Mathematisches Forschungsinstitut Oberwolfach

Report No. 53/2003

Kodierungstheorie

December 7th – December 13th, 2003

The conference "Coding Theory" intended to be a platform where the rather inhomogeneous coding community could exchange ideas. Both the engineers could present their mathematical problems and the mathematicians could report their progress. The result was a lively meeting with an open exchange of ideas and lots of discussion. Madhu Sudan presented his wonderful idea of using coding theory in computer science and mathematics for showing that problems are "hard". Another interesting development reported at the conference was the construction of asymptotically good towers of curves over finite fields over cubic extensions. Besides that new and interesting developments were reported about space-time codes and LDPC codes. The theme 'sequences' also got a fair share of attention. A number of talks were devoted to Codes over Galois rings. There were also a few informal talks outside the official program dealing with Weierstrass points on curves over finite fields and the Kissing Number in dimension 4.

In the view of the organizers it was a highly successful meeting in a good atmosphere with lots of discussions. Everybody was pleased with the excellent working conditions offered by Oberwolfach. Thanks are due to the staff for their very efficient and pleasant help.

Abstracts

Codes over Galois Ring

Gilberto Bini

We shall briefly recall some basic facts on trace codes over finite fields. In particular, we will focus on generalizations of dual Melas codes. After such an overview, we will introduce the Galois ring set-up in which we try to extend some of the techniques over fields. For these purposes, we need some results on exponential sums over Galois rings. Finally, we give a lower bound on the minimum Hamming distance of the generalized (Gray) image of our trace codes over rings.

Weight distribution of cyclic codes

Hans Dobbertin

Self-Dual Divisible Codes

Iwan Duursma

The best known asymptotic upper bound for binary self-dual codes is due to Krasikov-Litsyn (2000), with a different proof by Rains (2003). As $n \to \infty$

$$\frac{d}{e} \leq \frac{1}{2}\left(1 - \frac{1}{\sqrt[4]{5}}\right) < \frac{1}{6}.$$

We give a short elementary proof of this result. It uses a new description of the relation on the low weight coefficients of a self-dual divisible code.

An Explicit Tower over Cubic Finite Fields and Zink's Lower Bound

Arnaldo Garcia

(joint work with Juscelino Bezerra and Henning Stichtenoth)

For an infinite sequence $\mathcal{F}$ of curves C_n over $\mathbb{F}_l$, $n \in \mathbb{N}$, with increasing genera we are interested in the asymptotic behaviour of the ratios (number of rational points of C_n)/(genus of C_n); the limit of the ratios above is called the limit of the sequence and it is denoted by $\lambda(\mathcal{F})$. It follows from Weil's theorem that $\lambda(\mathcal{F}) \leq 2\sqrt{l}$, for any $\mathcal{F}$ over $\mathbb{F}_l$. Ihara was the first one to notice that the bound above can be improved significantly, and his ideas lead to the following bound due to Drinfeld-Vladut: $\lambda(\mathcal{F}) \leq \sqrt{l} - 1$, for any $\mathcal{F}$ over $\mathbb{F}_l$

When $l = q^2$ the bound of Drinfeld-Vladut is sharp, i.e. there are sequences $\mathcal{F}$ over $\mathbb{F}_{q^2}$ with $\lambda(\mathcal{F}) = q - 1$. Using degenerations of Shimura modular surfaces, Zink has shown the existence of sequences $\mathcal{F}$ over $\mathbb{F}_{p^3}$, p a prime number, such that $\lambda(\mathcal{F}) \geq \frac{2(p^2-1)}{p+2}$.

The goal of the talk is to present a new sequence $\mathcal{F}$ over $\mathbb{F}_{q^3}$, q any prime power, such that its limit satisfies $\lambda(\mathcal{F}) \geq \frac{2(q^2-1)}{q+2}$. This new sequence is recursively defined by the following equation over $\mathbb{F}_{q^3}$:

$$\frac{1-y}{y^q} = \frac{x^q + x - 1}{x}$$

This new sequence gives rise to long linear codes, through Goppa's construction, with limit parameters above the so-called Gilbert-Varshamov bound.

On the Missing Evaluation Codes from Order Domain Theory

Olav Geil
(joint work with Henning E. Andersen)

We introduce new classes of evaluation codes related to order domains of any transcendence degree. In particular we introduce improved constructions of a class of one-point geometric Goppa codes. The new constructions take into account not only the value semigroup of the order function but take into account also the size of the field as well as the actual polynomials that defines the order domain. The methods also reveals the fact that many one-point geometric Goppa codes have in fact much better parameters than predicted by the usual Goppa bound.

Additive Autocorrelation of Binary Sequences and Functions

Guang Gong

We investigate the additive autocorrelation of binary periodic sequences and functions which are their trace representations. A function from $GF(2^n)$ to $GF(2)$ or a boolean function in n valuables has two-level autocorrelation if and only if it is bent which only exists for n even. We discuss the odd case of n. By introducing the indicator function of the Hadamard transform of a binary sequence of period $N|2^n-1$, we are able to determine the additive autocorrelation of some known binary sequences with 2-level (multiplicative) autocorrelation. We also present the resiliency and propagation properties of booleans of the binary sequences with 2-level (multiplicative) autocorrelation.

On the Weights of 2-D Cyclic Codes

Cem Güneri

Extending the approach used for cyclic codes we give a trace representation for 2-D cyclic codes via Delsarte's Theorem. This relates the weight of a codeword to the number of rational points on several Artin-Schreier curves. Using this relation, we state a lower bound on the minimum distance of a large class of 2-D cyclic codes.

List Decoding: Recent Progress and Challenges Ahead

Venkatesan Guruswami

List decoding is the problem of finding all codewords of a code that are within a certain distance of the received word. Though introduced independently by Elias and Wozencraft in the late 50's, only recently is the development of list decoding algorithms getting the attention that it deserves. List decoding permits recovery beyond that possible using classical unique decoding algorithms, and enables approaching capacity even when the noise model is "adversarial" as opposed to obeying an assumed probabilistic model. This talk is a tutorial/survey into the subject of list decoding — it will briefly discuss the combinatorial results that indicate the potential of list decoding and set the stage for new algorithmic questions, followed by a peek into the substantial recent progress on the algorithmic front. The talk will also highlight several intriguing challenges (combinatorial, algorithmic, and complexity-theoretic) concerning list decoding that lie ahead of us.

On the Algebraic Design of Space-Time codes

A. Roger Hammons Jr.

General binary design criteria are presented for BPSK and QPSK modulated space-time codes. The rank of (binary projections of) the unmodulated codewords, as binary matrices over the binary field, is a sufficient criterion: full binary rank guarantees full spatial diversity. This leads to fundamental stacking constructions that include optimal d_{free} convolutional codes, Galois field theoretic block codes, and dyadic constructions that guarantee full spatial diversity for an arbitrary number of transmit antenna.

Crosscorrelation of m-sequences: New 4-valued decimations

Tor Helleseth

(joint work with Hans Dobbertin, Patrick Felke and Petri Rosendahl)

Let $\{s(t)\}$ and $\{s(dt)\}$ be two binary m-sequences of period 2^n-1 that differ by a decimation d where $gcd(d, 2^n-1) = 1$. The crosscorrelation function between two m-sequences is defined by

$$C_d(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s(t+\tau)-s(dt)}.$$

It is well known that the crosscorrelation function takes on at least three distinct values when the two sequences are cyclically distinct i.e., when $d \neq 2^i \ (mod\ 2^n-1)$ for all integers i . Several decimations d giving exactly three values are known. The main result here is to find new values of d for which exactly four values occur.

Let $n = 2k$ and let d be of the form $d = (2^k-1)s+1$ where $s = 2^r \cdot (2^r \pm 1)^{-1} \ (mod\ 2^k+1)$. Let $v_2(x)$ be the largest positive integer u such that 2^u divides x. In the case when $v_2(r) < v_2(k)$ the decimations above give four valued crosscorrelation functions. The complete distribution of the values and the number of occurrences of each value is also calculated. We conjecture that these decimations include all 4-valued cases with $n = 2k$ and d of the form $d = (2^k - 1)s + 1$.

Concatenated Codes and Their Decoding

Jorn Justesen

(joint work with Tom Hoholdt, Christian Thommesen)

Concatenated codes remain the most important tool for constructing long binary codes. We consider constructions from I outer Reed-Solomon (or algebraic geometry) codes over F_{2^m} and binary inner (n, mI) codes. The inner codes are decoded ML by trellis decoding or a similar technique. The error-correcting capability can be improved by using methods that extend the decoding of the outer codes. The Bleichenbacher-Kaiyias-Yung algorithm is considered in particular, and a simplified version based on syndrome equations is presented.

Graph covers and iteratively decodable codes

Ralf Koetter
(joint work with P.O. Vontobel)

Codes on graphs commonly refer to codes over a suitably chosen alphabet that are described in graphical models. Given a bipartite graph one vertex class is identified with variables and the other class represents local constraints on subsets of the variables. The most important classes of codes on graphs are the so called Low-density Parity-Check codes by Gallagher and the enormously important turbo codes. While the performance of codes on graphs is unsurpassed — due to a very efficient, locally operating decoding algorithm — the understanding of these codes is still far from complete. We address the problem of characterizing the performance of finite length LDPC codes utilizing the notion of pseudodistance which is a function of the code, the graph, and the decoding algorithm. It turns out that the erratic behavior of the decoding algorithm is caused by code configurations in finite graph covers which have a nice an elegant description over the real numbers.

Error-correction capability of binary linear codes beyond half the minimum distance

Vladimir I. Levenshtein
(joint work with Tor Helleseth and Torleiv Klove)

The monotone structure of correctable and uncorrectable errors given by the complete decoding for a binary code is investigated. New bounds on the error-correction capability of linear codes beyond half the minimum distance are presented, both for the best codes and for arbitrary codes under some restrictions on their parameters. It is proved that some known families of linear codes of low rate are as good as the best codes in an asymptotic sense. A construction of a linear code is given which has the same length and dimension as the simplex code but smaller probability of error decoding on the binary symmetric channel for all p, $0 < p < 1/2$.

Mathematical problems related to PAPR reduction

Simon N. Litsyn

We consider the problem of decreasing peak-to-average power ratio reduction in multicarrier communication systems. In the mathematical setting it reduces to analysis of trigonometric polynomials with coefficients restricted to some finite subset of complex plain. We start with an analysis of ratio between continuous and discrete maxima achieved by the values of these polynomials. We further relate constructions of codes to estimates of some mixed exponential sums, and provide an improvement on earlier known results.

On Structured-Summary Propagation and LFSR Synchronization

Hans-Andrea Loeliger
(joint work with Justin Dauwels, Matthias Frey, Patrick Merkli, Maja Ostojic, Benjamin Vigoda)

The talk has two themes. The first theme is the synchronization (state estimation) of linear-feedback shift register (LFSR) sequences that are observed via a noisy channel. An extremely simple (suboptimal) estimation algorithm is obtained by forward-only message

passing through an obvious factor graph. This algorithm may be viewed as passing the received noisy sequence through a "soft" version of the LFSR. It is also shown that this idea can be extended to continous-time dynamical systems.

The second theme is the general idea to improve message passing algorithms on graphs with annoying short cycles by introducing messages with some nontrivial Markov structure. The idea is worked out for the synchronization of noisy LFSR sequences.

Rate-Diversity Tradeoff of Space-Time Codes and Optimal Constructions

Hsiao-Feng Lu
(joint work with P. Vijay Kumar)

Let M be the number of transmit antennas and let T be length of a channel fading block, an $(M \times T)$ space-time code $\mathcal{S}$ is a collection of $(M \times T)$ matrices with components drawn from a finite fixed set $\mathcal{A}$, the signal alphabet. The transmit diversity gain d achieved by the code $\mathcal{S}$ is defined as the minimal rank of the difference between any two code matrices. Assuming $M \leq T$, there is a tradeoff between the code rate R and the transmit diversity gain d achieved by $\mathcal{S}$.

We present a unified space-time code construction that gives rise to classes of block and convolutional codes achieving this optimal tradeoff over a wide variety of signal alphabet $\mathcal{A}$ and over any number of transmit antenna. We also show that when coding is applied simultaneously to several consecutive fading blocks, one is governed by a different rate-diversity tradeoff, where larger diversity gains and higher rates can be jointly obtained. Systematic constructions of codes that achieve this new tradeoff are also provided.

Codes on the Fiber Products of Kummer Covers

Hiren Maharaj

We give a simple technique to obtain explicit bases for Riemann-Roch spaces of invariant divisors G of curves which are fiber products of Kummer covers of the projective line. As a bonus one obtains exact dimensions and good codes on such curves. Similar techniques can be used to obtain information on the weight distribution of these codes. Moreover, if none of the places in the support of G ramify, it can be shown that Goppa's lower bound on the minimum distance is exact.

Cyclic Codes and Genus 2 Curves

Gary McGuire
(joint work with J. F. Voloch)

We discuss a class of binary cyclic codes and their dual codes. We relate the weights appearing in the dual codes to the numbers of rational points on a family of genus 2 curves. We determine all the possibilities for the number of points on a genus 2 curve with 2-rank 1 over a finite field of order 2^m. This determines the weights in the corresponding cyclic code.

Construction of Sequences and Cyclic Difference Sets Using d-Homogeneous Functions with Difference-balanced Property

Jong-Seon No

Let $n,\ m,\ k$, and l be positive integers such that $n = (2m+1)k, l|k$ and p an odd prime. Let $H(x)$ be a d-homogeneous function from the finite field F_{p^n} with p^n elements to its subfield F_{p^l} with difference-balanced property. Let α be a primitive element in F_{p^n}. Let $\mathrm{tr}_{p^l}^{p^n}(\cdot)$ be the trace function from F_{p^n} to F_{p^l}. Using Helleseth-Gong sequences [*IEEE Trans. Inform. Theory*, pp. 2868-2872, Nov. 2002], a d-homogeneous function from F_{p^n} to F_{p^l} with difference-balanced property can be constructed as $H(x) = \sum_{i=0}^{m} u_i \mathrm{tr}_{p^l}^{p^n}(x^{\frac{p^{2ik}+1}{2}})$, for $u_i \in F_p$, which is the only d-homogeneous function with difference-balanced property except for p-ary m-sequences and GMW sequences. Then we can construct the cyclic difference set with Singer parameters $(\frac{p^n-1}{p^l-1}, \frac{p^{n-l}-1}{p^l-1}, \frac{p^{n-2l}-1}{p^l-1})$ defined by $D_1 = \{\, \alpha^t \mid H(\alpha^t) = 0, 0 \le t < \frac{p^n-1}{p^l-1}\}$ and the cyclic relative difference set with Singer parameters $(\frac{p^n-1}{p^l-1}, p^l - 1, p^{n-l}, p^{n-2l})$ defined by $D_2 = \{\, x \mid H(x) = 1, x \in F_{p^n}^*\}$. Using Helleseth-Gong sequences, p-ary extended sequences with ideal autocorrelation property, p-ary d-form sequences with ideal autocorrelation property, and p-ary unified (extended and d-form) sequences with ideal autocorrelation property can be constructed.

Constructive Asymptotic Codes with an Improvement on the Tsfasman-Vlăduţ-Zink and Xing Bounds

Ferruh Özbudak
(joint work with Harald Niederreiter)

Let $\mathbb{F}_q$ be the finite field of order q and α_q be the well-known function ([2], Section 1.3.1) in the theory of asymptotic algebraic codes. A central problem in algebraic coding theory is to find lower bounds on $\alpha_q(\delta)$ for $0 < \delta < (q-1)/q$. A classical lower bound is the asymptotic Gilbert-Varshamov bound which says that

$$\alpha_q(\delta) \ge 1 - \delta \log_q(q-1) + \delta \log_q \delta + (1-\delta)\log_q(1-\delta) \quad \text{for } 0 < \delta < \frac{q-1}{q}.$$

Let $N_q(g)$ denote the maximum number of rational places that a global function field of genus g with full constant field $\mathbb{F}_q$ can have. We recall the quantity

$$A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}$$

from the theory of global function fields. In an important breakthrough Tsfasman, Vlăduţ, and Zink [3] showed that one can beat the asymptotic Gilbert-Varshamov bound by using Goppa's algebraic-geometry codes [1]. The Tsfasman-Vlăduţ-Zink bound in [3] says that

$$\alpha_q(\delta) \ge 1 - \delta - \frac{1}{A(q)} \qquad \text{for } 0 \le \delta \le 1. \tag{1}$$

Recently Xing [4] improved Tsfasman-Vlăduţ-Zink bound (1) and he showed that for any $\delta \in (0,1)$ we have

$$\alpha_q(\delta) \ge 1 - \delta - \frac{1}{A(q)} + \sum_{i=2}^{\infty} \log_q\left(1 + \frac{q-1}{q^{2i}}\right). \tag{2}$$

The proof of (2) given in [4] proceeds in a nonconstructive manner.

In this talk we present an improvement on the Xing bound (2) and thus also on the Tsfasman-Vlăduţ-Zink bound (1). Moreover, the proof of our bound is obtained constructively in a certain range for δ. Namely we prove constructively that

$$\alpha_q(\delta) \geq 1 - \delta - \frac{1}{A(q)} + \log_q\left(1 + \frac{1}{q^3}\right) \tag{3}$$

for any δ in the range

$$\delta \in \left(0, 1 - \frac{2}{A(q)} - \frac{4q-2}{(q-1)(q^3+1)}\right].$$

References

[1] Goppa, V.D.: Codes on algebraic curves (in Russian). Dokl. Akad. Nauk SSSR **259**, 1289–1290 (1981)

[2] Tsfasman, M.A., Vlăduţ, S.G.: Algebraic-Geometric Codes. Kluwer, Dordrecht (1991)

[3] Tsfasman, M.A., Vlăduţ, S.G., Zink, T.: Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. Math. Nachr. **109**, 21–28 (1982)

[4] Xing, C.P.: Nonlinear codes from algebraic curves improving the Tsfasman-Vlăduţ-Zink bound. IEEE Trans. Inform. Theory **49**, 1653–1657 (2003)

Information-Lossless Space-Time Block Codes From Division Algebras

B. Sundar Rajan & B. Al Sethuraman

(joint work with V. Shashidhar)

We describe a very general technique for constructing space-time block codes over any signal set $S \subseteq \mathbb{C}$ and for any number of transmit antennas, using representations of finite-dimensional cyclic division algebras $(K/F, \sigma, \delta)$ in $M_n(K)$, where $n = [K : F]$ and $< \sigma >= Gal(K/F)$. Here, F is a suitable subfield of $\mathbb{C}$ containing $\mathbb{Q}(S)$; we show that by choosing F, K, and δ appropriately, we can obtain codes that are information-lossless. We exhibit performance characteristics of our codes that show that our codes outperform previously known codes in terms of both information-losslessness and error probability.

Algebraic Constructions of Low Density Parity Check Codes

Joachim Rosenthal

(joint work with Pascal Vontobel, Christine Kelley and Deepak Sridhara)

Low density parity check codes perform outstanding and can be decoded with a complexity which grows linearly in the block length. The performance was shown for randomly constructed codes of large block length. Algebraically constructed codes should possess several properties. In this talk it is shown how to construct LDPC codes with large girth and good expansion rate using Ramanujan graphs. The idea of these constructions comes from work of Margulis who showed how to design codes without short cycles starting from a Cayley graph. Mimicking this construction we describe a new class of powerful regular and irregular LDPC codes.

LDPC Codes

Mohammad Amin Shokrollahi

The theory of LDPC codes has attracted a lot of attention lately. In this talk I will describe the basic concepts of these codes, their analysis, and some of their applications.

Cyclic codes over rings and pseudo-random sequences

Patrick Solé

Recently we have explored cyclic codes over cyclic rings $\mathbf{Z}_{p^m}$, with either $p = 2$ and $m > 2$ [2, 3], or $m = 2$ and $p > 2$ [1].
The tools used to bound the correlation include the local Weil bound, a Galois property of the generalized Gray map, analogues of the Nechaev permutation, but also the Most significant Bit map, and the Discrete Fourier Transform.
Three notions of non-linearity in the sense

- block codes
- linear shift registers
- boolean functions

respectively, will be explored in turn. Applications to PAPR reduction will be sketched out [4, 5].

References

[1] (with S. Ling) "Non-linear $p-$ary sequences", J. of the AAECC, J. of the AAECC 14 (2003) 117–125.
[2] (with J. Lahtonen, S. Ling, D. Zinoviev) "Z8-Kerdock codes and pseudo random binary sequences", J. Of Complexity, to appear
[3] (avec D. Zinoviev) "The Most Significant Bit of Maximum Length Sequences Over $\mathbf{Z}_{2^l}$: Autocorrelation and Imbalance", IEEE Transactions on Information Theory, submitted.
[4] (avec D. Zinoviev) "Low Correlation, High Nonlinearity Sequences for multi-code CDMA", IEEE Transactions on Information Theory submitted.
[5] (avec D. Zinoviev) "Weighted degree trace codes for PAPR reduction", IEEE Transactions on Communications submitted.

List Decoding and Computational Complexity

Madhu Sudan

We describe the notion of list-decoding and show how it is intimately connected to questions in computational complexity, by giving three examples. The first shows how it relates complexity of general functions to that of Boolean functions, while preserving quantitative hardness. The second shows how it can be used to amplify the hardness of functions in certain complexity classes. The third shows how a dramatic improvement to the state of the art with respect to list-decoding could lead to an efficient solution to the problem of factoring integers.

Recent Advances in Algebraic Decoding of Reed-Solomon Codes

Alexander Vardy
(joint work with Ralf Koetter, Jun Ma, Farzad Parvaresh)

Reed-Solomon codes are the most widely used error-correcting codes in digital communications and data storage. Recently, several breakthroughs have been achieved in improving the error-correction capability of Reed-Solomon decoders. The story begins with the work of Sudan [18], who showed that list-decoding of Reed-Solomon can be viewed as a bivariate interpolation problem, thereby correcting more errors than previously thought possible. The second key achievement was the work of Guruswami-Sudan [5]. Guruswami-Sudan [5] correct even more errors by interpolating through each point not once, but m times, where m is an arbitrary integer. For $m \to \infty$, the list-decoding algorithm of [5] corrects up to $n - \sqrt{kn}$ errors, which is better than $(n-k)/2$ for all rates k/n. The third step was taken in the work of [8, 9], which showed how the interpolation multiplicities in the algorithm of [5] should be chosen to achieve *soft-decision decoding* of Reed-Solomon codes. These developments have the potential to drastically change the way Reed-Solomon codes are decoded, and have sparked a flurry of research in the area. This research can be roughly subdivided into two major thrusts.

Multiplicity assignments: The choice of interpolation multiplicities in the algorithm of [5] determines the decoder performance, and remains a key problem in the area. Koetter-Vardy [9] derive an efficient multiplicity assignment scheme that maximizes the so-called *expected score*, and show that this assignment is optimal for $n \to \infty$ if the goal is to minimize the probability of decoding failure. The work of [15] improves substantially upon [9], by recasting the problem into a geometric framework in Euclidean space or, alternatively, by approximating the distribution of the score by a Gaussian. Finally, the problem of assigning interpolation multiplicities so as to maximize the cost of a correctable error pattern with respect to an *arbitrary* additive cost structure is introduced and essentially solved in [10].

Fast interpolation and factorization: The main computational steps in list-decoding of [5, 18] as well as algebraic soft-decoding of [9] are bivariate interpolation and factorization. Various efficient algorithms for this purpose were proposed in [1, 2, 4, 6, 13, 14, 17]. While polynomial-time, these algorithms are still far too complex for practical implementation. In [11, 7], we present a series of transformations that convert the original interpolation problem into another *reduced interpolation problem*, whose computational cost N is orders of magnitude smaller. This reduces the decoding complexity by a factor of at least $n^2/(n-k)^2$, and makes soft-decision RS decoding quite feasible in practice. Moreover, Feng-Giraud [3] propose a divide-and-conquer method that reduces the asymptotic complexity of interpolation and factorization from $O(N^2)$ to $O(N \log^2 N)$. The divide-and-conquer approach of [3] is extended in [16] and improved upon in [12].

References

[1] A. Ahmed, R. Koetter, and N. Shanbhag, "VLSI architectures for soft-decision decoding of Reed-Solomon codes," *IEEE Trans. VLSI Systems*, submitted for publication, March 2003.

[2] D. Augot and L. Pecquet, "A Hensel lifting to replace factorization in list-decoding ofalgebraic-geometric and Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2605–2614, November 2000.

[3] G.-L. Feng and X. Giraud, "Fast algorithms in Sudan decoding procedure for Reed-Solomon codes," preprint, January 2002.

[4] S. Gao and M.A. Shokrollahi, "Computing roots of polynomials over function fields of curves," pp. 114–228 in Coding Theory and Cryptography, David Joyner (Ed.), Springer-Verlag 1999.

[5] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1755–1764, September 1999.
[6] R. Kötter, *On Algebraic Decoding of Algebraic-Geometric and Cyclic Codes*, Ph.D. Thesis, University of Linköping, Sweden, 1996.
[7] R. Koetter, J. Ma, and A. Vardy, "Efficient interpolation and factorization in algebraicsoft-decoding of Reed-Solomon codes," preprint, 2003.
[8] R. Koetter and A. Vardy, "Algebraic soft-decoding of Reed-Solomon codes," in *Proc. IEEE Symp. Inform. Theory*, Sorrento, Italy, June 2000.
[9] R. Koetter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2809–2825, 2003.
[10] R. Koetter and A. Vardy, "Decoding of Reed-Solomon codes for additive cost functions," *Proc. IEEE Symp. Inform. Theory*, Lausanne, July 2002.
[11] R. Koetter and A. Vardy, "A complexity reducing transformation in algebraic list-decoding of Reed-Solomon codes," in *Proc. IEEE Inform. Theory Workshop*, Paris, France, April 2003.
[12] J. Ma, P. Trifonov, and A. Vardy, "Divide-and-conquer interpolation for list decoding of Reed-Solomon codes," submitted to the *IEEE Symp. Inform. Theory*, Chicago, IL, July 2004.
[13] R.R. Nielsen and T. Høholdt, Decoding Reed-Solomon codes beyond half the minimum distance, in *Proc. International Conf. Coding Theory, Cryptography, and Related Areas*, pp. 221–236, Guanajuato, Mexico, 1998.
[14] V. Olshevsky and M.A. Shokrollahi, "A displacement structure approach to efficient decoding of Reed-Solomon and algebraic-geometric codes," in *Proceedings 31-st ACM Symp. Theory of Computing* (STOC), pp. 235–244, Atlanta, GA., May 1999.
[15] F. Parvaresh and A. Vardy, "Multiplicity assignments for algebraic soft-decoding of Reed-Solomon codes," preprint, also in *Proc. IEEE Symp. Inform. Theory*, Yokohama, Japan, July 2003.
[16] F. Parvaresh and A. Vardy, "Polynomial matrix-chain interpolation in Sudan-type Reed-Solomon decoders," preprint, submitted to the *IEEE Symp. Inform. Theory*, Chicago, IL, July 2004.
[17] R.M. Roth and G. Ruckenstein, "Efficient decoding of Reed-Solomon codes beyond half the minimum distance", *IEEE Trans. Inform. Theory*, vol. 46, pp. 246–258, January 2000.
[18] M. Sudan, "Decoding of Reed-Solomon codes beyond the error correction bound," *Journal of Complexity*, vol. 12, pp. 180–193, 1997.

Self-dual doubly even group codes

Wolfgang Willems
(joint work with Conchita Martínez-Pérez)

In the literature on coding one hardly find methods from representation theory though representations naturally come in if the automorphism group of the code is non-trivial. Exploiting such methods we are able to reprove known facts on group codes like the Sloane-Thompson theorem which says that a binary self-dual group code is never doubly even provided the Sylow 2-subgroups of the underlying group are cyclic. But we also get new interesting results in which representation theory and coding theory is very much related. For instance, there exists $C = C^{\perp} \leq K \oplus KG$ where K is a binary field and G a finite group if and only if all irreducible representations of G over K are of odd dimension. Such self-dual codes are doubly even if $|G| \equiv -1 \bmod 8$ which proves the converse of Gleason's theorem for extended group codes.

Maximal Curves

Michael Zieve

A celebrated result of Andre Weil asserts that the number of $\mathbb{F}_q$-rational points on a genus-g curve is at most $q + 1 + 2g\sqrt{q}$. The curves achieving this upper bound are called *maximal curves*. I surveyed the known maximal curves, described some new results (joint with Emrah Çakçak and Eric Rains), and gave evidence towards a precise new conjecture which would explicitly describe all maximal curves.

Abstracts of Informal Evening Talks

A family of caps of order $3q^2$ in $AG(4,q)$

Jürgen Bierbrauer
(joint work with Yves Edel)

Caps in projective spaces are sets of points no 3 of which are collinear. They are equivalent with linear codes of minimum distance 4. The maximum cardinality of a cap in $PG(n,q)$ is known in general only for projective dimension $n \leq 3$, due to the presence of quadratic forms of Witt index 1.

We construct a family of complete $(3q^2+4)$-caps in $AG(4,q)$ for $q = 2^{odd}$ as an extended dual BCH-code of length $3(q^2+1)$. The determination of the weight distribution of the corresponding 5-dimensional code with dual distance 4 relies on the spectrum of the number of rational points of a family of elliptic curves. These representation numbers also determine the weight distributions of the Kloostermann codes, the Zetterberg codes and two famous families of constacyclic quaternary codes [2]. The cap also can be described as union of the pairwise intersections of three parabolic quadrics. Over $\mathbb{F}_8$ we obtain an $[200, 5, 168]$-code.

References

[1] J.Bierbrauer and Y.Edel: *Caps of order $3q^2$ points in affine 4-space in characteristic 2,, Finite Fields and Their Applications,* to appear.

[2] D. N. Gevorkyan, A. M. Avetisyan and G. A. Tigranyan: *On the structure of two-error-correcting in Hamming metric over Galois fields,* in: Computational Techniques (in Russian) 3, Kuibyshev 1975, 19-21.

Analysis of one-point Goppa codes from the Weierstrass semigroup perspective

Maria Bras-Amorós

In this talk we study the minimum distance bounds and the different improvements of one-point Goppa codes from the perspective given by the Weierstrass semigroups. We introduce a new class of numerical semigroups, which we call the class of *acute* semigroups and we prove that they generalize symmetric and pseudo-symmetric numerical semigroups, Arf numerical semigroups and the semigroups generated by an interval. For a numerical semigroup $\Lambda = \{\lambda_0 < \lambda_1 < \dots\}$ denote $\nu_i = \#\{j \mid \lambda_i - \lambda_j \in \Lambda\}$. Given an acute numerical semigroup Λ we find the smallest non-negative integer m for which the order bound on the minimum distance of one-point Goppa codes with associated semigroup Λ satisfies $d_{ORD}(C_i)(:= \min\{\nu_j \mid j > i\}) = \nu_{i+1}$ for all $i \geq m$. We prove that the only numerical semigroups for which the sequence (ν_i) is always non-decreasing are ordinary numerical semigroups. Furthermore we show that a semigroup can be uniquely determined by its sequence (ν_i).

The kissing number in four dimensions

Oleg R. Musin

The kissing number τ_n is the maximal number of equal size nonoverlapping spheres in n dimensions that can touch another sphere of the same size. The number τ_3 was the subject of a famous discussion between Isaac Newton and David Gregory in 1694. The Delsarte method gives an estimate $\tau_4 \leq 25$. In this paper we present an extension of the Delsarte method for spherical codes and use it to prove that $\tau_4 = 24$. We also present a new proof that $\tau_3 = 12$.

Edited by Cem Güneri and Ferruh Özbudak

Participants

Dr. Harinaivo Andriatahiny
aharinaivo@yahoo.fr
Lot II N 174 FD Analamahitsy
101 Antananarivo – Madagascar

Prof. Dr. Angela Barbero
angbar@wmatem.eis.uva.es
Dept. Matematica Aplicada
Ingeniero Indust.
Paseo del Cauce s/n
E-47011 Valladolid

Dr. Jürgen Bierbrauer
jbierbra@mtu.edu
Dept. of Math. Sciences
Michigan Technological University
1400 Townsend Drive
Houghton, MI 49931 – USA

Dr. Gilberto Bini
gbini@science.uva.nl
Korteweg-de Vries Instituut
Faculteit WINS
Universiteit van Amsterdam
Plantage Muidergracht 24
NL-1018 TV Amsterdam

Dr. Maria Bras-Amoros
mbras@ccd.uab.es
Departament D'Informatica
Unitat de Combinatoria i
Comunicacio Digital
Univ. Autonoma de Barcelona
E-08193 Bellaterra

Prof. Dr. Hans Dobbertin
Hans.Dobbertin@rub.de
Lehrstuhl Informationssicherheit
NA 5/72
Ruhr-Univeristät Bochum
Universitätsstr. 150
D–44780 Bochum

Prof. Dr. Iwan Duursma
duursma@math.uiuc.edu
Dept. of Mathematics, University of
Illinois at Urbana-Champaign
273 Altgeld Hall MC-382
1409 West Green Street
Urbana, IL 61801-2975 – USA

Prof. Dr. Arnaldo Garcia
garcia@impa.br
Institute of Pure and Applied Math.
IMPA
Estrada Dona Castorina 110
Rio de Janeiro RJ 22460-320 – Brazil

Prof. Dr. Gerard van der Geer
geer@science.uva.nl
Korteweg-de Vries Instituut
Faculteit WINS
Universiteit van Amsterdam
Plantage Muidergracht 24
NL-1018 TV Amsterdam

Dr. Olav Geil
olav@math.auc.dk
Dept. of Mathematical Sciences
University of Aalborg
Fredrik Bajers Vej 7G
DK-9220 Aalborg East

Prof. Dr. Guang Gong
ggong@calliope.uwaterloo.ca
Department of Electicial and
Computer Engineering
University of Waterloo
Waterloo ONT N2L 3G1 – Canada

Prof. Dr. Cem Güneri
guneri@sabanciuniv.edu
Sabanci Universitesi
Orhanli
Tuzla
34956 Istanbul – Turkey

Prof. Dr. Venkatesan Guruswami
venkat@cs.washington.edu
Department of Computer Science
& Engineering
University of Washington
Box 352350
Seattle WA 98195-2350 – USA

Dr. A. Roger Hammons
rhammons@corvis.com
Roger.Hammons@jhuapl.edu
Applied Physics Laboratory
Johns Hopkins University
1110 Johns Hopkins Road
Laurel MD 20723-6099 – USA

Prof. Dr. Tor Helleseth
Tor.Helleseth@ii.uib.no
torh@ii.uib.no
Department of Informatics
University of Bergen
Hoyteknologisenteret
N-5020 Bergen

Prof. Dr. Tom Hoeholdt
T.Hoeholdt@math.dtu.dk
Department of Mathematics
Technical University of Denmark
Bldg. 303
DK-2800 Lyngby

Prof. Dr. Jorn Justesen
jju@com.dtu.dk
COM
Technical University Denmark
Bygning 371
DK-2800 Lyngby

Prof. Dr. Ralf Kötter
koetter@vivc.edu
koetter@uiuc.edu
Coordinated Science Laboratory
University of Illinois at
Urbana-Champaign
1101 W. Springfield Avenue
Urbana, IL 61801 – USA

Prof. Dr. Vijay Kumar
vijayk@usc.edu
EE-Systems
EEB 500
University of Southern California
3740 McClintock Avenue
Los Angeles CA 90089-2565 – USA

Prof. Dr. Vladimir I. Levenshtein
leven@spp.keldysh.ru
M.V. Keldysh Institute of Applied
Mathematics
Russian Academy of Sciences
Miusskaya pl. 4
125047 Moscow – Russia

Prof. Dr. Simon N. Litsyn
litsyn@eng.tau.ac.il
Dept. of Electrical Engineering Systems
Tel Aviv University
Ramat Aviv 69978 – Israel

Prof. Dr. Hans-Andrea Loeliger
loeliger@isi.ee.ethz.ch
Institut für Signalverarbeitung
ETH Zentrum
ETF E 101
CH-8092 Zürich

Dr. Hsiao-Feng Lu
hsiaofel@commsci1.usc.edu
EE-Systems
EEB 500
University of Southern California
3740 McClintock Avenue
Los Angeles CA 90089-2565 – USA

Prof. Dr. Werner Lütkebohmert
lubo@mathematik.uni-ulm.de
Abteilung Reine Mathematik
Universität Ulm
D–89069 Ulm

Prof. Dr. Hiren Maharaj
maharaj@math.psu.edu
maharaj@oeaw.ac.at
hmahara@clemson.edu
Dept. of Mathematical Sciences
Clemson University
Martin Hall
Clemson, SC 29634-0975 – USA

Prof. Dr. Gary McGuire
gmg@maths.may.ie
Department of Mathematics
National University of Ireland
Maynooth
Co. Kildare – Ireland

Prof. Dr. Oleg R. Musin
omusin@mail.ru
oleg_musin@hotmail.com
musin@gislab.geogr.msu.su
Moscow State University
Institute for Mathematical Study of
Complex Systems
Novoyasenevskiy pr. 19-1-31
Moscow 117593 – Russia

Prof. Dr. Jong-Seon No
jsno@snu.ac.kr
School of Electrical Engineering
and Computer Science
Seoul National University, San 56-1
Shilim-dong Kwanak-gu
Seoul 151-742 – Korea

Prof. Dr. Ferruh Özbudak
ozbudak@arf.math.metu.edu.tr
Dept. of Mathematics
Middle East Technical University
06531 Ankara – Turkey

Prof. Dr. B. Sundar Rajan
bsrajan@ece.iisc.ernet.in
Dept. of Electrical Communication
Engineering
Indian Institute of Science
Bangalore 560 012 – India

Domingo Ramirez-Alzola
mtpraald@lg.ehu.es
Euskal Herriko Univertsitatea
Zientzi Fakultatea
Matematika Saila
644 Posta Kutxatila
E-48.080 Bilbo

Prof. Dr. Joachim Rosenthal
Rosenthal.1@nd.edu
Department of Mathematics
University of Notre Dame
Notre Dame IN 46556-4618 – USA

Prof. Dr. B.Al Sethuraman
al.sethuraman@csun.edu
Department of Mathematics
California State University at
Northridge
Northridge CA 91330-8313 – USA

Dr. Mohammad Amin Shokrollahi
amin.shokrollahi@EPFL.CH
EPFL
IC-IIF-ALGO
Bat. PSE. A
CH-1015 Lausanne

Prof. Dr. Patrick Sole
ps@essi.fr
Laboratoire d'Informatique
Signaux et Systems de
Sophia Antipolis (I3S)
250, rue Albert Einstein
F-06560 Valbonne

Prof. Dr. Henning Stichtenoth
stichtenoth@uni-essen.de
mat310@uni-essen.de
henning@sabanciuniv.edu
FB 6 - Mathematik
Universität Duisburg-Essen
Standort Essen
D–45117 Essen

Prof. Dr. Madhu Sudan
madhu@mit.edu
Dept. of Elec. Eng. and CS
MIT
NE43-307
200 Tech Square
Cambridge MA 02139-3594 – USA

Prof. Dr. Horacio Tapia-Recillas
htr@xanum.uam.mx
htr@servidor.unam.mx
Universidad Autonoma Metropolitana
(UAM) Departamento de Matematicas
Iztapalapa 09340
Av. San Rafael Atlixco 186
09340 Mexico D.F.– Mexico

Prof. Dr. Alexander Vardy
vardy@kilimanjaro.ucsd.edu
UCSD
Mail Code 0407
9500 Gilman Drive
La Jolla CA 92093 – USA

Prof. Dr. Wolfgang Willems
willems@mathematik.uni-magdeburg.de
Fakultät für Mathematik
Otto-von-Guericke-Universität
Magdeburg
Universitätsplatz 2
D–39106 Magdeburg

Prof. Dr. Oyvind Ytrehus
oyvind@ii.uib.no
Department of Informatics
University of Bergen
Hoyteknologisenteret
N-5020 Bergen

Dr. Michael Zieve
zieve@idaccr.org
Center for Communications Research
805 Bunn Drive
Princeton NJ 08540 – USA