ZiF Workshop Search Methodologies II

Bielefeld, Germany, October 25 -29, 2010

Program and Booklet of Abstracts

Organizers:	Chairmen:
Rudolf Ahlswede	Harout Aydinian
Ferdinando Cicalese	Christian Deppe

Contents

SEARCH METHODOLOGIES

In 1979 one of the first books on search (and surely the first in Germany) was written, translated into Russian 1982, and finally into English in 1987. We

> "treat only search problems for which we know what our goal is and which search methods are available. Within this framework we look for search strategies which are as good as possible (successful, fast, economical, simple).
>
> We want to use our concepts and classifications to make a contribution to working out the essential, common points of the various search problems. This ought to help the reader to understand more quickly the problems of this nature and get a quick grasp of the most recent results. At the same time, we would like to inspire as many readers as possible to engage in research. By contrasting the various search problems and the methods for their solution, we hope finally to improve the exchange of information between scientists in the various fields. The necessity for this is underscored simply by the fact that certain results are 'discovered' again and again.
>
> We intentionally dispense with a uniform and universally polished theory of searching because this leads to premature conclusions in such a dynamic field and tempts one to leave further developments to the *perpetuum mobile* of the mathematical apparatus. We are interested in maintaining a certain consciousness of the problems and not in preventing controversies on the various assumptions and working methods. That is why we choose 'Search Problems' and not 'The Theory of Searching' for the title of this book."

Perhaps the most natural example of a search problem is the task to find an unknown element in a finite set by asking questions concerning containment in a subset. In the three decades which passed since then there has been an explosion of developments in search for instance in Computer Science, Image Reconstruction, Machine Learning, Information Theory (classical and quantum theoretical), and Operation Research. Time seems to be mature for more theoretical understanding with the goal of a general Theory of Search, since there are already parallels in methods in different disciplines like data transmission over noisy channels with feedback corresponds to search with random answers and foraging of animals corresponds to search for information in the internet. A search structure is defined by a space of objects searched for and a space of tests (questions). In specifying a search problem performance criteria have to be chosen. Furthermore we distinguish combinatorial and probabilistic models. Especially important is the study of adaptive and non-adaptive strategies as well as the analysis of their intermediate forms. **There is reason for optimism.**

Three decades ago it was often asked whether search is a scientific subject! In the article "Breaking Network Logjams" in Scientific American, pages 78-85, June 2007 one finds

> "On the Internet and other shared networks, information currently gets relayed by routers – switches that operate at nodes where signaling pathways, or links, intersect. The routers shunt incoming messages to links heading toward the messages' final destinations. But if one wants efficiency, are routers the best devices for these intersections? Is switching even the right operation to perform?
>
> Until seven years ago, few thought to ask such questions. But then Rudolf Ahlswede of the University of Bielefeld in Germany, along with Ning Cai, Shuo-Yen Robert Li and Raymond W. Yeung, all then at the University of Hong Kong, published groundbreaking work that introduced a new approach to distributing information across shared networks. In this approach, called network coding, routers are replaced by coders, which transmit evidence about messages instead of sending the messages themselves. When receivers collect the evidence, they deduce the original information from the assembled clues.
>
> Although this method may sound counterintuitive, network coding, which is still under study, has the potential to dramatically speed up and improve the reliability of all manner of communications systems and may well spark the next revolution in the field. Investigators are, of course, also exploring additional avenues for improving efficiency; as far as we know, though, those other approaches generally extend existing methods."

By now network coding has started a revolution in communication networks!

Information flows in search are more like flows of bits in transmission than flows of water or electricity (obeying Kirchhoff's law). This is especially transparent in the first example above.

So far we have discussed one-sided search, that is, the targets are passive. Two-sided search, which was pioneered by B.O. Koopman, includes for instance search in game trees and rendezvous search. Quantum searching has analogue models and genuine novelties.

Monday Search in Graphs and Networks October 25, 2010	
	- Chairman H. Aydinian -
9:00	F. Cicalese, Welcoming Address
9:10	R. Ahlswede, Towards a Theory of Search
9:30	I. Althöfer, Search in Game Trees and Game Graphs
10:30	*- Coffee Break -*
	- Chairman C. Deppe -
11:00	U. Lorenz, Searching for Solutions of Hard Problems
11:30	O. Teytaud, Monte-Carlo Tree Search: a New Paradigm for Computational Intelligence
12:00	T. Jacobs, Searching in Trees
12:30	*- Lunch -*
	- Chairman H. Aydinian -
14:30	B. Keszegh, Path-Search in a Pyramid and Other Graphs
15:00	M. Milanic, Haplotype Inference and Graphs of Small Separability
15:30	E. Triesch, A Lower Bound for the Complexity of Monotone Graph Properties
16:00	*- Coffee Break -*
	- Chairman C. Deppe -
16:30	S. Riis, A New Max-Flow Min-Cut Theorem for Information Flows
17:00	C. Sohler, Streaming Algorithms for the Analysis of Massive Data Sets
	Discussion

Tuesday Combinatorial Search October 26, 2010	
	- Chairman H. Aydinian -
9:00	C. Colbourn, Combinatorial t-Restrictions and Combinatorial Search
10:00	A. Macula, Combinatorial Method for Anomaly Detection
10:30	*- Coffee Break -*
	- Chairman C. Deppe -
11:00	G. Katona, Average Length in q-ary Search with Restricted Sizes of Question Sets
11:30	H. Aydinian, On Generic Erasure Correcting Sets and Related Problems
12:00	E. Porat, An Extension of List Disjunct Matrices that can Correct Errors in Test Outcomes
12:30	*- Lunch -*
	- Chairman H. Aydinian -
14:30	E. Czabarka, Full Transversals and Mixed Orthogonal Arrays
15:00	L. Székely, M-part Sperner families
15:30	V. Lebedev, Shadows Under the Word-Subword Relation
16:00	*- Coffee Break -*
	- Chairman C. Deppe -
16:30	K. Kobayashi, Some Structures of Tower of Hanoi with Four Pegs
17:00	V. Blinovsky, Solutions of Some Problems from Extremal Combinatorics
	Discussion

Wednesday Problem Session October 27, 2010	
9:00	*- Chairman H. Aydinian -*
10:30	*- Coffee Break -*
11:00	*- Chairman C. Deppe -*
12:30	*- Lunch -*

Thursday Other Theories of Search October 28, 2010	
	- *Chairman H. Aydinian* -
9:00	E. Kranakis, Rendezvous Search and Exploration with Mobile Agents
10:00	E. Konstantinova, Search Problems on Cayley Graphs
10:30	- *Coffee Break* -
	- *Chairman C. Deppe* -
11:00	O. Milenkovic, Sublinear Compressive Sensing via Dense Belief Propagation
12:00	S. Kannan, Sampling from Constrained Multivariate Distributions
12:30	- *Lunch* -
	- *Chairman H. Aydinian* -
14:30	L. Grover, Quantum Searching - Old & New
16:00	- *Coffee Break* -
	- *Chairman C. Deppe* -
16:30	R. Reischuk, Searching for Hidden Information
	Discussion

Friday	Combinatorial Search and Group Testing October 29, 2010
	- Chairman H. Aydinian -
9:00	A. D'yachkov, DNA Codes for Additive Stem Distance
9:30	A. Voronina, DNA Codes for Non-Additive Stem Distance
10:00	V. Rykov, An Application of Superimposed Coding Theory to the Multiple Access OR Channel and Two-Stage Group Testing Algorithms
10:30	*- Coffee Break -*
	- Chairman C. Deppe -
11:00	H. Chang, Identification and Classification Problems on Pooling Designs for Inhibitor Complex Models
11:30	H.-B. Chen, Pooling Designs with Sensitive and Efficient Decoding
12:00	P. Damaschke, Randomized and Competitive Group Testing in Stages
12:30	*- Lunch -*
	- Chairman H. Aydinian -
14:30	A. De Bonis, Combinatorial Group Testing for Corruption Localizing Hashing
15:00	C. Deppe, Threshold and Majority Group Testing
15:30	D. Gerbner, Search with Density Tests
16:00	*- Coffee Break -*
	- Chairman C. Deppe -
16:30	F. Cicalese, Superselectors: Efficient Constructions and Applications
	Discussion

Invited survey talks: I. Althöfer, C. Colbourn, L. Grover, E. Kranakis, and O. Milenkovic

SEARCH IN GAME TREES AND GAME GRAPHS

Ingo Althöfer

Friedrich-Schiller-Universität Jena
Fakultät für Mathematik und Informatik
Institut für Angewandte Mathematik
D-07737 Jena

*** On the History of Computer Chess**
Tarrasch (1908) - Zermelo (1912) - Shannon (1950) - Deep Blue (1997)

*** Error propagation in Game Trees and Pathology in Game Search**
Observation in practice: Searching deeper helps
Observation in theoretical models: Searching deeper degrades quality

*** Computer Olympiads, the early Years**
From London(1989) to Taipeh(2005)
Transfer from chess to other games where alpha-beta game tree search works.

*** Monte Carlo Game Tree Search**
B. Abramson: Expected Outcome (1987, 1990)
B. Bruegmann: Monte Carlo Go (1993)

− − −− > Breakthrough in 2006 < − − −−
L. Kocsis and C. Szepesvari: Bandit based Monte-Carlo Planning
(multi-armed bandit models: exploitation vs exploration)
R. Coulom: Efficient Selectivity and Backup Operators in Monte-Carlo Tree Search

*** Game Inventing With Computer Help**
interactive: I. Althöfer. Computer-Aided Game Inventing. Report, 2003.
http://www.minet.uni-jena.de/preprints/althoefer_03/CAGI.pdf

fully automatic: C. Browne. Automated Generation and Evaluation of
Recombination Games. PhD Thesis, QUT, 2008.
Downloadable from http://www.cameronius.com/cv/

*** Computer Olympiads 2006++: The Fruits of Monte Carlo**

15	2010	Kanazawa	Japan
14	2009	Pamplona	Spain
13	2008	Beijing	China
12	2007	Amsterdam	The Netherlands
11	2006	Turin	Italy

− − − > Connection games and Games of territory < − − −
Go: MC since 2006; first win (by MC) on 9x9 in 2006,
first win on 19x19 in 2007.
Amazons: MC since 2008; first win in 2008.
Hex: MC since 2008; first win in 2009.
Havannah: since 2009, only MC-bots.

*** Roulette with 2 Actors - Bold Play and Timid Play in Contest**
Bold Strategy: L.E. Dubbins and L.J. Savage. Inequalities for Stochastic
Processes; How to Gamble If You Must. Dover Publications, 1967.
Timid Strategy: S.M. Ross. Dynamic programming and gambling models.
Advances in Applied Probability 6 (1974), 593-606.
Player vs Bank: T. Lucke genannt Schoenberg. Analyse von verallgemeinerten
Roulette-Modellen mit zwei Akteuren. Diplomarbeit, FSU Jena, 2010.
http://www.althofer.de/diplomarbeit-lucke-genannt-schoenberg.pdf

ON GENERIC ERASURE CORRECTING SETS AND RELATED PROBLEMS

Harout Aydinian

Universität Bielefeld
Fakultät für Mathematik
Postfach 10 01 31
D - 33615 Bielefeld

Iterative decoding techniques, especially when applied to low-density parity-check codes, have recently attracted a lot of attention (see [1], [2]). It is known that a binary linear code $\mathcal{C}$ is capable of correcting those and only those erasure patterns that do not contain the support of a non-zero codeword. These patterns are called *correctable* for $\mathcal{C}$. Hollmann and Tolhuizen (see [3],[4]) observed that given a linear code $\mathcal{C}$, any correctable erasure pattern can be iteratively decoded provided a chosen parity check matrix contains sufficiently many rows. A parity–check matrix of a linear code $\mathcal{C}$ is defined as a matrix whose rows span the dual code $\mathcal{C}^{\perp}$. This motivated them to introduce the notion of *generic erasure correcting sets*. A generic (r, s)–erasure correcting set, generates for all binary linear codes of codimension r a parity check matrix that allows iterative decoding of all correctable erasure patterns of size s or less. More formally, a subset $\mathcal{A}$ of a binary vector space $\mathbb{F}_2^r$ is called generic (r, s)–erasure correcting set if for any binary linear code $\mathcal{C}$ of length n and codimension r, and any parity check $r \times n$ matrix H of $\mathcal{C}$, the set of parity check equations $\mathcal{H}_{\mathcal{A}} = \{\mathbf{a}H : \mathbf{a} \in \mathcal{A}\}$ enables iterative decoding of all correctable erasure patterns of size s. The problem is to derive bounds on the minimum size $F(r, s)$ of generic erasure correcting sets and to find explicit constructions for such sets. Hollmann and Tolhuizen also introduced the stronger notion of (r, s)–generating sets and derived bounds for their minimum size $G(r, s)$.
In this talk we present improved lower and upper bounds for $F(r, s)$ and $G(r, s)$. We observe that these two concepts are closely related to intersecting codes, an area, in which $G(r, s)$ has been studied primarily with respect to ratewise performance. We derive connections and discuss some other related problems. Finally, we show that hypergraph covering can be used for both problems to derive good upper bounds.

References

[1] C. Di, D. Proietti, I.E. Telatar, T.J. Richardson, and R.L. Urbanke, Finite-length analysis of low-density parity-check codes on the binary erasure channel, IEEE Trans. Inform. Theory vol. 48 , no. 6, 1570–1579, 2002.

[2] M. Schwartz and A. Vardy, On the stopping distance and the stopping redundancy of codes, IEEE Trans. Inform. Theory, vol. 52, no. 3, 922–932, 2006.

[3] H.D.L. Hollmann and L.M.G.M. Tolhuizen, Generic erasure correcting sets: Bounds and constructions, J. Combin. Theory A 113, 1746–1759, 2006.

[4] H.D.L. Hollmann and L.M.G.M. Tolhuizen, On parity-check collections for iterative erasure decoding that correct all correctable erasure patterns of a given size, IEEE Trans. Inform. Theory, vol. 53, no. 2, 823–828, 2007.

This is joint work with Rudolf Ahlswede.

SOLUTIONS OF SOME PROBLEMS FROM EXTREMAL COMBINATORICS

Vladimir Blinovsky

Institute of Information Transmission Problems
Russian Academy of Sciences
B. Karetnii per 19
Russia - Moscow 127 994

I would like to present here the solutions of some combinatorial problems which arise in different areas of extremal combinatorics and which I have solved recently. We omit some definitions, which can be found in the bibliography at the end of this article.
The next result was stated as a conjecture in several places, see e.g. [1]

Theorem 1. *The following polynomial in* $\lambda \in [0,(q-1)/q],\ q = 2,3,\dots$ *is* $\cap-$*convex*

$$\rho_q(\lambda) = \sum_{j_i:\ \sum_{i=1}^q j_i = L+1} \left(1 - \frac{\max\{j_1,\dots,j_q\}}{L+1}\right)\binom{L+1}{j_1,\dots,j_q}\left(\frac{\lambda}{q-1}\right)^{L+1-j_q}(1-\lambda)^{j_q}.$$

The next result was stated as a conjecture also in [1] as the second open problem.

Theorem 2. *The following inequality is valid*

$$\sum_{i=1}^{\ell}(-1)^{i+q}\binom{L+1}{i}(a_{i,q}+a_{i,q-1})\ln\frac{\cosh\left(\frac{L+1}{2}-i\right)\xi}{\cosh\frac{L+1}{2}\xi} \le 0,$$

where $q = 1,2,\dots,\ell = \lfloor (L+1)/2\rfloor, \xi \in R^1$ *and*

$$a_{i,q} = \frac{(L+1)\binom{L-i-q-1}{L-2q-1} + i\binom{L-i-q-1}{L-2q-2}}{\binom{2q}{q}}.$$

This result finds applications in the list decoding for discrete channels and was proved in [3].
On the set 2^X the natural partial order by inclusion is defined. Next we assume that $f_1,\dots,f_n$ are nonnegative monotone nondecreasing functions $2^X \to \mathbb{R}$. The mathematical expectation of the random variable $f : 2^X \to \mathbb{R}$ by the measure μ we denote as $\langle f\rangle_\mu$. For the subset $\delta \subset \{1,\dots,n\}$ we set

$$\mathbb{E}_\delta = \langle \prod_{i\in\delta} f_i\rangle_\mu.$$

Let

$$\sigma = \{\sigma_1,\dots,\sigma_\ell\}-$$

be the partition of the set $\{1,\dots,n\}$ on nonintersecting subsets. Denote

$$\mathbb{E}_\sigma = \prod_{i=1}^{\ell}\mathbb{E}_{\sigma_i}.$$

Also denote $\lambda_i = |\sigma_i|$. We have $\sum_{i=1}^{\ell}\lambda_i = n$. Denote $\lambda(\sigma) = (\lambda_1,\dots,\lambda_\ell)\ \ \lambda_1 \ge \dots \ge \lambda_\ell$. For the partition λ of n we set

$$E_\lambda = \sum_{\sigma:\ \lambda(\sigma)=\lambda}\mathbb{E}_\sigma.$$

Notation $\lambda \vdash n$ means that λ is the partition of n. The following general conjecture was formulated in [4] . There exist numbers $c_\lambda \in \mathbb{Z}\setminus 0$, such that functional

$$E_n(f_1,\dots,f_n) = \sum_{\lambda\vdash n} c_\lambda E_\lambda$$

satisfies the following conditions:

1. $E_n(f_1, \dots, f_n) \geq 0$,
2. For arbitrary $n \geq 3$ there exists constant d_n such that $E_n(f_1, \dots, f_{n-1}, 1) = d_n E_{n-1}(f_1, \dots, f_{n-1})$.
3. $E_n(1, \dots, 1) = 0$.

We prove in [6] that this conjecture is true for the choice

$$c_\lambda = (-1)^{\ell(\lambda)-1} \prod_{i=1}^{\ell} (\lambda_i - 1)!$$

The next Theorem shows a natural generalization of Plotkin's bound for list-of-L decoding case. It was proved in [6].

Theorem 3. *For given number of codewords $M > L$, in Hamming $q-$ary space of length n, the minimal radius $t = \tau n$ of list-of-L decoding satisfies the inequality*

$$\tau / \rho_q((q-1)/q) \leq \frac{M^L}{(M-1)\dots(M-L)}.$$

The next result is the complete intersection theorem for the set of permutations, where we say that two permutation has intersection t iff they have t common cycles. It is proved in [7]

Theorem 4. *The maximal volume $V(n)$ of the set Σ of $t-$intersected permutations of $[n]$ is the maximum over $r = 0, 1, \dots$ of the value*

$$\sum_{i=t+r}^{t+2r} \binom{t+2r}{i} \sum_{j=0}^{n-t-2r} \binom{n-t-2r}{j} f(n-i-j),$$

where $f(i) = i! \sum_{j=0}^{i} \frac{(-1)^j}{j!}$ and this bound is tight.

The methods applied for these results can be extended to solve other combinatorial problems.

References

[1] V.Blinovsky General Theory of Information Transfer an Combinatorics, LNCS, Vol.4123, 2006, pp.1075

[2] V.Blinovsky, On the convexity of a function in coding theory. Problemy Peredachi Informatsii 44 (2008), no. 1, 38–44; translation in Probl. Inf. Transm. 44 (2008), no. 1, 34–39

[3] V.Blinovsky, Reliability function for binary memoryless channel, Probl. Inf. Transm., (2010), no.4, to appear

[4] Richards D. Algebraic methods toward higher– order probability inequalities, II// The Annals of Probability. 2004. V.32. N2. P. 1509– 1544.

[5] V.Blinovsky, A proof of a correlation inequality. Problemy Peredachi Informatsii 45 (2009), no. 3, 79–84.

[6] V.Blinovsky, A generalization of Plotkin's bound to the case of multiple packings. Problemy Peredachi Informatsii 45 (2009), no. 1, 3–7; translation in Probl. Inf. Transm. 45 (2009), no. 1, 1–4

[7] V.Blinovsky, Complete intersection theorem for the set of permutations, Prob. Inf Transm., accepted

IDENTIFICATION AND CLASSIFICATION PROBLEMS ON POOLING DESIGNS FOR INHIBITOR COMPLEX MODELS

Huilan Chang

National Chiao Tung University
Department of Applied Mathematics
2F, Science Building
1001 Ta Hsueh Road
Taiwan - Hsinchu, 30010

Pooling designs are common tools to efficiently distinguish positive clones from negative ones in clone library screening. In some applications, there is a third type of clones called inhibitors whose effect is in a sense to obscure the positive clones in pools. Furthermore, a subset of clones (rather than a single clone), called a complex, can induce a positive effect.

The group testing model which takes inhibitors (respectively complexes) into consideration is referred to as an inhibitor model (respectively a complex model). These two models have been well studied in the group testing literature. We [1] first studied group testing problems in a new pooling design environment by allowing the coexistence of inhibitors and complexes . We devoted our attention to nonadaptive algorithms and extended to the error-tolerance case. Later [2], to identify positive complexes, we attached a novel property inclusiveness to a design. This property and a well-studied property disjunctness lead to a significant improvement in the decoding procedure. In addition to the identification problem where only positive items are identified, we also attempted to classify all items. We prove that the well-studied "$(d, r; z]$-disjunct matrices" are sufficient for the classification problems and associated with fast decoding procedures.

References

[1] F. H. Chang, H. Chang, and F. K. Hwang, Pooling designs for clone library screening in the inhibitor complex model, J. Comb. Optim. (2010) DOI 10.1007/s10878-009-9279-9.

[2] H. Chang, H. B. Chen, and H. L. Fu, Identification and classification problems on pooling designs for inhibitor model, Journal of Computational Biology 17 (2010) 927-941.

POOLING DESIGNS WITH SENSITIVE AND EFFICIENT DECODING

Hong-Bin Chen

National Chiao Tung University
Department of Applied Mathematics
Taiwan - Hsinchu, 30010

The classic pooling problem is to identify an unknown set P of at most d positive samples among a given collection N of total n samples. We are allowed to test any subset $Q \subset N$ and the response to the test indicates whether $Q \cap P = \emptyset$ or not. The study of efficiently decodable pooling designs has been an important issue in the literature. This talk presents a new pooling design that produces an efficient and sensitive decoding algorithm. Specifically, the decoding complexity is sensitive to the actual number of positive samples to be identified, i.e., the decoding complexity becomes time-efficient with less positive samples. This method improves upon previous results by a factor of $1/2$ in terms of decoding complexity in the worst case.

The proposed pooling design also proves efficient on two variations of pooling problems, the inhibitor model and the mutually obscuring positives model, where little was known about efficient decoding algorithms.

SUPERSELECTORS: EFFICIENT CONSTRUCTIONS AND APPLICATIONS

Ferdinando Cicalese
Dipartimento di
Informatica ed Applicazion
Universita' di Salerno
I - Baronissi (SA) - 84081

Superimposed codes represent the main tool for the efficient solution of several problems arising in compressed sensing, cryptography and data security, computational biology, multi-access communication, database theory, pattern matching, distributed colouring, and circuit complexity, among the others.

It has also become apparent that combinatorial structures strictly related to superimposed codes lie at the heart of an even vaster series of problems. E.g., selectors were instrumental to obtain fast broadcasting algorithms in radio networks, (p, k, n)-selectors were the basic tool for the first two-stage group testing algorithm with an information theoretic optimal number of tests, (d, ℓ)-disjunct matrices were a crucial building block for the efficiently decodable non-adaptive group testing procedures.

We shall focus on a new combinatorial structure, superselectors, which encompasses and unifies all of the combinatorial structures mentioned above (and more). When appropriately instantiated, superselectors asymptotically match the best known constructions of (p, k, n)-selectors, (d, l)-list-disjunct matrices, monotone encodings and (k, α)-FUT families, $MUT_k(r)$-families for multiaccess channel.

This is joint work with Ugo Vaccaro.

COMBINATORIAL T-RESTRICTIONS AND COMBINATORIAL SEARCH

Charlie Colbourn

Arizona State University
School of Computing, Informatics
and Decision Systems Engineering
P.O. Box 878809
USA - Tempe, Arizona 85287-8809

Many fundamental combinatorial problems can be expressed in the following framework. Let Σ be a set of symbols, which may be finite or infinite. Let $t > 0$ be an integer. Let A be an $m \times t$ matrix with symbols from Σ. For $X \subset \Sigma_t$, the integer variable $p(A, X)$ counts the rows of A that appear in X. A basic t-restriction on A is a requirement that $p(A, X)$ be at least, or at most, or exactly, a specified constant. Then a t-restriction P on A is a logical formula whose terms are basic t-restrictions. For a matrix M that is $m \times k$ for $k \geq t$, M satisfies P when for every way to select t columns of M (in order), the $m \times t$ submatrix so formed satisfies P . A typical combinatorial example is a pairwise balanced design; take $\Sigma = \{0, 1\}$, and treat the $b \times v$ incidence matrix of blocks against points. Then the 2-restriction satisfied is that there is an integer λ so that $p(A, (1, 1)) = \lambda$ for every $b \times 2$ submatrix A of the incidence matrix. Standard combinatorial designs, such as balanced incomplete block designs, t-designs, packings, and coverings all fit into this framework. When the alphabet is larger, we encounter orthogonal arrays, covering arrays, and error-correcting codes (packing arrays). Moreover, many different types of so-called hash families are obtained by considering larger subsets for X in the basic restrictions. More interesting (for this talk) is that disjunct matrices (cover-free families) are also defined by a t-restriction, opening the door to group testing and combinatorial search. Matrices used for finding an interaction fault, or learning an unknown function, nonadaptively, are defined by closely related t-restrictions. In this talk, we (briefly) survey uses of block designs, orthogonal arrays, covering arrays, and hash families for search. Then, using the framework of t-restrictions, a general recursive construction for search and measurement matrices is developed. Finally we outline how parts of the theory of compressive sensing can be developed within this framework.

FULL TRANSVERSALS AND MIXED ORTHOGONAL ARRAYS

Eva Czabarka

University of South Carolina
Department of Mathematics
USA - Columbia, SC 29208

Transversals essentially give the profile matrices of homogeneous more-part Sperner families. More precisely, given an M-partition $X_1 \uplus \cdots \uplus X_M$ of $[n]$ with $|X_i| = n_i$, an $(L_1, \ldots, L_M)$-transversal is an $\mathcal{I} \subseteq \Pi = [0, n_1] \times \cdots \times [0, n_M]$ such that for any $j \in [M]$ and $x_i \in [0, n_i]$ we have

$$|\{k : (x_1, \ldots, x_{j-1}, k, x_{j+1}, \ldots, x_M) \in \mathcal{I}\}| \leq L_j.$$

The size of a transversal is at most $\min\left(\frac{L_i}{n_i+1} \prod_{j=1}^{M} (n_j + 1)\right)$, and a transversal is full if it reaches this size. We prove that full transversals always exist, and even more, if a necessary divisibility condition holds, one can partition Π into full transversals. We pose some extremal problems on full transversals.

This is joint work with H. Aydinian, K. Engel, P.L. Erdős and L.A. Szekely.

RANDOMIZED AND COMPETITIVE GROUP TESTING IN STAGES

Peter Damaschke

Chalmers University
Department of Computer Science
and Engineering
S - 41296 Göteborg

Suppose that we are given a set of n elements d of which are defective. A group test can check for any subset, called a pool, whether it contains a defective. By the trivial information-theoretic lower bound, at least $d \log(n/d)$ queries are needed (where log is base 2). A strategy may work in stages of parallel queries. It is known that $O(d \log(n/d))$ queries in 2 stages are sufficient, but the searcher must know d in advance. For unknown d we have a negative result implying that constantly many stages are not enough to solve the problem deterministically with $O(d \log(n/d))$ queries. As opposed to that, some randomized strategy succeeds in 2 stages, with any desired success probability. (As a side remark, in our randomized strategies we distinguish between probably correct outcome and verified outcome.) Key ingredient of such competitive and minimal adaptive group testing strategies is an estimate of d within a constant factor. It can be obtained by $O(\log n)$ randomized nonadaptive queries, and for a certain natural type of random pools we can also prove that $\Omega(\log n)$ tests are needed. This proof is based on an analysis of the influence of tests on the searcher's ability to distinguish between any two candidate numbers with a constant ratio. A challenge is to get optimal constant factors in the query complexity. We developed some practical tools for that, using optimization software. Next, we devise randomized strategies that work in constantly many stages and achieve the optimal query bound (with hidden factor 1) asymptotically, if d does not grow too much with n.

This is joint work with Azam Sheikh Muhammad; parts have been published in FCT 2009, COCOA 2010, and *Discrete Mathematics, Algorithms and Applications.*

COMBINATORIAL GROUP TESTING FOR CORRUPTION LOCALIZING HASHING

Annalisa De Bonis

Università di Salerno
Dipartimento di Informatica
ed Applicazioni
Via Ponte Don Melillo
I - 84084 Fisciano (SA)

Efficient detection of integrity violations is crucial for the reliability of both data at rest and data in transit. Data integrity may be compromised by several factors including unintended memory or hardware faults, or malicious intrusions by an attacker interested in performing unauthorized modifications to the data. Practical scenarios where maintaining data integrity is of special interest include: sensitive data stored on various types of computer memories or backed up in storage facilities, and data or software downloaded from Internet Web sites. In these scenarios it would be very desirable to have the capability of obtaining information about the location of corrupted data blocks. For instance, in the case of file download from a web site, localizing the corruptions would avoid to repeat the entire download procedure since only part of the data would need to be retransmitted. Similarly, in the case of corruption of stored information, the cost of data recovery could be highly reduced if the virus diagnostic procedure, typically launched after the stored data is detected to have been corrupted, could concentrate on a small area of infected data.

In our model, the adversary's attack consists in replacing up to a certain number v of segments of the original message by new segments each of which preserves the length of the original segment. Each corrupted segment contains an unknown number of blocks, with a block consisting either of a single bit or of a fixed number of consecutive bits. While ideally one would want to exactly locate all changes, in practice this capability may be expensive, and one may be content with localizing or finding a superset T of any changes. The accuracy of the superset T with respect to the actual changes is a metric of special interest, called localization factor, and is formally defined as the ratio of $|T|$ over the minimum total size of v segments that an adversary can modify in order to change the original message x to its corrupted version x'.

Di Crescenzo et al. (2009) have shown that collision-intractable hash functions can be used not only to detect unexpected modifications in data but also to localize the corrupted area in the modified data, thus introducing the notion of corruption localizing hashing. According to their definition, a corruption-localizing hash scheme consists of a hashing algorithm that is used in synergy with a localization algorithm to determine the positions of corrupted blocks in the input data. The hashing algorithm is based on a family of collision-intractable hash functions that compress an arbitrarily large input to a fixed-size output. In general each output has a very large set of inputs that are mapped to it, yet the collision-intractability property states that any efficient algorithm will find two preimages for the same output only with small probability.

The basic idea of corruption-localizing hash schemes is to define a collection L of segment lists of the original message x and to compute the hash value of each segment list in L. Let x' denote the corrupted version of the original message x. If the hash value of a segment list of x is equal to the hash value of the corresponding segment list of x' then no segment in the segment list has been corrupted (unless collisions were found in the collision-intractable hash function), whereas if those two values are different then at least one segment in the segment list has been corrupted.

Testing whether a collision-resistant hash function maps two segment lists to the same value corresponds to posing a YES/NO query of the form "Does the tested segment list contain at least one corrupted segment?" thus implying that the problem of determining the corrupted segments in x' by a corruption-localizing hash scheme can be regarded as an instance of the group testing problem. Therefore, we rephrase our corruption localization problem as a particular instance of group testing and observe that strategies for non-adaptive group testing can be used as a basis of corruption-localizing hash schemes.

An immediate application of conventional combinatorial group testing solutions can be used to exactly determine v data corruptions of at most B blocks with a cost proportional to

$$O((vB)^2 \log(n/(vB)))$$

in terms of time and storage complexity (which is not better than trivial solutions already for relatively small values of B; i.e., for B equal to square root of n). Our solutions show how to use combinatorial group testing to localize the corruptions up to a small constant with a cost polylogarithmic in n. To improve on the above mentioned bound, we crucially use the fact that we are not required to determine the exact locations of all corrupted blocks since we are only asked to determine a collection of segments such that each corrupted block falls in any one of those segments and such that the resulting localization factor is as small as possible. Moreover, we can exploit the additional information that corruptions occur in segments of at most B blocks.
Our main result consists of a scheme with (arbitrarily small) constant localization factor and cost proportional to $O(v(\log B)\log(n/v))$. We remark that previously known schemes achieve constant localization factor only in the presence of a constant number of corruptions.

This is joint work with Giovanni Di Crescenzo.

THRESHOLD AND MAJORITY GROUP TESTING

Christian Deppe

Universität Bielefeld
Fakultät für Mathematik
Postfach 10 01 31
D - 33615 Bielefeld

We consider two generalizations of group testing: threshold group testing (introduced by Damaschke [4]) and majority group testing (a further generalization, including threshold group testing and a model introduced by Lebedev [5]).

In this paper we give a simple adaptive strategy for threshold group testing which improves the strategy of [4].

We show that each separating code gives a nonadaptive strategy for threshold group testing for some parameters. This is a generalization of results on "guessing secrets" [1], introduced in [3].

We introduce threshold codes and show that each threshold code gives a nonadaptive strategy for threshold group testing. We show that there exist threshold codes such that we can improve the lower bound of [2] for the rate of threshold group testing.

We consider majority group testing if the number of defective elements is unknown (otherwise it reduces to threshold group testing). We show that cover-free codes and separating codes give strategies for majority group testing. We give a lower bound for the rate of majority group testing.

References

[1] N. Alon, V. Guruswami, T. Kaufman, and M. Sudan, Guessing secrets efficiently via list decoding, 13th SODA, 254-262, 2002.

[2] H.-B. Chen and H.-L. Fu, Nonadaptive algorithms for threshold group testing, Discrete Appl. Math. 157, No. 7, 1581-1585, 2009.

[3] F. Chung, R. Graham, and F.T. Leighton, Guessing secrets, Electronic J. on Combinatorics, 8, 1-25, 2001.

[4] P. Damaschke, Threshold group testing, General Theory of Information Transfer and Combinatorics, R. Ahlswede et al. editors, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 707-718, 2006.

[5] V.S. Lebedev, Separating codes and a new combinatorial search model, Probl. Peredachi Inf. 46, No. 1, 38, 2010.

This is joint work with Rudolf Ahlswede and Vladimir Lebedev.

DNA CODES FOR ADDITIVE STEM DISTANCE

Arkadii D'yachkov

Moscow State University
Faculty of Mechanics & Mathematics
Department of Probability Theory
Russia - Moscow 119899

We study the new concept of combinatorial coding theory called an additive (non-additive) stem similarity between two q-ary sequences which is calculated as the maximal number of common blocks of length 2 containing adjacent symbols in their common Hamming subsequences (in their common subsequences). For $q = 4$, the stem similarity and the corresponding stem distance are used to describe a mathematical model of thermodynamic similarity that adequately rejects the "hybridization potential" of two DNA sequences (strands). We will also consider a more advanced approach called the "nearest-neighbor thermodynamics" involving a weight function (stem w-similarity) defined for each these type of stems [1]-[2].

DNA code is a collection of DNA sequences (codewords) which is invariant under the Watson-Crick transformation and if a pair of its codewords does not form the Watson-Crick duplex, then the thermodynamic similarity between these codewords should be less than a fixed level. We present some optimal constructions of linear DNA codes called maximum distance separable (MDS) codes for additive stem distance. These constructions are compared with conventional MDS codes for Hamming distance.

For the case of additive stem w-similarity, we discuss methods [1] to prove upper and lower bounds on the rate of DNA codes analogous to the well-known Plotkin upper bound and lower random coding bound (Gilbert-Varshamov bound), i.e., we obtain a critical relative distance for DNA codes. These methods take into account a "Markovian" specification of the additive stem distance as well as a structure of DNA code which is identified by its invariance under Watson-Crick transformation. In particular, our lower bound is established with the help of an ensemble of random codes where the distribution of independent codewords is given by a stationary Markov chain, and we apply the large deviations techniques [3] to a sum of random variables connected via Markov chain.

For the case of non-additive stem w-similarity, we prove a random coding bound on the rate of DNA codes with the help of ensembles of DNA strands [2] whose sequence composition is restricted in a manner similar to the restrictions in binary Fibonacci sequences. Such combinatorial ensemble can be interpreted as an analog of Markov chain in which the corresponding transitions are forbidden.

References

[1] A. G. D'yachkov, A. N. Voronina, "DNA Codes for Additive Stem Similarity," Problems of Information Transmission, vol. 45, n. 2, pp. 348-367, 2009.

[2] A. G. D'yachkov, A. J. Macula, T. E. Renz, V. V. Rykov, "Random Coding Bounds for DNA Codes Based on Fibonacci Ensembles of DNA Sequences," in 2008 IEEE Int. Symp. Information Theory, Toronto, Canada, 2008, pp. 2292-2296.

[3] Dembo, A., Zeitouni, O., Large Deviations Techniques and Applications, Boston, MA: Jones and Bartlett, 1993.

This is joint work with Anna Nikitichna Voronina.

SEARCH WITH DENSITY TESTS

Dániel Gerbner

Rényi Institute
Reáltanoda utca 13-15
H - 1053, Budapest

Let $[n] = \{1, \ldots, n\}$ be our underlying set. Suppose that there are some defective elements in this set. We can ask subsets of $[n]$. In the most usual setting the answer for a question $A \subset [n]$ is yes if and only if it contains at least one defective element. The goal is to find all of them. One can easily see that in this generality the best solution is to ask every set of size 1.
There are several modified versions of this problem. Often the exact number of defective elements is known, or there is an upper bound on the number of defective elements.
Another version of the problem is when the maximum size of a test is bounded. Too large tests are not supposed to be reliable, because a small number of defective elements cannot be recognized there.
In this paper we assume the defective elements can be recognized if and only if their size is large enough compared to the size of the test. More precisely for a question $A \subset [n]$ the answer is yes if and only if there are at least $\alpha|A|$ defective elements in A. Our goal is to find at least m defective elements using this kind of questions.

Definition 1. *Let $g(n, k, \alpha, m)$ be the least number of questions needed in this setting, i.e. to find m defective elements in an underlying set of size n which contains at least k defective elements, where the answer is yes for a question $A \subset [n]$ if and only if there are at least $\alpha|A|$ defective elements in A.*

We suppose through the whole paper that $k \geq m$ and $0 < \alpha < 1$. Let $a = \lfloor \frac{1}{\alpha} \rfloor$. This is the largest size of a set where the answer "no" has the usual meaning, namely that there are no defective elements in the set. We prove the following theorems.

Theorem 2. $g(n, k, \alpha, m) \geq \log(n - k + 1)$.

Theorem 3. *If a is an integer, $k \geq n/a - \log \frac{n}{a}$, then $g(n, k, \alpha, 1) \leq \lceil \log n \rceil$.*

Theorem 4. *$n/a + m \log a - c_1(k) \leq g(n, k, \alpha, m) \leq n/a + m \log a + c_2(k)$, where $c_1(k)$ and $c_2(k)$ depend only on k.*

This is joint work with Balázs Keszegh, Dömötör Pálvölgyi, and Gábor Wiener.

QUANTUM SEARCHING - OLD & NEW

Lov Kumar Grover

Lucent Technologies
600-700 Mountain Avenue
USA - Murray Hill, NJ 07974

Quantum computers can be in multiple states at the same time and by proper design can be programmed to carry out multiple computations at the same time which beyond the dreams of the most accomplished JAVA programmer. Yet it has been a big challenge to harness the power implicit in this parallelism. To date only two major applications of quantum computing have been discovered - factorization and searching. This talk will introduce the concepts of quantum searching and briefly describe two recent research applications - partial quantum searching & fixed point quantum searching.

> The 19th century was known as the Machine Age, the 20th century will be known as the Information Age, I believe the 21st century will be the Quantum Age.
>
> - Paul Davies

SEARCHING IN TREES

Tobias Jacobs

National Institute of Informatics
2-1-2 Hitotsubashi,
Japan - Chiyoda-ku, Tokyo 101-8430

The well known binary search method can be described as the process of identifying some marked node from a line graph T by successively querying edges. An edge query e asks in which of the two subpaths induced by $T \setminus e$ the marked node lies. This identification procedure can be naturally generalized to the case where $T = (V, E)$ is a tree instead of a line.

In this talk I will give an overview on problems of determining (near-) optimal search strategies for trees. A search strategy is represented by a binary decision tree D, whose internal nodes and leaves are associated with edges and nodes from the input tree T, respectively (see Figure 1 below). Different problem versions are induced by different kinds of quality measures for decision trees.

The conceptually most simple variant, minimizing the worst case number of search queries (or, equivalently, the depth of D), turns out to be also computationally the easiest problem case, admitting a linear time optimal algorithm. In contrast, when the goal is to compute an average-case optimal search strategy for a given probability distribution on the nodes of T, the problem becomes NP-hard. Here, constant factor approximation algorithms are known.

A number of open questions arise when the query costs are non-uniform, i.e., each edge of T is associated with a certain cost. Here both the worst and average case minimization problems are hard to solve optimally, but, except for the logarithmic bounds inherited from the general binary identification problem, nothing is known about approximability.

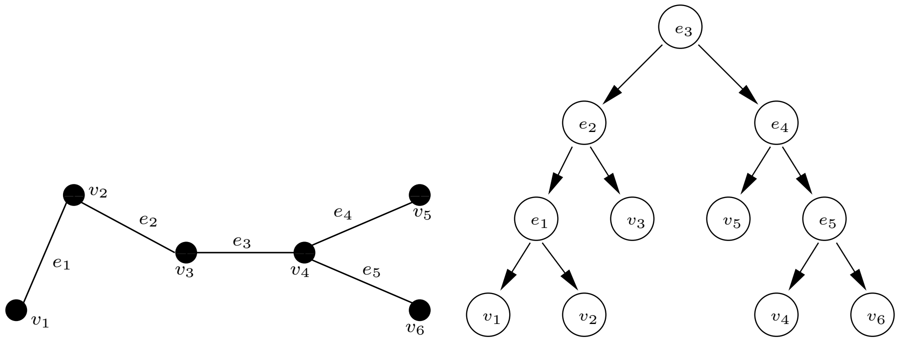

Figure 1 A tree T (left side) and a possible search tree D for T (right side).

SAMPLING FROM CONSTRAINED MULTIVARIATE DISTRIBUTIONS

Sampath Kannan

University of Pennsylvania
Department of Computer
and Information Science
USA - Philadelphia, PA 19104

Making a set of interrelated inferences is a problem that we face in many domains, especially ones where we deal with large amounts of data. For example, in computational biology we might have gene finding and transcription factor finding programs, each producing a distribution of likely starting points on the genome for the element they are seeking. But these inferences are interrelated because domain knowledge tells us that transcription factors occur reasonably close to genes. Similarly, identifying a human figure in an image may involve identifying arms, legs, torso, head etc., each identified probabilistically, but with constraints relating their positions. In a lighter vein, solving crossword puzzles, sudoku, and other grid puzzles can also be thought of as having distributions on values that can fill each square, but constraints relating these values.
We model all of these problems abstractly as follows: We are given random variables $X_1, X_2, \ldots, X_n$ with a prior joint distribution $D(x_1, x_2, \ldots, x_n)$ on them. We are also given linear equality and inequality constraints relating these random variables. We then consider the problems of finding the joint distribution under these constraints, finding marginals, or sampling from the constrained joint distribution. We show tight necessary and sufficient conditions for these problems to be efficiently solvable.

This is joint work with Zhiyi Huang.

AVERAGE LENGTH IN Q-ARY SEARCH WITH RESTRICTED SIZES OF QUESTION SETS

Gyula O. H. Katona

Alfred Renyi Institute of Mathematics
Hungarian Academy of Sciences
P. O. Box: 127
H - 1364 Budapest

Let $[n] = \{1, 2, \ldots, n\}$ be a finite set, and x an unknown element of $[n]$. We want to find x using an adaptive algorithm using the following type of tests. One test uses a partition of $[n]$ into subsets $A_0, A_1, \ldots, A_q$ satisfying $|A_1|, |A_2|, \ldots, |A_q| \le \ell$ where ℓ is a positive integer, but there is no size restriction on A_0. The result of the test tells which one of the A's contains x. Suppose that x is chosen randomly with a uniform distribution. An algorithm consisting of such tests minimizing the average number of steps is found.

PATH-SEARCH IN A PYRAMID AND OTHER GRAPHS

Balázs Keszegh

Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences
13-15 Reáltanoda u.
H - 1053 Budapest

We are given a directed acyclic (multi)graph G with one source and a set $E' \subset E(G)$ such that for every non-sink vertex $v \in V(G)$ there is exactly one outgoing edge at v which is in E'. It determines a path from the source to a sink. We can think of it as a switch in every vertex, which determines which way the water arriving to that vertex flows further.
We are interested in determining either the sink the flow arrives, or the whole path. The questions we can ask correspond to the vertices of the graph, and the answer describes the switch, i.e. tells which outgoing edge is in E'.

Definition 1. *Fixing a k, $p_k(G)$ is the minimal number of rounds we need to determine the path, if in each round we can ask k questions. Similarly, $s_k(G)$ is the minimal number of rounds we need to determine the sink, if in each round we can ask k questions.*

Clearly $s_k(G) \leq p_k(G)$ for every k. Also, $p_k(G) \geq p_{k+1}(G)$ and $s_k(G) \geq s_{k+1}(G)$ for every k.
The *pyramid graph* $Py(n)$ is a directed graph defined in the following way. $Py(n)$ has $N = n(n-1)/2$ vertices on n levels, for $1 \leq i \leq n$ the ith level having i vertices $v_{i,1}, v_{i,2} \dots v_{i,i}$, and from every vertex $v_{i,j}$ where $1 \leq i \leq n-1$ and $1 \leq j \leq i$, there is a *left outgoing edge* going to $v_{i+1,j}$ (its *left child*)and a *right outgoing edge* going to $v_{i+1,j+1}$ (its *right child*). $Py(n)$ has one *root* on the top, $v_{1,1}$ and n *sinks* on the bottom, the vertices on the nth level. A *pyramid path* is a directed path starting at the root and ending in one of the sinks.
Soren Riis proposed the problem of finding $p_k(Py(n))$ and $s_k(Py(n))$.
We conjecture the following.

Conjecture 2. *$s_k(Py(n)) = p_k(Py(n)) = \lceil n - 1/l \rceil$ if k is the lth triangle-number (i.e. $k = l(l-1)/2$).*

Conjecture 3. *$s_k(Py(n)) = p_k(Py(n))$ for every k and n.*

We verify Conjecture 2 for $l = 1, 2$ (i.e. $k = 1, 3$) and also we solve the case $k = 2$. The upper bounds follow from simple algorithms. All the lower bounds follow from the following theorem:

Theorem 4. *For arbitrary k, $p_k(Py(n)) \geq s_k(Py(n)) \geq \lceil \frac{2}{k+1}(n-1) \rceil$.*

We also investigate p_1 and s_1 for general acyclic graphs and eg. we determine p_k and s_k for complete binary trees.

This is joint work with Dániel Gerbner.

SOME STRUCTURES OF TOWER OF HANOI WITH FOUR PEGS

Kingo Kobayashi

National Institute of Information
and Communications Technology (NiCT)
4-2-1 Nukui-Kitamachi
Koganei
Japan - Tokyo 184-8795

While A. Brousseau considered the tower with more than three pegs, and gave a formula of “minimum” number of moves to transfer all disks at a peg to another peg. However, his proof had a defect in proving the optimality. Thus, the problem of Hanoi tower with more than three pegs is still open.

In this talk, we concentrate the situation of four pegs. Then, the configuration of disks distributed among pegs is called the state that is represented by a d-dimensional vector $(x_1, x_2, \ldots, x_d)$ where $x_i \in \{1, 2, 3, 4\}$ and d is the number of disks. The state $(x_1, x_2, \ldots, x_d)$ means that the largest disk is situated at the peg x_1, the second large disk is situated at the peg x_2, etc. At any peg, the arrangement of disks is uniquely determined, that is, larger disk should be covered by smaller disk. A legal move is a conveyance of one top disk from a peg to another without violation of disk size order. Without any loss of generality, the initial state is $(1, \ldots, 1)$ and the final state is $(3, \ldots, 3)$. The problem is to determine the minimum number of moves from the initial state to the final state.

We will study the numbers of moves to reach the set of midpoints from the initial state, where the set of midpoints is the set of states that are appeared just at the occasion when the largest disk can be moved to another pole. Thus, a midpoint is a state $(1, x_2, \ldots, x_d)$ such that $x_i \in \{2, 4\}$ if we assume to move the stack from the peg 1 to the peg 3. Then the cardinality of the set of midpoints is 2^{d-1}. If we treat the problem of tree pegs, the cardinality of the midpoints set is always one. In this talk, we introduce a recursive formula to give the profile of numbers of moves to reach the set of midpoints from the initial state. The formula is made by two functions, that is, rotation and translation on the state vectors defined by reverse and termwise-minimization operations. Moreover, we will give a promising procedure to describe the optimal path of moves.

References

[1] B.A.Brousseau, Tower of Hanoi with More Pegs, J. Recreational Mathematics, Vol.8(3), 1975-76.

SEARCH PROBLEMS ON CAYLEY GRAPHS

Elena Konstantinova

Siberian Branch of Russian Academy
of Sciences
Sobolev Institute of Mathematics
Pr. Koptuyga 4
RU - 630090 Novosibirsk

We consider some combinatorial problems on Cayley graphs from a search point of view. The most of Cayley graphs presented in the talk have connections with communication networks.

RENDEZVOUS SEARCH AND EXPLORATION WITH MOBILE AGENTS

Evangelos Kranakis

Carleton University
School of Computer Science
1125 Colonel By Drive
Canada - Ottawa, Ontario K1S 5B6

Mobile agents are autonomous, intelligent computer software with limited memory and computation capability moving in a network. They are modelled by automata having either discrete or continuous transitions and can be either deterministic, non-deterministic, or randomized. They are employed by another entity in a network to which they must report their findings. The network model is derived from distributed computing and it is a connected graph whose vertices are computing nodes and edges correspond to communication links. It may be static, dynamic, or evolving depending on the status of its various components. Depending on the model being considered, nodes and links of the network may have distinct labels typically forming an overlay over an existing physical infrastructure Given a model for both the agents and the network, the graph exploration problem is that of designing an algorithm for the agent that allows it to visit all of the nodes and/or edges of the network. Coupled with this problem is when autonomous, co-operative mobile agents are searching for a particular node or item in the network. Closely related is also the rendezvous problem whereby two or more mobile agents starting from different nodes are required to gather at a single node of a network or even execute jointly a network task. These problems as well as similar related problems including swarming, cascading, community formation, etc. are commonplace not only in the Internet but also in P2P, Information and Social networks. In this talk we will survey a variety of efficiency measures and computation models involving trade-offs between time and memory required by the mobile agents for completing any of the tasks formulated above in various settings (deterministic, randomized) and types of networks (including trees, rings, tori, and arbitrary graphs).

SHADOWS UNDER THE WORD-SUBWORD RELATION

Vladimir Lebedev
Russian Academy of Sciences
Institute of Problems of Information
Transmission
Bol'shoi Karetnyi per. 19
Russia - Moscow 101447

For an alphabet $\mathcal{X} = \{0, 1, \ldots, q-1\}$ we consider the set $\mathcal{X}^k$ of words $x^k = x_1 x_2 \cdots x_k$ of length k. For a word $a^k = a_1 a_2 \cdots a_k \in \mathcal{X}^k$ we define the shadow of a^k by $\operatorname{shad}(a^k) = a_2 a_3 \cdots a_k \cup a_1 a_2 \cdots a_{k-1}$.

Now for any subset $A \subset \mathcal{X}^k$ we define the shadow

$$\operatorname{shad}(A) = \bigcup_{a^k \in A} \operatorname{shad}(a^k). \tag{24.1}$$

We are interested in finding

$$\nabla_k(q, N) = \min\{|\operatorname{shad}(A)| : A \subset \mathcal{X}^k, |A| = N\}. \tag{24.2}$$

We define now our main concept.

Definition. *For non-negative integers l (left), m (middle), and r (right) satisfying $l \geq r$ and $k = l + m + r$, we define the basic set $\mathcal{B}(k, l, r)$ in $\mathcal{X}^k$ as follows:*

$$\mathcal{B}(k, l, r) = \bigcup_{s=0}^{l-r} \mathcal{X}^{l-s} 0^m \mathcal{X}^{r+s}. \tag{24.3}$$

For example $\mathcal{B}(7, 3, 1)$ is the union of the rows in the matrix

$$\begin{array}{ccccccc} \mathcal{X} & \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X} \\ \mathcal{X} & \mathcal{X} & 0 & 0 & 0 & \mathcal{X} & \mathcal{X} \\ \mathcal{X} & 0 & 0 & 0 & \mathcal{X} & \mathcal{X} & \mathcal{X} \end{array}$$

Theorem. *For $N = q^{l+r} + q^{l+r-1}(l-r)(q-1)$ and $k = l + m + r > 2l \geq 2r \geq 2$ we have*

$$\frac{1}{q} N < \nabla_k(q, N) \leq \frac{1}{q}\left(1 + \frac{1}{l - r + 1}\right) N. \tag{24.4}$$

This is joint work with Rudolf Ahlswede.

SEARCHING FOR SOLUTIONS OF HARD PROBLEMS

Ulf Lorenz
Technische Universität Darmstadt
FB Mathematik, Optimierung
Dolivostrae 15
64293 Darmstadt

We assume that some computational problem is given and that our aim is to find a solution for this problem. The first part of the talk touches complexity theory. We present the complexity classes P, NP and PSPACE and show how the corresponding classes influence the structure of solutions. A solution of an NP complete problem corresponds to a path, and a solution of a PSPACE complete problem corresponds to a tree.

The second part of the talk is about game tree searching in computer chess. The minimax principle is introduced, as well as game trees and the Alphabeta-algorithm. The computers aim is to find a good decision in a given chess position. Because, in most positions, a chess program cannot find an optimal move, it utilizes heuristic evaluations and a game tree search. I.e., chess programs compute minimax values, basing on estimations of position values. The last 50 years show that this technique leads to good playing, and we show why it works: Under some necessary and sufficient conditions, the game tree acts as an error filter in our game tree model.

The third part bridges the gap between PSPACEc games and mathematical optimization where we especially focus on so called quantified linear programs. Quantified linear programs are linear programs together with a quantifier string which determines how the variables are individually quantified: either existentially or universally. The continuous version has interesting polyhedral properties and the integer variant is PSPACE complete and has therefore similarity with chess. Relaxations and bound computations allow to cut off certain parts of the search tree, such that for these cut subtrees it is possible to find solutions to subproblems without searching.

COMBINATORIAL METHOD FOR ANOMALY DETECTION

Anthony J. Macula

SUNY College at Geneseo
JEANSEE.LLC
USA - Geneseo, NY 14454

We discuss a combinatorial method for detecting anomalies in typical aircraft data. This method relies on the combinatorial mixing and compression of the fields in the raw data records. This approach reduces complexity of the data to be profiled and allows for the efficient profiling and detection of anomalies arising from combinations of data fields.

HAPLOTYPE INFERENCE AND GRAPHS OF SMALL SEPARABILITY

Martin Milanic

Univerza na Primorskem
Fakulteta za matematiko
naravoslovje in informacijske tehnologije
FAMNIT
Glagoljaska 8
6000 Koper
Slovenia

One of the main computational problems following the completion of the Human Genome Project is the problem of inferring biologically meaningful haplotype data from the genotype data of a population. Humans are diploid organisms, i.e., their DNA is organized in pairs of (almost identical) chromosomes. For each pair of chromosomes, one chromosome copy is inherited from the father and the other copy is inherited from the mother. It is important to know the exact sequence of bases on the father and mother chromosomes. However, experimentally it is much easier and less expensive to collect a "conflated" (mixed) description of the two chromosomes, which only tells us for each position whether the two chromosomes are identical or not. This conflated description is referred to as a genotype. The description of the data from one of the pair of chromosomes is called a haplotype. Resolving (or explaining) a genotype g requires determining two haplotypes such that, if they are assumed to be the two chromosome copies, their conflated version gives exactly the genotype g. More generally, given a set G of genotypes, the Haplotype Inference problem requires to determine a set of haplotypes such that each genotype $g \in G$, g is explained by two haplotypes from the set. Because of its importance the haplotyping problem is being extensively studied, under many objective functions, one of which is *Parsimony*.

An instance of the parsimony haplotyping problem is said to be k-bounded if for every position, at most k of the given genotypes arise from chromosomes that differ at that position. There is a close connection between the k-bounded parsimony haplotyping problem and so-called *graphs of separability at most k*, defined as graphs in which every two non-adjacent vertices can be separated by a set of at most k other vertices: A graph G is of separability at most k if and only if G is isomorphic to the compatibility graph of some k-bounded parsimony haplotyping instance.

For $k \in \{0, 1\}$, the only connected graphs of separability at most k are complete graphs and block graphs, respectively. For $k \geq 3$, graphs of separability at most k form a rich class of graphs containing all graphs of maximum degree k. We prove several characterizations of graphs of separability at most 2 (which generalize complete graphs, cycles and trees), including a structure theorem with nice algorithmic implications—some of which cannot be extended to graphs of higher separability—and a characterization of graphs of separability at most 2 in terms of minimal forbidden induced subgraphs and minimal forbidden induced minors.

This is joint work with Ferdinando Cicalese.

SUBLINEAR COMPRESSIVE SENSING VIA DENSE BELIEF PROPAGATION

Olgica Milenkovic

University of Illinois Department of Electrical
and Computer Engineering
William L. Everitt Laboratory
211 W. California Ave.
USA - Urbana, Illinois 61801-2918

Compressive sensing (CS) is a new sampling technique which reduces the complexity of sparse data acquisition. One of the major obstacles for practical deployment of CS techniques is the signal reconstruction time. We propose a new compressive sensing scheme, based on codes of graphs, that allows for joint design of sensing matrices and logarithmic complexity reconstruction algorithms. The compressive sensing matrices can be shown to offer asymptotically optimal performance when used in combination with Orthogonal Matching Pursuit (OMP) methods. For more elaborate greedy reconstruction schemes, we propose a new family of list decoding, reinforced, and multiple-basis belief propagation algorithms. Our simulation results indicate that reinforced BP CS schemes offer very good complexity-performance trade-offs for several classes of sparse signals. is NP-hard. This issue has led to a large body of work in CS theory centered around the design of measurement and reconstruction algorithms with tractable reconstruction complexity.

This is joint work with Wei Dai and Vin Pham Hoa.

AN EXTENSION OF LIST DISJUNCT MATRICES THAT CAN CORRECT ERRORS IN TEST OUTCOMES

Ely Porat

Department of Computer Science
Bar-Ilan University
Ramat Gan 52900, Israel

A (d, l)-list disjunct matrix is a non-adaptive group testing primitive that given a set of n items with at most d "defectives", with a small number of tests, outputs a set of items which contains all the defectives plus at most $l1$ non-defective items. These primitives have found many applications as stand alone objects and as building blocks in the construction of other combinatorial objects. In this paper, we formulate and study an extension of list disjunct matrices that can correct errors in test outcomes. We present two procedures that convert error-tolerant list disjunct matrices in a black-box manner into error-tolerant list disjunct matrices that are also efficiently decodable.

SEARCHING FOR HIDDEN INFORMATION

K. Rüdiger Reischuk

Universität zu Lübeck
Institut für Theoretische Informatik
Ratzeburger allee 160 - Geb. 64
D - 23538 Lübeck

The aim of steganography is to hide secret messages in unsuspicious covertexts in such a way that the mere existence of a hidden message is concealed. The basic scenario assumes two communicating parties Alice (sender) and Bob (receiver) as well as an adversary Eve who is often also called a “warden” due to Simmons’ motivation as secret communication among prisoners. Eve wants to find out whether Alice and Bob are exchanging hidden messages among their covertext communication. A useful stegosystem has to satisfy two conditions – (a) *reliability*, i.e. the ability of Alice to effectively transmit secret information to Bob and (b) *security*, i.e. the ability to prevent Eve from distinguishing between original covertexts and modified stegotexts.

In the past few years some advances have been achieved in the development of theoretical foundations of steganography. Using notions from cryptography such as *indistinguishability* and adapting them to a steganographic scenario, one can construct stegosystems that are provably secure against passive and active detection procedures. However, since their transmission rate is quite low they do not provide a solution in practice.

For embedding information into covertexts that can hardly be detected, the amount of knowledge about the covertext channel – on the one hand available to the encoder and on the other hand given to the adversary – turns out to be crucial. In reality, Alice neither has zero nor full knowledge, but rather something in between, since she has the option to choose which kind of covertext channels (pictures, texts, music, ...) to use. Eve has to accept this choice, and both can then try to learn more about the channel in order the generate good stegotexts, resp. in order to recognize them.

We propose a more realistic and flexibel model for steganography, called *grey-box steganography*, in which the encoder has *partial knowledge* of the covertext channel. It generalizes the two extremes, a *black-box* setting, where the encoder does not have any knowledge (also called universal steganography), and a *white-box* scenario, where Alice has perfect information. The task to design efficient grey-box stegosystems is analysed and its different subtasks are investigated, in particular the algorithmic learning problem for the covertext channel.

Searching for hidden information in the steganographic setting can be considered as a 2-person game where the first player tries to minimize the chance of detection by the other one. We discuss several notions how to measure the success probability. It can be shown that they correspond to different levels of knowledge of both players.

A NEW MAX-FLOW MIN-CUT THEOREM FOR INFORMATION FLOWS

Soren Riis

Queen Mary, University of London
Department of Computer Science
UK - London E1 4NS

We present a theorem that concerns dispersion of information in communication networks. The theorem resembles, but is fundamentally different from the celebrated max-flow min-cut theorem for commodity networks. The main result is linked to important search problems and this is illustrated by examples, counter examples as well as numerical calculations.

AN APPLICATION OF SUPERIMPOSED CODING THEORY TO THE MULTIPLE ACCESS OR CHANNEL AND TWO-STAGE GROUP TESTING ALGORITHMS

Vyacheslav V. Rykov

University of Nebraska at Omaha
Department of Mathematics
6001 Dodge St.,
USA - Omaha, NE 68182-0243

A multiple access channel is a medium that allows multiple terminal stations to communicate with a central station. We will consider a system containing a large amount of terminal stations and a multiple access OR channel connecting the terminal stations to the central station, as in the slotted ALOHA system [1]. We implement the superimposed code constructions [2],[3] to the discussed multiple access information transmission model for the calculation of bounds on the multiple access channel capacity. Recent results in Superimposed Coding Theory [4] provide the possibility of improving the known bounds [5]. We will show that the multiple access OR channel capacity is bounded below by $\ln 2$. On the application to Group Testing the obtained bound on the channel capacity allows us to nd the asymptotic upper bound on the number of tests required in two-stage group testing [4]. We will show that, if t is the size of a population and s is the number of defective units among the population, then for large t and $s \ln 2 \log_2 t$, the number of tests with superimposed output, required to nd s defective units, $N \leq (\log_2 t)^2(1 + o(1))$ with probability 1.

References

[1] A.G. Dyachkov, V.V. Rykov, "Superimposed Codes and ALOHA System", Diskrete Strukturen in der Mathematik, University of Bielefeld, 98-018, 1998.

[2] W.H. Kautz, R.C. Singleton, "Nonrandom Binary Superimposed Codes", IEEE Trans. Inform. Theory, vol. 10, no. 4, pp. 363-377, 1964.

[3] A.G. Dyachkov, A.J. Macula, V.V. Rykov, "New Constructions of Superimposed Codes". IEEE Trans. on Information Theory, vol. 46, no. 1, pp. 284-290, 2000.

[4] A.J. Macula, V.V. Rykov, S. Yekhanin, "Trivial two-stage group testing for complexes using almost disjunct matrices", Discrete Appl. Math. 137, no. 1, 97107, 2004.

[5] A.G. Dyachkov, V.V. Rykov, "Superimposed Codes for Multiple Accessing of the OR-channel," 1998 IEEE International Symposium on Information Theory, Boston, USA, August 1998.

This is joint work with Vladimir Umtsev and Anthony Macula.

STREAMING ALGORITHMS FOR THE ANALYSIS OF MASSIVE DATA SETS

Christian Sohler

Technische Universität Dortmund
Fakultät für Informatik
Lehrstuhl 2
D - 44221 Dortmund

Massive data sets occur in many applications of Computer Science. Examples include the WWW, internet traffic logs, and operating system calls. Often data is read sequentially in the form of a data stream, which is too large to be stored in main memory and sometimes even too large to be stored at all. If we want to analyze such massive data sets to, say, build a search engine, detect spreading viruses, or optimize a systems performance, we need special algorithms that use only little memory and process the input sequentially. Such algorithms are called streaming algorithms. In this talk I will give an introduction to streaming algorithms and explain the two major algorithmic concepts used in this area. I will discuss their applications in the development of streaming algorithms for data analysis and close with a discussion of future directions of research.

M-PART SPERNER FAMILIES

László Székely

Department of Mathematics
University of South Carolina
USA - Columbia, SC 29208

A Sperner family is an antichain in the subset lattice. The maximum size of Sperner families is $\binom{n}{\lfloor\frac{n}{2}\rfloor}$, and maximum size Sperner families are one of the two middle levels in the Boolean lattice. Katona and Kleitman noticed that the same bound holds for 2-part Sperner families, but does not hold for 3 or more-part Sperner families. We investigate, and in a sense characterize, those Sperner type problems, for which the $\binom{n}{\lfloor\frac{n}{2}\rfloor}$ bound is valid. We will also consider several generalizations of Sperner families, and show a new conjecture on multi-partite Sperner systems of maximum size.

This is a joint work with H. Aydinian, E. Czabarka and P.L. Erdös.

MONTE-CARLO TREE SEARCH: A NEW PARADIGM FOR COMPUTATIONAL INTELLIGENCE

Olivier Teytaud

Université Paris-Sud
TAO, projet Inria
LRI, Batiment 490 - Bureau 85
F - 91405 Orsay cedex

We will introduce the recent Monte-Carlo Tree Search algorithm and present some of its main successes (including the game of Go, but also industrial applications). We will also present some extensions (continuous domains, partially observable cases), and the main directions of research (introducing supervised learning, mixing with handcrafted value functions) - and also the main limitations of the approach - we are still very far from the abstraction power of the human brain.

A LOWER BOUND FOR THE COMPLEXITY OF MONOTONE GRAPH PROPERTIES

Eberhard Triesch
RWTH Aachen
Lehrstuhl für Mathematik
Templergraben 55
D - 52056 Aachen

For a graph property $\mathcal{P}$ on n vertices, denote by $c(\mathcal{P})$ the number of edges which must be tested in the worst case in order to determine whether a graph has property $\mathcal{P}$ or not.
In 1973, Aanderaa and Rosenberg conjectured that there exists some $\gamma > 0$ such that

$$c(\mathcal{P}) \geq \gamma n^2$$

for all nontrivial monotone graph properties $\mathcal{P}$, which was proved one year later by Rivest and Vuillemin with $\gamma = 1/16$.
In 1984 Kahn, Saks and Sturtevant [2] proved by a topological method that $c(\mathcal{P}) \geq (n^2/4)o(n^2)$.
We describe a way to apply their method in order to increase the lower bound to $(8/25)n^2 o(n^2)$ ([1]).
Though it is the first improvement of the bound from[2] since 1984, the proof is not complicated and gives some hope for further improvements.

References

[1] T. KORNEFFEL, E.TRIESCH, An asymptotic bound for the complexity of monotone graph properties, to appear in Combinatorica.

[2] J. KAHN, M. SAKS AND D. STURTEVANT, A topological approach to evasiveness, Combinatorica 4 (1984), pp. 297306.

This is joint work with Torsten Korneffel.

DNA CODES FOR NON-ADDITIVE STEM DISTANCE

Anna Nikitichna Voronina
Lomonosov Moscow State University
Faculty of Mechanics and Mathematics
Department of Probability Theory
Vorob'evy gory
Russia - 119992 Moscow

We study the new concept of combinatorial coding theory called an additive (non-additive) stem similarity between two q-ary sequences which is calculated as the maximal number of common blocks of length 2 containing adjacent symbols in their common Hamming subsequences (in their common subsequences). For $q = 4$, the stem similarity and the corresponding stem distance are used to describe a mathematical model of thermodynamic similarity that adequately rejects the "hybridization potential" of two DNA sequences (strands). We will also consider a more advanced approach called the "nearest-neighbor thermodynamics" involving a weight function (stem w-similarity) defined for each these type of stems [1]-[2].

DNA code is a collection of DNA sequences (codewords) which is invariant under the Watson-Crick transformation and if a pair of its codewords does not form the Watson-Crick duplex, then the thermodynamic similarity between these codewords should be less than a fixed level. We present some optimal constructions of linear DNA codes called maximum distance separable (MDS) codes for additive stem distance. These constructions are compared with conventional MDS codes for Hamming distance.

For the case of additive stem w-similarity, we discuss methods [1] to prove upper and lower bounds on the rate of DNA codes analogous to the well-known Plotkin upper bound and lower random coding bound (Gilbert-Varshamov bound), i.e., we obtain a critical relative distance for DNA codes. These methods take into account a "Markovian" specification of the additive stem distance as well as a structure of DNA code which is identified by its invariance under Watson-Crick transformation. In particular, our lower bound is established with the help of an ensemble of random codes where the distribution of independent codewords is given by a stationary Markov chain, and we apply the large deviations techniques [3] to a sum of random variables connected via Markov chain.

For the case of non-additive stem w-similarity, we prove a random coding bound on the rate of DNA codes with the help of ensembles of DNA strands [2] whose sequence composition is restricted in a manner similar to the restrictions in binary Fibonacci sequences. Such combinatorial ensemble can be interpreted as an analog of Markov chain in which the corresponding transitions are forbidden.

References

[1] A. G. D'yachkov, A. N. Voronina, "DNA Codes for Additive Stem Similarity," Problems of Information Transmission, vol. 45, n. 2, pp. 348-367, 2009.

[2] A. G. D'yachkov, A. J. Macula, T. E. Renz, V. V. Rykov, "Random Coding Bounds for DNA Codes Based on Fibonacci Ensembles of DNA Sequences," in 2008 IEEE Int. Symp. Information Theory, Toronto, Canada, 2008, pp. 2292-2296.

[3] Dembo, A., Zeitouni, O., Large Deviations Techniques and Applications, Boston, MA: Jones and Bartlett, 1993.

This is joint work with Arkadii D'yachkov.

LIST OF PARTICIPANTS

1. Rudolf Ahlswede
Universität Bielefeld
Fakultät für Mathematik
Postfach 10 01 31
D -33615 Bielefeld
Tel.: +49 (0)521 106-4789
ahlswede@math.uni-bielefeld.de

2. Ingo Althöfer
Friedrich-Schiller-Universität Jena
Fakultät für Mathematik und Informatik
Institut für Angewandte Mathematik
D-07737 Jena
Tel.: +49 (0)3641 946-210
Fax: +49 (0)3641 946-202
ingo.althoefer@uni-jena.de

3. Harout Aydinian
Universität Bielefeld
Fakultät für Mathematik
Postfach 10 01 31
D - 33615 Bielefeld
Tel.: +49 (0)521 106-4790
ayd@math.uni-bielefeld.de

4. Vladimir Blinovsky
Institute of
Information Transmission Problems
Russian Academy of Sciences
B. Karetnii per 19
Russia - Moscow 127 994
Tel.: +7 926 831 9597
vblinovs@yandex.ru

5. Minglai Cai
Universität Bielefeld
Fakultät für Mathematik
Postfach 10 01 31
33501 Bielefeld
Tel.: +49 (0)521 106-4775
mlcai@math.uni-bielefeld.de

6. Huilan Chang
National Chiao Tung University
Department of Applied Mathematics
2F, Science Building
1001 Ta Hsueh Road
Taiwan - Hsinchu, 30010
Tel.: +886 3 571 2121 ext.56435
huilan0102@gmail.com

7. Hong-Bin Chen
National Chiao Tung University
Department of Applied Mathematics
Taiwan - Hsinchu, 30010
Tel.: +886 3 57-1212 ext. 56464
Fax: +886 3 57-679
andanchen@gmail.com

8. Ferdinando Cicalese
Dipartimento di
Informatica ed Applicazion
Universita' di Salerno
I - Baronissi (SA) - 84081
Tel.: +39 089 969717
Fax : +39 089 969600
cicalese@dia.unisa.it

9. Charlie Colbourn
Arizona State University
School of Computing, Informatics
and Decision Systems Engineering
P.O. Box 878809
USA - Tempe, Arizona 85287-8809
Tel.: +1 480 727-6631
Fax: +1 480 965-2751
colbourn@asu.edu

10. Eva Czabarka
University of South Carolina
Department of Mathematics
USA - Columbia, SC 29208
czabarka@math.dot.edu

11. Peter Damaschke
Chalmers University
Department of Computer Science
and Engineering
S - 41296 Göteborg
Tel.: +46 31 772-5405
ptr@chalmers.se

12. Annalisa De Bonis
Università di Salerno
Dipartimento di Informatica
ed Applicazioni
Via Ponte Don Melillo
I - 84084 Fisciano (SA)
Tel.: +39 (0)89 96-9719
Fax: +39 (0)89 96-9600
debonis@dia.unisa.it

13. Gianluca De Marco
Università degli Studi di Salerno
Dipartimento di Informatica
ed Applicazioni
Via Ponte don Melillo
I - 84084 Fisciano (SA)
Tel.: +39 (0)89 96-9721
demarco@dia.unisa.it

14. Christian Deppe
Universität Bielefeld
Fakultät für Mathematik
Postfach 10 01 31
D - 33615 Bielefeld
cdeppe@math.uni-bielefeld.de

15. Arkadii D'yachkov
Moscow State University
Faculty of Mechanics & Mathematics
Department of Probability Theory
Russia - Moscow 119899
dyachkov@mech.math.msu.su

16. Dániel Gerbner
Rényi Institute
Reáltanoda utca 13-15.
H - 1053, Budapest
Tel.: +36 30 306-5464
gerbner@renyi.hu

17. Lov Kumar Grover
Lucent Technologies
600-700 Mountain Avenue
USA - Murray Hill, NJ 07974
lov.grover@gmail.com

18. Tobias Jacobs
National Institute of Informatics
2-1-2 Hitotsubashi,
Japan - Chiyoda-ku, Tokyo 101-8430
Tel.: +81 (0)90 810-88547
Fax: +49 (0)3212-122-4657
jacobs@nii.ac.jp

19. Sampath Kannan
University of Pennsylvania
Department of Computer
and Information Science
USA - Philadelphia, PA 19104
Tel.: +1 215 681-9012
kannan@central.cis.upenn.edu

20. Gyula O. H. Katona
Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences
P. O. Box: 127
H - 1364 Budapest
Tel.: +36 1 483-8318
Fax: +36 1 483-8333
ohkatona@renyi.hu

21. Balázs Keszegh
Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences
13-15 Reáltanoda u.
H - 1053 Budapest
Tel.: +36 70 237-5593
Fax: +36 1 483-8333
keszegh@renyi.hu

22. Kingo Kobayashi
National Institute of Information
and Communications Technology (NiCT)
4-2-1 Nukui-Kitamachi
Koganei
Japan - Tokyo 184-8795
Tel.: +81 42 327-6806
kingo@nict.go.jp

23. Munjong Kolss
Universität Bielefeld
Abteilung Evolutionsbiologie
Morgenbreede 45
D - 33615 Bielefeld
Tel.: +49 (0)521 106-2719
munjong.kolss@uni-bielefeld.de

24. Elena Konstantinova
Siberian Branch of Russian Academy
of Sciences
Sobolev Institute of Mathematics
Pr. Koptuyga 4
RU - 630090 Novosibirsk
e_konsta@math.nsc.ru

25. Evangelos Kranakis
Carleton University
School of Computer Science
1125 Colonel By Drive
Canada - Ottawa, Ontario K1S 5B6
Tel.: +1 613 521-0154
kranakis@scs.carleton.ca

26. Vladimir Lebedev
Russian Academy of Sciences
Institute of Problems of Information
Transmission
Bol'shoi Karetnyi per. 19
Russia - Moscow 101447
lebedev37@mail.ru

27. Ulf Lorenz
Technische Universität Darmstadt
FB Mathematik, Optimierung
Dolivostrae 15
64293 Darmstadt
Tel.: +49 (0)6151 16-2961
lorenz@mathematik.tu-darmstadt.de

28. Anthony J. Macula
    SUNY College at Geneseo
    JEANSEE.LLC
    USA - Geneseo, NY 14454
    Tel.: +1 585 243-5749
    macula@geneseo.edu

29. Martin Milanič
    Univerza na Primorskem
    Fakulteta za matematiko
    naravoslovje in informacijske tehnologije
    FAMNIT
    Glagoljaška 8
    6000 Koper
    Slovenia
    Tel.: +386 (0)5 611 7580
    Fax: +386 (0)5 611 7571
    martin.milanic@upr.si

30. Olgica Milenkovic
    University of Illinois
    Department of Electrical
    and Computer Engineering
    William L. Everitt Laboratory
    211 W. California Ave.
    USA - Urbana, Illinois 61801-2918
    Tel.: +1 217 244-7358
    milenkov@ad.uiuc.edu

31. Ely Porat
    Department of Computer Science
    Bar-Ilan University
    Ramat Gan 52900, Israel
    Tel.: +972-3-531-8075
    Fax.: +972-3-736-0498
    porately@cs.biu.ac.il

32. K. Rüdiger Reischuk
    Universität zu Lübeck
    Institut für Theoretische Informatik
    Ratzeburger allee 160 - Geb. 64
    D - 23538 Lübeck
    Tel.: +49 (0)451 500-5310
    Fax: +49 (0)451 500-5301
    reischuk@tcs.uni-luebeck.de

33. Soren Riis
    Queen Mary, University of London
    Department of Computer Science
    UK - London E1 4NS
    smriis@dcs.qmul.ac.uk

34. Vyacheslav V. Rykov
    University of Nebraska at Omaha
    Department of Mathematics
    6001 Dodge St.,
    USA - Omaha, NE 68182-0243
    Tel.: +1 402 554-3117
    Fax: +1 402 554-2975
    vrykov@mail.unomaha.edu

35. Christian Sohler
    Technische Universität Dortmund
    Fakultät für Informatik
    Lehrstuhl 2
    D - 44221 Dortmund
    Tel.: +49 (0)176 238 799 44
    christian.sohler@tu-dortmund.de

36. László Székely
    Department of Mathematics
    University of South Carolina
    USA - Columbia, SC 29208
    Tel.: +1 803 777-6262
    Fax: +1 803 777-3783
    szekely@math.sc.edu

37. Olivier Teytaud
    Université Paris-Sud
    TAO, projet Inria
    LRI, Batiment 490 - Bureau 85
    F - 91405 Orsay cedex
    Tel.: +33 01 69 15 66 07
    Fax: +33 01 69 15 65 86
    olivier.teytaud@inria.fr

38. Eberhard Triesch
    RWTH Aachen
    Lehrstuhl für Mathematik
    Templergraben 55
    D - 52056 Aachen
    Tel.: +49 (0)241 809 4995
    Fax: +49 (0)241 809 2136
    triesch@math2.rwth-aachen.de

39. Ugo Vaccaro
    Dipartimento di
    Informatica ed Applicazion
    Universita' di Salerno
    I - Baronissi (SA) - 84081
    Tel.: +39 089 969717
    Fax : +39 089 969600
    cicalese@dia.unisa.it

40. Anna Nikitichna Voronina
    Lomonosov Moscow State University
    Faculty of Mechanics and Mathematics
    Department of Probability Theory
    Vorob'evy gory
    Russia - 119992 Moscow
    Tel.: +7 916 116-0386
    annnoy@mail.ru