japan and Hungary, and have close collaborations with research institutes in the United States of America, Canada, India, Japan, Singapore, Austria, Germany, Holland, Hungary, Italy and Israel. We regularly receive a large number of visitors from around the world.

We are especially proud of the individual distinctions awarded to the members of our team. In 2006, Iordanis Kerenidis received a Marie Curie Reintegration Grant on his return to Europe from the United States. In 2006, while she was still at LRI, Julia Kempe received the CNRS Bronze Medal and the Irène Joliot-Curie Prize from the French Ministry of Education and the EADS Foundation for the Young Woman Scientist of the year. In 2007 Sylvie Corteel's application for an ERC Starting Grant was ranked among the top 400 out of more than 9000, and later she received the ANR IComb young researcher individual grant.

Key Publications

- A. Abouelaoualim, K. C. Das, W. F. de la Vega, M. Karpinski, Y. Manoussakis, C. Martinhon, and R. Saad. Cycles and paths in edge-colored graphs with given degrees. *Journal of Graph Theory*, 2009
- J.-P. Allouche, C. Frougny, and K. Hare. On univoque Pisot numbers. *Math. Comp.*, 76:1639–1660, 2007
- S. Corteel and L. K. Williams. A Markov chain on permutations which projects to the PASEP. *Int. Math. Res. Not. IMRN*, (17), 2007. Art. ID rnm055, 27
- M. de Rougemont, E. Fischer, and F. Magniez. Approximate satisfiability and equivalence. In *IEEE Logic in Computer Science*, pages 421–430, 2006
- RD de Wolf, Gavinsky, J. Kempe, I. Kerenidis, and R. Raz. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of 39th ACM STOC*, pages 516–525, 2007. quant-ph/0611209
- S. Laplante, T. Lee, and M. Szegedy. The quantum adversary method and formula size lower bounds. *Computational Complexity, Special Issue on Complexity 2005*, 15(2):163–196, 2006
- F. Magniez, A. Nayak, J. Roland, and M. Santha. Search via quantum walk. In *Proceedings of 39th ACM Symposium on Theory of Computing*, pages 575–584, 2007
- H. Räcke and A. Rosén. Distributed online call control on general networks. In *SODA*, pages 791–800, 2005

2/ Algo

Research Description

The members of the group have worked over the past four years in three main research fields: algorithms, quantum computing and combinatorics. The obtained results have been published in international scientific conferences and journals of the highest level.



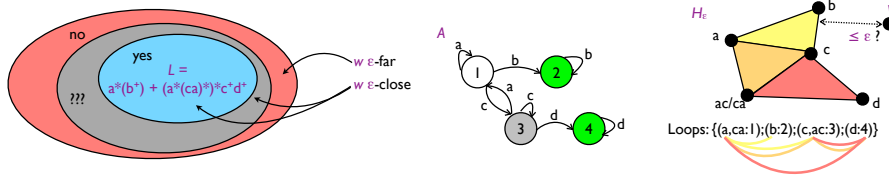


Figure 2.1: Geometric embedding of a regular language for property testing

Algorithms

In the area of algorithms, we have mostly concentrated on the design and analysis of approximation and online algorithms, property testing and algorithmic game theory.

Approximation and online algorithms We have given probabilistic approximation algorithms for various problems. For example, we have given a randomized distributed algorithm for the maximum matching problem on general graphs, both for the unweighted and the weighted versions [115]. Our algorithm is the first to have a logarithmic time complexity (in the size of the graph) and guarantee a constant approximation factor. We have also given the first distributed algorithm for the maintenance of an (approximated) matching in dynamic graphs (where nodes appear and disappear). We have also given algorithms for the scheduling of packets with deadlines. This is a probabilistic approximation algorithm that uses the “classical” method of randomized rounding in a new way, where the proof of correctness uses random variables that given upper bounds on the quantities that have to be bounded (rather than use the quantities themselves). The algorithm has an approximation ratio of $\log^* n$ (where n is the size of the graph) which means that it “practically” has a constant approximation ratio.

Property testing We have defined ϵ -equivalence, an approximate version of the classical notion of equivalence between two structures, built upon the notion of approximation for property testing [94]. By geometric embedding (see Figure 2.1), we have shown that ϵ -equivalence can be efficiently decided in a number of important cases where the exact case is difficult to decide, or even undecidable. The context is that of words and trees with edit-distance with reordering [38]. The ϵ -equivalence of two regular properties on words, defined with monadic formulas of the second order, can be tested in time polynomial in the size of the automaton (or the regular expression), for a fixed ϵ , while the exact version is PSPACE-complete. Our tester extends to infinite regular languages and algebraic grammars. The first extension has a direct application in linear temporal logic (LTL). For algebraic grammars, the tester has exponential complexity, while the exact version is undecidable. Finally, the algebraic grammars are testable, while they are not for the general case of edit distance without reordering. We generalize approximate verification and introduce it to probabilistic systems, and get testers for deciding if the probability that a system verifies a certain property is higher than a certain threshold λ . These testers approximated execution traces by their statistics. It is then natural to approximate a probabilistic system, where the number of states is big, by a statistical representation, as this is done for evolutionary games. One studies if it is possible to approximate properties on long sequences. We have developed a self-tester that does not rely on measurement tools or sources of classical or quantum states, or even on the dimension of the physical system [116]. Thus we can test a whole circuit. This work has both theoretical and practical importance, since it is motivated by the three recent implementations of quantum apparatus based on RMN, for which even classical states are difficult to prepare.

Algorithmic game theory We have considered games with complete information with $r \geq 2$ players, and have studied approximated Nash Equilibria in the additive and multiplicative sense, where the number of pure strategies of each player is n . It is known that no FPTAS exists for this problem, and the main open question is to know if a PTAS exists. One of the main papers of in this subject is by Lipton et al. (EC 2003), but it considered only the case of two players, and additive approximation: it shows how to approximate a known Nash Equilibrium, using strategies with small support, by random sampling according to given strategies. We have extended this results by considering an arbitrary number of players, and have obtained lower bounds on the size of the supports [95].

Quantum computing

In quantum computing, we focused on different but interrelated areas of quantum information and computation. In quantum algorithms, we studied the Hidden Subgroup Problem in depth, one of the most important and difficult problems in quantum computation. We also provided quantum algorithms for several non-abelian cases, including groups with small commutator, groups with large center, extraspecial groups and nil-2 groups [108, 109]. Another interesting algorithmic tool that our team studied is the use of quantum walks for speeding up classical search problems [118, 144].

In quantum complexity, we provided exponential separations between the power of quantum and classical one-way communication complexity [8, 124] (see Sidebar *The power of Quantum communication*). We also studied quantum non-locality as well as the amount of classical and quantum communication, with or without entanglement, required to simulate any non-signaling distribution [22, 23].

Finally, we have been very active in exploring connections between classical and quantum computation, by showing how quantum techniques can be useful in the study of classical complexity theory. In particular, we provided optimal lower bounds for locally decodable error correcting codes by quantum arguments and methods of relating classical circuit and formula size lower bounds to quantum communication complexity and Kolmogorov complexity [114, 35, 36].

Combinatorics

The main lines of research in combinatorics include enumerative combinatorics, combinatorics of words, arithmetical combinatorics, discrete mathematics (and their links to theoretical computer science and to number theory), statistical physics, and algorithmic graph theory. We work on such topics as: Dejean's conjecture [67], repetitions in infinite sequences [61, 3, 45], enumerating discrete plane shapes [121, 120, 29, 12], partitions and their arithmetical and combinatorial properties [13, 68, 71, 70, 105, 63, 15], symbolic dynamics, sofic systems, sand piles, cellular automata [52], automatic sequences, and graphs and colors [90, 25, 42, 43, 41, 24, 136, 44].

Examples of our results in combinatorics include:

We showed that the number of fully packed loop configurations corresponding to a matching with m nested arches is polynomial in m if m is large enough, thus essentially proving two conjectures by Zuber [12]. We studied links between permutation tableaux coming from algebraic geometry and the PASEP model [Par-



Sidebar

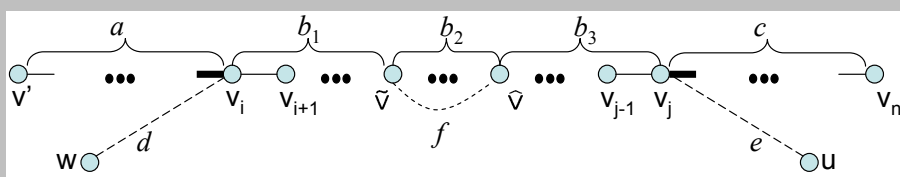
Approximate Distributed Matching

The classical problem of matching is that of finding a pairing in a set of entities (i.e., each entity can participate in at most one pair), with the aim of maximizing some objective function. Two classical objective functions are the number of pairs (when not every pair is possible), or the sum of values attributed to each possible pair. This problem is naturally modeled by an unweighted or weighted graph.

In the distributed setting an algorithm has to solve this problem in a distributed manner, where initially each node only knows its adjacent edges. The question is in fact if the problem can be solved optimally, or approximated well, with only relatively local information for each node (i.e., quickly, without communicating the whole input to all nodes).

We give probabilistic distributed algorithms to approximate weighted matching on general graphs [115]. For every $\epsilon > 0$, our algorithms guarantee an expected approximation ratio of $4 + \epsilon$ and have (deterministic) running time (number of communication rounds) of $O(\epsilon^{-1} \log \epsilon^{-1} \log n)$, where n is the number of nodes in the graph.

These are the first distributed algorithms for the problem that run in logarithmic time and guarantee constant approximation ratio. We also consider the model of dynamic graphs, where nodes (with all their incident edges) are inserted and deleted one at a time. We give a distributed algorithm which maintains a $(1 + \epsilon)$ -approximate unweighted matching in $O(1/\epsilon)$ time per insertion or deletion, for any given $\epsilon > 0$. For dynamic weighted graphs we give a distributed algorithm that maintains a constant-approximation weighted matching, and runs in constant time per insertion or deletion.



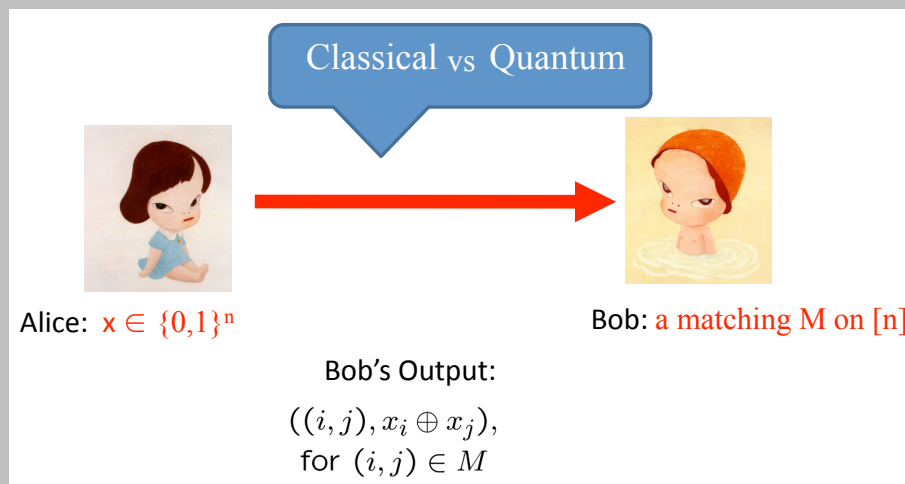
Schematic representation of one (of 4) cases for the analysis of the distributed approximation algorithm for matching on dynamic graphs. Thick lines represent the current matching. Node v' is a new node and is added to the matching along an augmenting path connecting v' and v_n .

The power of Quantum Communication

Imagine the scenario where Alice and Bob are spatially separated and communicate over a channel in order to solve the following distributed task. Alice receives for each of n athletes a uniform color, either red or blue. Bob receives a pairing of the athletes in teams of two. Alice doesn't know the teams and Bob doesn't know the color of the athletes' uniforms. The goal is for Bob to output for one team of his choice, whether the uniforms of the two athletes are the same or not. However, only Alice can send messages to Bob. The question is how much communication is necessary?

One can formulate this problem mathematically in the following way: Alice receives an n -bit string x and Bob receives a matching M on the indices from 1 to n . The goal is for Bob to output some edge of the matching $(i, j) \in M$ with the corresponding value $x_i \oplus x_j$ (see Figure below).

This simple task provides a strong proof that quantum communication is much more efficient than classical communication. In a series of works [8, 124], we showed that the necessary communication over classical channels has to be always at least on the order of \sqrt{n} bits, while we provided a protocol that uses quantum communication of only $\log n$ bits. This was the first proof that quantum one-way communication can be exponentially better than the classical one.



Hidden Matching Problem

tially Asymmetric Self Exclusion Process] in statistical physics [74, 9, 73, 16] (see sidebar *The PASEP model*).

We proved combinatorially that the PASEP stationary distribution can be computed by using the generating function of permutation tableaux. We found new applications of a somewhat old combinatorial result about discrete dynamical systems to properties of non-integer numeration bases. We studied arithmetical and algorithmic properties of those bases for which the number 1 admits a unique representation. The methods are both theoretical and computational. In a sequence of papers, we considered the asymptotic minimal frequency of a letter in some infinite sequences with prescribed properties such as avoiding some pattern or repetitions. The continuing algorithmic improvements at obtaining both lower and upper bounds leads to an exact value for some of these frequencies. Most of these known frequencies are, somewhat surprisingly, rational numbers [7, 59, 57, 54]. Finally, we investigated problems in colored graphs motivated by both their theoretical interest and applications in various fields. In particular, we focussed on problems arising in molecular biology that are formulated using colored graphs, that is graphs with colored edges and/or vertices. In these graphs the motivating problems correspond to extracting subgraphs such as Hamiltonian and Eulerian paths or cycles colored in a specified pattern [84, 1].

2/ Algo

Strategic Planning

Original LRI Goals

Much of our work over the past four years falls within LRI's main research challenges.

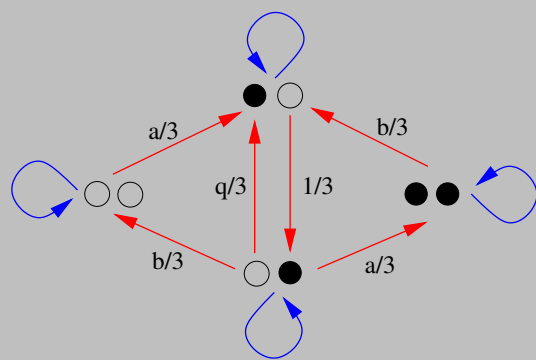
Quantum computation has been put forward as a viable way to overcome current computational limitations. Its goal is to understand the inherent computational power of nature and examine quantum phenomena that appear when the scale of computation reaches the atomic scale. According to Moore's law, in fewer than twenty years, miniaturization will reach a scale at which quantum phenomena prevail. Hence, the study of quantum computation is essential in post-Moore world.

Although quantum computing is a relatively new research area, there have already been numerous very exciting results. Shor's algorithm for factoring large numbers shows that quantum computers are probably more powerful than classical ones, since factoring remains difficult for any classical computer. Moreover, the ability to communicate over quantum channels has made it possible to revisit unconditionally secure cryptography.

Our work on sublinear algorithms has many applications with respect to the *massive data* challenge. The goal is to show that approximation and randomized techniques can lead to efficient and practical algorithms for dealing with very large quantities of data that cannot be stored in (fast) memory for processing, e.g., streaming algorithms. Another direction involves the treatment of large transition systems with a compact representation encountered in software engineering. We have several projects whose objective is to develop software that both scales well and guarantees the quality of the result.

The PASEP model

We are given a one-dimensional lattice of n sites, such that each site i ($1 \leq i \leq n$) is either occupied by a particle or is empty. At most one particle may occupy a given site. During each infinitesimal time interval dt , each particle in the system has a probability dt of jumping to the next site on its right (for particles on sites $1 \leq i < n$) and a probability $q dt$ of jumping to the next site on its left (for particles on sites $1 < i \leq n$). Furthermore, a particle is added at site $i = 1$ with the probability $a dt$ if site 1 is empty and a particle is removed from site n with probability $b dt$ if this site is occupied.



The state diagram of the PASEP model for $n = 2$

The figure above illustrates the four states, with transition probabilities, for the case $n = 2$. Note that the probabilities of the loops are determined from the figure by the fact that the sum of the probabilities on all outgoing arrows from a given state must be 1. We denote a state of the PASEP as a word in $\{o, \bullet\}^n$ where the symbol o (resp. \bullet) denotes the absence (resp. presence) of a particle.

The partially asymmetric exclusion process (PASEP) is an important model from statistical mechanics which describes a system of interacting particles hopping left and right on a one-dimensional lattice of N sites. It is partially asymmetric in the sense that the probability of hopping left is q times the probability of hopping right. The PASEP is regarded as a primitive model for biopolymerization, traffic flow, and formation of shocks; it also appears in a kind of sequence alignment problem in computational biology.

Recall that a *partition* $\lambda = (\lambda_1, \dots, \lambda_k)$ is a weakly decreasing sequence of non-negative integers. The *Young diagram* Y_λ of shape λ is a left-justified diagram of $m = \sum \lambda_i$ boxes, with λ_i boxes in the i -th row. We define a *permutation tableau* T to be a partition λ together with a filing of the boxes of Y_λ with 0's and 1's such that the following properties hold:

1. Each column contains at least one 1.
2. There is no 0 which has a 1 above it in the same column **and** a 1 to its left in the same row.



Sidebar

(continued)

0	1	1	0	0	1	0	1	0	1
1	1	1	1	0	1	1	1	1	
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	1		
0	0	0	1	1					
1	1								

A permutation tableau

The figure above gives an example of a permutation tableau T with $\lambda = (10, 9, 9, 8, 5, 2)$.

It has been observed that the (unique) stationary distribution of the PASEP has remarkable connections to combinatorics – see for example the papers of Derrida, and Duchi and Schaeffer –. We prove that in fact the (normalized) probability of being in a particular state of the PASEP can be viewed as a certain weight generating function for permutation tableaux of a fixed shape. (This result implies the previous combinatorial results.) This proof relies on the matrix ansatz of Derrida et al, and hence does not give an intuitive explanation of why one should expect the steady state distribution of the PASEP to involve such nice combinatorics.

Therefore we also define a Markov chain – which we call the PT chain – on the set of permutation tableaux which projects to the PASEP in a very strong sense. This gives a new proof of the previous result which bypasses the matrix ansatz altogether. Furthermore, via the bijection from permutation tableaux to permutations, the PT chain can also be viewed as a Markov chain on the symmetric group.

Another nice feature of the PT chain is that it possesses a certain symmetry which extends the “particle-hole symmetry” of the PASEP. More specifically, this is a graph-automorphism on the state diagram of the PT chain which is an involution; this has a simple description in terms of permutations.

Much of our research, especially in the area of on-line algorithms, is closely related to the area of *dynamic networks*. We develop algorithms that aim to maximize the performance of networks with limited resources, and provide proof of their performance guarantees.

Self Assessment

The number of graduate students has increased over the last four years: We currently have 12 Ph.D. students and we have supervised Master's theses of several students from the Master of Paris-Sud, as well as from MPRI. Most permanent members of our group with an Habilitation supervise Ph.D. students.

We collaborate with several groups at LRI, in particular BD, BioInfo, ForTeSE, Graphs, and Parall. We expect that most of these collaborations will yield scientific publications.

Relationship to LRI Strategic Plan

Our group is a federation of autonomous researchers. It is well integrated in the international scientific community. The number of high level publications and research grants are witnesses of the high scientific quality of the work of the members of our group. Scientific excellence is and will remain in the future our main and highest aspiration. Nevertheless several common directions are present in the research conducted by the members of our group, and these form the federating factors of our group. We plan on continuing to do research within these areas.

Algorithms

In the area of algorithms we plan to continue our research in approximation and online algorithms, property testing, and algorithmic game theory. Many of the questions to be studied in these area require, or can benefit from, probabilistic approaches. They thus fall within one of the strategic topics defined by the laboratory for the next years: *uncertainty and approximation*.

Approximation and online algorithms We plan to push further our understanding of the power of randomization in approximation and online algorithms. We are, for example, specifically interested in the following problems: (1) improving our previous results on the known approximation ratios for graph partitioning problems (sometimes under certain conditions on the graph) (2) studying streaming algorithms in distributed settings, and giving algorithms for this setting that do not rely on routing paths and (3) improving our previous results on time-constrained scheduling in (linear) networks. We are further interested, in the context of online algorithms, in the question of how can "advice" given to online algorithms improve their competitive ratio.

Property testing In addition to pursuing the direction of our previous works in Property Testing, our goal is to apply ideas and techniques from property testing to the area of Streaming Algorithms, and to work specifically on problems for which the Property Testing approach was studied before. The main motivation is to remove the approximation required by Property Testing, and to adapt the previous testers to Streaming Algorithms. By reading once and sequentially

the entire input with polylogarithmic memory space, we hope to remove the approximation inherent to property testing. If this attempt is unsuccessful, we will keep the same approximation of Property Testing, but we will try to improve the dependency of the approximation parameter, when it is intractable for practical applications.

Algorithmic game theory We intend to investigate how the sampling based techniques for computing approximate additive equilibria of Lipton et al., can be generalized to the multiplicative case. The introduction of the more general McDiarmid's inequality, instead of the more classical Hoeffding's bound, results in a finer analysis, but the exact limitations of the multiplicative case remain open. The study of the convergence of various dynamics towards approximate Nash equilibria, such as the fictitious player, is a promising area. Some specific conditions, such as the ones presented by Chien and Sinclair, are often necessary to prove fast convergence results. Under such hypotheses, we hope to provide a method for the analysis of approximate mechanisms, that is algorithms which guarantee some conditions of an approximate equilibria.

Quantum computing

Quantum computation is the study of quantum phenomena that appear when the scale of computation reaches atomic scale. By Moore's law, current transistors will reach this scale by the year 2020. Therefore, it is essential and urgent to study the power and limitations of computing via quantum systems in order to envision computation well beyond this horizon.

Our first goal is to study the power of quantum algorithms and especially algorithms for the Hidden Subgroup Problem and algorithms which are based on quantum walks. Efficient solutions to some cases of the hidden subgroup problem (HSP), a paradigmatic group theoretical problem, constitute probably the most notable success of quantum computing. Even though this problem is abstract in nature, the most important result in quantum algorithms, Shor's algorithm for factorization and discrete logarithm are special cases thereof.

After settling the abelian case, substantial research was devoted to the Hidden Subgroup Problem in some finite non-abelian groups. Beside being the natural generalization of the abelian case, the interest of this problem is enhanced by the fact, that important algorithmic problems, such as graph isomorphism, can be cast in this framework. Our approach for addressing this task will be twofold. On the one hand, we will try to extend the standard algorithm for the abelian case to non-abelian groups using non-abelian quantum Fourier transforms. This requires finding new implementation techniques for this transform, and the determination of classes of group where the analogue of the standard abelian algorithm is sufficient for solving the HSP. On the other hand, we also try to exploit some limited commutativity properties of the given non-abelian group to reduce the problem to simpler instances. We believe that in order to obtain substantial progress on algorithmic questions, new algorithmic techniques have to be developed. To date, there are only a few such techniques, and most efficient quantum algorithms rely on the quantum Fourier transform.

An important part of our effort will be dedicated to the research into new algorithmic techniques, and in particular we intend to explore quantum walks. A particularly promising algorithmic application of quantum walks is searching, and our group has made several important contributions in this direction. We were the first to point out this potential of quantum walks when we designed a quantum walk based simulation of Grover search. In this context, it is important to continue working on the potential applications of random walks. In particular, we

would like to investigate matrix multiplication, and the complexity of deciding if a binary operation is associative. We would also like to relate quantum walk based search algorithms to the classical hitting time base techniques. In a different direction, we would like to understand better whether quantum walks can be used to generate certain important quantum states. For instance to solve the Graph Isomorphism Problem it would be sufficient to generate a uniform superposition over all permutations of a graph.

Moreover, we would like to study the limitations of quantum computation as well. Even though many problems that are considered hard for classical computers become easy in the presence of quantum computers, there are still many problems that remain intractable even for quantum computers. We plan to continue to study quantum lower bounds, in the quantum query model. Another model we wish to study are time-space tradeoffs. Here, the goal is to see how many more queries are required if the algorithm can only use a limited amount of quantum memory, and vice versa. In quantum complexity, we would like to study the role of quantum vs classical advice and proofs. In particular, we would like to study whether the class of problems solved in quantum polynomial time with quantum advice can be solved with classical advice. Another question we would like to address concerns QMA, the quantum analogue of the class NP. Here, the goal is to prove whether a quantum proof is necessary, or whether a classical proof is sufficient.

In the process of better understanding the power of quantum information not only for computational tasks but also for tasks that require communication and interaction, we would like to investigate the model of communication complexity. Communication complexity is related to circuit lower bounds, data structures, automata and many other areas of theoretical computer science. The model of communication complexity was first defined by Yao, that has found applications in many areas. In this setting, two parties, Alice and Bob, are given some initial inputs and they try to solve a problem that depends on these inputs. Their goal is to compute the answer using the minimum amount of communication. Alternatively, Alice and Bob try to encode the necessary information about their inputs as succinctly as possible. It is very intriguing to study the relation between classical and quantum communication complexity and hence get a better understanding of classical and quantum information

Our objective is to study the relation between classical and quantum communication complexity and hence gain better understanding of classical and quantum information. A number of problems in communication complexity have been already found where quantum protocols need significantly less communication than classical protocols solving the same problem. We would like to continue this line of research and tackle some of the important open questions regarding quantum communication complexity, including separations of classical and quantum communication for total functions and the role of entanglement. Just as the probabilistic method has become an extremely versatile method of proving purely deterministic statements in combinatorics by appealing to probabilistic techniques, we would like to explore the possibility of a general quantum method for applying techniques from quantum information theory to problems in classical complexity theory.

Combinatorics

This group works with a ANR-funded project, “random generation: models, methods and algorithms” (GAMMA). The goal is to develop a set of fundamental methods and algorithms for the random generation of complex combinatorial structures. Such objects appear in a variety of applications, especially in computer science.

Random generation plays an important role in domains dealing with enormous volumes of data, for example in interaction networks (computer, sociological, biological networks); in this case, random generation allows the comparison of models and the evaluation of their adequacy for real data. Random testing and model checking are two additional fields of application for random generation. One of the main issues there arises when choosing appropriate data for testing, and designing efficient methods for fast generation of this data. In many cases the problem can be described in terms of graphs or automata, so that the data are specified as paths, or words. In these cases where intensive generation is required, the samplers have to be very efficient.

A second purpose is to create a strong team at the Université Paris-Sud to study the interactions between combinatorics and other fields, such as number theory, basic hypergeometric series, representation theory, geometry and mathematical physics. We will study these interactions from the perspective of two combinatorial objects that are generalizations of *integer partitions*. The theory of integer partitions is a thrilling field that has been developed primarily in the USA by combinatorialists, algebraists, analysts, and number-theoreticians such as G.E. Andrews, B. Berndt, K. Ono, R. Stanley, J. Lepowsky, their students and many others. A number of strong young researchers in partition theory have recently relocated or returned to Europe. More than ever, the time is now right to begin building a strong European group. For the first time, in 2006 in France, a workshop focusing on partitions in Europe was organized, with 10 speakers and some 20 participants. Over the coming 4 years we shall demonstrate the success of our project by organizing the next editions of this workshop and building it into a regular conference of international stature, reflecting the emerging role of European researchers as leaders in the field.

The two aforementioned generalizations of partitions that will form the focus of our investigations are *permutation tableaux* and *overpartitions*. Permutation tableaux arise from the enumeration of totally positive Grassmann cells in algebraic geometry and they have been recently found to play a key role in certain statistical physics models. Overpartitions come from the combinatorics of basic hypergeometric series and have many connections to number theory, algebra and mathematical physics. We believe that overpartitions are also the most natural objects to study the representation theory of Lie superalgebras. Over the next 4 years we shall demonstrate that much of the classical theory of partitions is part of a broader picture involving these new objects.

We want also to focus on problems in colored graphs. The motivation is both their theoretical interest and applications in various fields. In particular, problems arising in molecular biology are often formulated using colored graphs, i.e. graphs with colored edges and/or vertices. Given such a graph, original problems correspond to extract subgraphs such as Hamiltonian and Eulerian paths or cycles colored in a specified pattern.

Another aim of this group is to define new decidable invariants for shift equivalence of irreducible sofic shifts. Sofic shifts are sets of bi-infinite labels in a labeled graph. If the graph can be chosen strongly connected, the sofic shift is said to be irreducible. A particular subclass of sofic shifts is the class of shifts of finite type, defined by a finite set of forbidden blocks. Two sofic shifts X and Y are conjugate if there is a bijective block map from X onto Y . It is an open question to decide whether two sofic shifts are conjugate, even in the particular case of irreducible shifts of finite type. There are many invariants for conjugacy of shifts, algebraic or combinatorial. For instance the entropy is a combinatorial invariant which gives the complexity of allowed blocks in a shift. The zeta function is another invariant which counts the number of periodic orbits in a shift.

Honors

Prizes and Awards

- S. Corteel, ranked among the top 400 out of more than 9000 for her application for an *2007 ERC Starting Grant*. Later she received the ANR IComb young researcher individual grant.
- J. Kempe, *Prix Irene Joliot-Curie de la jeune femme scientifique*, 2006
- J. Kempe, *Medaille Bronze du CNRS*, 2006
- I. Kerenidis, *Recipient of Marie Curie International Reintegration Grant*, 2006-2008

Keynote Addresses

International

- S. Corteel, *Partitions, q-series and applications*, Penn State (US), 2008
- I. Kerenidis, *Workshop on Quantum Information Processing (QIP)*, MIT, Cambridge (US), 2005
- I. Kerenidis, *1st Athens Colloquium on Algorithms and Complexity (ACAC)*, Athens (Greece), August 2006
- I. Kerenidis, *Workshop "Locally decodable codes, private information retrieval, privacy-preserving data-mining, and public key encryption with special properties"*, Institute for Pure and Applied Mathematics (IPAM), Los Angeles, October 2006
- I. Kerenidis, *International Conference on Information Theoretic Security (ICITS)*, Madrid (Spain), May 2007
- I. Kerenidis, *2nd Athens Colloquium on Algorithms and Complexity (ACAC)*, Athens (Greece), August 2007
- S. Laplante, *Computability in Europe*, Swansea University (UK), 2006
- S. Laplante, *Computability in Europe*, University of Sienna (Italy), 2007
- F. Magniez, *Workshop Advances in Quantum Algorithms*, Waterloo (Canada), June 2007
- F. Magniez, *Dagstuhl Seminar 05291: Sublinear Algorithms*, Dagstuhl (Germany), July 2005
- M. Santha, *Dagstuhl Seminar 05201: Design and Analysis of Randomized and Approximation Algorithms*, Dagstuhl (Germany), May 2005
- M. Santha, *Dagstuhl Seminar 05291: Sublinear Algorithms*, Dagstuhl (Germany), July 2005
- M. Santha, *Workshop on Quantum Computing and Cryptography*, Fields Institute, Toronto (Canada), September 2006
- M. Santha, *5th International Conference on Theory and Applications of Models of Computation (TAMC)*, Xian (China), 2008

France

- I. Kerenidis, *Journées du GdR Informatique Mathématique*, Paris, January 2008
- S. Laplante, *Colloque du GdR Information et communication quantiques*, Paris, October 2008

- F. Magniez, *Journées du GdR Informatique Mathématique*, Paris, January 2007
- M. Santha, *Colloque du GdR Information et communication quantiques*, Paris, October 2008

2/ Algo

Evaluation of Research

Editorial Boards

International

- *Annals of Combinatorics*, Springer: S. Corteel
- *ACM Transactions on Computing Theory*, Springer: S. Laplante
- *Algorithmica* special issue on Quantum Computation (to appear in 2009): F. Magniez
- *IJEB, International Journal on Electronic Business*, Inderscience: M. De Rougemont

Program Committees

Chair

- CGCS, *International Combinatorics, Geometry and Computer Science Conference*, CIRM, Marseille Luminy: Y. Manoussakis (2007)
- QIP, *Workshop on Quantum Information Processing*, Paris: M. Santha (2006)

Member (international events)

- CiE, *Computability in Europe*: S. Laplante (2008)
- STACS, *Symposium on Theoretical Aspects of Computer Science*: S. Laplante (2007), F. Magniez (2008)
- FCT, *International Symposium on Fundamentals of Computation Theory*: F. Magniez (2007)
- QIP, *Workshop on Quantum Information Processing*: F. Magniez (2006)
- SOFSEM, *Conference on Current Trends in Theory and Practice of Informatics*: F. Magniez (2005)
- PODC, *ACM Symposium on Principles of Distributed Computing*: A. Rosen (2008)
- APPROX, *International Workshop on Approximation Algorithms for Combinatorial Optimization Problems*: A. Rosen (2008)
- SCN, *Conference on Security and Cryptography for Networks*: A. Rosen (2008)
- WAOA, *Workshop on Approximation and Online Algorithms*: A. Rosen (2005, 2007)
- WEA, *International Workshop on Experimental Algorithms*: A. Rosen (2006)
- IPDPS, *International Parallel and Distributed Processing Symposium*: A. Rosen (2006)
- SPAA, *ACM Symposium on Parallelism in Algorithms and Architectures*: A. Rosen (2005)
- ICALP, *International Colloquium on Automata, Languages and Programming*: A. Rosen (2005)
- ESA, *European Symposium on Algorithms*: A. Rosen (2005)
- PODS, *Symposium on Principles of Database Systems*: M. De Rougemont (2005)
- AQIS, *Asian Conference on Quantum Information Science*: M. Santha (2007)
- QIPC, *European Workshop on Quantum Information Processing and Communication*: M. Santha (2006)
- EQIS, *Erato Conference on Quantum Information Science*: M. Santha (2005)

Evaluation Committees and Invited Expertise

International

- Evaluation committee NSERC (Canada): S. Corteel
- ERC Starting grants: F. Magniez
- Israel Science Foundation (ISF), Israel: F. Magniez, A. Rosen
- Information Society Technologies, Future and Emerging Technologies: M. Santha (committee and invited expertise)

France

- ANR, Programme Domaines Emergents (DEFIS): S. Laplante (committee)
- ANR: S. Laplante, F. Magniez

2/ Algo

Volunteer Professional Service

Management Positions in Scientific Organisations

- GdR Information et Communication Quantique: I. Kerenidis, steering committee
- GdR Informatique Mathématique, GT Informatique Quantique: F. Magniez, responsable
- GdR Informatique Mathématique, GT Complexité et Modèles Finis: M. De Rougemont, responsable
- IUT Orsay: D. Gouyou-Beauchamps, head of the CS department
- Digiteo: M. Santha, programme committee
- LRI: S. Corteel, Y. Manoussakis, laboratory council
- Université Paris-Sud: F. Magniez, A. Rosen, hiring committee
- Université Paris-Sud: Y. Manoussakis, conseiller aux thèses
- Greek-French Master on Computer Sciences (University of Crete, Université Paris-Sud, Université Joseph Fourier (Grenoble)): Y. Manoussakis, responsable

Organisation of Conferences and Scientific Events

- *IEEE Conference on Computational Complexity*, Paris, 2009: I. Kerenidis, S. Laplante (chair), F. Magniez, A. Rosen, M. Santha
- *Workshop Quantum Information Processing*, Paris, 2006: S. Laplante, F. Magniez, M. Santha (chair)
- CGCS, *International Combinatorics, Geometry and Computer Science Conference*, CIRM, Marseille Luminy, 2007: Y. Manoussakis
- *Workshop Bertinoro workshop on adversarial modeling and analysis of communication networks*, Bertinoro (Italy), 2006 : A. Rosen, organization
- *Trimester Quantum Information, Computation and Complexity* at Institut Henri Poincaré, Paris, 2006: M. Santha

Working Groups

- GdR Informatique Mathématique, GT Aléa: S. Corteel, D. Gouyou-Beauchamps



- GdR Informatique Mathématique, GT Combinatoire algébrique: S. Corteel
- GdR Informatique Mathématique, GT Informatique Quantique: I. Kerenidis, S. Laplante, F. Magniez, M. Santha
- GdR Information et Communication Quantique: I. Kerenidis, S. Laplante, F. Magniez, M. Santha
- GdR Informatique Mathématique, GT Complexité et Modèles Finis: S. Laplante, F. Magniez, M. De Rougemont, M. Santha
- GdR Informatique Mathématique, GT Combinatoire des mots, algorithmique du texte et du génome: P. Ochem

Other Professional Service

- Steering committee of the annual *Fundamentals of Computation Theory*: M. Santha
- Steering committee of the annual workshop *Quantum Information Processing*: M. Santha
- Steering committee of the annual *Symposium on Theoretical Aspects of Computer Science*: M. Santha

2/ Algo

Contracts and grants

Contracts and grants (jan 2005 - dec 2008)				
Type	Name	Managing Institution	Start / Duration	Amount
Europe	CSQIP	Université Paris-Sud 11	10.2008 / 39 mo.	138 k€
Europe	QAP	Université Paris-Sud 11	11.2005 / 48 mo.	158 k€
Europe	QCCC	Université Paris-Sud 11	05.2006 / 24 mo.	80 k€
Europe	RESQ	Université Paris-Sud 11	12.2002 / 36 mo.	283 k€
ANR	ALGOQP	CNRS	12.2005 / 42 mo.	280 k€
ANR	ICOMB	Université Paris-Sud 11	07.2008 / 60 mo.	340 k€
ANR	VERAP	CNRS	01.2008 / 36 mo.	122 k€
Public	Cryptanalyse Quantique	CNRS	08.2002 / 36 mo.	62 k€
Public	GAP	CNRS	08.2003 / 36 mo.	8 k€
Public	GT CMF	CNRS	01.2007 / 36 mo.	8 k€
Public	GT IQ	CNRS	01.2006 / 48 mo.	8 k€
Public	HSP	CNRS	01.2008 / 24 mo.	7 k€
Public	JST-ICT	CNRS	01.2008 / 48 mo.	90 k€
Public	Réseaux quantiques	CNRS	07.2003 / 36 mo.	41 k€
Public	VERA	CNRS	09.2003 / 35 mo.	50 k€
CIFRE	MASA	Université Paris-Sud 11	01.2003 / 36 mo.	12 k€

CSQIP

Partners: EU : Université Paris-Sud and Universität Erlangen-Nürnberg (Germany); Canada: University of Calgary (Alberta) and University of Waterloo (Ontario)

Type: Europe
Amount: 138 k€
Duration: 39 months
Scientific director for LRI:
Frédéric MAGNIEZ

This project will formally initiate student and faculty exchange across several Canadian and EU institutions which have a strong research effort in quantum information processing (QIP). The project will consolidate and expand existing collaborations so as to provide a larger pool of talented students access to expertise available beyond their home institutions and get credit for this international experience. The project will also provide a platform for developing a standardized suite of courses dedicated to the rapidly developing field of QIP.

QAP

Partners: 35 sites (see web site)

The EU Integrated Project Qubit Applications (or QAP) is a partnership of 35 academic and industrial groups at the cutting edge of quantum information research. Initiated in 2005, QAP's mission is to develop and implement novel applications for quantum information processing, and to explore theoretical concepts of quantum information. QAP partners have published over 600 papers in a variety of journals to date, including prestigious titles such as Nature, Science, Physical Review Letters, Nature Photonics among others. These papers mark a significant contribution to the worldwide effort to understand, control and utilize quantum systems, and reflect the diverse range of interests within the collaboration.

See <http://www.qubitapplications.com/default.asp>

Type: Europe
Amount: 158 k€
Duration: 48 months
Scientific director for LRI:
Miklos SANTHA

QCCC

Partners: LRI

The goal of the Marie Curie International Reintegration Grant was to facilitate the integration of Iordanis Kerenidis in the institutional European research environment after an extended stay outside the EU. It provided funding for scientific travel as well as for the employment of a postdoctoral fellow. The research topic covers quantum computation, communication and cryptography.

Type: Europe
Amount: 80 k€
Duration: 24 months
Scientific director for LRI:
Iordanis KERENIDIS

RESQ

Partners: 11 sites (see web site)

RESQ is an interdisciplinary project regrouping physicists, computer scientists, mathematicians and statisticians. One of the main objectives of the project is to bridge the cultural gap between these different disciplines and to develop a community of scientists from these disciplines that can work together and communicate together.

See <http://www.ulb.ac.be/project/RESQ/index.html>

Type: Europe
Amount: 283 k€
Duration: 36 months
Scientific director for LRI:
Miklos SANTHA

ALGOQP

Partners: LRI

Our project consists in joining the strengths of experts in both randomized and quantum computation. Our global objective is to make progress on both quantum and probabilistic computation, and also, by joining forces, to ensure that the flow of techniques goes

Type: ANR
Amount: 280 k€
Duration: 42 months
Scientific director for LRI:
Sophie LAPLANTE



in both directions, from randomized computation to quantum and back. In the randomized model our emphasis is on sublinear algorithms for large data sets, in particular property testing, approximate verification, and online algorithms. In quantum computation, we will continue to work on algorithms for the hidden subgroup problem, vector lattice problems, among others. At the intersection of quantum and randomized computation, our goal is to study random and quantum walks, communication complexity, and lower bound methods for circuit and formula size complexity.

ICOMB

Partners: LRI

The goal of this proposal is to create a strong team at the Université Paris-Sud to study the interactions between combinatorics and other fields, such as number theory, basic hypergeometric series, representation theory, geometry and mathematical physics. We will study these interactions from the perspective of two combinatorial objects that are generalizations of integer partitions.

Type: ANR
Amount: 340 k€
Duration: 60 months
Scientific director for LRI:
Sylvie CORTEEL

VERAP

Partners: LRI, Equipe de Logique (Univ. Paris 7)

This research project extends the VERA project, which introduced efficient methods to approximately verify that a Transition System satisfies some Property. We consider Probabilistic systems, where both non-deterministic and probabilistic transitions coexist. We extend the approach of Equivalence testers, consider Black-Box testing and Streaming testers.

Type: ANR
Amount: 122 k€
Duration: 36 months
Scientific director for LRI:
Michel DE ROUGEMONT

See <http://www.lri.fr/~mdr/verap>

JST-ICT

Partners: France: LRI Université Paris-Sud, LIG Université de Grenoble; Japon: University of Tokyo, Saitama University, Fujitsu Labs, NII

The JST-CNRS "Quantum Computation: Theory and Feasibility" project is collaboration between Japanese and French research groups, to investigate the fundamental abilities of Quantum Information / Computation and the feasibility of large-scale QIP. Our challenge in this project would be to achieve the synergy of information/computer science and mathematical/theoretical physics in order to explore the future of Quantum Information in a cohesive and effective way.

Type: Public
Amount: 90 k€
Duration: 48 months
Scientific director for LRI:
Iordanis KERENIDIS

See <http://www.qis.ex.nii.ac.jp/jstcnrs/index.html>

Réseaux quantiques

Partners: LRI, INRIA Rocquencourt

The subject of this project is the study of the interface between cryptography, communication and algorithms for quantum networks.

Type: Public
Amount: 41 k€
Duration: 36 months
Scientific director for LRI:
Julia KEMPE

VERA

Partners: LRI, Equipe de Logique (Univ. Paris 7)

This research project studies various notions of approximation in the context of formal verification. Given a program, a system, a protocol, it is often a hard problem to prove that it satisfies a specification. We propose an approach where we can efficiently prove that it approximately satisfies a specification.

Type: Public
Amount: 50 k€
Duration: 35 months
Scientific director for LRI:
Michel DE ROUGEMONT

2/ Algo

Collaborations

Cooperation Agreements

- Partitions d'entiers à l'interface de la combinatoire, des q-series et de la théorie des nombres, ACI Jeunes chercheurs, 40 KEUR, Coordinator: S. Corteel. Partners: LaBRI, Institut Camille Jordan
- Random generation: models, methods and algorithms, ANR Blanc, 300 KEUR, Coordinators: S. Corteel, F. Fiorenzi. Partners: LIP6, LIAFA, LIPN, IGM
- (*) Quantum Computation: Theory and Feasibility, Japan Science and Technology Agency (JST) and CNRS, 90 KEUR, Coordinator: I. Kerenidis. Partners: LIG Université de Grenoble, University of Tokyo (Japon), Saitama University (Japon), Fujitsu Labs (Japon), NII (Japon)
- Quantum algorithms and complexity theory, France-Canada Research Foundation, 14 KEUR, Coordinator: F. Magniez. Partner: Institute for Quantum Computing, University of Waterloo (Ontario, Canada)
- (*) Collaborative student training in Quantum Information Processing, EU-Canada Transatlantic Exchanger Partnerships (TEP) Programme, 138 KEUR, Coordinator: F. Magniez. Partners: Universität Erlangen-Nürnberg (Germany), University of Calgary (Alberta, Canada) and University of Waterloo (Ontario, Canada)
- (*) The hidden subgroup problem in quantum computing, CNRS, 6.8 KEUR, Coordinator: M. Santha. Partner: Hungarian Academy of Sciences (Hungary)

(*): Collaborations that are already listed in Section "Contracts and grants".

Collaborations Leading to Joint Publications

Below we only list a sample of our main collaborations with joint publications.

France

- E. Kashefi, Université de Grenoble: Quantum computing
- M.-P. Béal, D. Perrin, University of Marne la Vallée: Combinatorics
- R. Lassaigne, J. Lovejoy, University of Paris 7: Verification, Combinatorics
- P. Baptiste, C. Dürr, Ecole Polytechnique: Algorithms, Quantum computing

Europe

- H. Buhrmann, R. de Wolf, CWI (Amsterdam): Quantum computing

- M. Karpinski, University of Bonn: Algorithms
- K. Friedl, Budapest University of Technology and Economics (Budapest): Algorithms, Quantum computing
- G. Ivanyos, SZTAKI (Budapest): Algorithms, Quantum computing
- H. Räcke, Warwick University (UK): Algorithms

USA

- C. Mathieu, Brown University: Algorithms
- W. van Dam, University of California, Santa Barbara: Quantum computing
- M. Chrobak, University of California, Riverside: Algorithms
- U. V. Vazirani, University of California, Berkeley: Algorithms, Quantum computing
- A. Kitaev, D. Mayers, Caltech: Quantum computing
- P. Hitczenko, Drexel University, Philadelphia: Combinatorics
- L. K. Williams, Harvard University: Combinatorics
- T.S. Jayram, IBM Almaden Research Center: Quantum computing
- J. Roland, NEC Labs, Princeton: Quantum computing
- S. Lee, C. D. Savage, North Carolina State University: Combinatorics
- M. Szegedy, Rutgers University: Complexity, Quantum computing
- R. Kannan, Yale University: Algorithms

Other countries

- P. Høyer, University of Calgary (Canada): Quantum computing
- M. Mosca, A. Nayak, University of Waterloo (Canada): Quantum computing
- P. Leroux, Université du Québec (Canada): Combinatorics
- P. Sen, Tata Institute of Fundamental Research, Mumbai (India)
- Z. Lotker, Ben-Gurion University (Israel): Algorithms
- A. Kesselman, Intel Corporation (Israel): Algorithms
- D. Aharonov, Hebrew University, Jerusalem (Israel): Quantum computing
- Z. Bar-Yossef, E. Fischer, Technion Institute (Israel): Algorithms, Quantum computing
- O. Regev, B. Patt-Shamir, Tel-Aviv University (Israel): Algorithms, Cryptography, Quantum computing

2/ Algo

Dissemination and Technology Transfer

Popularisation of Research Results

- *Comment calculer quantique*, La Recherche, (398):30-37, 2006, J. Kempe, S. Laplante and F. Magniez

Summer Schools, Tutorials, Invited Seminars

International

- S. Corteel. Invited at the semester *Combinatorics and Statistical Physics*, Schrödinger Institute, Austria, 2008

- S. Corteel. Invited at the Semester in *Algebraic combinatorics*, Mittag-Leffler Institute, Sweden, 2005

France

- I. Kerenidis, S. Laplante, F. Magniez. Invited at the trimester *Quantum Information, Computation and Complexity* at Institut Henri Poincaré, Paris, 2006
- S. Laplante, F. Magniez. Course at *Ecole de printemps d'informatique théorique*, Montignac, 2005

2/ Algo

Training and Education

Defended Habilitations (jan 2005 - sept 2008)			
Name	First name	Date	Position
DURR	Christoph	10.2005	CR CNRS, LIX
LAPLANTE	Sophie	12.2005	PR, Université Paris-Sud
MAGNIEZ	Frédéric	05.2007	CR CNRS, LRI

Defended doctorates (jan 2005 - sept 2008)			
Name	First name	Date	Position
ABOUELAOUALIM	Abdelfattah	09.2007	Post-doc (France)
ALBERT	Julien	07.2006	
DEGORRE	Julien	09.2007	Post-doc (France)
GOULARAS	Dionysis	09.2005	Associate professor, Univ. Istanbul (Turkey)
HESS	Claudia	01.2008	R&D Engineer (Germany)
MOHAMMAD-NOORI	Morteza	07.2005	Assistant Professor, Tehran (Iran)
NADEAU	Philippe	09.2007	Post-doc abroad
VERHOEVEN	Yves	11.2005	French Foreign Ministry
VERT	Régis	06.2006	R&D Engineer

Graduate Courses

- Master Parisien de Recherche en Informatique, Université Paris 7, *Aspects algorithmiques de la combinatoire*: S. Corteel
- Master Informatique, Université Paris-Sud; and Master Parisien de Recherche en Informatique, Université Paris 7, *Quantum information and applications*: I. Kerenidis, S. Laplante, F. Magniez, M. Santha
- Master Informatique, Université Paris-Sud; and Master Parisien de Recherche en Informatique, Université Paris 7, *Advanced algorithms and complexity*: F. Magniez, A. Rosen, M. De Rougemont, M. Santha, N. Vishnoi
- Master Logique Mathématique et Fondements de l'Informatique, Université Paris 7, *Logique, complexité et jeux*: M. De Rougemont

Publications

Journal articles

Major international journals

- [1] A. Abouelaoualim, K. C. Das, W. F. de la Vega, M. Karpinski, Y. Manous-sakis, C. Martinhon, and R. Saad. Cycles and paths in edge-colored graphs with given degrees. *Journal of Graph Theory*, 2009.
- [2] A. Abouelaoualim, K. C. Das, L. Faria, Y. Manoussakis, C. Martinhon, and R. Saad. Paths and trails in edge-colored graphs. *Theoretical Computer Science*, 2009.
- [3] B. Adamczewski and J.-P. Allouche. Reversals and palindromes in continued fractions. *Theoret. Comput. Sci.*, 380:220–237, 2007.
- [4] M. Adler and A. Rosén. Tight bounds for the performance of longest in system on DAGs. *J. Algorithms*, 55(2):101–112, 2005.
- [5] D. Aharonov, J. Kempe, Z. Landau, S. Lloyd, O. Regev, and W. van Dam. Adiabatic quantum computation is equivalent to standard quantum computation. *SIAM J. Comput.*, 37(1):166–194, 2007.
- [6] W. Aiello, Y. Mansour, S. Rajagopalan, and A. Rosén. Competitive queue policies for differentiated services. *J. Algorithms*, 55(2):113–141, 2005.
- [7] J.-P. Allouche, J. Shallit, and G. Skordev. Self-generating sets, integers with missing blocks and substitutions. *Discrete Math.*, 292:1–15, 2005.
- [8] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. *Siam J. C.*, 2008. Earlier version in STOC'03. quant-ph/0208062.
- [9] R. Brak, S. Corteel, J. Essam, R. Parviainen, and A. Rechnitzer. A combinatorial derivation of the PASEP stationary state. *Electron. J. Combin.*, 13(1), 2006. Research Paper 108, 23 pp. (electronic).
- [10] X. L. Breton. Linear independence of automatic formal power series. *Discrete Math.*, 306:1776–1780, 2006.
- [11] H. Buhrman, C. Dürr, M. Heiligman, P. Høyer, F. Magniez, M. Santha, and R. de Wolf. Quantum algorithms for element distinctness. *SIAM Journal on Computing*, 34(6):1324–1330, 2005.
- [12] F. Caselli, C. Krattenthaler, B. Lass, and P. Nadeau. On the number of fully packed loop configurations with a fixed associated matching. *Electronic Journal of Combinatorics*, 11(2), 2005.
- [13] S. Corteel, W. M. Y. Goh, and P. Hitczenko. A local limit theorem in the theory of overpartitions. *Algorithmica*, 46(3-4):329–343, 2006.
- [14] S. Corteel and J. Lovejoy. An iterative-bijective approach to generalizations of Schur's theorem. *European J. Combin.*, 27(4):496–512, 2006.

- [15] S. Corteel and O. Mallet. Overpartitions, lattice paths, and Rogers-Ramanujan identities. *J. Combin. Theory Ser. A*, 114(8):1407–1437, 2007.
- [16] S. Corteel and P. Nadeau. Bijections for permutation tableaux. *European J. Combin.*, 2008. To appear.
- [17] W. Dam, F. Magniez, M. Mosca, and M. Santha. Self-testing of universal and fault-tolerant sets of quantum gates. *SIAM Journal on Computing*, 37(2):611–629, 2007.
- [18] W. F. de la Vega and M. Karpinski. 1.0957-approximation algorithm for random max-3sat. *RAIRO Operations Research*, 41:95–103, 2007.
- [19] W. F. de la Vega and Z. Tuza. Groupies in random graphs. *IPL*, 2008. to appear.
- [20] M. de Rougemont and D. Gross-Amblard. Uniform generation in spatial constraint databases and applications. *J. Comput. Syst. Sci.*, 72(4):576–591, 2006.
- [21] M. de Rougemont, S. Laplante, R. Lassaigne, F. Magniez, and S. Peyronnet. Probabilistic abstraction for model checking: An approach based on property testing. *ACM Transaction on Computational Logic*, 2007.
- [22] J. Degorre, S. Laplante, and J. Roland. Simulating quantum correlations as a distributed sampling problem. *Phys. Rev. A*, 72, 2005.
- [23] J. Degorre, S. Laplante, and J. Roland. Simulation of bipartite qudit correlations. *Phys. Rev. A*, 75(1), 2007.
- [24] L. Esperet, A. Labourel, and P. Ochem. On induced-universal graphs for the class of bounded-degree graphs. *Inform. Process. Lett.*, 108(5):255–260, 2008.
- [25] L. Esperet and P. Ochem. On circle graphs with girth at least five. *Discrete Math.*, 2008. In press.
- [26] K. Friedl, G. Ivanyos, M. Santha, and Y. Verhoeven. On the black-box complexity of Sperner’s lemma. *Theory of Computing Systems*, 2008. To appear.
- [27] A. Gál and A. Rosén. Omega(log n) lower bounds on the amount of randomness in 2-private computation. *SIAM J. Comput.*, 34(4):946–959, 2005.
- [28] D. Goncalves and P. Ochem. On star and caterpillar arboricity. *Discrete Math.*, 2008. In press.
- [29] D. Gouyou-Beauchamps and P. Leroux. Enumeration of symmetry classes of convex polyominoes on the honeycomb lattice. *Theoretical Computer Science*, 346(2-3):307–334, 2005.
- [30] M. E. Haddad, Y. Manoussakis, and R. Saad. On antisymmetric routings of networks. *JCMCC*, 2009.
- [31] E. Kashefi and I. Kerenidis. Statistical zero knowledge and quantum one-way functions. *Theoretical Computer Science*, 378(1):101–116, 2007.
- [32] J. Kempe, A. Kitæev, and O. Regev. The complexity of the local hamiltonian problem. *SIAM Journal of Computing*, 35(5):1070–1097, 2006.
- [33] I. Kerenidis and D. Nagaj. On the optimality of quantum encryption schemes. *Journal of Mathematical Physics*, 47(092102), 2006.



- [34] A. Kesselman and A. Rosén. Scheduling policies for CIOQ switches. *J. Algorithms*, 60(1):60–83, 2006.
- [35] S. Laplante, T. Lee, and M. Szegedy. The quantum adversary method and formula size lower bounds. *Computational Complexity, Special Issue on Complexity 2005*, 15(2):163–196, 2006.
- [36] S. Laplante and F. Magniez. Lower bounds for randomized and quantum query complexity using Kolmogorov arguments. *SIAM Journal on Computing*, 38(1), 2008.
- [37] F. Magniez. Multi-linearity self-testing with relative error. *Theory of Computing Systems (TOCS)*, 38(5):573–591, 2005.
- [38] F. Magniez and M. de Rougemont. Property testing of regular tree languages. *Algorithmica*, 49(2):127–146, 2007.
- [39] F. Magniez and A. Nayak. Quantum complexity of testing group commutativity. *Algorithmica*, 48(3):221–232, 2007.
- [40] F. Magniez, M. Santha, and M. Szegedy. Quantum algorithms for the triangle problem. *SIAM Journal on Computing*, 37(2):413–424, 2007.
- [41] Y. Manoussakis. Longest cycles in 3-connected graphs. *Graphs and Combinatorics*, 2009.
- [42] M. Montassier, P. Ochem, and A. Pinlou. Strong oriented chromatic number of planar graphs without short cycles. *DMTCS*, 10(1):1–24, 2008.
- [43] P. Ochem and A. Pinlou. Oriented colorings of partial 2-trees. *Inform. Process. Lett.*, 108(2):82–86, 2008.
- [44] P. Ochem, A. Pinlou, and E. Sopena. On the oriented chromatic index of oriented graphs. *J. Graph Theory*, 57(4):313–332, 2008.
- [45] P. Ochem, N. Rampersad, and J. Shallit. Avoiding approximate squares. *IJFCS*, 19(3):633–648, 2008.
- [46] A. Rosén and M. S. Tsirkin. On delivery times in packet networks under adversarial traffic. *Theory Comput. Syst.*, 39(6):805–827, 2006.
- [47] M. Santha and M. Szegedy. Quantum and classical query complexities of local search are polynomially related. *Algorithmica*, 2008. To appear.
- [48] J. Sudjana, L. Magnin, R. G.-P. Sánchez, and N. J. Cerf. Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching. *Physical Review A*, 76:052301, 2007.
- [49] Y. Verhoeven. Enhanced algorithms for local search. *Inf. and Process. Lett.*, 97 (5):171–176, 2006.
- [50] Y. Verhoeven. A lower bound on the competitiveness of memoryless algorithms for a generalization of the cnn problem. *Theor. Comput. Sci.*, 359 (1-3):58–68, 2006.

Other journals

- [51] G. Allouche, J.-P. Allouche, and J. Shallit. Kolam indiens, dessins sur le sable aux îles Vanuatu, courbe de Sierpinski et morphismes de monoïde. *Ann. Inst. Fourier*, 56:2115–2130, 2006.

- [52] J.-P. Allouche. Automates et algébricités. *J. Théorie des Nombres Bordeaux*, 17:1–11, 2005.
- [53] J.-P. Allouche. Note on an integral of Ramanujan. *Ramanujan J.*, 14:39–42, 2007.
- [54] J.-P. Allouche. A note on univoque self-Sturmian numbers. *RAIRO, Informatique Théorique et Applications*, 42:659–662, 2008.
- [55] J.-P. Allouche and M. M. France. Euler, Pisot, Prouhet-Thue-Morse, Wallis and the duplication of sines. *Monatsh. Math.*, 155:301–315, 2008.
- [56] J.-P. Allouche and C. Frougny. Univoque numbers and an avatar of Thue-Morse. *Acta Arith.*, 2008. À paraître.
- [57] J.-P. Allouche, C. Frougny, and K. Hare. On univoque Pisot numbers. *Math. Comp.*, 76:1639–1660, 2007.
- [58] J.-P. Allouche, N. Rampersad, and J. Shallit. On integer sequences whose first iterates are linear. *Aequ. Math.*, 69:114–127, 2005.
- [59] J.-P. Allouche, J. Shallit, and J. Sondow. Summation of series defined by counting blocks of digits. *J. Number Theory*, 123:133–143, 2007.
- [60] J.-P. Allouche and N. Sidorov. Periodic unique beta-expansions: the Sharkovskii ordering. *Ergodic Th. Dyn. Syst.*, 2008. À paraître.
- [61] J.-P. Allouche and G. Skordev. Von Koch and Thue-Morse revisited. *Fractals*, 15:405–409, 2007.
- [62] J.-P. Allouche and J. Sondow. Infinite products with strongly B -multiplicative exponents. *Annales Univ. Sci. Budapest., Sect. Comp.*, 28:35–53, 2008.
- [63] G. Andrews, S. Corteel, and C. Savage. On q -series identities arising from Lecture Hall partitions. *Int. J. Number Theory*, 2008. To appear.
- [64] K. Brown, J. Kempe, M. Storcz, J. Vala, K. Whaley, and F. Wilhelm. Full protection of superconducting qubit systems from coupling errors. *Phys. Rev. B*, 72:064511, 2005. cond-mat/0407780.
- [65] A. Chailloux and I. Kerenidis. Increasing the power of the verifier in quantum zero knowledge, 2007. quant-ph/0711.4032.
- [66] A. Chailloux and I. Kerenidis. The role of help in classical and quantum zero knowledge, 2007. Cryptology ePrint 2007/421 and quant-ph/0711.4251.
- [67] J. Chalopin and P. Ochem. Dejean’s conjecture and letter frequency. *RAIRO: Theoret. Informatics Appl.*, 42(3):477–480, 2008.
- [68] S. Corteel. Crossings and alignments of permutations. *Adv. in Appl. Math.*, 38(2):149–163, 2007.
- [69] S. Corteel, I. M. Gessel, C. D. Savage, and H. S. Wilf. The joint distribution of descent and major index over restricted sets of permutations. *Ann. Comb.*, 11(3-4):375–386, 2007.
- [70] S. Corteel, S. Lee, and C. D. Savage. Five guidelines for partition analysis with applications to lecture hall-type theorems. In *Combinatorial number theory*, pages 131–155. de Gruyter, Berlin, 2007.
- [71] S. Corteel and J. Lovejoy. Overpartitions and the q -bailey identity. *Proc. Edinburgh Math. Soc.*, 2008. To appear.



- [72] S. Corteel, J. Lovejoy, and O. Mallet. An extension to overpartitions of the Rogers-Ramanujan identities for even moduli. *J. Number Theory*, 2008. To appear.
- [73] S. Corteel and L. K. Williams. A Markov chain on permutations which projects to the PASEP. *Int. Math. Res. Not. IMRN*, (17), 2007. Art. ID rnm055, 27.
- [74] S. Corteel and L. K. Williams. Tableaux combinatorics for the asymmetric exclusion process. *Adv. in Appl. Math.*, 39(3):293–310, 2007.
- [75] M. de Rougemont and A. Vieilleribière. Approximate schemas, source-consistency and query answering. *International Journal on Intelligent Database Systems*, 2008. To appear.
- [76] K. Djemal, D. Goularas, and Y. Mannoussakis. 3d image modeling and specific treatments in orthodontics domain. *Journal of Applied Bionics and Biomechanics*, 4/3:111–124, 2007.
- [77] J. Fern, J. Kempe, S. Sastry, and S. Simic. Fault-tolerant quantum computation - a dynamical systems approach. *IEEE Transactions on Automated Control*, 51(3):448–459, 2006. quant-ph/0409084.
- [78] C. Hess. Trust-based recommendations for publications - a multi-layer network approach. Doctoral Consortium at the 9th European Conference on Research and Advanced Technology for Digital Libraries (ECDL 2005), Vienna, Austria, September 2005.
- [79] C. Hess. Trust-based recommendations for publications - a multi-layer network approach. *IEEE Technical Committee on Digital Libraries (TCDL) Bulletin*, 2(2), 2006. Revised Paper from the Doctoral Consortium at the 9th European Conference on Research and Advanced Technology for Digital Libraries (ECDL 2005), Vienna, Austria.
- [80] J. Kempe. Discrete quantum walks hit exponentially faster. *Probability Theory and Related Fields*, 133(2):215–235, 2005.
- [81] J. Kempe, L. Pyber, and A. Shalev. Permutation groups, minimal degrees and quantum computing. *Groups, Geometry, and Dynamics*, 1(4):553–584, 2007.
- [82] I. Kerenidis and R. Raz. The one-way communication complexity of the Boolean Hidden Matching problem, 2006. quant-ph/0607173.
- [83] P. Zoller, T. Beth, D. Binosi, R. Blatt, H. Briegel, D. Bruss, T. Calarco, J. 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. Lütkenhaus, S. Massar, J. Mooij, M. 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.

Conference articles

Major international conferences and workshops

- [84] A. Abouelaoualim, K. C. Das, L. Faria, Y. Manoussakis, C. Martinhon, and R. Saad. Paths and trails in edge-colored graphs. In *Proceedings of LATIN 2008, Brazil*, 2008.
- [85] D. Aharonov, D. Gottesman, S. Irani, and J. Kempe. The power of quantum systems on a line. In *FOCS*, pages 373–383, 2007.
- [86] J.-P. Allouche and A. Sapir. Restricted towers of Hanoi and morphisms. In *DLT (Palermo, 2005)*, volume 3572 of *Lecture Notes in Comput. Sci.*, pages 1–10. Springer, 2005.
- [87] A. Ambainis, J. Kempe, and A. Rivosh. Coins make quantum walks faster. In *Proc. 16th ACM SODA*, pages 1099–1108. ACM, 2005. quant-ph/0402107.
- [88] L. Antunes, S. Laplante, A. Pinto, and L. Salvador. Cryptographic security of individual instances. In *Proceedings of International Conference on Information Theoretic Security 2007*, 2007. To appear.
- [89] A. Chailloux, D. F. Ciocan, I. Kerenidis, and S. Vadhan. Interactive and noninteractive zero knowledge are equivalent in the help model. In *Proceedings of IACR Fifth Theory of Cryptography Conference (TCC)*, 2008.
- [90] M. Dah and Y. Manoussakis. On the network security games. In *22nd European Conference on Operations Research, Prague*, 2007.
- [91] W. de la Vega and C. Kenyon-Mathieu. Linear programming relaxations of maxcut. In *SODA*, pages 53–61, 2007.
- [92] W. F. de la Vega, R. Kannan, M. Karpinski, and S. Vempala. Tensor decomposition and approximation schemes for constraint satisfaction problems. In *STOC '05: Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pages 747–754, New York, NY, USA, 2005. ACM.
- [93] M. de Rougemont. Approximate schemas and query answering. In *Second Franco-Japanese Workshop on Information Search, Integration and Personalization, ISIP'05*, 2005.
- [94] M. de Rougemont, E. Fischer, and F. Magniez. Approximate satisfiability and equivalence. In *IEEE Logic in Computer Science*, pages 421–430, 2006.
- [95] M. de Rougemont, S. Hemon, and M. Santha. Approximate nash equilibria for multi-player games. In *Proceedings of 1st International Symposium on Algorithmic Game Theory*, LNCS 4997, pages 267–278. Springer, Berlin, 2008.
- [96] M. de Rougemont and C. Hess. A model of uncertainty for near-duplicates in document reference networks. In *ECDL*, pages 449–453, 2007.
- [97] M. de Rougemont and A. Vieillerivière. Approximate data exchange. In *International Conference on Database Technology, (ICDT)*, pages 44–58, 2007.
- [98] M. de Rougemont and A. Vieillerivière. Property testing for approximate search and integration. In *Third Franco-Japanese Workshop on Information Search, Integration and Personalization, ISIP'07*, 2007.
- [99] R. de Wolf, D. Gavinsky, and J. Kempe. Strength and weaknesses of quantum fingerprinting. In *Proc. 21st IEEE CCC*, pages 288–295. IEEE, 2006.



- [100] R. de Wolf, D. Gavinsky, J. Kempe, and O. Regev. Bounded-error quantum state identification and exponential separations in communication complexity. In *Proc. 38th STOC*, pages 594–603. ACM, 2006. quant-ph/0511013.
- [101] K. Friedl, G. Ivanyos, and M. Santha. Efficient testing of groups. In *Proceedings of 36th ACM Symposium on Theory of Computing, Baltimore, USA*, pages 157–166. ACM, 2005.
- [102] K. Friedl, G. Ivanyos, M. Santha, and Y. Verhoeven. On the black-box complexity of sperner’s lemma. In *Proceedings of 15th International Symposium on Fundamentals of Computation Theory, Lübeck, Germany*, LNCS 3623, pages 245–257. Springer, Berlin, 2005.
- [103] K. Friedl, G. Ivanyos, M. Santha, and Y. Verhoeven. Locally 2-dimensional sperner problem complete for the polynomial parity argument classes. In *Proceedings of 6th Italian Conference on Algorithms and Complexity, Roma, Italy*, LNCS 3998, pages 380–391. Springer, Berlin, 2006.
- [104] E. Gordon and A. Rosén. Competitive weighted throughput analysis of greedy protocols on DAGs. In *PODC*, pages 227–236, 2005.
- [105] D. Gouyou-Beauchamps and P. Nadeau. Signed enumeration of ribbon tableaux with local rules and generalizations of the schensted correspondence. In *Proceedings of 19th International Conference on Formal Power Series & Algebraic Combinatorics, July 2-6, 2007, Nankai University, Tianjin, China*, 2007.
- [106] C. Hess and K. Stein. Efficient calculation of personalized document rankings. In *Proceedings of the Twentieth International Conference on Artificial Intelligence (IJCAI 2007)*, January 2007.
- [107] C. Hess, K. Stein, and C. Schlieder. Trust-enhanced visibility for personalized document recommendations. In *Proceedings of the 21st Annual ACM Symposium on Applied Computing*, Dijon, France, April 2006.
- [108] G. Ivanyos, L. Sanselme, and M. Santha. An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups. In *Proceedings of 24th Symposium on Theoretical Aspects of Computer Science, Aachen, Germany*, LNCS 4393, pages 586–597. Springer, Berlin, 2007.
- [109] G. Ivanyos, L. Sanselme, and M. Santha. An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. In *Proceedings of 8th Latin American Symposium on Theoretical Informatics, Buzios, Brazil*, LNCS 4957, pages 759–771. Springer, Berlin, 2008.
- [110] J. Kempe and A. Shalev. The hidden subgroup problem and permutation group theory. In *Proc. 16th ACM SODA*, pages 1118–1125. ACM, 2005. quant-ph/0406046.
- [111] I. Kerenidis. Quantum multiparty communication complexity and circuit lower bounds. *Mathematical Structures in Computer Science*, 2007. To appear. Special issue for TAMC 2007.
- [112] I. Kerenidis. Quantum multiparty communication complexity and circuit lower bounds. In *Proceedings of 4th Annual Conference on Theory and Applications of Models of Computation (TAMC)*, 2007. quant-ph/0504087.
- [113] S. Laplante. Lower bounds using Kolmogorov complexity. In *Logical Approaches to Computational Barriers, Second Conference on Computability in Europe, CiE 2006*, pages 297–306, 2006.

- [114] S. Laplante, T. Lee, and M. Szegedy. The quantum adversary method and formula size lower bounds. In *Proceedings of IEEE Conference on Computational Complexity*, pages 76–90, 2005.
- [115] Z. Lotker, B. Patt-Shamir, and A. Rosén. Distributed approximate matching. In *PODC*, pages 167–174, 2007.
- [116] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier. Self-testing of quantum circuits. In *Proceedings of 33rd International Colloquium on Automata, Languages and Programming*, volume 4051 of *Lecture Notes in Computer Science*, pages 72–83. Verlag, 2006.
- [117] 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. Verlag, 2005.
- [118] F. Magniez, A. Nayak, J. Roland, and M. Santha. Search via quantum walk. In *Proceedings of 39th ACM Symposium on Theory of Computing*, pages 575–584, 2007.
- [119] 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, 2005.
- [120] P. Nadeau. Walks reaching a line. In S. Felsner, editor, *Proceedings of European Conference on Combinatorics, Graph Theory and Applications (EuroComb '05), Berlin*, volume AE of *DMTCS Proceedings*, pages 401–406. Discrete Mathematics and Theoretical Computer Science, 2005.
- [121] P. Nadeau. A general bijection for walks on the slit plane. In *Proceedings of 18th International Conference on Formal Power Series & Algebraic Combinatorics, June 2006, San Diego, CA, USA*, 2006.
- [122] J. Naor, A. Rosén, and G. Scalosub. Online time-constrained scheduling in linear networks. In *INFOCOM*, pages 855–865, 2005.
- [123] H. Räcke and A. Rosén. Distributed online call control on general networks. In *SODA*, pages 791–800, 2005.
- [124] RD de Wolf, Gavinsky, J. Kempe, I. Kerenidis, and R. Raz. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of 39th ACM STOC*, pages 516–525, 2007. quant-ph/0611209.
- [125] A. Rosén and G. Scalosub. Rate vs. buffer size: greedy information gathering on the line. In *SPAA*, pages 305–314, 2007.

Other conferences and workshops

- [126] P. Baptiste, M. Chrobak, C. Dürr, and F. Sourd. Preemptive multi-machine scheduling of equal-length jobs to minimize the average flow time. In *Proc. of the 7th Workshop on Models and Algorithms for Planning and Scheduling Problems (MAPSP)*, 2005.
- [127] H. Cheng, M. de Rougemont, and L. Jun. Approximate validity of xml streaming data. In *9th International Conference on Web-age Information Management*, 2008.



- [128] C. Cosenza, K. Djemal, D. Goularas, and Y. Manoussakis. Divitor client/server application (digitalization, visualisation and treatment in orthodontics). In *Proceedings of the 5th International Network Conference (INCO5), 2005, Samos, Greece, 2005*.
- [129] C. Cosenza, K. Djemal, D. Goularas, and Y. Manoussakis. Specific 3d treatment in orthodontic domain. In *International Symposium on Robotics and Automation (ISRA 2006), 2006, Mexico, ISBN: 970-769-070-4., 2006*.
- [130] C. Cosenza, K. Djemal, D. Goularas, and Y. Manoussakis. Adaptive triangulation method for management of the topology changes in 3d boundary reconstruction. In *Proceeding of the 4th IEEE Conference on Systems Signals and Devices, 2007, Hammamet, Tynisia, 2007*.
- [131] J. Degorre and J. Roland. An intuitive approach for the simulation of quantum correlations. In *26th Symposium on Information Theory in the Benelux, 2005*.
- [132] D. Gouyou-Beauchamps. Enumerations de tableaux de rubans. In *Journées Pierre Leroux, 8-9 septembre 2006, LaCIM-UQAM, Montréal, Canada, 2006*.
- [133] C. Hess and K. Stein. Personalized document rankings by incorporating trust information from social network data into link-based measures. In *Proceedings of the IJCAI 2007 Workshop on Text Mining & Link Analysis, jan 2007*.
- [134] E. Kashefi and I. Kerenidis. Statistical zero knowledge and quantum one-way functions. In *Proceedings of PQCrypto 2006: International Workshop on Post-Quantum Cryptography, 2006*.
- [135] A. Vieillerivière and D. Forge. Some properties of directed switching games on oriented matroids. In *Oriented Matroids and matroids, 2005*.

Edited books

- [136] Y. M. Eds. *Combinatorics, Geometry and Computer Science*. Elsevier Science, 2008. To appear.

Dissemination

- [137] J. Kempe, S. Laplante, and F. Magniez. Comment calculer quantique. *La Recherche*, (398):30–37, 2006.

Other publications

- [138] J.-P. Allouche and V. Berthé. Some applications of combinatorics on words in number theory. In *Applied Combinatorics on Words*, pages 520–578. Cambridge University Press, 2005.
- [139] S. Corteel and P. Hitczenko. Generalizations of Carlitz compositions. *J. Integer Seq.*, 10(8):Article 07.8.8, 13 pp. (electronic), 2007.
- [140] S. Corteel, G. Louchard, and R. Pemantle. Common intervals in permutations. *Discrete Math. Theor. Comput. Sci.*, 8(1):189–216 (electronic), 2006.

- [141] J. Degorre, M. Kaplan, S. Laplante, and J. Roland. The communication complexity of non-signaling correlations. Technical Report quant-ph/0804.4859, arXiv e-Print archive, 2008.
- [142] J. Kempe. *Decoherence*, chapter Approaches to Quantum Error Correction, pages 85–123. Progress in Mathematical Physics. Birkhäuser, 2006.
- [143] J. Kempe. *Lecture Notes on Quantum Information*, chapter Quantum Algorithms, pages 87–102. Wiley-VCH, 2006.
- [144] M. Santha. Quantum walk based search algorithms. In *Proceedings of 5th International Conference on Theory and Applications of Models of Computation, Xian, China, LNCS 4978*, pages 31–46. Springer, Berlin, 2008.
- [145] K. Stein and C. Hess. Information retrieval in trust-enhanced document networks. In M. Ackermann, B. Berendt, M. Grobelnik, A. Hotho, D. Mladenic, G. Semeraro, M. Spiliopoulou, G. Stumme, V. Svatek, and M. van Someren, editors, *Semantics, Web, and Mining. European Web Mining Forum, EMWF 2005, and Knowledge Discovery and Ontologies, KDO 2005, Porto, Portugal, October 2005, Revised Selected and Invited Papers, LNAI 4289*. Springer, 2006.

Theses and habilitations

- [146] C. Dürr. Tomographie discrète, calcul quantique et ordonnancement. Habilitation, Université Paris-Sud, France, 2005.
- [147] S. Laplante. Applications de la complexité de Kolmogorov à la complexité classique et quantique. Habilitation, Université Paris-Sud, France, 2005.
- [148] F. Magniez. Vérification approchée - Calcul quantique. Habilitation, Université Paris-Sud, France, 2007. Record number 1018.

