ÖAW AUSTRIAN ACADEMY OF SCIENCES

RICAM
JOHANN · RADON · INSTITUTE
FOR COMPUTATIONAL AND APPLIED MATHEMATICS

RICAM Special Semester on Multivariate Algorithms and Their Foundations in Number Theory

Workshop 1
Pseudo-Randomness and Finite Fields

Book of Abstracts

Linz, Austria
October 15-19, 2018

	Monday Oct. 15	Tuesday Oct. 16	Wednesday Oct. 17	Thursday Oct. 18	Friday Oct. 19
08:30 - 08:50	REGISTRATION				
08:50 - 09:00	Opening				
	Chair: Schmidt	Chair: Topuzoğlu	Chair: Roche-Newton	Chair: Meidl	Chair: Panario
09:00 – 09:45	**Davis**	**Kyureghyan**	**Petridis**	**Buratti**	**Wang**
09:45 - 10:30	**Xiang**	**Panario I**	**Rudnev**	**Wassermann**	**Sheekey**
10:30 – 11:00	*Coffee Break*	*Coffee Break*	*Coffee Break*	*Coffee Break*	*Coffee Break*
11:00 – 11:30	**Zhou**	**Rosenthal**	**Shkredov**	**Zumbrägel**	**Roche-Newton**
11:30– 14:00	*Lunch Break*	*Lunch Break*	*Photo & Lunch Break*	*Lunch Break*	*Lunch Break*
	Chair: Jedwab	Chair: Gomez		Chair: Mérai	Chair: Pirsic
14:00 – 14:45	**Katz**	**Schmidt**		**van Greevenbroek**	**Siddhanti**
14:45 – 15:15	**Swaenepoel**	**Micheli**		**Rivat**	**Meidl**
15:15 – 15:45	*Coffee Break*	*Coffee Break*		*Coffee Break*	*Coffee Break*
15:45 – 16:15	**Topuzoğlu**	**Su**	**Guided City Tour (Start 14:00, Science Park 2)**	**Sarközy**	**Panario II**
16:15 – 16:45	**Mérai**	**Yayla**		**Mauduit**	**Qureshi**
16:45 – 17:15	**Anbar**	**Thomson**		**Lampe**	*End of Workshop*
	17:15 Reception				
				19:00 Conference Dinner	

Modified planar and bent$_4$ functions
Nurdagül Anbar Meidl
Sabancı University Istanbul

Abstract

Modified planar functions are introduced by Zhou (J. Combin. Des. 21(12), 563–584, 2013) to describe $(2^n, 2^n, 2^n, 1)$ relative difference sets (RDS) R as a graph of a function on the finite field $\mathbb{F}_{2^n}$. These are analogs of planar functions in odd characteristic p to describe $(p^n, p^n, p^n, 1)$ RDSs. In this talk, we point out that the projections of R are $(2^n, 2, 2^n, 2^{n-1})$ RDS that can be described by bent$_4$ functions, and we investigate the equivalence of their relative difference sets. In particular, we show that two extended affine equivalent bent functions may give rise to bent$_4$ functions whose corresponding RDSs are inequivalent.

This is joint work with Wilfried Meidl and Alexander Pott.

Tiling rings with "precious" differences
Marco Buratti
Universitá di Perugia

Abstract

We determine the maximum size of a difference packing of a ring R whose blocks are all multiples of $\{1, \varphi, \varphi^2\}$ with φ gold (that is a solution of $x^2 - x - 1 = 0$ in R) or all multiples of $\{1, \psi, \psi^2, \psi^3\}$ with ψ platinum (that is a solution of $x^3 + x^2 - 1 = 0$ in R). As a special consequence, we get a few more classes of values of v for which now we can claim that an optimal $(v, 4, 1)$ optical orthogonal code exists.
We think that this golden context is the right one for reformulating an old difference family construction of the present author (improving a much older one by R.C. Bose) in terms of golden elements of a field.

Construction of bent functions using covering extended building sets
James A. Davis
University of Richmond

Abstract

There are $99,270,589,265,934,370,305,785,861,242,880$ ($\approx 2^{106}$) 8-variable bent functions. The two best understood construction methods, Maiorana-McFarland ($\mathcal{M}$) ($\approx 2^{81.38}$) and Partial Spread ($\mathcal{PS}$) ($\approx 2^{85}$), dont come close to constructing all 8-variable bent functions. We propose adapting a construction method from difference sets known as covering EBSs to find bent functions. We show that all bent functions in $\mathcal{M}$ can be constructed via covering EBSs. Moreover, we provide examples of 8-variable bent functions constructible by covering EBS that are not in $\mathcal{M}$, thus demonstrating that this new construction method is a generalization of $\mathcal{M}$. We indicate how to construct many different types of covering EBSs that will produce bent functions not in $\mathcal{M}$.

This is joint work with John Clikeman and David Clayton.

A new structure for difference matrices over abelian p-groups

Koen van Greevenbroek
Simon Fraser University

Abstract

A difference matrix over a group is a discrete structure that is intimately related to many other combinatorial designs, including mutually orthogonal Latin squares, orthogonal arrays, and transversal designs. Interest in constructing difference matrices over 2-groups has been renewed by the recent discovery that these matrices can be used to construct large linking systems of difference sets, which in turn provide examples of systems of linked symmetric designs and association schemes. We survey the main constructive and nonexistence results for difference matrices, beginning with a classical construction based on the properties of a finite field. We then introduce the concept of a contracted difference matrix, which generates a much larger difference matrix. We show that several of the main constructive results for difference matrices over abelian p-groups can be substantially simplified and extended using contracted difference matrices. In particular, we obtain new linking systems of difference sets of size 7 in infinite families of abelian 2-groups, whereas previously the largest known size was 3.

This is joint work with Jonathan Jedwab.

Weil sums of binomials: properties and applications

Daniel Katz
California State University

Abstract

We present a survey on Weil sums in which an additive character of a finite field F is applied to a binomial whose individual terms (monomials) become permutations of F when regarded as functions. Then we indicate how these Weil sums are used in applications, especially how they characterize the nonlinearity of power permutations and the correlation of linear recursive sequences over finite fields. In these applications, one is interested in the spectrum of Weil sum values that one obtains as one varies the coefficients in the binomial. We review the basic properties of such spectra, and then give a survey of current topics of research: Archimedean and non-Archimedean bounds on the sums, the number of values in the spectrum, and the presence or absence of zero in the spectrum. We indicate some important open problems and discuss progress that has been made on them.

Results on permutation polynomials of shape $x^t + \gamma Tr_{q^n/q}(x^d)$

Gohar Kyureghyan
University of Rostock

Abstract

The maps of shape $T(x) = x^t + \gamma Tr_{q^n/q}(x^d)$ combine in an interesting way the additive and multiplicative structures of $\mathbb{F}_{q^n}$ and serve as a source for maps with special properties required in different areas of applications. In this talk we briefly survey known results on such permutations and continue their study. We prove that if $T(x)$ is bijective on $\mathbb{F}_{q^n}$ then necessarily $\gcd(t, q^n - 1) = 1$. We show that $F(x) = x^{q^2+q-1} + Tr_{q^3/q}(x)$ has very special properties on $\mathbb{F}_{q^3}$ by determining explicitly its iterates, the inverse map, the set of fixed points and its cycle structure.

This is joint work with Daniel Gerike.

Cluster algebras over finite fields
Philipp Lampe
University of Kent

Abstract

Cluster algebras, which are defined by mutations of seeds, occur naturally in algebraic combinatorics. First of all we explain how to mutate a seed. Next, we show how to generate systems of integers through mutations of seeds. We indicate under which circumstances the systems are finite or can be used to generate periodic sequences, linear recurrence relations, or non-linear recurrence relations. Then we study the behaviour of the seeds when reducing modulo a prime. In particular, for certain types of seeds we give formulae for the number of solutions over finite fields in terms of zeta functions and we indicate how to generate pseudorandom sequences from non-linear recurrence relations.

The weight of irreducible polynomials over a finite field
Christian Mauduit
Université d'Aix-Marseille

Abstract

This talk concerns the weight of irreducible polynomials over a finite field, i. e. the number of non-zero coefficients of these polynomials. We introduce polynomial analogs of the methods introduced by Gallagher-Vaughan, Bassily-Kátai and Drmota-Mauduit-Rivat which lead to upper bounds for the associated exponential sums. This allows us to study the distribution of the weight of irreducible polynomials and to provide an asymptotic for the number of irreducible polynomials of a given degree whose weight is close to the expected value.

This is joint work with Mireille Car.

Bent functions and their duals
Wilfried Meidl
RICAM

Abstract

Weakly regular bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ have the property that their dual is again a bent function. In particular the dual of a Boolean bent function is bent. This does in general not apply to non-weakly regular bent functions. Many classical constructions of bent functions result in (weakly) regular bent functions, sporadic examples of non-weakly regular bent functions indicated that non-weakly regular bent functions can have both, a bent dual and a dual which is not bent. In the meantime some constructions of infinite classes of non-weakly regular bent function are known. The first published constructions yield bent functions for which the dual is a bent function though. By now also the existence of infinitely many bent functions for which the dual is not bent is confirmed by explicit constructions in any odd characteristic. This talk discusses the recent developments and open problems on duality for bent functions and on concepts of duality also for vectorial bent functions.

This is joint work with Ayça Çeşmelioğlu and Alexander Pott.

Pseudorandom walks on elliptic curves
László Mérai
RICAM

Abstract

We give an overview of pseudorandom number generators (PRNGs) based on elliptic curves over finite fields. Many PRNGs are defined via a recursion law $P_n = \psi(P_{n-1})$ for some initial point $P_0 \in E$ and a rational map (morphism) $\psi : E \to E$ of the curve E. An example for such PRNGs is the so-called power generator, where ψ is a scalar multiplication: $\psi : P \mapsto eP$ for some integer $e \geq 2$. We consider in detail the case when ψ is an arbitrary endomorphism of the curve.
We present bounds on the discrepancy and linear complexity of the obtained sequences.

Fractional jumps
Giacomo Micheli
EPFL and University of Oxford

Abstract

In this talk we explain how to produce pseudorandom number generators using Fractional Jumps of transitive projective maps. The concept of Fractional Jump intertwines the theory of projective automorphisms with the theory of polynomials over finite fields, analytic number theory, and in turn leads to competitive pseudorandom number generation. Furthermore, our theory covers entirely the theory of Inversive Congruential Generator (ICG) sequences. The sequences produced using our generators have the same discrepancy bound but improved computational complexity with respect to the classical ICG sequences.

A survey on iterations of mappings over finite fields
Daniel Panario
Carleton University

Abstract

We survey iterations of polynomials and rational functions over finite fields. We show precise information on periodicity and permutational properties for some classical functions over finite fields including some quadratic polynomials, Chebyshev, Rédei, linearized and power maps. It seems hard to predict the periodicity behavior of generic functions over a finite field, so we provide heuristic arguments aiming at understanding their behavior in comparison to random uniform mappings over a finite field. We conclude showing a well known methodology that provides many results about uniform random mappings.

This is joint work with Rodrigo Martins and Claudio Qureshi.

Pseudorandomness of large sets in finite fields
Giorgis Petridis
University of Georgia

Abstract

Large subsets of vector spaces share many properties with random sets. We present examples of this phenomenon for large subsets of finite fields. We focus on results with straightforward proofs but also explain in broad terms the tools that allow one to go a step further.

On the dynamics of Chebyshev polynomials over finite fields
Claudio Qureshi
University of Campinas

Abstract

In this talk we describe the dynamics of Chebyshev polynomials over finite fields through their functional graph. We use our structural results to obtain estimates for some parameters such that the expected value for the period and preperiod, the average number of connected components, the expected rho length, among others. By comparing these parameters with the corresponding ones for random mappings, we briefly discuss how far are these polynomials from being random. This talk is based on joint work with Daniel Panario.

Digits of primes and squares
Joël Rivat
Université d'Aix-Marseille

Abstract

We will give a survey of our results on the digits of primes and squares (joint works with Michael Drmota and Christian Mauduit).

Some non-trivial constructions in sum-product and discrete geometry problems
Oliver Roche-Newton
RICAM

Abstract

This talk will consider the following question of Rudnev: given four pencils of n lines in the plane $\mathbb{F}^2$, what is the maximum number of points where four lines cross? The question was motivated by the sum-product problem, and in particular, constructing many intersection points corresponds to constructing a graph which determines few sums and products. The question was considered by Alon, Ruzsa and Solymosi, and improved upper and lower bounds were given in a joint paper with Audie Warren.

If time permits, I will discuss related work on new constructions for the Elekes-Szabó problem.

Masking an algebraic structure in code based cryptography
Joachim Rosenthal
University Zürich

Abstract

With the realization that a quantum computer would make many practically used public key cryptographic systems obsolete it became an important research topic to design public key systems which are expected to be secure even if a powerful quantum computer would exist. Such systems are nowadays called post-quantum crypto systems.

Some of the major candidates in post-quantum cryptography are based on the difficulty of decoding a general linear code up to half the minimum distance. On the other hand there are many codes with special algebraic structure which can be decoded efficiently. In this talk we survey ideas how the algebraic structure of e.g. a Reed-Solomon code can be hidden.

Results of the talk were jointly derived with Karan Khathuria and Violetta Weger.

Point-plane incidences and some applications in positive characteristic

Misha Rudnev
University of Bristol

Abstract

The point-plane incidence theorem states that the number of incidences between n points and $m \geq n$ planes in the projective three-space over a field F, is

$$O(m\sqrt{n} + mk),$$

where k is the maximum number of collinear points, with the extra condition $n < p^2$ if F has characteristic $p > 0$. This theorem also underlies a state-of-the-art Szemerédi-Trotter type bound for point-line incidences in F^2, due to Stevens and de Zeeuw.

This review focuses on some recent, as well as new, applications of these bounds that lead to progress in several open geometric questions in F^d, for $d = 2, 3, 4$. These are the problem of the minimum number of distinct nonzero values of a non-degenerate bilinear form on a point set in $d = 2$, the analogue of the Erdős distinct distance problem in $d = 2, 3$ and additive energy estimates for sets, supported on a paraboloid and sphere in $d = 3, 4$. It avoids discussing sum-product type problems (corresponding to the special case of incidences with Cartesian products), which have lately received more attention.

Quasi-random graphs and pseudo-random binary sequences

András Sárközy
Eötvös Loránd University Budapest

Abstract

The notion of quasi-random graphs was introduced in 1987 by F. R. K. Chung, R. L. Graham and R. M. Wilson, resp. A. Thomason. Jointly with J. Borbély we have shown that there is a strong connection between this notion and the pseudo-randomness of (finite) binary sequences. This connection can be utilized for constructing large families of quasi-random graphs by considering graphs defined by a circular adjacency matrix whose first column is a binary sequence with strong pseudo-random properties. Starting out from this construction principle one may extend, generalize and sharpen some definitions and results on quasi-randomness of graphs.

Bilinear forms on finite abelian groups and Butson matrices

Bernhard Schmidt
Nanyang Technological University Singapore

Abstract

Bilinear forms over finite fields are well understood and have been used for the construction of numerous combinatorial objects such as combinatorial designs and substructures of finite geometries. There exists a theory of bilinear forms on finite abelian groups, too, but their applications to combinatorics, except for the special case of forms on additive groups of finite fields, are rare. We will show how that any symmetric and nondegenerate bilinear form on a finite abelian group can be used to construct Butson matrices. Here, by a Butson matrix, we mean a square matrix whose entries are complex roots of unity and whose rows are pairwise orthogonal with respect to the standard Hermitian inner product.

This is joint work with Tai Do Duc.

MRD codes: constructions and connections

John Sheekey
University College Dublin

Abstract

Rank-metric codes are codes consisting of matrices with entries in a finite field, with the distance between two matrices being the rank of their difference. Codes with maximum size for a fixed minimum distance are called Maximum Rank Distance (MRD) codes. Such codes were constructed and studied independently by Delsarte (1978), Gabidulin (1985), Roth (1991), and Cooperstein (1997). Rank-metric codes have seen renewed interest in recent years due to their applications in random linear network coding.

MRD codes also have interesting connections to other topics such as semifields (finite nonassociative division algebras), finite geometry, linearized polynomials, and cryptography. In this chapter we will survey the known constructions and applications of MRD codes, and present some open problems.

On actions of $\mathrm{SL}_2(\mathbb{F}_p)$ *and* $\mathrm{Aff}(\mathbb{F}_p)$ *on* $\mathbb{F}_p$ *and the sum–product phenomenon*

Ilya Shkredov
Steklov Mathematical Institute

Abstract

Let p be a prime number, $\mathbb{F}_p$ be the prime field and $A \subseteq \mathbb{F}_p$ be a set. Define the sumset and the product set of A as

$$A+A = \{a+b \ : \ a,b \in A\} \qquad \text{and} \qquad AA = \{ab \ : \ a,b \in A\}\,.$$

The sum–product phenomenon says that for any sufficiently small set A one has

$$\max\{|A+A|, |AA|\} \gg |A|^{1+c_1}\,,$$

where $c_1 > 0$ is an absolute constant. Several years ago it was realised that the sum–product phenomenon is connected with the growth in $\mathrm{SL}_2(\mathbb{F}_p)$, namely, with the result of Helfgott

$$|AAA| \gg |A|^{1+c_2}\,, \qquad \forall A \subseteq \mathrm{SL}_2(\mathbb{F}_p)\,,$$

where $c_2 > 0$ is another absolute constant and $A \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ is a sufficiently small set of matrices. Similar result takes place for the affine group $\mathrm{Aff}(\mathbb{F}_p)$. We will give a survey on the subject and will describe several applications of the sum–product phenomenon to problems of Additive Combinatorics and Number Theory. In particular, we obtain an application to the theory of the continued fractions, namely, to a problem of Zaremba.

Differential fault attack on hardware stream ciphers A technical survey

Akhilesh Siddhanti
BITS Pilani KK Birla Goa Campus

Abstract

Stream ciphers are often employed to provide fast and secure operations under resource-constrained environments. However, when it comes towards implementing the same cipher in hardware, the main question is whether the cipher continues to hold the same security level. Allowing faults to inject into a cipher can seriously compromise its security. In this work, we discuss the Differential Fault Attack (DFA) against several stream ciphers. The list includes hardware eStream candidates namely Grain, MICKEY, Trivium; lightweight stream ciphers like Sprout, Plantlet, Lizard; and a CAESAR finalist ACORN. We conclude that by injecting few faults, one can cryptanalyze all the ciphers referred above. We revisit these attacks with considerable details in this technical survey. Thus the designers should seriously consider the impact of such fault attacks on their hardware stream ciphers. We conclude with a proposal for a software where one can input the design of a stream cipher and the tool will evaluate its resistance against DFA.

This is joint work with Subhamoy Maitra.

On the stability of periodic binary sequences with zone restriction

Ming Su
Nankai University

Abstract

Traditional global stability measure for sequences is hard to determine because of large search space. We propose the k-linear complexity with a zone restriction for measuring the local stability of sequences. For any binary sequence with period 2^n, we show that the k-linear complexity is identical to the k-linear complexity within a zone, whose length is much smaller than the whole period when the k-error linear complexity is large. Accordingly, we can efficiently determine the global stability by studying a local stability. Moreover, we extend this result to several other binary sequences with even period that is not a power of 2. We also completely determine the spectrum of 1-error linear complexity with any zone length for an arbitrary 2^n-periodic binary sequence.

This is joint work with Qiang Wang.

Digital questions in finite fields

Cathy Swaenepoel
Aix-Marseille Université

Abstract

The connection between the arithmetic properties of an integer and the properties of its digits in a given basis produces a lot of interesting questions and many papers have been devoted to this topic. In the context of finite fields, the algebraic structure permits to formulate and study new problems of interest which might be out of reach in $\mathbb{N}$. This study was initiated by C. Dartyge and A. Sárközy.

We will devote our interest to several new questions in this spirit:

1. estimate precisely the number of elements of some special sequences of $\mathbb{F}_q$ whose sum of digits is fixed;
2. given subsets $\mathcal{C}$ and $\mathcal{D}$ of $\mathbb{F}_q$, find conditions on $|\mathcal{C}|$ and $|\mathcal{D}|$ to ensure that there exists $(c,d) \in \mathcal{C} \times \mathcal{D}$ such that the sum of digits of cd belongs to a predefined subset of $\mathbb{F}_p$;
3. estimate the number of elements of an interesting sequence of $\mathbb{F}_q$ with preassigned digits.

The notion of digits in $\mathbb{F}_q$ is directly related to the notion of trace which is of basic importance in the study of finite fields and our results may also be formulated in this direction.

Hypercubes with elementary interval regularity

David Thomson
Carleton University

Abstract

In this talk, we discuss constructions of a particular type of combinatorial hypercube with regularity constraints given by the elementary intervals for (t, m, s)-nets. We give constructions for these hypercubes using linear forms over finite fields and MDS codes; the latter enforces even stronger constraints. By construction, these hypercubes give $(0, d, d)$-nets in base q^d, for some prime power q and positive integer d. We also give an upper bound on the number of simultaneously orthogonal such hypercubes, where the notion of orthogonality extends naturally from Latin squares.

This is joint work with Melissa Huggan, Gary L. Mullen and Brett Stevens.

Irreducible factors of a class of permutation polynomials
Alev Topuzoğlu
Sabancı University Istanbul

Abstract

I will present our recent results on the degrees of the irreducible factors of a large class of permutation polynomials of a finite field.

This is joint work with Tekgül Kalaycı and Henning Stichtenoth.

Polynomials over finite fields: an index approach
Qiang Wang
Carleton University

Abstract

The degree of a polynomial is an important parameter in the study of numerous problems on polynomials over finite fields. Recently, a new notion of the index of a polynomial over a finite field is introduced to study the distribution of permutation polynomials over finite fields. This parameter also turns out to be very useful in studying value set size bounds, character sum bounds, among others. In this talk we survey this new index approach and focus on some recent results on permutation polynomials over finite fields.

q-analogs of group divisible designs
Alfred Wassermann
University of Bayreuth

Abstract

A well known class of objects in combinatorial design theory are group divisible designs. Here, we introduce the q-analogs of group divisible designs. It turns out that there are interesting connections to scattered subspaces, q-Steiner systems, packing designs and q^r-divisible projective sets.

We give necessary conditions for the existence of q-analogs of group divisible designs, construct an infinite series of examples, and provide further existence results with the help of a computer search.

One example is a $(6, 3, 2, 2)_2$ group divisible design over $GF(2)$ which is a packing design consisting of 180 blocks that such every 2-dimensional subspace in $GF(2)^6$ is covered at most twice.

This is joint work with Marco Buratti, Michael Kiermaier, Sascha Kurz and Anamari Nakić.

Cyclotomy, difference sets, sequences with low correlation, strongly regular graphs, and related geometric substructures
Qing Xiang
University of Delaware

Abstract

In this talk, we survey constructions of and nonexistence results on combinatorial/geometric structures which arise from unions of cyclotomic classes of finite fields. In particular, we survey both classical and recent results on difference sets related to cyclotomy, and cyclotomic constructions of sequences with low correlation. We also give an extensive survey of recent results on constructions of strongly regular Cayley graphs and related geometric substructures such as m-ovoids and i-tight sets in classical polar spaces.

This is joint work with Koji Momihara and Qi Wang.

Families of sequences with good family complexity and cross-correlation measure

Oğuz Yayla
Hacettepe University Ankara

Abstract

The quality of a pseudorandom sequence are screened by statistical test packages (for example L'Ecuyer's TESTU01, Marsaglia's Diehard or the NIST battery) as well as by theoretical results on certain measures of pseudorandomness such as the correlation measure of order ℓ first introduced by Mauduit and Sárközy. Here we focus on theoretical results. In many applications such as cryptography one needs a large family of good pseudorandom sequences and has to prove bounds on several figures of merit. In this talk we study two such measures the family complexity, short f-complexity, and the cross-correlation measure of order ℓ of families of sequences. We consider sequences not only on binary alphabet but also on k-symbols (k-ary) alphabet. We now start with binary alphabet and deal with k-symbol alphabet. We use the notation Φ_ℓ° for the cross correlation Φ_ℓ evaluated for fixed $M = F$ and $d_i = 0$ for all $i \in \{1, 2, \ldots, l\}$. In this study we generalize some known methods on construction of the family of binary pseudorandom sequences. We prove a bound on the f-complexity of the family of binary sequences of Legendre-symbols of monic irreducible polynomials $f_i(x) = x^d + a_2 i^2 x^{d-2} + a_3 i^3 x^{d-3} + \cdots + a_{d-2} i^{d-2} x^2 + a_d i^d$ defined as

$$\mathcal{F} = \left\{ \left(\frac{f_i(n)}{p} \right)_{n=1}^{p-1} : i = 1, \ldots, p-1 \right\}.$$

We show that this family as well as its dual family have both a large family complexity and a small cross-correlation measure up to a rather large order. Next, we present a new family of binary sequences

$$\mathcal{F} = \left\{ \left(\frac{f_\beta(n)}{p} \right)_{n=1}^{p-1} : \beta \in \mathbb{F}_{p^d} \backslash \mathbb{F}_p \text{ and nonconjugate} \right\}$$

for $f_\beta(x) = (x - \beta)(x - \beta^p) \cdots (x - \beta^{p^{d-1}})$. We prove that $\mathcal{F}$ has high f-complexity and low cross-correlation measure. Then we extend some known methods to the family of sequences on k-symbols alphabet.

The author is supported by TÜBİTAK under Grant No. 116R026.

Maximum rank-distance codes with maximum idealisers

Yue Zhou
National University of Defense Technology, Changsha

Abstract

Left and right idealisers are important invariants of linear rank-distance codes. In case of maximum rank-distance (MRD for short) codes in $\mathbb{F}_q^{n \times n}$ the idealisers have been proved to be isomorphic to finite fields of size at most q^n. Up to now, the only known MRD codes with maximum left and right idealisers are generalized Gabidulin codes, which were first constructed in 1978 by Delsarte and later generalized by Kshevetskiy and Gabidulin in 2005. In this talk we classify MRD codes in $\mathbb{F}_q^{n \times n}$ for $n \leq 9$ with maximum left and right idealisers and connect them to Moore type matrices. Besides generalized Gabidulin codes, it turns out that there is a further family of rank-distance codes providing MRD ones with maximum idealisers for $n = 7$, q odd and for $n = 8$, $q \equiv 1 \pmod 3$. These codes are not equivalent to any previously known MRD code. Moreover, we show that this family of rank-distance codes does not provide any further examples for $n \geq 9$.

This talk is based on a joint-work with Bence Csajbók, Olga Polverino and Giuseppe Marino.

Indiscreet logarithms?

Jens Zumbrägel
University of Passau, Germany

Abstract

Our modern public-key cryptography originates from seminal work by Diffie and Hellman, and is since connected with the difficulty of the discrete logarithm problem. However, for finite fields of small characteristic, this problem turns out to be not as intractable as thought for a long time. In fact, some striking observations have recently led to considerable record computations, asymptotically faster algorithms and severe consequences for the security of certain cryptosystems.

This talk aims to illustrate the main mathematical ideas behind these rather new developments. In particular, we discuss an approach to obtain a rigorously provable quasi-polynomial time algorithm for computing discrete logarithms in finite fields of small characteristic.

The presentation is based on joint works with Faruk Göloğlu, Robert Granger, Thorsten Kleinjung and Gary McGuire.