ZIF COOPERATION GROUP
SEARCH METHODOLOGIES

Zentrum für interdisziplinäre Forschung
Center for Interdisciplinary Research
Universität Bielefeld

Workshop "Search Methodologies III"

September 3 - 7, 2012

Convenors:
Ferdinando Cicalese
Christian Deppe

PROGRAM AND BOOKLET OF ABSTRACTS

Contents

SEARCH METHODOLOGIES

In 1979, Rudolf Ahlswede and Ingo Wegener wrote one of the first books on search (and surely the first in Germany). In the introduction the authors wrote that they would

> "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."

Three decades ago it was often asked whether search is a scientific subject at all! Instead, in the three decades passed since the appearance of Search Problems, there has been an explosion of developments in the research field of "search". New models, novel techniques and analytical tools have been developed for attacking problems of search within Computer Science, Image Reconstruction, Machine Learning, Information Theory (classical and quantum theoretical), and Operation Research. 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.

Time seems to be mature for a more comprehensive understanding of such a broad area of research, with the goal of defining the nature, scope (and the borders) of a general Theory of Search.

A broad class of search problems are defined in terms of a space of objects and a space of tests (questions). Different performance criteria can be chosen, e.g., number of tests performed, time of computation, space requirements, *et cetera*. Furthermore one distinguishes between combinatorial and probabilistic models. Especially important is the study of adaptive and non-adaptive strategies as well as the analysis of their intermediate forms.

These specifications define a first basic classification which captures most models we deal with in one-sided search, where, so to speak, the targets are passive. Lifting the assumption that the target is passive, i.e., does not change or move, during the process, like in two-sided search pioneered by B.O. Koopman, the new model includes for instance search in game trees and rendezvous search. Furthermore, Quantum searching has analogue models and genuine novelties. More needs to be done, and will be done.

Monday September 03, 2012	
	- Chair H. Aydinian -
9:00	Opening Joanna Pfaff-Czarnecka (Member of ZiF's Board of Directors), Ferdinando Cicalese and Christian Deppe, Welcoming Address
9:15	E. Czabarka, K-Dimensional M-part Sperner Families and Mixed Orthogonal Arrays
10:10	*- Coffee Break -*
	- Chair H. Aydinian -
10:40	M. Bodewig, Completeness and Multiplication of Fix-Free Codes Regarding Ahlswede's 3/4-Conjecture
11:20	R. Reischuk, The Smoothed Competitive Ratio of Online Caching
12:30	*- Lunch -*
	- Chair C. Deppe-
14:00	S. Riis, Search Problems Related to Dispersion, Graph Entropy and Guessing Games
15:10	I. Althöfer, Strange Phenomena in Monte-Carlo Game Tree Search
15:50	*- Coffee Break -*
	- Chair C. Deppe -
16:10	U. Tamm, Multiparty Communication Complexity of Vector–Valued and Sum–Type Functions
16:50	RUMP Session
18:30	Welcome Dinner

Tuesday September 04, 2012	
	- Chair F. Cicalese -
9:00	A. Rudra, Group Testing and Coding Theory
10:00	V. Lebedev, Group Testing with Two Defectives
10:40	*- Coffee Break -*
	- Chair F. Cicalese -
11:00	P. Damaschke, On Optimal Strict Multistage Group Testing
11:40	V. Rykov: On Superimposed Codes and Designs
12:30	*- Lunch -*
	- Chair H. Aydinian-
14:30	A. D'yachkov, Superimposed Codes and Non-Adaptive Threshold Group Testing
15:10	N. Polyanskii, Random Coding Bounds on the Rate for Non-Adaptive Threshold Group Testing
15:50	*- Coffee Break -*
	- Chair H. Aydinian -
16:10	M. Aldridge, Adaptive Group Testing: a Channel Coding Approach
16:50	M. Malioutov, On Connection with Compressed Sensing and Some Other New Developments in the Search Theory
17:30	RUMP Session

Wednesday September 05, 2012	
	- Chair C. Deppe -
9:15	E. Triesch, Upper and Lower Bounds for Competitive Group Testing
9:55	H. Aydinian, Quantum Error Correcting: An Introduction
10:35	*- Coffee Break -*
	- Chair C. Deppe -
11:00	G. Katona, When the Lie Depends on the Target
11:40	G. De Marco, Computing Majority with Triple Queries
12:30	*- Lunch -*
	- Chair F. Cicalese -
14:30	D. Gerbner, Majority and Plurality Problems
15:10	G. Wiener, On a Problem of Rényi and Katona
15:50	*- Coffee Break -*
	- Chair F. Cicalese -
16:10	E. Porat, Efficient Signature Scheme for Network Coding
16:50	RUMP Session
18:30	Conference Dinner

Thursday September 06, 2012	
	- Chair H. Aydinian -
9:00	L. Gasieniec, Communication-Less Agent Location Discovery
10:00	E. Kranakis: Boundary Patrolling by Mobile Agents
10:40	*- Coffee Break -*
	- Chair H. Aydinian -
11:00	O. Teytaud, Search with Partial Information
11:40	B. Balkenhol, Fuzzy Self-Learning Search
12:30	*- Lunch -*
	- Chair F. Cicalese -
14:30	A. Dress, Using Suffix Trees for Alignment-Free Sequence Comparison and Phylogenetic Reconstruction
15:10	Zs. Lipták, Some Problems and Algorithms in Non-Standard String Matching
15:50	*- Coffee Break -*
17:00	Sightseeing Tour

Friday September 07, 2012	
	- Chair C. Deppe -
9:00	L. Székely, Some Constructions for the Diamond Problem
9:40	V. Balakirsky, Extracting Significant Parameters from Noisy Observations and Their Use for Authentication
10:20	*- Coffee Break -*
	- Chair C. Deppe -
10:40	RUMP Session
12:30	*- Lunch -*

ADAPTIVE GROUP TESTING: A CHANNEL CODING APPROACH

Matthew Aldridge
University of Bristol
School of Mathematics
University Walk
UK - Bristol, BS8 1TW

Group testing is the combinatorial problem of identifying the defective items in a population by grouping items into test pools. Recently, nonadaptive group testing - where all the test pools must be decided on at the start - has been studied from an information theory point of view. Using techniques from channel coding, upper and lower bounds have been given on the number of tests required to accurately recover the defective set, even when the test outcomes can be noisy. In this talk, we give the first information theoretic result on adaptive group testing - where the outcome of previous tests can influence the makeup of future tests. We show that adaptive testing does not help much, as the number of tests required obeys the same lower bound as nonadaptive testing. Our proof uses similar techniques to the proof that feedback does not improve channel capacity.

STRANGE PHENOMENA IN MONTE-CARLO GAME TREE SEARCH

Ingo Althöfer

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

In a game tree, pure Monte Carlo search with integral parameter T (called MC(T) for short) runs as follows. In the current position, for each feasible move T random games are generated. The move with the best average score is played. Of course, often pure Monte Carlo will not play a game-theoretically perfect move. We report on several phenomena of pure Monte Carlo.

(1) **The BASIN STRUCTURE in Self Play**
When MC(T) plays versus MC(2T), typically MC(T) wins less than half of the games. Often there is an intermediate value T* such that the winning quota of MC(T) vs MC(2t) is smallest for this T*.

(2) **LAZINESS of Monte Carlo**
In positions where the winning probability in random games is far away from 50

(3) **Asymptotically Perfect Play of Pure Monte Carlo in BOARD FILLING GAMES**

(4) **Monte Carlo Anomalies**
There are situations where pure Monte Carlo converges to perfect play but MC(t) is clearly better than MC(T) for some pairs (t,T) of small parameters with t ¡ T.

Acknowledgement
Some of the results were achieved in collaboration with Matthias Beckmann (on 1) and Wesley Turner (on 4).

QUANTUM ERROR CORRECTION: AN INTRODUCTION

Harout Aydinian

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

We will give a brief introduction to the basics of quantum error correcting codes. Quantum error correction is needed to protect quantum information from errors due to decoherence and other quantum noise. Error correction is especially important in quantum computers, because efficient quantum algorithms make use of large scale quantum interference. The first quantum error correcting codes discovered by Shor, Steane, and Caldebank show that quantum error correction is possible, based on principles similar to classical error correction. Stabilizer codes are an important class of quantum codes which are the quantum analogues of classical additive codes.

EXTRACTING SIGNIFICANT PARAMETERS FROM NOISY OBSERVATIONS AND THEIR USE FOR AUTHENTICATION

Vladimir Balakirsky

American University of Armenia
Engineering Research Center
Marshal Baghramyan Ave., 40
AM - 0019 Yerevan

We deal with the setup when data, received at the enrollment stage, have to be mapped to a relatively short record that is stored in the database. At the verification stage, an investigation of other received data and the content of the database results in the acceptance (received data represent a noisy version of previous observations) or the rejection decision. The privacy protection requirements lead to the design of secret sharing schemes where a part of the secret, created at the enrollment stage, is published and another part is hidden by a one-way hash function. The hidden part has to be decoded after noisy observations arrive at the verification stage. An efficiency of the scheme essentially depends on parameters, extracted from the data, that are used to form the secret. They are called significant parameters. We present extracting algorithms and demonstrate the procedures for fingerprint-type images, available in digital format.

FUZZY SELF-LEARNING SEARCH

Bernhard Balkenhol
infinity3 GmbH
Boulevard 11
D - 33613 Bielefeld

A search algorithm will be presented which is used to find products in a huge database on the basis of incomplete or inaccurate data. A customer searches for a product in an online-store. To find his product he enters keywords which may be incomplete or inaccurate. The goal of the algorithm is to give the customer an ordered list of possible products such that the product he was searching for appears within the first ten suggestions.

COMPLETENESS AND MULTIPLICATION OF FIX-FREE CODES REGARDING AHLSWEDE'S 3/4-CONJECTURE

Michael Bodewig

RWTH Aachen University
Lehrstuhl für Mathematik
D - 52056 Aachen

Given a nonnegative sequence α of integers with Kraftsum at most 3/4, Ahlswede *et al.* proposed in [1] the existence of a fix-free code with exactly α_n words for any length n.
According to Kraft's inequality, complete codes have the highest possible Kraftsum 1 among the class of thin fix-free codes. Their specific structure and property of delivering fix-free codes with Kraftsum at most 3/4 by leaving out words make them an interesting subject of study.
We describe the construction of a three-parametric class of complete fix-free codes. Using both so called n-closed systems and multiplication, these complete fix-free codes are used to enlarge the class of known fix-free codes.
In addition, we present a sufficient criterium for the conjecture in terms of elementary sequence-shiftings preserving the fix-freedom of the associated code.

This is joint work with Eberhard Triesch.

[1] Ahlswede, R., Balkenhol, B., Khachatrian, L.: Some properties of fix-free codes. Proc. Int. Seminar Coding Theory and Combinator., Thahkadzor, Armenia (1996) 20–33

LEARNING A HIDDEN GRAPH

Huilan Chang

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

Classical group testing is a search paradigm where the goal is the identification of individual positive elements in a large collection of elements by asking queries of the form “Does a set of elements contain a positive one?”. A graph reconstruction problem that generalizes the classical group testing problem is to reconstruct a hidden graph from a given family of graphs by asking queries of the form “Whether a set of vertices induces an edge”. Reconstruction problems on families of Hamiltonian cycles, matchings, stars and cliques on n vertices have been studied where algorithms of using at most $2n\lg n$, $(1 + o(1))(n\lg n)$, $2n$ and $2n$ queries were proposed, respectively. In this talk we improve them to $(1+o(1))(n\lg n)$, $(1+o(1))(n\lg n2)$, $n+2\lg n$ and $n+\lg n$, respectively. Threshold group testing is another generalization of group testing which is to identify the individual positive elements in a collection of elements under a more general setting, in which there are two fixed thresholds l and u, with $l < u$, and the response to a query is positive if the tested subset of elements contains at least u positive elements, negative if it contains at most l positive elements, and it is arbitrarily given otherwise. For the threshold group testing problem with $l = u1$, we show that p positive elements among n given elements can be determined by using $O(p\lg n)$ queries, with a matching lower bound.

[Joint work with Hong-Bin Chen, Hung-Lin Fu, and Chie-Huai Shi.]

RESTRICTED ISOMETRY OF FOURIER MATRICES AND LIST DECODABILITY OF RANDOM LINEAR CODES

Mahdi Cheraghchi

Carnagie Mellon University
Computer Science Department
Gates-Hillman Complex 7223
5000 Forbes Avenue
USA - Pittsburgh, PA 15213

We prove that a random linear code over $\mathbb{F}_q$, with probability arbitrarily close to 1, is list decodable at radius $1 - 1/q - \varepsilon$ with list size $L = O(1/\varepsilon^2)$ and rate $R = \Omega_q(\varepsilon^2/(\log^3(1/\varepsilon)))$. Up to the polylogarithmic factor in $1/\varepsilon$ and constant factors depending on q, this matches the lower bound $L = \Omega_q(1/\varepsilon^2)$ for the list size and upper bound $R = O_q(\varepsilon^2)$ for the rate. Previously only existence (and not abundance) of such codes was known for the special case $q = 2$ (Guruswami, Håstad, Sudan and Zuckerman, 2002).
In order to obtain our result, we employ a relaxed version of the well known Johnson bound on list decoding that translates the *average* Hamming distance between codewords to list decoding guarantees. We furthermore prove that the desired average-distance guarantees hold for a code provided that a natural complex matrix encoding the codewords satisfies the Restricted Isometry Property with respect to the Euclidean norm (RIP-2). For the case of random binary linear codes, this matrix coincides with a random submatrix of the Hadamard-Walsh transform matrix that is well studied in the compressed sensing literature.
Finally, we improve the analysis of Rudelson and Vershynin (2008) on the number of random frequency samples required for exact reconstruction of k-sparse signals of length N. Specifically, we improve the number of samples from $O(k \log(N) \log^2(k)(\log k + \log\log N))$ to $O(k \log(N) \log^3(k))$. The proof involves bounding the expected supremum of a related Gaussian process by using an improved analysis of the metric defined by the process. This improvement is crucial for our application in list decoding.

[Joint work with Venkatesan Guruswami and Ameya Velingker.]

K-DIMENSIONAL M-PART SPERNER FAMILIES AND MIXED ORTHOGONAL ARRAYS

Eva Czabarka

University of South Carolina
Department of Mathematics
USA - Columbia, SC 29208
czabarka@math.sc.edu

Aydinian *et al.* [J. Combinatorial Theory A **118**(2)(2011), 702–725] substituted the usual BLYM inequality for L-Sperner families with a set of M inequalities for $(m_1, m_2, \ldots, m_M; L_1, L_2, \ldots, L_M)$ type M-part Sperner families and showed that if all inequalities hold with equality, then the family is homogeneous. Aydinian *et al.* [Australasian J. Comb. **48**(2010), 133–141] observed that all inequalities hold with equality if and only if the transversal of the Sperner family corresponds to a simple mixed orthogonal array with constraint M, strength $M-1$, using $m_i + 1$ symbols in the i^{th} column. In this paper we define k-dimensional M-part Sperner multi-families with parameters $L_P : P \in \binom{[M]}{k}$ and prove $\binom{M}{k}$ BLYM inequalities for them. We show that if $k < M$ and all inequalities hold with equality, then these multi-families must be homogeneous with profile matrices that are strength $M-k$ mixed orthogonal arrays. For $k = M$, homogeneity is not always true, but some necessary conditions are given for certain simple families. Following the methods of Aydinian *et al.* [Australasian J. Comb. **48**(2010), 133–141], we give new constructions to simple mixed orthogonal arrays with constraint M, strength $M-k$, using $m_i + 1$ symbols in the i^{th} column. We extend the convex hull method to k-dimensional M-part Sperner multi-families, and allow additional conditions providing new results even for simple 1-part Sperner families.

[Joint work with Harout Aydinian and László A. Székely.]

ON OPTIMAL STRICT MULTISTAGE GROUP TESTING

Peter Damaschke
Chalmers University
Department of Computer Science
and Engineering

This ongoing work is an effort to construct provably optimal strategies that find up to d defectives among n elements by group tests in s stages, for specific parameters n, d, s. We focus on strict group testing, i.e., the strategies shall identify up to d defectives or report that more than d defectives are present. The main challenge is to prove lower bounds on test numbers. One of our tools is a characterization of 1-stage pooling designs, given an arbitrary family of candidate sets for the defectives. The optimal test number is then the chromatic number of a certain conflict graph. This generalizes the well-known d-disjunctness property for strict 1-stage group testing when the candidate sets are all d-subsets. So far we are able to calculate exact test numbers for $n < 11$ (and any d and s) and almost exact test numbers for some larger n, comparable to the range considered by Huang and Hwang (2001) for the case $s = 1$.

[Joint work with Azam Sheikh Muhammad, supported by the Swedish Research Council.]

COMPUTING MAJORITY WITH TRIPLE QUERIES

Gianluca De Marco

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

Consider a bin containing n balls colored with two colors. In a k-query, k balls are selected by a questioner and the oracle's reply is related (depending on the computation model being considered) to the distribution of colors of the balls in this k-tuple; however, the oracle never reveals the colors of the individual balls. Following a number of queries the questioner is said to determine the majority color if it can output a ball of the majority color if it exists, and can prove that there is no majority if it does not exist. We investigate two computation models (depending on the type of replies being allowed). We give algorithms to compute the minimum number of 3-queries which are needed so that the questioner can determine the majority color and provide tight and almost tight upper and lower bounds on the number of queries needed in each case.

USING SUFFIX TREES FOR ALIGNMENT-FREE SEQUENCE COMPARISON AND PHYLOGENETIC RECONSTRUCTION

Andreas Dress
infinity3 GmbH
Boulevard 11
D - 33613 Bielefeld

In [QI, J., Wang, B., Hao, B., 2004. Whole proteome prokaryote phylogeny without sequence alignment: a k-string composition approach, Molecular Evolution 58, 1–11], Hao Bailin and coworkers presented a method for alignment-free sequence comparison that was based on a clever variant k-string comparison of protein sequences. In this work, they restricted their attention to comparing strings of fixed length k. In joint work with Alberto Apostolico and Olgert Denas, it was shown that making appropriate use of suffix trees and reinterpreting – and, thus, generalizing – their variant of k-string comparison from an information-theoretic point of view, one can not only speed up the required search procedures by several orders of magnitude, but at the same time take account of all (informative) strings of actually any lengths. In my lecture, I will shortly sketch our approach and present some of our results.

SUPERIMPOSED CODES AND NON-ADAPTIVE THRESHOLD GROUP TESTING

Arkadii D'yachkov

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

I will discuss superimposed codes and non-adaptive group testing designs arising from the potentialities of compressed genotyping models in molecular biology. The given talk was motivated by the 30th anniversary of D'yachkov-Rykov recurrent upper bound on the rate of superimposed codes published in 1982. I was also inspired by recent results obtained for non-adaptive threshold group testing which develop the theory of superimposed codes.

COMMUNICATION-LESS AGENT LOCATION DISCOVERY

Leszek A. Gasieniec
University of Liverpool
Department of Computer Science
Ashton Building, Ashton Street
UK - Liverpool L69 3BX

We study randomised distributed communication-less coordination mechanisms for *n* uniform anonymous agents located on a circle and a line segment. We assume the agents are located at arbitrary but distinct positions, unknown to other agents. The agents perform actions in synchronised rounds. At the start of each round an agent chooses the direction of its movement (clockwise or anticlockwise), and moves at unit speed during this round. Agents are not allowed to overpass, i.e., when an agent collides with another it instantly starts moving with the same speed in the opposite direction. Agents cannot leave marks on the ring, have zero vision and cannot exchange messages. However, on the conclusion of each round each agent has access to (some, not necessarily all) information regarding its trajectory during this round. This information can be processed and stored by the agent for further analysis.
The location discovery task to be performed by each agent is to determine the initial position of every other agent and eventually to stop at its initial position. Our first result [1] is a fully distributed randomised (Las Vegas type) algorithm, solving the location discovery problem w.h.p. in $O(nlog^2 n)$ rounds under assumption that the information concerning trajectories of the agents on the ring is very limited. Further we show that with the full access to agents' trajectories the time complexity of the discovery process can be dramatically improved [2]. We conclude our presentation with a study on agent location discovery on a line segment.

Literature:

[1]Tom Friedetzky, Leszek Gasieniec, Thomas Gorry, and Russell Martin, Observe and remain silent (Communication-less agent location discovery), To appear in the Proceedings of MFCS 2102.

[2] Jurek Czyzowicz, Leszek Gasieniec, Adrian Kosowski, Evangelos Kranakis, Oscar Morales Ponce, and Eduardo Pacheco, Position Discovery for a System of Bouncing Robots, To appear in the Proceedings of DISC 2102.

[Joint work with Tom Friedetzky, Thomas Gorry, and Russell Martin.]

MAJORITY AND PLURALITY PROBLEMS

Dániel Gerbner

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

Given a set of n balls each colored with a color, a ball is said to be majority, k-majority, plurality if its color class has size larger than half of the number of balls, has size at least k, has size larger than any other color class; respectively. We address the problem of finding the minimum number of queries (a comparison of a pair of balls if they have the same color or not) that is needed to decide whether a majority, k-majority or plurality ball exists and if so then show one such ball. We consider both adaptive and non-adaptive strategies and in certain cases, we also address weighted versions of the problems.

SEARCH IN HAMMING SPACE, MASTERMIND GAME ETC.

Grigory A. Kabatyansky

Dobrushin Mathematical Laboratory
Institute of Information Transmission Problems
Russian Academy of Sciences
Bolshoy Karetniy 19
RU - Moscow GSP-4 101 447

A new approach to investigating the Mastermind game and related problems, among them uniquely decodable codes for noiseless adder channel, based on ideas and methods of coding theory is proposed. This approach leads to improved bounds in various problems associated with the rigidity of Hamming spaces.

[Joint work with Vladimir Lebedev and Simon J. Thorpe.]

WHEN THE LIE DEPENDS ON THE TARGET

Gyula O. H. Katona

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

The following model is considered. There is exactly one unknown element in the n-element set. A question is a partition of S into three classes: (A, L, B). If $x \in A$ then the answer is "yes" (or 1), if $x \in B$ then the answer is "no" (or 0), finally if $x \in L$ then the answer can be either "yes" or "no". In other words, if the answer "yes" is obtained then we know that $x \in A \cup L$ while in the case of "no" answer the conclusion is $x \in B \cup L$. The mathematical problem is to minimize the minimum number of questions under certain assumptions on the sizes of A, B and L. This problem has been solved under the condition $|L| \geq k$ by the author and Krisztián Tichler in previous papers for both the adaptive and non-adaptive cases. In this paper we suggest to solve the problem under the conditions $|A| \leq a, |B| \leq b$. We exhibit some partial results for both the adaptive and non-adaptive cases. We also show that the problem is closely related to some known combinatorial problems. Let us mention that the case $b = n - a$ has been more or less solved in earlier papers.

BOUNDARY PATROLLING BY MOBILE AGENTS

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

We study a problem concerning the traversal of a rectifiable curve with $k \geq 1$ mobile robots so as to minimize the idle time (i.e., duration of time any point on the curve is left unvisited by a mobile agent). At any time during the traversal the speed of the robots cannot exceed a max value (set equal to 1 for all robots). The rectifiable curve can be either closed (e.g., cycle) or open (e.g., segment) and consists of alternating contiguous subsegments of vital intervals (that must be traversed) and neutral intervals (that do not have to be traversed).Given such a rectifiable curve, our goal is to give algorithms describing the motion boundaries and movement of the robots within the curve so that the idle time is optimized. Despite its apparent simplicity, designing such algorithms and proving their correctness turns out to be quite a challenging problem. We give optimal algorithms for solving this problem in the case where the rectifiable curve is either a (straight line) segment or a cycle.

GROUP TESTING WITH TWO DEFECTIVES

Vladimir Lebedev
Institute of Information Transmission Problems
Russian Academy of Sciences
Bolshoy Karetniy 19
RU - Moscow GSP-4 101 447

We consider classical group testing $(2, N)$ problem to finding $D = 2$ defective elements from N elements. We present adaptive algorithm $W(k)$ such that the $(2, w_t)$ problem can be solved in t tests. We show that for any $\varepsilon > 0$ there exist constant $k(\varepsilon)$ and algorithm $W(k)$ such that asymptotically $w_t = (1 - \varepsilon)2^{(t+1)/2}$ for $t \to \infty$.

SOME PROBLEMS AND ALGORITHMS IN NON-STANDARD STRING MATCHING

Zsuzsanna Lipták
University of Verona
Department of Computer Science
Strada Le Grazie, 15
I - 37134 Verona

In recent years, many new string problems have been introduced which are motivated by applications from molecular biology, but which are also of independent interest. In this talk, I will discuss two of these: weighted string matching and jumbled string matching.
The classical exact string matching problem is: Given a string s over a (finite) alphabet and a query string t, find all occurrences of t as substring of s. In weighted string matching, every character of the alphabet is assigned a (real or integer) weight (or mass), and the query is a (real or integer) number, the query mass: We want to find all occurrences of substrings whose total mass equals the query. In jumbled string matching, we have a standard alphabet but the query is a "jumbled string": the vector specifying the multiplicities of each character, also called Parikh vector.
For example, with $w(a) = 2$, $w(b) = 3$ and $w(c) = 5$, the string $s = abacab$ has three occurrences of mass 7, and three occurrences of the Parikh vector $(2, 1, 1)$. Both of these problems can be viewed as special cases of approximate string matching.
I will talk about different approaches and algorithms for several variants of these problems. I will also sketch the connections to a certain class of binary strings, the prefix normal strings. A binary string s is prefix normal if, for every $k \leq |s|$, no substring of length k has more a's than the prefix of length k. For example, *aababaaab* is not prefix normal because the substring *aaa* has more a's than the prefix *aab*. Using the prefix normal forms of a string, it is possible to answer quickly jumbled pattern matching queries.

ON CONNECTION WITH COMPRESSED SENSING AND SOME OTHER NEW DEVELOPMENTS IN THE SEARCH THEORY

Mikhail Malyutov

Northeastern University
Department of Mathematics
567 Lake Hall
USA - Boston, MA 02115

Common features and distinctions between the Search theory and now extremely popular Compressed Sensing are outlined. The analysis methods in used in these two theories are compared. Capacity in the search theory with stationary noise is studied.

CONSTRUCTION OF SEMI-QUANTITATIVE GROUP TESTING DESIGNS

Olgica Milenkovic

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

Semi-quantitative group testing is a pooling paradigm inspired by practical problems arising in compressive high-throughput sequencing. The pooling scheme is, in general, non-binary and it allows for test outputs that indicate the range of values of the positives in the test. We discuss two constructive methods: one for the sparse positives regimes and one for an arbitrary number of positives. In the first case, we propose a concatenated disjunct coding scheme with efficient belief propagation decoding. For the second scenario, we extend a design by Lindstroem in terms of modulating it by Reed-Solomon codes.

RANDOM CODING BOUNDS ON THE RATE FOR NON-ADAPTIVE THRESHOLD GROUP TESTING

Nikita Polyansky
Moscow State University
Faculty of Mechanics & Mathematics
Department of Probability Theory
RU - Moscow 119899

I will discuss analytical properties of the random coding bound on the rate for non-adaptive threshold group testing presented in the talk of Arkadii Dyachkov

EFFICIENT SIGNATURE SCHEME FOR NETWORK CODING

Ely Porat

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

Network coding helps maximize the network throughput. However, such schemes are also vulnerable to pollution attacks in which malicious forwarders inject polluted messages into the system. Traditional cryptographic solutions such as digital signatures are not suited for network coding in which nodes do not forward the original packets, but rather linear combinations of the data they receive. We describe a secure scheme that uses batch techniques and selective verification to efficiently verify the integrity of the received packets. For real peer-to-peer networks, our scheme is much more efficient than previously suggested schemes.

THE SMOOTHED COMPETITIVE RATIO OF ONLINE CACHING

Rüdiger Reischuk

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

Solving an optimization problem that is described by a sequence of requests online means that the requests are received one after the other and one has to serve each request immediately. Thus, one has to make decisions that may influence the future without knowing which requests will come later. Typical problems considered in this setting are bin-packing, scheduling, data caching or the k-server problem as a generic problem.

To measure the performance of an online algorithm it is compared to an optimal offline algorithm that constructs a solution after knowing the whole request sequence. The quotient of these two values is called the competitive ratio.

We concentrate on the caching problem – the question which data to keep in the fast cache of a processor instead of the slow main memory – for which optimal online and offline algorithms are known. The worst-case competitive ratio of this problem is very large and much worse than what is typically observed in practice. We analyze the average-case complexity of this problem in a smoothed discrete setting.

For continuous data smoothed analysis has been applied by Spielman and Teng to Linear Programming. Their results give a better explanation concerning the runtime of the Simplex Algorithm.

A smoothed analysis of competitive ratios is a new task. Several variants for such a setting are discussed and first results are presented that give a more accurate picture concerning the complexity of online caching.

SEARCH PROBLEMS RELATED TO DISPERSION, GRAPH ENTROPY AND GUESSING GAMES

Soren Riis

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

We introduce the (private) entropy of a directed graph (in a new network coding sense) as well as a number of related concepts. We show that the entropy of a directed graph is identical to its guessing number and can be bounded from below with the number of vertices minus the size of the graph's shortest index code. We show that the Network Coding solvability of each specific multiple unicast network is completely determined by the entropy (as well as by the shortest index code) of the directed graph that occur by identifying each source node with each corresponding target node. Shannon's information inequalities can be used to calculate upper bounds on a graph's entropy as well as calculating the size of the minimal index code. Recently, a number of new families of so-called non-shannon-type information inequalities have been discovered. It has been shown that there exist communication networks with a capacity strictly less than required for solvability, but where this fact cannot be derived using Shannon's classical information inequalities. Based on this result we show that there exist graphs with an entropy that cannot be calculated using only Shannon's classical information inequalities, and show that better estimate can be obtained by use of certain non-shannon-type information inequalities.

GROUP TESTING AND CODING THEORY

Atri Rudra

The State University of New York, Buffalo
Department of Computer
Science & Engineering
12 Capen Hall
USA - Buffalo, New York 14260-1660

Group testing was formalized by Dorfman in his 1943 paper and was originally used in WW-II to identify soldiers with syphilis. The main insight in this application is that blood samples from different soldiers can be combined to check if at least one of soldiers in the pool has the disease. Since then group testing has found numerous applications in many areas such as (computational) biology, combinatorics and (theoretical) computer science.

Theory of error-correcting codes, or coding theory, was born in the works of Shannon in 1948 and Hamming in 1950. Codes are ubiquitous in our daily life and have also found numerous applications in theoretical computer science in general and computational complexity in particular.

Kautz and Singleton connected these two areas in their 1964 paper by using ”code concatenation” to design good group testing schemes. All of the (asymptotically) best know explicit constructions of group testing schemes use the code concatenation paradigm. In this talk, we will focus on the ”decoding” problem for group testing: i.e. given the outcomes of the tests on the pools, identify the infected soldiers. Recent applications of group testing in data stream algorithm require sub-linear time decoding, which is not guaranteed by the traditional constructions.

The talk will first survey the Kautz-Singleton construction and then will will show how recent developments in list decoding of codes lead in a modular way to sub-linear time decodable group testing schemes.

ON SUPERIMPOSED CODES AND DESIGNS

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

We will discuss superimposed codes and non-adaptive group testing designs arising from the potentialities of compressed genotyping models in molecular biology. The given survey is also motivated by the 30th anniversary of our recurrent upper bound on the rate of superimposed codes published in 1982.

SOME CONSTRUCTIONS FOR THE DIAMOND PROBLEM

László Székely

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

There is much interest recently in excluded subposets. Given a fixed poset P, how many subsets of $[n]$ can found without a copy of P realized by the subset relation? The hardest and most intensely investigated problem of this kind is when P is a *diamond*, i.e. the power set of a 2 element set. In this paper, we show that even asymptotic results for the diamond problem imply *exact* results for some posets related to Cayley graphs of abelian groups. The connection is realized by the convergence of Markov chains on groups.

[Joint work with Éva Czabarka.]

MULTIPARTY COMMUNICATION COMPLEXITY OF VECTOR–VALUED AND SUM–TYPE FUNCTIONS

Ulrich Tamm

Marmara University
German Language Department
of Business Informatics
TR - 34722 Istanbul

Rudolf Ahlswede's work on communication complexity dealt with functions defined on direct sums: vector–valued functions and sum–type functions. He was interested in single–letter characterizations and provided several lower bound techniques to this aim. In this paper we shall review these lower bounds and extend them to the "number in hand" multiparty model of communication complexity.

SEARCH WITH PARTIAL INFORMATION

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

Searching a target (pursuit, rendez-vous) is sometimes a problem with no information (blind search), sometimes a problem with full information (indeed the easiest case, from a complexity point of view), sometimes with no information at all (indeed more complex, yet it is not so intuitive). The most difficult case is the partial information case. Various formalizations lead to different conclusions; the talk will give an overview of known and new results, depending on the detailed assumptions.

UPPER AND LOWER BOUNDS FOR COMPETITIVE GROUP TESTING

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

We consider algorithms for adaptive group testing problems when nothing is known in advance about the number of defectives. Du and Hwang suggested to measure the quality of such algorithms by its so-called competitive ratio. We develop an algorithm with competitive ratio smaller than 1.5 and prove a lower bound for the best possiblecompetitive ratio.

ON A PROBLEM OF RÉNYI AND KATONA

Gábor Wiener

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

We are dealing with the classical problem of determining the minimum size of a separating system consisting of sets of size at most k. The problem was raised by Rényi, the first and most important results are due to Katona; Wegener and Ahlswede also proved important bounds. We give a simple, short proof of a strengthening of Katona's main theorem determining the minimum size of a separating system of sets of size at most k.

LIST OF PARTICIPANTS

1. Matthew Aldridge
   University of Bristol
   School of Mathematics University Walk
   UK - Bristol, BS8 1TW
   Tel.: +44 7507 163818
   m.aldridge@bristol.ac.uk

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)521 106-4789
   ayd@math.uni-bielefeld.de

4. Vladimir Balakirsky
   American University of Armenia
   Engineering Research Center
   Marshal Baghramyan Ave., 40
   AM - 0019 Yerevan
   Tel.: +7 812 594-4962
   v_b_balakirsky@rambler.ru

5. Bernhard Balkenhol
   infinity3 GmbH
   Boulevard 11
   D - 33613 Bielefeld
   bernhard.balkenhol@infinity-3.de

6. Michael Bodewig
   RWTH Aachen University
   Lehrstuhl fr Mathematik
   D - 52056 Aachen
   Tel.: +49 (0)241 80-94604
   Fax: +49 (0)241 80-92136
   bodewig@math2.rwth-aachen.de

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

8. Ning Cai
   University of Xidian
   The State Key Laboratory
   of Integrated Services Network
   China - Xian
   Tel.: +86 (0)29 8820-4275
   Fax: +86 (0)29 8820-4215
   caining@mail.xidian.edu.cn

9. 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

10. Mahdi Cheraghchi
    Carnagie Mellon University
    Computer Science Department
    Gates-Hillman Complex 7223
    5000 Forbes Avenue
    USA - Pittsburgh, PA 15213
    Tel.: +1 512 586-5075
    Fax: +1 412 268-5574
    cheraghchi@gmail.com

11. 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

12. Eva Czabarka
    University of South Carolina
    Department of Mathematics
    USA - Columbia, SC 29208
    Tel.: +1 803 422-8944
    Fax: +1 803 777-3783
    czabarka@math.sc.edu

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

14. 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

15. 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

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

17. Andreas Dress
infinity3 GmbH
Boulevard 11
D - 33613 Bielefeld
Tel.: +49 (0)521 69-532
Fax: +49 (0)521 521-4403
dress@infinity-3.de

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

19. Leszek A. Gsieniec
University of Liverpool
Department of Computer Science
Ashton Building, Ashton Street
UK - Liverpool L69 3BX
Tel.: +44 (0)151 795-4290
Fax: +44 (0)151 795-4235
l.a.gasieniec@liverpool.ac.uk

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

21. Gisbert Janßen
Technische Universität München
Lehrstuhl fr Theoretische Informationstechnik
Building N4, Room N4412
Arcisstr. 21
D - 80333 München
Tel.: +49 (0)89 289-23247
gisbert.janssen@tum.de

22. Grigory A. Kabatyansky
Dobrushin Mathematical Laboratory
Institute of Information Transmission Problems
Russian Academy of Sciences
Bolshoy Karetniy 19
RU - Moscow GSP-4 101 447
kaba@iitp.ru

23. 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

24. 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

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

26. Zsuzsanna Lipták
University of Verona
Department of Computer Science
Strada Le Grazie, 15
I - 37134 Verona
Tel.: +39 329 737-2046
zsuzsanna.liptak@univr.it

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

28. Mikhail Malyutov
Northeastern University
Department of Mathematics
567 Lake Hall
USA - Boston, MA 02115
m.malioutov@neu.edu

29. 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

30. Tim Nattkemper
Universität Bielefeld
Center of Excellence
- Cognitive Interaction Technology -
CITEC
Postfach 10 01 31
D - 33501 Bielefeld
Tel.: +49 521 106-6059
tim.nattkemper@uni-bielefeld.de

31. Nikita Polyansky
Moscow State University
Faculty of Mechanics & Mathematics
Department of Probability Theory
RU - Moscow 119899
nikitapolyansky@gmail.com

32. 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

33. 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

34. Soren Riis
Queen Mary, University of London
Department of Computer Science
UK - London E1 4NS
smriis@dcs.qmul.ac.uk
Tel.: +44 020 759 331 3012
soren.riis@eecs.qmul.ac.uk

35. Atri Rudra
The State University of New York, Buffalo
Department of Computer
Science & Engineering
12 Capen Hall
USA - Buffalo, New York 14260-1660
Tel.: +1 716 225-1655
Fax: +1 716 645-3654
atri@buffalo.edu

36. 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

37. Jens Stoye
Universität Bielefeld
Technische Fakultät
Genominformatik
Postfach 10 01 31
D - 33501 Bielefeld
Tel.: +49 (0)521 106-3852
Fax: +49 (0)521 106-6495
jens.stoye@uni-bielefeld.de

38. 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

39. Ulrich Tamm
Marmara University
German Language Department
of Business Informatics
TR - 34722 Istanbul
Tel.: +49 (0)173 290 8622
ulrich.tamm@yahoo.com

40. 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

41. 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

42. Gábor Wiener
Hungarian Academy of Sciences
Alfred Renyi Institute of Mathematics
P.O. Box 127
H - 1364 Budapest
Tel.: +36 1 4633-162
Fax: +36 1 4633-157
wiener@cs.bme.hu