B.2 / Research groups

Algorithms and Complexity

équipe Algorithmique & Complexité

Responsable : Miklos Santha

Dans les quatre dernières années des changements radicaux ont eu lieu dans l'équipe. Avec l'arrivée de Sophie Laplante et Frédéric Magniez en 2000 et celle de Julia Kempe en 2001, elle a atteint sa taille historiquement la plus élevée : quatorze personnes permanentes. Ces arrivées ont renforcé en particulier le thème calcul quantique, et grâce à cette politique courageuse de recrutement, le LRI est reconnu aujourd'hui comme un des principaux pôles dans ce domaine.

Par la suite la taille du groupe a diminué, et en 2004 il n'y avait plus que dix membres permanents. Jean-Pierre Tillich a rejoint l'INRIA comme chargé de recherche en 2001, et trois de nos membres sont devenus professeurs d'université : Alain Denise à Paris-Sud en 2002, Claire Kenyon à l'École Polytechnique en 2002 (en détachement de son poste à Orsay) et finalement Stéphane Boucheron à Paris 7 en 2004. Nous sommes fiers des promotions de nos anciens collègues, nous les remercions pour leurs apports à la vie de notre groupe, et nous leur souhaitons beaucoup de succès dans leurs nouveaux emplois.

Quant à la production scientifique, l'équipe a maintenu sa place en toute première ligne en Europe dans le domaine de l'informatique théorique. Elle a publié quasiment dans chacun des meilleurs colloques du domaine : FOCS, STOC, ICALP, STACS, MFCS, FSTTCS, SODA, SWAT, LICS, FPSAC, COMPLEXITY. En particulier, elle a eu 14 publications à FOCS et STOC, les deux colloques généralistes reconnus comme les plus prestigieux. Elle a eu également un grand nombre de publications dans diverses revues internationales d'informatique théorique, de combinatoire, de mathématiques discrètes, de théorie des nombres, de probabilités discrètes et de physique. Les thèmes de recherches principaux développés durant ces années sont restés l'algorithmique, la combinatoire, la complexité et le calcul quantique.

Algorithms and Complexity

Head: Miklos Santha

In the last four years, the composition of our research group has gone through radical changes. With the arrival of Sophie Laplante and Frédéric Magniez in 2000, and of Julia Kempe in 2001, it has reached its historically largest size: fourteen permanents members. These arrivals have reinforced in particular the quantum computing theme of the group, and thanks to this courageous scientific policy and to the subsequent work, LRI is recognized today as a leading site in this field.

From this peak, the size of the group went down to ten permanent members by 2004. First Jean-Pierre Tillich joined INRIA as a researcher in 2001, and then three of our members became university professors: Alain Denise at Paris-Sud in 2002, Claire Kenyon at École Polytechnique also in 2002, and finally Stéphane Boucheron at Paris 7 in 2004. We are proud of the promotions of our former colleagues, thank them for their contributions to the life of the group, and wish them great success in their new scientific positions.

With respect to scientific production the group has maintained its status among the very best in Europe in theoretical computer science. We have published in almost all the high quality conferences in the field: FOCS, STOC, ICALP, STACS, MFCS, FSTTCS, SODA, SWAT, LICS, FPSAC, COMPLEXITY. In particular, we have had 14 publications in FOCS and STOC, the two most prestigious general conferences. We have also had a large number of publications in international journals in theoretical computer science, combinatorics, discrete mathematics, number theory, discrete probabilities and physics. The main research themes of the group over these years have remained algorithms, combinatorics, complexity and quantum computing.

Research Group Members

Personnel as of 01/01/2004

Full time faculty			
Name	*First Name*	*Position**	*Institution*
ALLOUCHE	Jean-Paul	DR2	CNRS
BOUCHERON	Stéphane	CR1	CNRS
DE ROUGEMONT	Michel	PR2	Université Paris II
DURR	Christoph	MC	IUT d'Orsay
FERNANDEZ DE LA VEGA	Wenceslas	CR1	CNRS
GOUYOU-BEAUCHAMPS	Dominique	PR1	IUT d'Orsay
KEMPE	Julia	CR2	CNRS
LAPLANTE	Sophie	MC	IUT d'Orsay
MAGNIEZ	Frédéric	CR2	CNRS
MANOUSSAKIS	Yannis	PR1	IUT d'Orsay
SANTHA	Miklos	DR2	CNRS

Doctoral students			
ABOUELAOUALIM	Abdelfattah	D	Université Paris XI
ALBERT	Julien	A	Université Paris XI
DEGORRE	Julien	A	Université Paris XI
GOULARAS	Dionysis	D	Sté ASTERION Productions
MOHAMMAD-NOORI	Morteza	D	CROUS Versailles
NADEAU	Philippe	AC	Université Paris XI
PHILIPPS	Pierre	D	ENS Lyon
VERHOEVEN	Yves	D	TELECOMS
VERT	Régis	D	Sté MASA

Temporary personnel			
ADAMCZEWSKI	Boris	Post-doc	CNRS
MILMAN	Pérola	Post-doc	EGIDE
PEYRONNET	Sylvain	ATER	Université Paris VII

** See the glossary for acronyms.*

Long term visitors

Name	*First Name*	*Nationality*	*Institution*	*Arrival*	*Departure*	*Funding*
BACSO	Gabor	Hungarian	Hungarian Academy of Sciences	1/09/00	30/09/00	CNRS-HAS
				17/11/01	6/12/01	CNRS-HAS
BAHADUR	Abhinav	Indian	IIT Bombay	15/5/04	31/7/04	CNRS, ACI
BEREND	Daniel	Israelian	Univ. Ben-Gourion, Beer Sheva	14/06/00	12/07/00	
CHROBAK	Marek	American	UC, Riverside	17/06/01	13/07/01	Ministère de la Recherche
CURRIE	James	Canadian	University of Winnipeg, Canada	20/07/04	30/06/05	sabbatical
DESHPANDE	Amit	Indian	Chennai Mathematical Institute	22/04/02	22/06/02	ENS
FRIEDL	Katalin	Hungarian	Hungarian Academy of Sciences	4/02/02	4/07/02	EGIDE, QAIP grant
HARRISS	Edmund	British	Imperial College Londres	8/10/02	8/12/02	
HAUPTMANN	German	Mathias		5/03/01	10/03/01	
HOYER	Peter	Danish	University of Aarhus, BRICS	31/07/00	6/08/00	
IVANYOS	Gabor	Hungarian	Hungarian Academy of Sciences	5/11/00	4/12/00	CEPHYTEN, QAIP grant
				12/11/01	12/12/01	EGIDE, QAIP grant
				22/01/02	22/02/02	EGIDE, QAIP grant
				8/03/04	2/04/04	CEPHYTEN, RESQ grant
KARLOFF	Howard	American	Georgia Institute of Technology	4/10/00	16/10/00	CNRS-NSF
KHOSROVSHAHI	Gholamreza	Iranian	School of Math. Tehran	19/07/01	2/08/01	
KIWI	Marcos	Chilian	University of Chile	4/02/01	18/02/01	Visiting professor, I.G.M.
LAPLANTE	Sophie	Canadian	University of Chicago	1/09/99	31/08/00	CRSNG
LEI	Yaohui	Chinese	Université de Montréal	1/09/01	31/08/02	CREPUQ fellowship
LOZANO	Antonio	Spanish	LITEC Zaragoza	18/02/02	18/07/02	EGIDE, QAIP grant
LUGOSI	Gabor	Hungarian	University Pompeu Fabra, Barcelone	12/01/00	11/02/00	Visiting professor, UPS
NDOUNDAM	René	Camerounian	Université de Yaoundé	15/01/03	14/07/03	EGIDE, ONU grant
RANDALL	Dana	American	Georgia Institute of Technology Atlanta	24/06/01	5/07/01	CNRS-NS
RAPAPORT	Ivan	Chilian	University of Chile	4/01/01	4/02/01	
				15/06/03	14/07/03	Visiting professor, UPS
REMPE	Lasse	German	University of Kiel	12/09/01	28/02/02	German fellowship
SALVADOR	Liliana	Portugese	University of Porto	27/07/03	25/08/03	EGIDE
				29/09/03	28/11/03	EGIDE
SCHULMAN	Leonard	American	Caltech, Pasadena	6/09/00	10/09/00	
SEN	Pranab	Indian	Tata Institute of Fondamental Research	1/07/01	1/07/02	EGIDE, QAIP grant
SZEGEDY	Mario	German	Rutgers University, NJ USA	3/09/03	2/11/03	EGIDE, RESQ grant
TUZA	Zsolt	Hungarian	Hungarian Academy of Sciences	14/06/00	30/06/00	CNRS-HAS
				10/10/00	17/10/00	CNRS-HAS
				12/10/01	30/10/01	CNRS-HAS
VAKHANIA	Nodari	Georgian	Autom. Univ. of the state Morelos, Mexico	1/10/03	31/12/03	CNRS
DE WOLF	Ronald	Dutch	CWI Amsterdam	31/07/00	6/08/00	
ZWISSIG	Thierry	Swiss	Université de Genève	4/02/02	15/02/02	
				1/04/02	12/04/02	

Group evolution

Arrivals

- Sophie Laplante (MC, IUT), 2000
- Frédéric Magniez (CR, CNRS), 2000
- Julia Kempe (CR, CNRS), 2001

Departures

- Jean-Pierre Tillich (CR, INRIA), 2001
- Alain Denise (Prof UPS, LRI, BioInfo group), 2002
- Claire Kenyon (Prof, Polytechnique), 2002
- Stéphane Boucheron (Prof, Paris-7), 2004

Research Description

We organize our research activity into four areas: algorithms, combinatorics, complexity and quantum computation.

Algorithms Research team

- *Permanent members: Christoph Dürr, Wenceslas Fernandez De La Vega, Yannis Manoussakis, Miklos Santha.*
- *Non-permanent members: Jérémy Barbay, Jean-Christophe Dubacq, David Gross-Amblard, Claire Kenyon, Grégory Olocco, Emmanuel Prouff, Vlady Ravelomanana, Julien Stern, Jean-Pierre Tillich, Yann Verhoeven.*

Coding

Given a set of n words with associated probabilities $p_1,\ldots,p_n$ and some alphabet Σ, the Huffman code is a prefix free code over Σ minimizing $sum\ |c_i|\ p_i$. In optical storage devices or even in the telegraph, each letter of Σ has a different length. We gave an approximation algorithm scheme for constructing the best Huffman code in that setting [130].

Due to the increasing amount of stolen music, the music industry proposed a watermarking system for audio-files and opened a contest. In [113] we succeded in removing the marks from the audio-files, showing that the SDMI system is not secure. We also developed a system to detect watermarkings in [156].

Using ideas of Carlach and Vervoux (Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, 1999) for block turbo-codes, we were able to construct specific *Tanner graphs*, which lead to codes with interesting properties [117, 151].

Approximation Algorithms

When an optimization problem is NP-complete, one might want to approximate it. Approximation schemes are algorithms which together with the problem description get a number ε and output a solution which is ε - close to the optimum. If the running time is not only polynomial in the size of the input but also in $\frac{1}{\varepsilon}$, then it is a *fully* polynomial time approximation scheme.

One example is the constraint satisfaction problem, where are given m clauses on n boolean variables. Depending on the variant, we might want to minimize or maximize the number of satisfied clauses, which contain literals combined with OR or with XOR. The nearest codeword problem can be encoded in that setting. We gave approximation schemes for various variants [109, 26, 34].

Answering a problem of Woeginger and Yu (Information Processing Letters, 1992) in the affirmative, we gave a fully polynomial-time approximation scheme for the problem of finding two disjoint non-empty subsets out of n integers, with a ratio between the total sums closest to 1 [35]. On the other hand, when the difference between the total sums meant to be minimized, the problem is $2nk$ –approximable in polynomial time unless P=NP, for any constant k (see fig 1).

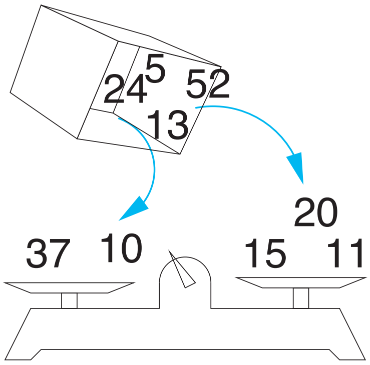


Figure 1: Finding two subsets of closest total sum.

A cut of an edge-weighted graph G is defined by a nontrivial vertex set, and its weight is the total weight of edges crossing the cut. Determining the maximal cut of a graph is a Max-SNP-hard problem, meaning there is no approximation scheme unless P=NP. We studied the special case when the graph has constant degree 3 [47], and we gave a randomized approximation scheme when the weights satisfy the triangle inequality [60].

We have obtained polynomial time approximation scheme for Min-Bisection [123] and Min-Sum Clustering [124]. We also studied the Bin-Covering problem [121], the Bin-Packing problem [140] and various other problems motivated by networks, in particular the Internet [66, 136, 72, 73].

Learning Theory and Stochastic Modelling

Statistical learning consists of infering dependences from emprirical data, which are supposed to be collected by sampling from an unknown probability distribution. In this non-standard statistical setting, it is crucial to develop data-driven risk estimates. In [33] (independent of Koltchinskii and Panchenko) we proposed to use the so-called Rademacher complexity to design data-dependent risk estimates. Thanks to the fact that in [42], we showed, among other properties, that those Rademacher complexities enjoy sub-Poissonian tail behavior, Rademacher complexities have become the standard tool to develop data-driven penalization techniques in model selection.

In [43, 38] we studied the Entropy method, which allows us to develop concentration inequalities for general functions of independent random variables.

In [64], a composite hypothesis testing problem was investigated in an information theoretical perspective, using large deviations theory.

We also applied techniques for analyzing random structures from interactive particle systems or queuing systems to the problems of studying the size of giant component in random graphs or to the classical allocation problems [32, 39, 40, 41].

Scheduling

In a scheduling problem we are given n tasks and wish to assign them to machines, usually in order to minimize the maximal completion time over all jobs. An incredible number of variants of this problem exist depending on the choice of machines, restrictions to the schedule or objective function (see the webpage of P. Brucker and S. Knust). The goal is to identify which are tractable in polynomial time, which are NP-complete, and to come up with the most efficient algorithm in the first case and with approximation algorithms in the second case.

In [28] we considered the problem of scheduling ***n*** jobs on ***m*** machines, where each job must be scheduled in parallel on a given set of machines, and each machine can execute at most one job at a time. In the case where jobs cannot be preempted, the problem is known to be NP-complete even for 3 machines, and we give an approximation scheme, improving on a constant approximation by Goemans (Discrete Applied Mathematics, 1995). In the preemptive case, the problem is NP-complete when the number of machines is unbounded, and for fixed ***m*** there was an algorithm with ***m*** in the exponent of the running time (Ph.D. thesis by A. Krämer, 1995) which we beat with a linear time algorithm.

When jobs have the same processing time, it allows exchanges on a schedule; an interesting structural property which can be exploited in algorithms. In [31] we improved a polynomial time algorithm for a preemptive scheduling problem with equal processing time, on a single machine, where the goal is to maximize the number of jobs scheduled inside an interval defined by a release time and a deadline. In [105] we consider a scheduling problem with equal processing time and given time windows in which scheduling is allowed. This problem appears in air traffic control, and we give results for different variants (see fig 2).

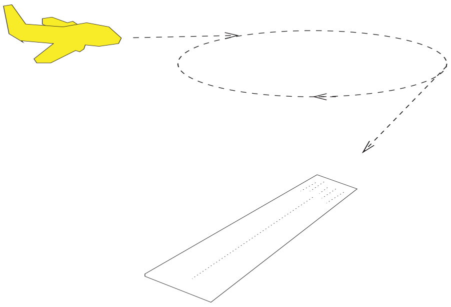


Figure 2: Aircrafts arrive at different moments at the airport and can wait some bounded time in a waiting loop before approaching the runway. The goal is to maximize the minimal distance between two landings.

We also studied the scheduling problem where each job has a given *execution cost* for being executed on a specific processor and any pair of jobs assigned to different processors have a given *communication cost*. For various variants we given exact polynomial time algorithms or an approximation scheme [61].

Cellular Automata

In order to understand the dynamics of cellular automata we studied their relationship with other models. In [125] we focused on signals encoded in higher dimensional cellular automata. In [52] we studied one-dimensional cellular automata under the theory of communication complexity (see fig 3).

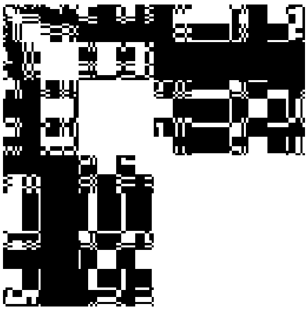


Figure 3: A communication matrix associated to the cellular automata 94 in Wolfram's numbering.

Key references

[31] P. Baptiste, M. Chrobak, C. Dürr, W. Jawor, and N. Vakhania. Preemptive scheduling of equal-length jobs to maximize weighted throughput. *Oper. Res. Lett.*, 32(3):258-264, 2004.

[34] C. Bazgan, W. Fernandez de la Vega, and M. Karpinski. Polynomial time approximation schemes for dense instances of minimum constraint satisfaction. *Random Structures Algorithms*, 23(1):73-91, 2003.

[35] C. Bazgan, M. Santha, and Z. Tuza. Efficient approximation algorithms for the subset-sums equality problem. *J. Comput. System Sci.*, 64(2):160-170, 2002.

[42] S. Boucheron, G. Lugosi, and P. Massart. A sharp concentration inequality with applications. *Random Structures Algorithms*, 16(3):277-292, 2000.

[60] W. Fernandez de la Vega and C. Kenyon. A randomized approximation scheme for metric MAX-CUT. *J. Comput. System Sci.*, 63(4):531-541, 2001. Special issue on FOCS 98 (Palo Alto, CA).

Combinatorics Research team

- *Permanent members: Jean-Paul Allouche (leader), Christoph Dürr, Dominique Gouyou-Beauchamps.*
- *Non-permanent members: Boris Adamczewski, Julien Albert, Morteza Mohammad-Noori, Philippe Nadeau, Jia-Yan Yao.*

The group works on combinatorics and related areas. Three directions can be roughly underlined:

Discrete Tomography

Tomography is the area of reconstructing ***k***-dimensional objects from ***(k-1)***-dimensional projections. In *discrete tomography* we usually want to reconstruct a 2-dimensional matrix from projections on the rows and columns. A well-known and standard problem consists of constructing a 0-1 matrix from which we only know the number of 1's in each column and in each row. (The matrix may not be unique.) This problem can be solved by a greedy polynomial-time algorithm. Now think of 1's representing pebbles, and suppose they are colored. The projections now count different colors separately. We succeeded to show that the problem is NP-complete for 3 colors [49], while previously this was known only for 6 colors. Unfortunately the 2 color case remains open. A generalization of this is the reconstructing problem of tilings, for a fixed set of tiles. First, attention was brought to the domino tiling case, which we could solve only partially [54]. In [48] we classify as best as we can the tile-sets for which the problem is NP-complete and the tile-sets for which it is polynomially solvable.

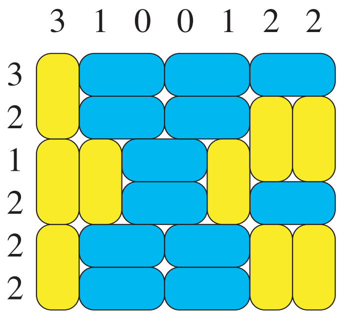


Figure 1: A domino tiling of a grid and its projections.

Enumerative combinatorics

Part of our work addresses questions in enumerative combinatorics, in particular the study of certain classes of polyominoes [132] and directed animals [50], as well as the study of sandpiles [51]. These combinatorial structures are related to models with phase transitions in statistical physics, or to discrete dynamical systems.

We have obtained enumeration results for several classes of convex polyominoes on the hexagonal lattice. These polyominoes are considered up to rotation and reflection, as objects living freely in space. We give explicit formulas or implicit functional equations for the generating series, which are convenient for computer algebra. Thus computation can be carried out up to area 70. We are also interested in enumeration of FPL configurations (Fully Packed Loops Configurations). There is a simple one-to-one correspondence between FPL and alternating-sign matrices. Recently, conjectures by J.-B. Zuber (CEA Saclay) have been proven in our subgroup, in conjunction with researchers at Claude Bernard University (Lyon-I).

Combinatorics on words

We focus in particular on (infinite) words generated by finite automata, also called "automatic sequences". The study of these sequences is at the frontier between combinatorics, theoretical computer science, number theory, harmonic analysis, fractals...

Although several results on the structure of automatic sequences as well as links and differences with cellular automata sequences have been obtained, a large part of our study deals with transcendence results for which the tools provided by finite automata prove very useful and give "simple" proofs. Transcendence of formal power series with nonzero characteristic has first been a natural domain to apply the theory of automatic sequences. More recent results deal with transcendence of real numbers: if the expansion of a real number in a given integer basis is "too regular", e.g., generated by a finite automaton, this number must be either rational or transcendental (it cannot be algebraic irrational). If the continued fraction expansion of a real number is "too regular", e.g., generated by a finite automaton, this number must be either quadratic or transcendental (it cannot be algebraic of degree larger than 3). Results in this direction can be found in [16] and [11] for example. A major achievement has been obtained by Adamczewski who proved the following result [5]: an irrational real number having block complexity in $O(n)$ must be transcendental (where the block complexity of an infinite sequence is given by the number of different subblocks of a given length occurring in the sequence). This result contains all previous results on the subject, although it is still far away of an old and still open conjecture by Borel, a weak form of which asserts that irrational numbers having a block complexity (in base b) strictly less than b^n must be transcendental.

Key references

[5] B. Adamczewski, Y. Bugeaud, and F. Luca. Sur la complexité des nombres algébriques. *Comptes Rendus de l'Académie des Sciences, Serie I*, 339(11-14), 2004.

[16] J.-P. Allouche, J. L. Davison, M. Queffélec, and L. Q. Zamboni. Transcendence of Sturmian or morphic continued fractions. *J. Number Theory*, 91(1):39-66, 2001.

[48] M. Chrobak, P. Couperus, C. Dürr, and G. Woeginger. On tiling under tomographic constraints. *Theoret. Comput. Sci.*, 290(3):2125-2136, 2003.

[50] S. Corteel, A. Denise, and D. Gouyou-Beauchamps. Bijections for directed animals on infinite families of lattices. *Ann. Comb.*, 4(3-4):269-284, 2000. Conference on Combinatorics and Physics (Los Alamos, NM, 1998).

[51] S. Corteel and D. Gouyou-Beauchamps. Enumeration of sand piles. *Discrete Math.*, 256(3):625-643, 2002. LaCIM 2000 Conference on Combinatorics, Computer Science and Applications (Montreal, QC).

Complexity Research team

- *Permanent members: Michel de Rougemont, Sophie Laplante, Frédéric Magniez, Miklos Santha.*
- *Non-permanent members: David Gross, Sylvain Peyronnet, Julien Stern.*

Logic brings some light on the inherent computational difficulty of problems, produces efficient methods for verification and a general framework where definability, provability are closely linked to complexity issues. In descriptive and algebraic complexity, one can produce upper bounds for decision, optimization and counting problems, as well as for their approximations.

Our work concerns Logic on finite models, Structural Complexity and Kolmogorov Complexity.

Logic

Model Checking is an important area of Logic in Computer Science. It proposes efficient techniques to verify a property of a transition system. Classical techniques use a compressed representation of relations such as OBDD or automata. We generalize this approach in two different ways: we first study definability question on compressed models and then study notions of approximate Model Checking.

Definability on compressed models

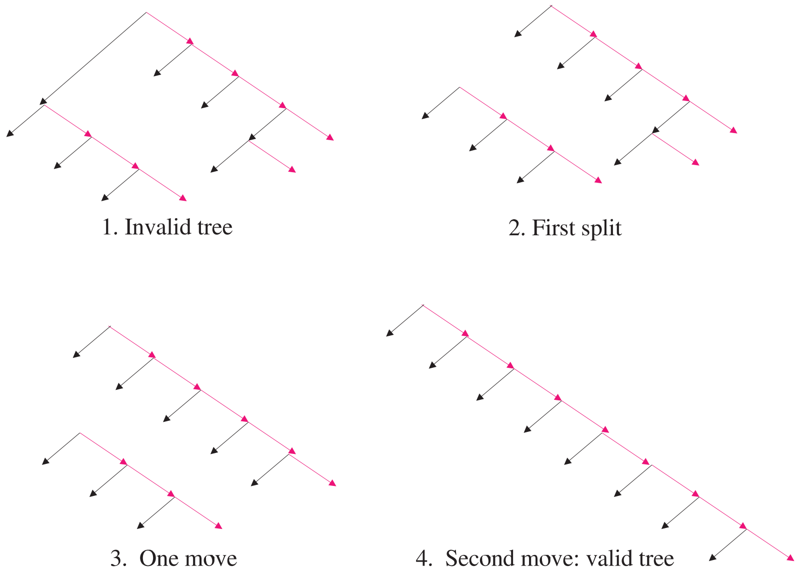
The Finite Model Theory tradition emphasizes methods of Model theory where complexity is measured by the number of variables, the number of alternations of the quantifiers or the length of the formulas, when a model is explicitly given. We consider models given in a compressed form and try to efficiently verify a property of the original structure. In [100], one studies finite compressed structures, for example the binary words compressed with various compression schemes. On the Run-length schema, any 1st order property on the words is also 1st order definable on the compressed words. On the Lempel-Ziv schema on the other hand, one shows that a 1st order property on the words is not necessarily 1st order definable on the compressed words but is definable in the FO(TC) logic. A property of words definable in the FO(TC) logic will be definable in the same logic on the compressed words, but with a double fixed-point arity. In [98] , we study the structure of automata for LZ-78, i.e. automata reading a compressed word and deciding a regular property. This type of result clarifies the role of the compression schemes for the verification of properties. It is important to know if specifications can be efficiently verified on compressed structures.

Approximate Model Checking

If exact Model Checking is too hard, from the complexity point of view, we study how to define “approximate verification”. In [144], we introduce an approximate verification based on property testing. If a specification has a tester, we show how to define a probabilistic abstraction of a syntactic program such that many errors will be detected with high probability. In the case of classes of regular trees, we develop testers in [149] and correctors in [114], particularly adapted to the correction and ranking of XML documents.

Structural Complexity

Testers have been used in numerical computation, structural complexity, and approximation algorithms. Nevertheless, only models for exact or approximate computations with absolute error had been considered. We showed that it was possible to generalize the testers in two important cases : when the authorized error is sublinear in the input size [77] ; and when the error is relative [148], i.e. proportional to the output size. We validated this extension by constructing testers for the linear or polynomial functions in the first case, and for the linear or multilinear functions in the second case. In [149], we studied property testing on the class of ordered trees and showed that regular tree properties have testers.



1. Invalid tree

2. First split

3. One move

4. Second move: valid tree

Figure 1: Operations on XML-trees to make them DTD-compliant (matching the document type definition).

Kolmogorov complexity

The work on Kolmogorov complexity concerns upper and lower bounds. It is a measure of the amount of randomness contained in the string. We have generalized this measure to quantum computing and have proven that it satisfies a certain number of important properties similar to its classical analog [110]. In [46], better bounds were given for a basic problem which has interesting consequences for the complexity of probabilistic classes, and for the comparison of counting and decision complexities. In [145], the link with quantum Kolmogorov complexity has been studied and allows to prove lower bounds for models of quantum computations.

Key references

[77] M. Kiwi, F. Magniez, and M. Santha. Approximate testing with error relative to input size. *J. Comput. System Sci.*, 66(2):371-392, 2003.

[100] F. Afrati, H. Leiß, and M. de Rougemont. Definability and compression. In *15th Annual IEEE Symposium on Logic in Computer Science (Santa Barbara, CA, 2000)*, pages 63-73. IEEE Comput. Soc. Press, Los Alamitos, CA, 2000.

[144] S. Laplante, R. Lassaigne, F. Magniez, S. Peyronnet, and M. Rougemont. Probabilistic abstraction for model checking: An approach based on property testing. In *Proceedings of 17th IEEE Symposium on Logic in Computer Science*, pages 30-39, 2002.

[145] 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*, 2004, pages 294-304.

[149] F. Magniez and M. Rougemont. Property testing of regular tree languages. In *Proceedings of 31st International Colloquium on Automata, Languages and Programming*, volume 3142 of *Lecture Notes in Comput. Sci.*, pages 932-944. Springer, 2004.

Quantum Computation Research team

- *Permanent members: Miklos Santha (head), Christoph Dürr, Julia Kempe, Sophie Laplante, Frédéric Magniez.*
- *Non-permanent members: Julien Degorre, Pierre Philipps, Yves Verhoeven, Perola Milman, Pranab Sen.*

Quantum computation has been a very active research area in the past 10 years. Feynman (Nobel prize 1965) initiated the idea of constructing a computer exploiting the laws of quantum mechanics, in order to solve problems that are intractable on classical machines. Today, two major results make the quantum model extremely attractive. Shor (Gödel prize 1999) found a quantum algorithm that factors any integer in polynomial time, rendering cryptosystems such as RSA vulnerable. Grover then found an optimal algorithm that finds a distinguished element in an unstructured space quadratically faster than any randomized algorithm.

Our research activity is first and foremost centered around studying the computational potential of quantum computing. We have contributed to the elaboration of the model, the development of complexity measures, and the construction of new quantum algorithms. We also have collaborations with physicists whose objective is to study the practical problems raised by the implementation of quantum computers.

Algorithms

Hidden Subgroup problem

Shor's Quantum algorithms for factoring and computing discrete logarithm come from the partial (ie, for abelian groups) resolution of a more general problem which is the Hidden Subgroup problem (HSP): Given a periodic function f on a group G, HSP is to determine efficiently the subgroup H of periods under the promise that f is injective on G/H. However, few results are known for non abelian groups. One of the most famous non abelian instances of HSP, where G is the symmetric group, is the Graph Isomorphism Problem which is one of the most important challenge of quantum computing.

We gave contributions to HSP twice. In [68], we showed how to combine Shor's results with the elegant theory of black-box groups of Babai and Beals. In particular, we generalized and simplified the previous works of Watrous (STOC'01) and Hallgren, Russell and Ta-Shma (STOC'00).

More recently [128], we solved HSP when the group G is solvable with constant exponent and constant length. This is proven by induction on the length of the composition series of G. Our induction is the first one to succeed for HSP. The base case is a partial solution of a largely studied problem (Ettinger, Høyer and Knill, STACS'99, Regev FOCS'02).

Another contribution is [129, 62], where we improved and extended a work of Buhrman, Fortnow, Newman, and Röhrig (SODA'03) constructing efficient quantum property testers for properties connected to HSP.

Collision problem

We also gave a new algorithm comparable to Grover's for the Collision problem: Given a non injective function f defined on a domain of size N, the problem is to find a collision pair (x,y) such that $x \neq y$ and $f(x)=f(y)$. This problem, which is purportedly hard classically, is important, because it is the basis of many cryptanalysis strategies against secret key cryptosystems. Moreover, the problem can be solved in time $O(N^{1/3})$ when the function has a linear number of collision pairs (Brassard, Høyer, and Tapp, ACM SIGACT News'97). This algorithm has been proven optimal (Aaronson, STOC'02 and Shi, FOCS'02).

We gave [115] a quantum algorithm in $O(N^{3/4})$ that finds a collision pair in the general case. The optimality of this algorithm was an open problem until this year. Recently, Ambainis showed that $N^{2/3}$ is the correct answer using a quantum walk based algorithm (Ambainis, FOCS'04), which is optimal due to Aaronson and Shi.

Local Search

A way of relaxing the minimum/maximum finding problem is to look for a solution which is optimal only in some neighborhood structure. Studying these new problems has lead Johnson, Papadimitriou and Yannakakis to introduce the Polynomial Local Search (PLS) class.

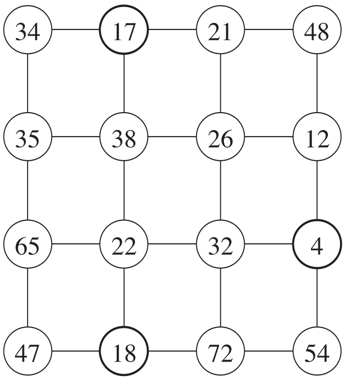


Figure 1: Finding a local minimum in a given graph

The class PLS is a subset of TFNP, the family of total function problems from NP. One can consider this class as a potential source of problems which might admit efficient quantum algorithms. Another important subclass of TFNP is PPP (Polynomial Pigeonhole Principle) which contains the Collision problem. Lower bounds by Aaronson and Shi imply that the deterministic and quantum query complexities of PPP problems are polynomially related.

We [154] proved an analogous result for PLS. As a consequence, if an efficient quantum algorithm is ever to be found for a problem in PLS, it must exploit its specific structure. Another consequence is the previously unknown relation between deterministic and randomized query complexities.

Graph properties

We considered quantum algorithms for natural graph problems both in the adjacency matrix model and in an adjacency list-like array model. We gave almost tight lower and upper bounds for the bounded error quantum query complexity of Connectivity, Strong Connectivity, Minimum Spanning Tree, and Single Source Shortest Paths. All our results improve classical ones.

Quantum Walks

In [87] we introduced a new quantum walk based algorithm to simulate Grover Search algorithm on an unstructured database. Our approach has been successfully applied and improved by Ambainis (FOCS'04) to give a tight algorithm for finding a collision pair when the number of such pairs is unknown. It has also been shown by Szegedy (FOCS'04) that quantum walks on graphs search is quadratically faster than classical walks.

In [137] we studied the hitting time of a discrete quantum walk and showed that its behaviour differs strikingly form its classical counterpart. We showed that on the hypercube of dimension n the quantum walk needs only time poly(n) to hit the opposite corner from the starting position, whereas a classical work needs exponential time to hit that corner.

Complexity

Complexity classes

A seminal result in classical complexity theory is the celebrated Cook-Levin theorem which states that 3-SAT is NP-complete. Kitaev gave a quantum analogue of the above results where NP is now the quantum analogue of the class MA, that is QMA. Kitaev found a natural analogue of the SAT problem, the Local Hamiltonian problem, whose k-local version is NP-hard for all $k \geq 2$, and QMA-complete for $k \geq 5$.

We [70] showed that already 3-local Hamiltonian is QMA-complete, by using a strong projection on the "legal" space of states. Moreover, we have recently extended this result to 2-local Hamiltonian (in submission).

Models

We have formally defined a quantum version of cellular automata, which is both a model of computation and a physical model [55]. We then solved the problem of detecting feasible instances. This was important to verify the modern version of Church-Turing Thesis in the quantum world. Independent of us, similar research on quantum cellular was done by van Dam and Watrous.

We have recently shown [102] that any standard quantum algorithm, i.e. based on the circuit model, can be equivalently represented as an adiabatic algorithm. This equivalence gives a strong indication that the adiabatic technique is a powerful technique that could lead to the discovery of new quantum algorithms. Adiabatic computing has been introduced by Farhi (Science'01).

Communication Complexity

We also have contributions [86, 135] in quantum Communication Complexity. Here two participants can use a quantum channel for communicating more efficiently than classically.

Physical Aspects

Quantum testing

The goal of quantum testing is to develop procedures to test whether a quantum computing device correctly computes what it purports to do. Mayers and Yao (FOCS'98) described how to carry out testing if a photon source is good enough to be used in the quantum key distribution protocol of Bennett and Brassard. We [157] showed that it is possible to test quantum gates classically.

Implementations

It has been shown earlier (Kempe et al. 2000) that the exchange interaction alone is universal, provided the quantum state is encoded in a specific fashion. In [67] we give the explicit encoding of one qubit into four qubits that achieves this.

In [71] we detail the proof that the XY-interaction (anisotropic exchange) is universal with encoding.

In [88] we study the robustness of several entangled states in the following model: each qubit is subject to a partially depolarizing channel with some noise rate.

We also have other contributions in the geometry of 2-qubit systems [82], the implementation of quantum algoritms using cavity QED [83], and the manipulation of phase gates using selective interaction [89].

Perspectives

We will continue to look for efficient algorithms. One of the algorithmic technique that we intend to explore is quantum walks. Recently, vast progress has been made in the application of quantum walks to improve quantum algorithms. Another important algorithmic technique that we intend to pursue is adiabatic computing. The equivalence of this model to the standard one motivates us to discover new algorithms based on adiabatic computing.

In classical cryptography, many cryptographic tasks require hardness assumptions. In the quantum world, there are provably secure protocols for key distribution based only on validity of quantum mechanics, with no hardness assumptions. A major open question, one which we would like to contribute to, is whether similar quantum protocols exist for other cryptographic tasks. Probably one of those protocols that has generated the most exciting developments recently is Coin flipping.

It may be possible to combine our approach of testing quantum gates with Mayers and Yao's for testing quantum sources so that the tester is not required to trust the measurement devices nor the source of classical and quantum states. This has both theoretical and practical interest since it is motivated by recent implementations of quantum computing based on NMR for which even classical states are hard to prepare.

Key references

[102] 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)*, 2004.

[126] C. Dürr, M. Heiligman, P. Høyer, and M. Mhalla. Quantum query complexity of some graph problems. In *Proceedings of the 31st International Colloquium on Automata, Languages* *and Programming (ICALP)*, pages 481-493, 2004.

[128] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden translation and orbit coset in quantum computing. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1-9, 2003.

[154] M. Santha and M. Szegedy. Quantum and classical query complexities of local search are polynomially related. In *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC)*, pages 494-501, 2004.

[157] W. van Dam, F. Magniez, M. Mosca, and M. Santha. Self-testing of universal and fault-tolerant sets of quantum gates. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC)*, pages 688-696, 2000.

Research Perspective

Our group is a federation of autonomous researchers, and is well integrated in the international scientific community. The number of high level publications and research grants witnesses the quality of its members. Scientific excellence is and will remain in the future as our highest aspiration.

Algorithmics remains our federating field. Nonetheless, with the departure of four senior members, this theme has suffered serious losses, and it needs reinforcing in the coming years. This could come from hiring new persons in the group and from promotion of our assistant professors.

We consider that teaching and advising of doctoral students remains a central piece of the healthy life of our group. We take our contributions to the new master programs very seriously, including the MPRI where seven team members give lectures, and one course is entirely taught by us. We feel that the fact that currently none of our members has a teaching position at the University Paris-Sud, Centre d'Orsay, is a serious drawback, and will try to correct it.

Between January and April 2006 we will co-organize the program "Quantum information, computation and complexity" at the Institut Henri Poincaré in Paris. During this semester will take place the ninth Workshop on Quantum Information Processing, organized by our group. This workshop is the single most important annual event in quantum computation.

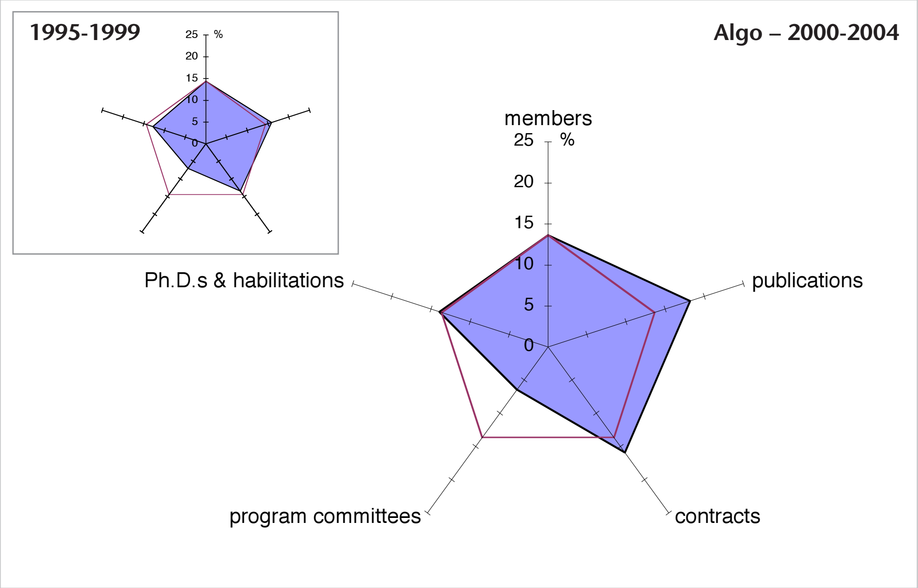
Finally we can only hope that our distinguished team member W. Fernandez de la Vega, praised by the international community for his high quality and innovative research work covering several fields over more than thirty years, will soon be promoted by the CNRS to the DR position.

B.2.3 / Algo

Highlights

During this period our group has produced 10 STOC papers (ACM Symposium on the Theory of Computing), 4 FOCS papers (IEEE Symposium on Foundations of Computer Science) which are the two best general conferences in theoretical computer science, together with 4 SODA papers (Symposium on Discrete Algorithms) and 3 CCC papers (IEEE Conferences on Computational Complexity). Jean-Paul Allouche has published an impressive list of 14 journal papers.

Our team is involved in few program committees but these are from prestigious conferences. The evolution over the years is quite smooth; the increase in contracts over the past four years is due to our research in quantum computing.



Radar views display a synthetic view of the activity of the group over the 1995-1999 and 2000-2004 periods, by means of five statistics:

- *Size of the group at the end of the period (01/01/1999, 01/01/2004),*
- *Number of publications (peer-reviewed journals, books, book chapters, major international conferences),*
- *Annualised amount in Euro of new contracts and grants,*
- *Number of participations in program committees (national and international),*
- *Number of defended Ph.D.s and habilitations.*

These statistics are displayed as a percentage with respect to the overall laboratory, together with a reference line corresponding to the size of the group. Data points outside the reference line show above-average performance whereas those inside the line show below-average performance, relative to the laboratory.

As with any statistics, these data must be interpreted carefully. In particular, they are not a direct measure of relative quality of the groups within the laboratory, because different research areas place different values and offer different opportunities with respect to these five measures.

Honors

Prizes and awards

- Christoph Dürr, best paper award at the *International Colloquium on Automata, Languages and Programming Conference track* A (ICALP'04), Turku, Finland, July 2004.
- Julia Kempe, *Bernard Friedman Memorial Prize for the best Ph.D. dissertation in the applied sciences, Department of Mathematics*, UC Berkeley in May, 2002.
- Frédéric Magniez, AFIT (*Association Française d'Informatique Théorique*) prize for best Ph.D. thesis in Theoretical Computer Science, 2000.

Keynote addresses

- Jean-Paul Allouche, *Aperiodic Order Workshop*, Edmonton, Canada, 2000.
- Jean-Paul Allouche, *Aperiodic Order Workshop*, Oberwohlfach, Allemagne, 2001.
- Jean-Paul Allouche, *29e École de Printemps d'Informatique Théorique*, Cessac, 2001.
- Jean-Paul Allouche, *Discrete Models. Combinatorics, Computation and Geometry*, IHP Paris, 2001.
- Jean-Paul Allouche, *Journées Montoises d'Informatique Théorique*, Montpellier, 2002.
- Jean-Paul Allouche, *Journées Arithmétiques*, Graz, Autriche, 2003.
- Julia Kempe, *International Conference on Quantum Information: Conceptual Foundations, Developments and Perspectives*, Oviedo, Spain, 2002.
- Julia Kempe, *Conference on Inhomogeneous Random Systems*, Cergy-Pontoise, France, 2003.
- Julia Kempe, invited talk in the *Workshop on Quantum Information Processing*, Waterloo, 2004.
- Frédéric Magniez and Miklos Santha, *1st Conference on Theoretical Aspects of Computer Science*, Tehran, 2000. Exact and Approximate Testing/Correcting of Algebraic Functions: A Survey, Lecture Notes in Comput. Science, volume 2292, pages 30-83.
- Frédéric Magniez, invited talk in the *Workshop on Quantum Information Processing*, Waterloo, 2004.
- Miklos Santha, *2nd European Quantum Information Processing and Communication Workshop*, Torino, 2001.
- Miklos Santha, *6th Workshop on Quantum Information Processing*, Berkeley, 2002.
- Miklos Santha, *Gordon Research Conference on Quantum Information Science*, Ventura, California, 2004.
- W. Fernandez De La Vega, *Journée de l'Informatique Messine*, 2000.

Other honors

- Miklos Santha, member of the *STACS steering committee (International Symposium on Theoretical Aspects of Computer Science)* since 2002.

Evaluation of research

Editorial boards

- *Advances in Applied Mathematics*: Jean-Paul Allouche
- *Journal de Théorie des Nombres de Bordeaux*: Jean-Paul Allouche
- *Journal of Integer Sequences*: Jean-Paul Allouche
- *Mathématiques et Sciences Humaines*: Jean-Paul Allouche
- Special issues of *Theoretical Computer Science*, 2001: Yannis Manoussakis, co-editors: G. Chang, M. Deza and J-M. Steyaert.

Program committees

International events

- 31st *Annual Conference on Current Trends in Theory and Practice of Informatics*, to be held at Slovak Republic, January 2005: Frédéric Magniez
- RNC6, *Real Numbers and Computers*, Schloss Dagstuhl, Germany, 2004; RNC5, Ecole Normale Supérieure de Lyon, 2003; RNC4, Schloss Dagstuhl, Germany, 2000: Jean-Paul Allouche
- 17th *Conference on Learning Theory*, Banff, Canada, 2004: Stéphane Boucheron
- *Conference on graph theory in memory of Claude Bergé*, 2004: W. Fernandez De La Vega
- ICALP, 29th and 31st *International Colloquium on Automata, Languages and Programming*, Malaga 2002, Turku, 2004: Claire Kenyon (2002), Miklos Santha (2004).
- 45th Annual IEEE *Symposium on Foundations of Computer Science*, Rome, 2004: Miklos Santha
- 14th *International Symposium on Fundamentals of Computation Theory*, Malmö, 2003: Miklos Santha
- IEEE *Conference on Computational Complexity*, 2002: Sophie Laplante
- FOCS, 43rd Annual IEEE *Symposium on Foundations of Computer Science*, Vancouver, 2002: Claire Kenyon.
- FPSAC, *Formal Power Series and Algebraic Combinatorics*, Scottsdale, Arizona, 2001: Alain Denise
- LICS, IEEE *Logic in Computer Science*, 2001: Michel de Rougemont
- CIAC, 4th *Italian Conference on Algorithms and Complexity*, Rome 2000: Yannis Manoussakis

National events

- EA01, *Cinquième Conférence Internationale sur l'évolution Artificielle*, Université de Bourgogne, 2001: Jean-Paul Allouche
- Huitièmes *Journées Montoises d'Informatique Théorique*, Université Marne-la-Vallée, 2000: Jean-Paul Allouche

Evaluation committees and invited expertise

- National committee for scientific research, *Comité National de la Recherche Scientifique*, section 01 (mathematics) and section 44 (bioinformatics): Jean-Paul Allouche, member
- EU IST Programme, FET ALCOM-FT Project, 2001, 2002, 2004: Miklos Santha, reviewer
- National Science Foundation ITR proposals, Washington D.C., 2003: Julia Kempe, panel member

Other evaluation activities

- Reviewer for several EU IST Programme: Miklos Santha
- Reviewer for Ph.D. dissertation: Yannis Manoussakis (1), Michel de Rougemont (1), Miklos Santha (1)

Volunteer professional service

Management positions in scientific organisations

- International Symposium on Fundamentals of Computation Theory, FCT: Miklos Santha, member of the steering committee since 1999.
- Workshop on Quantum Information Processing, QIP: Miklos Santha, member of the steering committee since 2002.
- European annual workshop on Kolmogorov complexity, TAI: Sophie Laplante, member of steering committee, 1998-2002.
- National network on Quantum Information and Communication (“*GdR Information et Communication Quantique*”): Miklos Santha, member of the board, 2001-2004.
- CNRS Working group (“Action Spécifique”) Nouveaux Modèles de Calcul: Algorithmes et Complexité: Miklos Santha, co-chair with Etienne Grandjean, 2001-2002.
- Jeune Equipe Informatique Quantique, funded by national program (“Action incitative”) for junior researchers: Miklos Santha, director, 2002-2003.

Organisation of conferences and scientific events

- Special day in honor of Kolmogorov’s 100th birthday, Complexity, Information, and Randomness: The Legacy of Andrei Kolmogorov held in conjunction with IEEE Conference on Computational Complexity 2003: Sophie Laplante, organizer.
- Meeting on the technical challenges for the developpement of web TV platforms for pupils, December 2003, Orsay, Paris: Yannis Manoussakis, organizer.
- Meeting on the use of new media and internet TV as educational tools, March 2003, Orsay, Paris: Yannis Manoussakis, organizer.
- *Journées de l’Action spécifique Nouveaux modèles de calcul*, November 2002, Paris: Sophie Laplante and Frédéric Magniez, organizers.
- RAND-APX workshop, April 2002, Paris: Christoph Dürr, Sophie Laplante, Frédéric Magniez and Miklos Santha, organizers.
- Workshop ALEA 2002, CIRM Marseille, March 2002: Dominique Gouyou-Beauchamps, co-organizer.
- Worskhop, “Complexity and finite models”, University Paris II, 2002: Michel de Rougemont, organizer.
- Workshop *Information Quantique: Aspects Théoriques* at the Institut Poincaré, Paris, November 2001: Miklos Santha, co-organizer.
- European annual workshop on Kolmogorov complexity, TAI, September 2001, Porquerolles, France: Sophie Laplante, local arrangements.
- *Journée de veille et prospective de l’ASTI: Le traitement quantique de l’information*, Paris, October 2000: Miklos Santha, organizer.
- Conference in the Honor of Michel Mendès France, Bordeaux, 2000: Jean-Paul Allouche, co-organizer.

Contracts and grants

Type	*Scientific Director*	*Project Name*	*Funding institution*	*Managing institution*	*Dates*	*Duration (months)*	*Total €*
IST	M. Santha	QAIP	EU	CEPHYTEN	01/02/00-31/12/02	36	159 921
IST	M. Santha	RESQ	EU	CEPHYTEN	20/12/02-19/12/05	36	283 000
IST	M. Santha	RAND APX	EU	CEPHYTEN	1/07/00-31/12/03	42	24 420
SOCRATE	Y. Manoussakis	WEB TV	EU	UPS/SAIC	01/10/02-30/09/04	24	25 000
IST	W. Fernandez de la Vega	APPOL	EU	CEPHYTEN	1/05/00-30/04/01	12	9 000
IST	W. Fernandez de la Vega	APPOL 2	EU	CEPHYTEN	01/11/01-31/10/04	36	28 440
IST	C. Kenyon	Approximation on online algo.	EU	CEPHYTEN	08/10/01-07/11/04	36	13 739
ACI	S. Boucheron	GAP (NIDM)	MENRT	CNRS	20/08/03-19/08/06	36	7 525
ACI	F. Magniez	Applications of quantum computation	MENRT	CNRS	16/08/02-15/08/05	36	62 708
ACI	Julia Kempe	Computer networks (SI)	MENRT	CNRS	25/07/03-10/07/06	36	41 806
ACI (SI)	M. de Rougement	Approximate verification	MENRT	CNRS	15/09/03-04/09/06	36	45 150
ACI	J.P. Tillich	Error correcting codes and cryptography	MENRT	CNRS	2001-2003		75 000
AI (JC)	M. Santha	Quantum computer science	CNRS STIC	CNRS	22/10/01-21/10/03	24	25 958
AS	M. Santha	New models of computation	CNRS STIC	CNRS	01/10/01-31/09/02	12	16 007
CIFRE	S. Boucheron	STE MASA		UPS/SAIC	13/01/03 - 12/01/06	36	12 501

Note: See the glossary for acronyms.

Summary of main projects

QAIP

Partners: CWI, Amsterdam, the Netherlands; University of Latvia, Riga, Latvia; Oxford University, UK; University of Bristol, UK; University of Aarhus, Denmark; Hebrew University, Jerusalem, Israel; Weizmann Institute, Rehovot, Israel; Technion, Haifa, Israel; University of Waterloo, Canada; McGill University, Montreal, Canada; Université de Montréal, Canada; University of Calgary, Canada; University of California at Berkeley, USA.

European Commission grant IST-1999-11234

QAIP (Quantum Algorithms and Information Processing), 01/01/2000-31/12/2002.

Scientific director for LRI: Miklos Santha.

QAIP's main objective was to study quantum computing from a computer science angle. The project has focused on showing that quantum computers are actually useful, by exhibiting tasks which they can do significantly better/faster than classical computers. Its goals were to develop new algorithms and analyse the complexity of relevant problems on a quantum computer; to develop new forms of cryptography that make use of quantum mechanics; and to develop and improve methods for error correction in quantum computers.

RESQ

European Commission grant IST-2001-37559, RESQ (Resources for quantum information), 01/01/2003-31/12/2005.

Scientific director for LRI: Miklos Santha.

Partners: Université Libre de Bruxelles, Belgium; CWI, Amsterdam, the Netherlands; University of Bristol, UK; Max Planck Institute for Quantum Optics, Germany; University of Utrecht, Netherlands; MTA SZTAKI, Hungary; University of Geneva, Switzerland; University of Cambridge, United Kingdom; University of Gdansk, Poland; University of Waterloo, Canada.

RESQ is an interdisciplinary project grouping together 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. More specific objectives of the project are to understand how quantum information can be manipulated in small scale systems; to improve our understanding of the nature of quantum information, both at a fundamental level and from the pragmatic point of view of testing quantum systems; to understand how information can be processed in distributed quantum systems, both from the point of view of algorithms and from the point of view of security and cryptography; and to design new quantum algorithms, study the power of quantum property testers, and explore the ingredients of a basic toolkit for designing quantum algorithms.

RAND-APX

European Commission grant IST-1999-14036 RAND-APX (Randomised and Approximate Computation), 01/07/2000-31/12/2003.

Scientific director for LRI: Miklos Santha.

Partners: University of Oxford, UK; University of Bonn, Germany; University of Edinburgh, UK; University of Leeds, UK; University of Lund, Sweden; Weizmann Institute, Israel.

The project's aim was to pursue studies in the areas of randomised, approximate, and quantum computation. It has covered novel and enhanced methods for the design and analysis of efficient randomised and quantum algorithms for problems of measurement and communication theory, which are totally intractable by existing methods.

WEB TV

European SOCRATE grant for the development of an Internet TV platform for pupils, 2002-2004.

Scientifc director: Yannis Manoussakis.

In the field of education, the use of the technology possibilities requires research and development to ensure the efficiency of these techniques. An important challenge is how to create and experiment with new learning paradigms that take into account this new technology. The WebTV project focuses on the growth and development of webcasting and streaming media over the Internet and their use in educational contexts where students are not simple consumers but creators and producers. The partners include European schools, private companies and educational and computer science university departments.

Collaborations

Cooperation agreements

- CNRS/NSF grant between Christoph Dürr (LRI), Philippe Baptiste (Polytechnique) and Marek Chrobak (UC Riverside), 2003-2006.
- EGIDE Pessoa bilateral grant between Sophie Laplante (LRI) and Luis Antunes (Universidade do Porto, Portugal), 2002-2004.
- EGIDE Procope bilateral grant between Michel de Rougemont (LRI) and Hans Leiss (Munich University), 2002.
- EGIDE Alliance bilateral grant between Michel de Rougemont (LRI) and Marta Kwiatkowksa (University of Birmingham), 2003-2004.

Collaborations leading to joint publications

We list the affiliations of some of our co-authors.

France

- Ecole Polytechnique (K. Artiouchine, P. Baptiste, C. Léonard)
- ENS Paris (J. Stern), ENS Lyon (E. Rémila, G. Theyssier)
- ENST, Paris (G. Zémor)
- INRIA Rocq. (P. Flajolet, H. Ollivier, M. Golin)
- INRIA Sophia Ant. (M. Cosnard)
- Lab. Leibniz, Grenoble (M. Mhalla)
- Math. Lab. of Univ. Paris-11 (E. Gassiat, P. Massart)
- Univ. of Bordeaux-1 (M. Bousquet-Mélou)
- Univ. of Caen (J.-C. Carlach)
- Univ. of Grenoble (C. Simon)
- Univ. of Montpelier-2 (V. Berthé)
- Univ. of Paris-13 (C. Banderier)
- Univ. of Paris-6 (J. Cassaigne, I. Guessarian)
- Univ. of Paris-7 (M. Courbage, R. Lassaigne, R. Mosseri)
- Univ. of Paris-8 (C. Carlet)
- Univ, of Toulouse-3 (F. Gamboa)
- Univ. of Versailles (D. Barth, D. Gardy)

Europe

- CWI, Amsterdam (H. Buhrman, R. de Wolf)
- IBM Research, Zurich (G. Cheliotis)
- MTA SZTAKI, Budapest (K. Friedl, G. Ivanyos, Z. Tuza)
- National Technical Univ. of Athens (F. Afrati)
- Max-Planck Institut Tübingen (O. Bousquet)
- Pompeu Fabra Univ., Barcelone (G. Lugosi)
- TU Graz (R. F. Tichy)
- Univ. of Aarhus (P. Bro Miltersen)
- Univ. of Bielefeld (M. Baake)
- Univ. of Athens (I. Milis)
- Univ. of Bonn (M. Karpinski)
- Univ. of Bremen (G. Skordev)
- Univ. of Cambridge, UK (R. R. Weber)
- Univ. of Kiel (A.V. Fishkin)
- Univ. of Munich (H. Leiss, K. Jansen)
- Univ. of Paderborn (S. L. Bezrukov, R. Elsässer, B. Monien, R. Preis)
- Univ. of Rome-1 (T. Calamoneri, I. Finocchi, R. Petreschi)
- Univ. of Szeged (J. Csirik)
- Univ. of Twente (G. Woeginger)

USA

- AT&T Labs (D. S. Johnson)
- Caltech (D. Bacon, D. Damanik, A. Kitaev, L. J. Schulman)
- dePaul Univ., Chicago (A. Berthiaume)
- Georgia Institute of Technology, Atlanta (D. Randall)
- Harvard Univ. (M. Mitzenmacher)
- IBM Watson Research Center (D. DiVincenzo)
- MIT (S. Lloyd, J. B. Orlin, P. W. Shor)
- NSA (M. Heiligman)
- Rutgers Univ. (M. Szegedy)
- UC Berkeley (D. Aharonov, P. Bartlett, R Jain, E. Mossel, Y. Peres, S. Myrgren, N. Shenvi, U. V. Vazirani, K.B. Whaley)
- UC Riverside (M. Chrobak, N. E. Young)
- UC Santa Barbara (W. van Dam)
- Univ. of Chicago (L. Fortnow)
- Univ. of Washington (A.R. Karlin)
- Yale Univ. (R. Kannan)

Other countries

- Hebrew University of Jerusalem (D. Malkhi, A. Shalev)
- Santiago de Chile (I. Rapaport, E. Goles, M. A. Kiwi)
- Tata Institute of Fundamental Research, India (J. Radhakrishnan)
- Technion (Y. Rabani)
- Tel Aviv Univ. (N. Alon, H. Kaplan, M. Krivelevich, O. Regev)
- Univ. Mexico (F. Luca, N. Vakhania)
- Univ. of British Columbia (W. Evans, J. Friedman)
- Univ. of Calgary (P. Høyer)
- Univ. of Québec, Montréal (P. Leroux)
- Univ. of Waterloo (A. Ambainis, M. Mosca, J. Shallit)
- Univ. of Toronto (D. Lidar)

B.2.9 / Algo

Dissemination and technology transfer

Summer schools, tutorials, invited seminars

- Stéphane Boucheron gave a course on Concentration Inequalities at the Machine Learning Summer School at Max-Planck Institut Tübingen, Germany, august 2003.
- Christoph Dürr gave a course on the quantum search algorithm at the Winter School *Logique et interaction* (Logic and interaction) in the section *algorithmic complexity* at Luminy, France, january 2002.
- Christoph Dürr gave an introduction to quantum computation at the *journées informatiques X-UPS* in the Ecole Polytechnique, may 2004.
- W. Fernandez De La Vega was "Mercator" invited professor for one year in Univ. of Bonn, Germany.
- Miklos Santha gave a course on *Exact and approximate testing/correcting of algebraic functions: A survey* at the *1st Summer School on Theoretical Aspects of Computer Science*, Tehran, july 2000. A corresponding survey with Marcos Kiwi and Frédéric Magniez was published in LNCS, volume 2292, pages 30-83.
- Miklos Santha gave introductory seminars to the students of the ENS Cachan in september 2001 and in september 2003 on quantum computing.
- Miklos Santha gave an introductory seminar on quantum computing for the students of the *Ecole Doctorale* at Paris-Sud in computer science, march 2003.

Training and education (doctoral and post-doctoral)

Defended habilitations

Name	Date defended	Current Position
DENISE Alain	10/12/01	Prof. LRI, Bioinformatics
BOUCHERON Stéphane	3/04/02	Prof. Paris-7
YAO Jia-Yan	26/06/03	Wuhan University, China

Defended doctorates

MAGNIEZ Frédéric	27/01/00	CR, CNRS
CORTEEL Sylvie	31/01/00	CR, CNRS
GROSS David	12/12/00	MC, Arts et Métiers, Paris
STERN Julien	23/03/01	created a company
VERHOEVEN Yann	11/06/01	INRIA, Sophia-Antipolis
BARBAY Jérémy	24/09/02	U. of Waterloo, Canada
OLOCCO Grégory	4/04/03	Air Liquide
PEYRONNET Sylvain	17/12/03	EPITA

Graduate courses

- DEA *Modélisation stochastique* 2000-2003, Information theory, compression and coding: Stéphane Boucheron, Jean-Pierre Tillich
- DEA *Algorithmique* 2000/2001, algorithms: Jean-Pierre Tillich
- DEA *Algorithmique* 2000/2002, enumerative combinatorics and random generation: Dominique Gouyou-Beauchamps
- DEA *Algorithmique* 2001/2003, quantum computation and quantum information theory: Frédéric Magniez, Miklos Santha
- DEA *Algorithmique* 2002/2003, quantum computation and quantum information theory: Christoph Dürr, Julia Kempe, Frédéric Magniez, Miklos Santha
- DEA *Algorithmique* 2002/2003, approximation algorithms and property testing: Sophie Laplante, Frédéric Magniez
- DEA *Algorithmique* 2003/2004, quantum computation and quantum information theory: Christoph Dürr, Miklos Santha
- DEA *Algorithmique* 2003/2004, property testing and communication complexity: Sophie Laplante, Frédéric Magniez
- DEA *Logique* de Paris VII 2003-2005, Logic and games, Michel de Rougemont
- *Master of Computer Sciences*, University of Crete, 2002-2004, Computational geometry/ Cryptography: Yannis Manoussakis

Publications

International peer-reviewed journals

[1] B. Adamczewski. Codages de rotations et phénomènes d'autosimilarité. *J. Théor. Nombres Bordeaux*, 14(2):351-386, 2002.

[2] B. Adamczewski. Balances for fixed points of primitive substitutions. *Theoret. Comput. Sci.*, 307(1):47-75, 2003. Words.

[3] B. Adamczewski. Répartition des suites (*n*&alpha;) *n* in *N* et substitutions. *Acta Arith.*, 112(1):1-22, 2004.

[4] B. Adamczewski. Transcendance "à la Liouville" de certains nombres réels. *C. R. Math. Acad. Sci. Paris*, 338(7):511-514, 2004.

[5] B. Adamczewski, Y. Bugeaud, and F. Luca. Sur la complexité des nombres algébriques. *Comptes Rendus de l'Académie des Sciences, Serie I*, 339(11-14), 2004.

[6] B. Adamczewski and J. Cassaigne. On the transcendence of real numbers with a regular expansion. *J. Number Theory*, 103(1):27-37, 2003.

[7] B. Adamczewski and D. Damanik. Linearly recurrent circle map subshifts and an application to Schrödinger operators. *Ann. Henri Poincaré*, 3(5):1019-1047, 2002.

[8] F. Afrati, E. Bampis, C. Kenyon, and I. Milis. A PTAS for the average weighted completion time problem on unrelated machines. *J. Sched.*, 3(6):323-332, 2000. Approximation algorithms, Part 2.

[9] F. Afrati, I. Guessarian, and M. de Rougemont. The expressiveness of DAC. *Theoret. Comput. Sci.*, 286(1):3-32, 2002. Mathematical foundations of computer science (Bratislava, 1997).

[10] F. Afrati, H. Leiß, and M. de Rougemont. Definability and compression. *Fund. Inform.*, 56(1-2):155-180, 2003. Special issue on computing patterns in strings.

[11] J.-P. Allouche. Nouveaux résultats de transcendance de réels à développement non aléatoire. *Gaz. Math.*, 84:19-34, 2000.

[12] J.-P. Allouche, M. Baake, J. Cassaigne, and D. Damanik. Palindrome complexity. *Theoret. Comput. Sci.*, 292(1):9-31, 2003. Selected papers in honor of Jean Berstel.

[13] J.-P. Allouche and M. Cosnard. The Komornik-Loreti constant is transcendental. *Amer. Math. Monthly*, 107(5):448-449, 2000.

[14] J.-P. Allouche and M. Cosnard. Non-integer bases, iteration of continuous real maps, and an arithmetic self-similar set. *Acta Math. Hungar.*, 91(4):325-332, 2001.

[15] J.-P. Allouche, M. Courbage, and G. Skordev. Notes on cellular automata. *Cubo Mat. Educ.*, 3(2):213-244, 2001.

[16] J.-P. Allouche, J. L. Davison, M. Queffélec, and L. Q. Zamboni. Transcendence of Sturmian or morphic continued fractions. *J. Number Theory*, 91(1):39-66, 2001.

[17] J.-P. Allouche, J.-M. Deshouillers, T. Kamae, and T. Koyanagi. Automata, algebraicity and distribution of sequences of powers. *Ann. Inst. Fourier (Grenoble)*, 51(3):687-705, 2001.

[18] J.-P. Allouche, M. Mendès France, and J. Peyrière. Automatic Dirichlet series. *J. Number Theory*, 81(2):359-373, 2000.

[19] J.-P. Allouche, N. Rampersad, and J. Shallit. On integer sequences whose first iterates are linear. *Aequ. Math.*, 2004. To appear.

[20] J.-P. Allouche, K. Scheicher, and R. F. Tichy. Regular maps in generalized number systems. *Math. Slovaca*, 50(1):41-58, 2000.

[21] J.-P. Allouche and J. Shallit. Sums of digits, overlaps, and palindromes. *Discrete Math. Theor. Comput. Sci.*, 4(1):1-10 (electronic), 2000.

[22] J.-P. Allouche and J. Shallit. The ring of *k*-regular sequences. II. *Words*, 307(1):3-29, 2003, Elsevier Science Publishers.

[23] J.-P. Allouche and G. Skordev. Schur congruences, Carlitz sequences of polynomials and automaticity. *Discrete Math.*, 214(1-3):21-49, 2000.

[24] J.-P. Allouche and G. Skordev. Remarks on permutive cellular automata. *J. Comput. System Sci.*, 67(1):174-182, 2003.

[25] N. Alon, W. F. de la Vega, R. Kannan, and M. Karpinski. Random sampling and approximation of max-csp problems. In *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC)*, pages 232-239, 2002.

[26] N. Alon, W. F. de la Vega, R. Kannan, and M. Karpinski. Random sampling and approximation of MAX-CSPs. *Journal of Computer and System Sciences*, 67(2):212-243, 2003, Elsevier Science Publishers. Special issue on STOC2002 (Montreal, QC).

[27] N. Alon, H. Kaplan, M. Krivelevich, D. Malkhi, and J. P. Stern. Scalable secure storage when half the system is faulty. *Inf. Comput.*, 174(2):203-213, 2002.

[28] A. K. Amoura, E. Bampis, C. Kenyon, and Y. Manoussakis. Scheduling independent multiprocessor tasks. *Algorithmica*, 32(2):247-261, 2002, Springer-Verlag.

[29] E. Bampis, A. Giannakos, A. Karzanov, Y. Manoussakis, and I. Milis. Perfect matching in general vs. cubic graphs: a note on the planar and bipartite cases. *Theor. Inform. Appl.*, 34(2):87-97, 2000.

[30] C. Banderier, M. Bousquet-Mélou, A. Denise, P. Flajolet, D. Gardy, and D. Gouyou-Beauchamps. Generating functions for generating trees. *Discrete Math.*, 246(1-3):29-55, 2002. Formal power series and algebraic combinatorics (Barcelona, 1999).

[31] P. Baptiste, M. Chrobak, C. Dürr, W. Jawor, and N. Vakhania. Preemptive scheduling of equal-length jobs to maximize weighted throughput. *Oper. Res. Lett.*, 32(3):258-264, 2004.

[32] D. Barraez, S. Boucheron, and W. Fernandez de la Vega. On the fluctuations of the giant component. *Combin. Probab. Comput.*, 9(4):287-304, 2000.

[33] P. Bartlett, S. Boucheron, and G. Lugosi. Model selection and error estimation. *Machine Learning*, 48:85-113, 2002.

[34] C. Bazgan, W. Fernandez de la Vega, and M. Karpinski. Polynomial time approximation schemes for dense instances of minimum constraint satisfaction. *Random Structures Algorithms*, 23(1):73-91, 2003.

[35] C. Bazgan, M. Santha, and Z. Tuza. Efficient approximation algorithms for the subset-sums equality problem. *J. Comput. System Sci.*, 64(2):160-170, 2002.

[36] A. Benkouar, Y. Manoussakis, and R. Saad. The number of edge-colored complete graphs with unique alternating hamiltonian cycles. *Discrete Mathematics*, 263:1-10, 2003, Elsevier Science Publishers.

[37] A. Berthiaume, W. van Dam, and S. Laplante. Quantum Kolmogorov complexity. *Journal of Computer and System Sciences*, 63(2):201-221, 2001, Elsevier Science Publishers. Special Issue on Complexity 2000.

[38] S. Boucheron, O. Bousquet, G. Lugosi, and P. Massart. Moment inequalities for functions of independent random variables. *Annals of Probability*, 2004.

[39] S. Boucheron and W. Fernandez de la Vega. On the independence number of random interval graphs. *Combin. Probab. Comput.*, 10(5):385-396, 2001.

[40] S. Boucheron and W. Fernandez de la Vega. On a square packing problem. *Combin. Probab. Comput.*, 11(2):113-127, 2002.

[41] S. Boucheron, F. Gamboa, and C. Léonard. Bins and balls: large deviations of the empirical occupancy process. *Ann. Appl. Probab.*, 12(2):607-636, 2002.

[42] S. Boucheron, G. Lugosi, and P. Massart. A sharp concentration inequality with applications. *Random Structures Algorithms*, 16(3):277-292, 2000.

[43] S. Boucheron, G. Lugosi, and P. Massart. Concentration inequalities using the entropy method. *Ann. Probab.*, 31(3):1583-1614, 2003.

[44] S. Boucheron and M. R. Salamatian. About priority encoding transmission. *IEEE Trans. Inform. Theory*, 46(2):699-705, 2000.

[45] H. Buhrman, C. Dürr, M. Heiligman, P. Høyer, F. Magniez, M. Santha, and R. de Wolf. Quantum algorithms for element distinctness. *SIAM J. Comput.*, inpress.

[46] H. Buhrman, L. Fortnow, and S. Laplante. Resource-bounded Kolmogorov complexity revisited. *SIAM J. Comput.*, 31(3):887-905 (electronic), 2001/02.

[47] T. Calamoneri, I. Finocchi, Y. Manoussakis, and R. Petreschi. On Max Cut in cubic graphs. *Parallel Algorithms Appl.*, 17(3):165-183, 2002.

[48] M. Chrobak, P. Couperus, C. Dürr, and G. Woeginger. On tiling under tomographic constraints. *Theoret. Comput. Sci.*, 290(3):2125-2136, 2003.

[49] M. Chrobak and C. Dürr. Reconstructing polyatomic structures from discrete X-rays: NP-completeness proof for three atoms. *Theoret. Comput. Sci.*, 259(1-2):81-98, 2001.

[50] S. Corteel, A. Denise, and D. Gouyou-Beauchamps. Bijections for directed animals on infinite families of lattices. *Ann. Comb.*, 4(3-4):269-284, 2000. Conference on Combinatorics and Physics (Los Alamos, NM, 1998).

[51] S. Corteel and D. Gouyou-Beauchamps. Enumeration of sand piles. *Discrete Math.*, 256(3):625-643, 2002. LaCIM 2000 Conference on Combinatorics, Computer Science and Applications (Montreal, QC).

[52] C. Dürr, I. Rapaport, and G. Theyssier. Cellular automata and communication complexity. *Theoretical Computer Science*, 322:355-368, 2004, Elsevier Science Publishers.

[53] J.-C. Dubacq, B. Durand, and E. Formenti. Kolmogorov complexity and cellular automata classification. *Theoret. Comput. Sci.*, 259(1-2):271-285, 2001.

[54] C. Dürr, E. Goles, I. Rapaport, and E. Rémila. Tiling with bars under tomographic constraints. *Theoret. Comput. Sci.*, 290(3):1317-1329, 2003.

[55] C. Dürr and M. Santha. A decision procedure for unitary linear quantum cellular automata. *SIAM J. Comput.*, 31(4):1076-1089 (electronic), 2002.

[56] M. El Haddad, Y. Manoussakis, and R. Saad. Upper bounds for the forwarding indices of communication networks. *Discrete Mathematics*, inpress, Elsevier Science Publishers.

[57] W. Evans, C. Kenyon, Y. Peres, and L. J. Schulman. Broadcasting on trees and the Ising model. *Ann. Appl. Probab.*, 10(2):410-433, 2000.

[58] W. Fernandez de la Vega. Random 2-SAT: results and problems. *Theoret. Comput. Sci.*, 265(1-2):131-146, 2001. Phase transitions in combinatorial problems (Trieste, 1999).

[59] W. Fernandez de la Vega and M. Karpinski. Polynomial time approximation of dense weighted instances of MAX-CUT. *Random Structures Algorithms*, 16(4):314-332, 2000.

[60] W. Fernandez de la Vega and C. Kenyon. A randomized approximation scheme for metric MAX-CUT. *J. Comput. System Sci.*, 63(4):531-541, 2001. Special issue on FOCS 98 (Palo Alto, CA).

[61] W. Fernandez de la Vega and M. Lamari. The task allocation problem with constant communication. *Discrete Appl. Math.*, 131(1):169-177, 2003. The Second International Colloquium “Journées de l’Informatique Messine” (Metz, 2000).

[62] K. Friedl, F. Magniez, M. Santha, and P. Sen. Quantum testers for hidden group properties. *Theoretical Computer Science, Special Issue on the 28th Symposium on Mathematical Foundations of Computer Science*, in press.

[63] J. Friedman and J.-P. Tillich. Laplacian eigenvalues and distances between subsets of a manifold. *J. Differential Geom.*, 56(2):285-299, 2000.

[64] E. Gassiat and S. Boucheron. Optimal error exponents in hidden Markov models order estimation. *IEEE Trans. Inform. Theory*, 49(4):964-980, 2003.

[65] D. Gouyou-Beauchamps and P. Leroux. Enumeration of symmetry classes of convex polyominoes on the honeycomb lattice. *Theoretical Computer Science*, inpress, Elsevier Science Publishers.

[66] M. E. Haddad, Y. Manoussakis, and R. Saad. Upper bounds for the forwarding indices of communication networks. *Discrete Mathematics*, inpress, Elsevier Science Publishers.

[67] 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.

[68] G. Ivanyos, F. Magniez, and M. Santha. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. *Internat. J. Found. Comput. Sci.*, 14(5):723-739, 2003. Quantum computing.

[69] J. Kempe. Quantum random walks - an introductory overview. *Contemporary Physics*, 44(4):302-327, 2003. lanl-arXiv quant-ph/0303081.

[70] J. Kempe and O. Regev. 3-local Hamiltonian is QMA-complete. *Quantum Information and Computation*, 3(3):258-264, 2003.

[71] J. Kempe and K. Whaley. Exact gate-sequences for universal quantum computation using the XY-interaction alone. *Phys. Rev. A*, 65 (5):052330, 2002.

[72] C. Kenyon. The evolution of Web-caching markets. *Computer*, 34(11):128-130, Nov. 2001.

[73] C. Kenyon and G. Cheliotis. Stochastic models for telecom commodity prices. *Computer Networks (Amsterdam, Netherlands: 1999)*, 36(5-6):533-555, Aug. 2001.

[74] C. Kenyon and M. Mitzenmacher. Linear waste of best fit bin packing on skewed distributions. *Random Structures and Algorithms*, 20(3):441-464, 2002.

[75] C. Kenyon and E. Rémila. A near-optimal solution to a two-dimensional cutting stock problem. *Math. Oper. Res.*, 25(4):645-656, 2000.

[76] C. Kenyon and S. Tompaidis. Options in leasing: the effect of idle time. *Operations Research*, 49(5):675-689, 2001.

[77] M. Kiwi, F. Magniez, and M. Santha. Approximate testing with error relative to input size. *J. Comput. System Sci.*, 66(2):371-392, 2003.

[78] F. Magniez. Multi-linearity self-testing with relative error. *Theory of Computing Systems*, 2004. inpress.

[79] Y. Manoussakis and H. Patil. Bipartite graphs and their degree sets. 15, 2003, Elsevier.

[80] Y. Manoussakis, H. Patil, and V. Sankar. Further results on degree sets for graphs. 1, 2001.

[81] Y. Manoussakis and Z. Tuza. Ramsey numbers for tournaments. *Theoret. Comput. Sci.*, 263(1-2):75-85, 2001. Combinatorics and computer science (Palaiseau, 1997).

[82] P. Milman and R. Mosseri. Topological phase for entangled two-qubit states. *Phys. Rev. Lett.*, 90(23):230403, 4, 2003.

[83] P. Milman, H. Ollivier, F. Yamaguchi, M. Brune, J. M. Raimond, and S. Haroche. Simple quantum information algorithms in cavity QED. *J. Modern Opt.*, 50(6-7):901-913, 2003. International Conference on Quantum Information, Conceptual Foundations, Developments and Perspectives (Oviedo, 2002).

[84] F. Noilhan and M. Santha. Semantical counting circuits. *Theory Comput. Syst.*, 36(3):217-229, 2003.

[85] H. Ollivier and P. Milman. Proposal for realization of a toffoli gate via cavity-assisted atomic collision. *Quantum Information & Computation*, 43:603, 2003.

[86] J. Radhakrishnan, P. Sen, and S. Venkatesh. The quantum complexity of set membership. *Algorithmica*, 34(4):462-479, 2002, Springer-Verlag.

[87] N. Shenvi, J. Kempe, and K. Whaley. A quantum random walk search algorithm. *Phys. Rev. A*, 67(5):052307, 2003. lanl-arXiv quant-ph/0210064.

[88] C. Simon and J. Kempe. Robustness of multiparty entanglement. *Phys. Rev. A*, 65 (5):052327, 2002.

[89] E. Solano, M. França Santos, and P. Milman. Quantum phase gate with a selective interaction. *Phys. Rev. A (3)*, 64(2):024304, 4, 2001.

[90] J.-P. Tillich. Edge isoperimetric inequalities for product graphs. *Discrete Math.*, 213(1-3):291-320, 2000. Selected topics in discrete mathematics (Warsaw, 1996).

[91] J.-P. Tillich and G. Zémor. Discrete isoperimetric inequalities and the probability of a decoding error. *Combin. Probab. Comput.*, 9(5):465-479, 2000.

Books

[92] J.-P. Allouche and V. Berthé. *Some applications of combinatorics on words in number theory in "Applied Combinatorics on Words", Lothaire*. Cambridge University Press, Cambridge, 2005. à paraître.

[93] J.-P. Allouche and J. Shallit. *Automatic sequences*. Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.

[94] R. Lassaigne and M. de Rougemont. *Logic and complexity*. Discrete Mathematics and Theoretical Computer Science (London). Springer-Verlag London Ltd., London, 2004.

Book chapters

[95] M. de Rougemont. Sécurité des services informatiques. In *Le pilotage du changement par les cybertechnologies*. Hermès, 2003.

[96] M. de Rougemont. Logic, randomness and cognition. In *Logic, Thought and Action*. D. Vanderveken, Kluwer Academic Publisher, 2004.

[97] M. Kiwi, F. Magniez, and M. Santha. Exact and approximate testing/correcting of algebraic functions: a survey. In *Theoretical aspects of computer science (Tehran, 2000)*, volume 2292 of *Lecture Notes in Comput. Sci.*, pages 30-83. Springer, Berlin, 2002.

[98] H. Leiß and M. de Rougemont. Automata on Lempel-Ziv compressed strings. In Computer science logic, volume 2803 of Lecture Notes in Comput. Sci., pages 384-396. Springer, Berlin, 2003.

Major international peer-reviewed conferences

[99] F. Afrati, E. Bampis, A. V. Fishkin, K. Jansen, and C. Kenyon. Scheduling to minimize the average completion time of dedicated tasks. In *FST TCS 2000: Foundations of software technology and theoretical computer science (New Delhi)*, volume 1974 of *Lecture Notes in Comput. Sci.*, pages 454-464. Springer, Berlin, 2000.

[100] F. Afrati, H. Leiß, and M. de Rougemont. Definability and compression. In *15th Annual IEEE Symposium on Logic in Computer Science (Santa Barbara, CA, 2000)*, pages 63-73. IEEE Comput. Soc. Press, Los Alamitos, CA, 2000.

[101] D. Aharonov, A. Ambainis, J. Kempe, and U. V. Vazirani. Quantum walks on graphs. In *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC)*, pages 50-59, 2001.

[102] 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)*, 2004.

[103] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Adiabatic quantum computation is equivalent to standard quantum computation. In *Proceedings of the 45th Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, 2004.

[104] J.-P. Allouche. Algebraic and analytic randomness. In *Noise, oscillators and algebraic randomness (Chapelle des Bois, 1999)*, volume 550 of *Lecture Notes in Phys.*, pages 345-356. Springer, Berlin, 2000.

[105] K. Artiouchine, P. Baptiste, and C. Dürr. Runway scheduling with holding loop. In *Discrete Optimization Methods in Production and Logistics (DOM)*, pages 96-101, Omsk-Irkutsk, Russia, 2004.

[106] J. Barbay and C. Kenyon. On the discrete Bak-Sneppen model of self-organized criticality. In *Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA-01)*, pages 928-933, New York, Jan. 7-9 2001. ACM Press.

[107] J. Barbay and C. Kenyon. Adaptive intersection and t-Threshold problems. In *Proceedings of the 13th Annual ACM-SIAM Symposium On Discrete Mathematics (SODA-02)*, pages 390-399, New York, Jan. 6-8 2002. ACM Press.

[108] D. Barth, S. Corteel, A. Denise, D. Gardy, and M. Valencia-Pabon. On the complexity of routing permutations on trees by arc-disjoint paths. In *Proceedings of Latin American Theoretical INformatics (LATIN)*, volume 1776 of *Lecture Notes in Computer Science*, pages 308-317, Punta del Este, 2000. Springer.

[109] C. Bazgan, W. F. de la Vega, and M. Karpinski. Approximability of dense instances of nearest codeword problem. In M. Penttonen and E. M. Schmidt, editors, *SWAT*, volume 2368 of *Lecture Notes in Computer Science*, pages 298-307. Springer, 2002.

[110] A. Berthiaume, W. van Dam, and S. Laplante. Quantum Kolmogorov complexity. In *15th Annual IEEE Conference on Computational Complexity (Florence, 2000)*, pages 240-249. IEEE Computer Soc., Los Alamitos, CA, 2000.

[111] S. L. Bezrukov, R. Elsässer, B. Monien, R. Preis, and J.-P. Tillich. New spectral lower bounds on the bisection width of graphs. In *Graph-theoretic concepts in computer science (Konstanz, 2000)*, volume 1928 of *Lecture Notes in Comput. Sci.*, pages 23-34. Springer, Berlin, 2000.

[112] S. L. Bezrukov, R. Elsässer, B. Monien, R. Preis, and J.-P. Tillich. New spectral lower bounds on the bisection width. In U. Brandes and D. Wagner, editors, *Graph-Theoretic Concepts in Computer Science, 26th International Workshop, WG 2000, Konstanz, Germany, June 15-17, 2000, Proceedings*, volume 1928 of *Lecture Notes in Computer Science*, pages 155-174. Springer, 2000.

[113] J. Boeuf and J. Stern. An analysis of one of the SDMI candidates. In I. S. Moskowitz, editor, *Information Hiding*, volume 2137 of *Lecture Notes in Computer Science*, pages 395-410. Springer, 2001.

[114] U. Boobna and M. de Rougemont. Correctors for XML data. In Z. Bellahsene, T. Milo, M. Rys, D. Suciu, and R. Unland, editors, *Database and XML Technologies, Second International XML Database Symposium, XSym 2004, Toronto, Canada, August 29-30*, volume 3186 of *Lecture Notes in Computer Science*, pages 97-111. Springer, 2004.

[115] H. Buhrman, C. Dürr, M. Heiligman, P. Høyer, F. Magniez, M. Santha, and R. de Wolf. Quantum algorithms for element distinctness. In *IEEE Conference on Computational Complexity*, pages 131-137, 2001.

[116] H. Buhrman, S. Laplante, and P. B. Miltersen. New bounds for the language compression problem. In *15th Annual IEEE Conference on Computational Complexity (Florence, 2000)*, pages 126-130. IEEE Computer Soc., Los Alamitos, CA, 2000.

[117] E. Cadic, J.-C. Carlach, G. Olocco, A. Otmani, and J.-P. Tillich. Low complexity tail-biting trellises of self-dual codes of length 24, 32 and 40 over GF(2) and z_4 of large minimum distance. In S. Boztas and I. Shparlinski, editors, *AAECC*, volume 2227 of *Lecture Notes in Computer Science*, pages 57-66. Springer, 2001.

[118] C. Carlet and E. Prouff. On plateaued functions and their constructions. In T. Johansson, editor, *FSE*, volume 2887 of *Lecture Notes in Computer Science*, pages 54-73. Springer, 2003.

[119] C. Carlet and E. Prouff. On a new notion of nonlinearity relevant to multi-output pseudo-random generators. In M. Matsui and R. J. Zuccherato, editors, *Selected Areas in Cryptography*, volume 3006 of *Lecture Notes in Computer Science*, pages 291-305. Springer, 2004.

[120] C. Carlet and E. Prouff. Vectorial functions and covering sequences. In G. L. Mullen, A. Poli, and H. Stichtenoth, editors, *International Conference on Finite Fields and Applications*, volume 2948 of *Lecture Notes in Computer Science*, pages 215-248. Springer, 2004.

[121] J. Csirik, D. S. Johnson, and C. Kenyon. Better approximation algorithms for bin covering. In *Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA-01)*, pages 557-566, New York, Jan. 7-9 2001. ACM Press.

[122] J. Csirik, D. S. Johnson, C. Kenyon, J. B. Orlin, P. W. Shor, and R. R. Weber. On the sum-of-squares algorithm for bin packing. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC)*, pages 208-217, 2000.

[123] W. F. de la Vega, M. Karpinski, and C. Kenyon. Approximation schemes for metric bisection and partitioning. In J. I. Munro, editor, *SODA*, pages 506-515. SIAM, 2004.

[124] W. F. de la Vega, M. Karpinski, C. Kenyon, and Y. Rabani. Approximation schemes for clustering problems. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, pages 50-58, 2003.

[125] J.-C. Dubacq and V. Terrier. Signals for cellular automata in dimension 2 or higher. In *LATIN 2002: Theoretical informatics (Cancun)*, volume 2286 of *Lecture Notes in Comput. Sci.*, pages 451-464. Springer, Berlin, 2002.

[126] C. Dürr, M. Heiligman, P. Høyer, and M. Mhalla. Quantum query complexity of some graph problems. In *Proceedings of the 31st International Colloquium on Automata, Languages and Programming (ICALP)*, pages 481-493, 2004.

[127] W. Fernandez de la Vega. The independence number of random interval graphs. In *Algorithms and complexity (Rome, 2000)*, volume 1767 of *Lecture Notes in Comput. Sci.*, pages 59-62. Springer, Berlin, 2000.

[128] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden translation and orbit coset in quantum computing. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1-9, 2003.

[129] K. Friedl, F. Magniez, M. Santha, and P. Sen. Quantum testers for hidden group properties. In LNCS, editor, *Proceedings of the 28th International Symposium on Mathematical Foundations of Computer Science (MFCS)*, volume 2747, pages 419-428, 2003.

[130] M. Golin, C. Kenyon, and N. E. Young. Huffman coding with unequal letter costs. In *Proceedings of the ACM Symposium on Theory of Computing (STOC)*, pages 785-791, May 2002.

[131] S.-D. Gouraud, A. Denise, M.-C. Gaudel, and B. Marre. A new way for automating statistical testing methods. In *Proceedings of IEEE Automated Software Engineering (ASE)*, San Diego, november 2001.

[132] D. Gouyou-Beauchamps and P. Leroux. Dénombrement des classes de symétries des polyominos hexagonaux convexes. In *16th Annual International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC04)*, June 28 - July 2 2004.

[133] D. Gross and M. de Rougemont. Uniform generation in spatial constraint databases and applications. In *Proceedings of the Nineteenth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS)*, pages 254-259, 2000.

[134] T. Hérault, R. Lassaigne, F. Magniette, and S. Peyronnet. Approximate probabilistic model checking. In B. Steffen and G. Levi, editors, *VMCAI*, volume 2937 of *Lecture Notes in Computer Science*, pages 73-84. Springer, 2004.

[135] R. Jain, J. Radhakrishnan, and P. Sen. Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states. In *Proc. 43rd Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 429-438, 2002.

[136] A. R. Karlin, C. Kenyon, and D. Randall. Dynamic TCP acknoledgement and other stories about e/(e-1). In Proceedings of the ACM Symposium on Theory of Computing (STOC), pages 502-509, 2001.

[137] J. Kempe. Quantum walks hit exponentially faster. In *RANDOM-APPROX 2003*, Lecture Notes in Computer Science, pages 354-369, Heidelberg, 2003. Springer.

[138] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local hamiltonian problem. In *Proc. of Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*, Lecture Notes in Computer Science. Springer-Verlag, 2004. to appear.

[139] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local hamiltonian problem. In *Proceedings of the 24th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*, 2004.

[140] C. Kenyon and M. Mitzenmacher. Linear waste of best fit bin packing on skewed distributions. In *41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000)*, pages 582-589. IEEE Comput. Soc. Press, Los Alamitos, CA, 2000.

[141] C. Kenyon, E. Mossel, and Y. Peres. Glauber dynamics on trees and hyperbolic graphs. In *FOCS*, pages 568-578, 2001.

[142] C. Kenyon, N. Schabanel, and N. E. Young. Polynomial-time approximation scheme for data broadcast. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC)*, pages 659-666, 2000.

[143] M. A. Kiwi, F. Magniez, and M. Santha. Exact and approximate testing/correcting of algebraic functions: A survey. In G. B. Khosrovshahi, A. Shokoufandeh, and M. A. Shokrollahi, editors, *Theoretical Aspects of Computer Science 2000*, volume 2292 of *Lecture Notes in Computer Science*, pages 30-83. Springer, 2000.

[144] S. Laplante, R. Lassaigne, F. Magniez, S. Peyronnet, and M. Rougemont. Probabilistic abstraction for model checking: An approach based on property testing. In *Proceedings of 17th IEEE Symposium on Logic in Computer Science*, pages 30-39, 2002.

[145] 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*, 2004, pages 294-304.

[146] R. Lassaigne and S. Peyronnet. Approximate verification of probabilistic systems. In H. Hermanns and R. Segala, editors, *PAPM-PROBMIV*, volume 2399 of *Lecture Notes in Computer Science*, pages 213-214. Springer, 2002.

[147] H. Leiss and M. de Rougemont. Automata on lempel-ziv structures. In M. Baaz and J. A. Makowsky, editors, *Computer Science Logic, 17th International Workshop, CSL 2003, 12th Annual Conference of the EACSL, and 8th Kurt Güdel Colloquium, KGC 2003, Vienna, Austria, August 25-30, 2003, Proceedings*, volume 2803 of *Lecture Notes in Computer Science*, Vienne, 2003. Springer.

[148] F. Magniez. Multi-linearity self-testing with relative error. In *STACS 2000 (Lille)*, volume 1770 of *Lecture Notes in Comput. Sci.*, pages 302-313. Springer, Berlin, 2000.

[149] F. Magniez and M. Rougemont. Property testing of regular tree languages. In *Proceedings of 31st International Colloquium on Automata, Languages and Programming*, volume 3142 of *Lecture Notes in Comput. Sci.*, pages 932-944. Springer, 2004.

[150] F. Noilhan and M. Santha. Semantical counting circuits. In *Algorithms and complexity (Rome, 2000)*, volume 1767 of *Lecture Notes in Comput. Sci.*, pages 87-101. Springer, Berlin, 2000.

[151] G. Olocco and A. Otmani. Low complexity tail-biting trellises for some extremal self-dual codes. In *Eight International Workshop On Algebraic and Combinatorial Coding Theory*, 2002.

[152] G. Olocco and J.-P. Tillich. Iterative decoding of a new family of block turbo-codes. In *Proceedings of 2nd International Symposium on Turbo Codes and Related Topics*, Brest, pages 302-306, 2000.

[153] G. Olocco and J.-P. Tillich. A family of self-dual codes which behave in many respects like random linear codes of rate 1/2. In *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, page 15, 2001.

[154] M. Santha and M. Szegedy. Quantum and classical query complexities of local search are polynomially related. In *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC)*, pages 494-501, 2004.

[155] J. Stern and J. P. Stern. Cryptanalysis of the otm signature scheme from fc'02. In *Financial Cryptography*, pages 138-148, 2003.

[156] J. P. Stern and J.-P. Tillich. Automatic detection of a watermarked document using a private key. In I. S. Moskowitz, editor, *Information Hiding*, volume 2137 of *Lecture Notes in Computer Science*, pages 258-272. Springer, 2001.

[157] W. van Dam, F. Magniez, M. Mosca, and M. Santha. Self-testing of universal and fault-tolerant sets of quantum gates. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC)*, pages 688-696, 2000.

Doctoral dissertations and Habilitations

[158] J. Barbay. *Analyse fine: bornes inférieures et algorithmes de calculs d'intersection pour moteurs de recherche*. Ph.D. thesis, Université Paris-Sud, 2002.

[159] S. Boucheron. *Problèmes d'informatique, techniques probabilistes*. Habilitation, Université Paris-Sud, 2002.

[160] S. Corteel. *Problèmes énumératifs issus de l'informatique, de la physique et de la combinatoire*. Ph.D. thesis, Université Paris-Sud, 2000.

[161] A. Denise. *Structures aléatoires, modèles et analyse des génomes*. Habilitation, Université Paris-Sud, 2001.

[162] D. Gross. *Approximation dans les bases de données contraintes*. Ph.D. thesis, Université Paris-Sud, 2000.

[163] F. Magniez. *Auto-test pour les calculs approché et quantique*. Ph.D. thesis, Université Paris-Sud, 2000.

[164] S. Peyronnet. *Model checking et vérification probabiliste*. Ph.D. thesis, Université Paris-Sud, 2003.

[165] J. Stern. *Contribution à une théorie de la protection de l'information*. Ph.D. thesis, Université Paris-Sud, 2001.

[166] Y. Verhoeven. *Quelques utilisations des arbres en combinatoire*. Ph.D. thesis, Université Paris-Sud, 2001.

[167] J.-Y. Yao. *Théorie des automates finis et applications*. Habilitation, Université Paris-Sud, 2003.