Plenary Talks

Code-Based Cryptography

Tanja Lange

(joint work with Daniel J. Bernstein and Christiane Peters)

Code-based cryptography is one of the candidates for post-quantum cryptography, i.e., cryptography that survives attacks by quantum computers (see `www.pqcrypto.org`). Even though the McEliece cryptosystem has been around as long as RSA, it is rarely used in practice. The security of McEliece's suggestion of using classical binary Goppa codes is reasonably well understood and encryption speeds are good. The main problem is that the size of the public key is significantly larger than for RSA or ECC.

In this talk, I will present 'wild Goppa codes' [1], a generalization of the codes used by McEliece. Wild Goppa codes are codes over small finite fields GF(q) obtained from Goppa polynomials of the form g^{q-1}. While the degree promises a minimum distance of at least $(q-1)\deg(g)$, these codes actually have minimum distance at least $q\deg(g)$. This helps to reduce the key size. Further generalizations are to consider polynomials of the form fg^{q-1} to have a larger pool of polynomials to choose from and to get a better balance for the degrees. As a second topic, I will present an information-set-decoding algorithm, called ball-collision decoding [2], that is not only faster than previous algorithms but even beats a lower bound claimed for information-set decoding.

References

[1] D. J. BERNSTEIN, T. LANGE, AND C. PETERS, *Wild McEliece*, in Selected Areas in Cryptography (17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers, A. Biryukov, G. Gong, and D. R. Stinson, eds., no. 6544 in Lecture Notes in Comput. Sci., 2010, pp. 143–158.

[2] ——, *Smaller decoding exponents: Ball-collision decoding*, in Advances in Cryptology - CRYPTO 2011 (Proceedings 31st Annual International Cryptology Conference, Santa Barbara CA, USA, August 14-18, 2011), P. Rogaway, ed., Lecture Notes in Comput. Sci., to appear.

Tanja Lange
Coding Theory and Cryptology
Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
tanja@hyperelliptic.org

Census of polynomials

Joachim von zur Gathen

(joint work with Raoul Blankertz, Mark Giesbrecht, Alfredo Viola, and Konstantin Ziegler)

The Prime Number Theorem and a well-known result of Gauß count (approximately or exactly) the number of prime (or irreducible) elements in $\mathbb{Z}$ or $\mathbb{F}_q[x]$. Leonard Carlitz, Stephen Cohen, and others considered this question for multivariate polynomials. The talk presents an exact formula for their number, and similarly for squareful und relatively irreducible (irreducible and not absolutely irreducible) polynomials, and approximations for the decomposable ones.

Further results deal with univariate decomposable polynomials $f = g \circ h = g(h) \in \mathbb{F}_q[x]$. The *tame case*, where the characteristic p of $\mathbb{F}_q$ does not divide $n = \deg f$, is fairly well-understood, and we obtain closely matching upper and lower bounds on the number of decomposable polynomials. In the opposite *wild case*, the bounds are less satisfactory.

We are then concerned with the easiest instance of the wild case, where $n = p^2$. Any (g, h) yields a decomposable $f = g \circ h$. We may assume g and h to have degree p and to be monic and original, that is, with constant coefficient 0. The crux of the matter is to count the number of *collisions*, where different (g, h) yield the same f. Besides the trivial case of pth powers, the additive polynomials $f = x^{p^2} + ax^p + bx$ are of interest. Mark Giesbrecht's talk reports on these. We now assume f to be not of this form.

Abhyankar introduced the *projective polynomial* $\psi = y^{p+1} - uy + u$. There is an intimate connection between collisions and the roots of ψ. As an example, take a nontrivial factorization $p - 1 = \ell m$ and a root $t \in \mathbb{F}_q^\times$ of ψ. Then

$$f = x(x^{\ell(p+1)} - ux^\ell + u)^m = (x(x^\ell - ut^{-1})^m) \circ (x(x^\ell - t)^m) = g \circ h.$$

While g and h depend on t, f does not. Thus two distinct roots of ψ yield a collision.

There is another, similar, type of collision from different roots of ψ. The main result here is that these are all possibilities, up to conjugation $(v^{-n}(x - f(w))) \circ f \circ (vx + w)$ by linear polynomials.

Work in progress is to simplify the current proof of this result, which relies on the ramification theory of function fields, and to determine exactly the number of such collisions.

Joachim von zur Gathen
B-IT, Universität Bonn
D-53113 Bonn
Germany
gathen@bit.uni-bonn.de

Bent Functions and Related Topics

Tor Helleseth

(joint work with A. Kholosha)

Bent functions were first introduced by Rothaus [2] in 1976 as binary Boolean functions $f(x) : \mathrm{GF}(2)^n \to \mathrm{GF}(2)$ with the important property of having the maximum distance to all affine functions. They are defined from the Walsh transform coefficients $S_b(f)$ for any $b \in GF(2)^n$ given by

$$S_f(b) = \sum_{x \in \mathrm{GF}(2)^n} (-1)^{f(x)+x \cdot b}$$

where $x \cdot b$ denotes the inner product between the two binary vectors.

Definition 1 *The Boolean function f is a bent function if $|S_f(b)| = \pm 2^{n/2}$ for all b in $GF(2)^n$.*

Bent functions have many applications to coding theory, cryptography and sequence designs. For many years, the focus was on the construction of binary bent functions. Bent functions can naturally be described as $f(x) = Tr_n(F(x))$, where $Tr_n()$ is the trace from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2)$, and $F(x)$ is a polynomial with coefficients in $\mathrm{GF}(2^n)$.

In 1985, Kumar, Scholtz and Welch [1] generalized bent functions to the case of an arbitrary finite field. In recent years, new results on nonbinary bent functions have appeared.

This talk gives an updated overview of some of the recent results and open problems on bent and generalized bent functions. This includes some recent constructions of weakly regular and non-weakly regular bent functions. Several connections between bent functions, difference sets, strongly regular graphs, Dickson polynomials, and exponential sums are also given.

References

[1] P. V. KUMAR, R. A. SCHOLTZ, AND L. R. WELCH, *Generalized bent functions and their properties*, J. Combin. Theory Ser. A, 40 (1985), pp. 90–107.

[2] O. S. ROTHAUS, *On "bent" functions*, J. Combinatorial Theory Ser. A, 20 (1976), pp. 300–305.

Tor Helleseth
The Selmer Center, Department of Informatics
University of Bergen
PB 7803, N-5020 Bergen
Norway
Tor.Helleseth@ii.uib.no

Finite Semifields

Olga Polverino

Semifields are algebras satisfying all the axioms for a skewfield except (possibly) associativity of multiplication. The first example of a finite semifield which is not a field was constructed by Dickson about a century ago and it is referred as *non-associative division ring*. From a geometric point of view, semifields coordinatize certain translation planes (called *semifield planes*) which are planes of Lenz–Barlotti class V. The equivalence relation with respect to which semifields are studied is the *isotopy*, introduced by A.A. Albert in 1942. This relation corresponds to the isomorphism relation between the associated translation planes.
Recently, the combination of geometric and algebraic techniques and the relationship between commutative semifields of odd order and planar DO polynomials have given new impulse to the theory and many examples of semifields have appeared in the literature. The increased number of examples have highlighted the need to distinguish, up to isotopy, the relevant families. One of the main tools used to this aim is the determination of "good" algebraic or geometric isotopy invariants (nuclei, center, associated linear set, autotopism group,....). In recent years, the most effective isotopy invariants for a finite semifield have been the associated linear set and its *nuclei*. These latter are finite fields contained in a semifield as substructures. The talk will review these results and the techniques used to obtain them.

Olga Polverino
Seconda Università degli Studi di Napoli
Dipartimento di Matematica
Via Vivaldi 43, 81100 Caserta
Italy
olga.polverino@unina2.it

Polynomials Modulo p and Some Generalizations

Michael I. Rosen

This talk will begin with an historical overview of some interesting questions regarding polynomials with rational integer coefficients. If $f(x)$ denotes such a polynomial and p is a prime, define N_p to be the number of solutions of $f(x)$ modulo p. If k is any non-negative integer less than or equal to the degree of $f(x)$ one can ask for the probability that $N_p = k$. Another question is what can be said about the average values of the numbers N_p? Suppose that $f(x)$ is irreducible. One can ask if $f(x)$ modulo p is irreducible for infinitely many p? A lot can be said about these questions by combining Galois theory with arithmetic density theorems due to Frobenius and Tchebotarev. In fact, Frobenius developed his density theorem in a successful attempt to prove an assertion of Kronecker, namely that the average value of the integers N_p is equal to the number of irreducible factors of $f(x)$.

Instead of $\mathbb{Z}[x]$, we will consider also the ring $A[x]$ where A is a polynomial ring over a finite field. Most of the results concerning above questions remain true in this new context. In particular, Kronecker's theorem remains true, and can be reformulated in a new and somewhat surprising way.

Next, we place these questions in the much wider context of Galois sets. For definiteness we will work of the rational numbers $\mathbb{Q}$. Let $\bar{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$, and let V denote a projective variety defined over $\mathbb{Q}$. A Galois set S is defined to be a finite subset of $V(\bar{\mathbb{Q}})$ which is Galois invariant. This means that the elements of S are permuted amongst themselves by the action of elements in $G_{\mathbb{Q}}$. We reformulate the questions raised for polynomials so as to apply to the category of Galois sets. We then reprove the classical theorems in this new context. One example of a Galois set is the set of roots of a polynomial with rational coefficients. Other interesting examples are intersection cycles, and points of order n in $E(\bar{\mathbb{Q}})$ where n is any positive integer and E is any abelian variety defined over $\mathbb{Q}$.

Michael I. Rosen
Brown University
michael_rosen@brown.edu

Contributed Talks

On codes over rings invariant under affine groups

Kanat Abdukhalikov

We consider extended cyclic codes of length p^n over the ring $\mathbb{Z}/p^e\mathbb{Z}$ (integers modulo p^e). Let $n = mt$. Then one can define the natural action of the group $\mathrm{AGL}_m(p^t)$ on the ambient space by permuting basic elements. Our goal is to study extended cyclic codes that are invariant under the group $\mathrm{AGL}_m(p^t)$.

The problem is well studied in case of codes over a field. Delsarte [4] gave a necessary and sufficient condition for extended cyclic codes to be invariant under the affine group $\mathrm{AGL}_m(p^t)$. Later, Berger and Charpin [3] found another condition equivalent to the one of Delsarte. In [2], we described extended cyclic codes of length p^n invariant under $\mathrm{AGL}_m(p^t)$, in terms of polynomial functions and defining sets, and gave one more necessary and sufficient condition for codes to be invariant under $\mathrm{AGL}_m(p^t)$. This condition is also generalized for codes over $\mathbb{Z}/p^e\mathbb{Z}$.

In the general case, there are no complete enumerations of such codes. In fact, only two important extremal cases, $m = 1$ and $m = n$, were studied in detail (see, for example, [1, 2]). Hou [5] presented an enumeration of invariant codes for the case $m = n/2$, but only for codes over fields. We will give a description of invariant codes over $\mathbb{Z}/p^e\mathbb{Z}$ and study their properties (duality, self-duality, etc.). Moreover, we present an enumeration and detailed investigation of invariant codes for the case $m = n/2$.

References

[1] K. ABDUKHALIKOV, *Affine invariant and cyclic codes over p-adic numbers and finite rings*, Des. Codes Cryptogr., 23 (2001), pp. 343–370.

[2] ——, *Defining sets of extended cyclic codes invariant under the affine group*, J. Pure Appl. Algebra, 196 (2005), pp. 1–19.

[3] T. P. BERGER AND P. CHARPIN, *The permutation group of affine-invariant extended cyclic codes*, IEEE Trans. Inform. Theory, 42 (1996), pp. 2194–2209.

[4] P. DELSARTE, *On cyclic codes that are invariant under the general linear group*, IEEE Trans. Information Theory, IT-16 (1970), pp. 760–769.

[5] X.-D. HOU, *Enumeration of certain affine invariant extended cyclic codes*, J. Combin. Theory Ser. A, 110 (2005), pp. 71–95.

Kanat Abdukhalikov
Institute of Mathematics
Kazakhstan
abdukhalik@yahoo.com

Quasi-Hermitian varieties in $\mathrm{PG}(r, q^2)$, q even

Angela Aguglia

A *quasi-Hermitian variety* in $\mathrm{PG}(r, q^2)$ is a point set which has the same intersection numbers with respect to hyperplanes as a non-singular Hermitian variety. Obviously, a Hermitian variety is a trivial quasi–Hermitian variety. There are known to exist quasi–Hermitian varieties which are not Hermitian; see [1], [2].

Using a procedure similar to that used in [1], a new example of a quasi–Hermitian variety $\mathcal{V}$ in $\mathrm{PG}(r, q^2)$, q an odd power of 2, is provided. In higher-dimensional spaces, $\mathcal{V}$ can be viewed as a generalization of the Buekenhout-Tits unital in the Desarguesian plane.

References

[1] A. AGUGLIA, A. COSSIDENTE, AND G. KORCHMÁROS, On quasi-Hermitian varieties, submitted.

[2] S. DE WINTER AND J. SCHILLEWAERT, *A note on quasi-Hermitian varieties and singular quasi-quadrics*, Bull. Belg. Math. Soc. Simon Stevin, 17 (2010), pp. 911–918.

Angela Aguglia
Politecnico di Bari
Italy
aguglia@poliba.it

Discrete Fourier Transform Based Multiplication for Elliptic Curve Cryptography

Selçuk Baktır

A. Schönhage and V. Strassen's approach [2] based on the discrete Fourier transform (DFT) has long had the best asymptotic complexity $O(m \log m \log\log m)$ for general multiplication of m-bit integers or $(m-1)^{st}$ degree polynomials. Martin Fürer recently improved upon this method [1], however both approaches are considered impractical for smaller operands, e.g. with less than 1024 bits, as used in elliptic curve cryptography.

In this work, we propose using the straightforward DFT to multiplication over a class of finite fields $\mathrm{GF}(p^m)$ relevant to elliptic curve cryptography and present practical cases for its efficient application. We believe that this largely neglected method may have practical performance advantages in elliptic curve cryptography.

References

[1] M. FÜRER, *Faster integer multiplication*, in STOC'07—Proceedings of the 39th Annual ACM Symposium on Theory of Computing, ACM, New York, 2007, pp. 57–66.

[2] A. SCHÖNHAGE AND V. STRASSEN, *Schnelle Multiplikation grosser Zahlen*, Computing (Arch. Elektron. Rechnen), 7 (1971), pp. 281–292.

Selçuk Baktır
TÜBİTAK BİLGEM
selcuk.baktir@uekae.tubitak.gov.tr

Projective permutation polynomials and flag-transitive linear spaces

John Bamberg

(joint work with Michael Pauley)

In 1994, Buekenhout, Delandtsheer, Doyen, Kleidman, Liebeck and Saxl announced the classification of finite flag-transitive linear spaces, with a catch; the exception being those which have an automorphism group which can be embedded into $\mathrm{A\Gamma L}(1,q)$ (for some q). The speaker, together with Michael Pauley, used certain types of projective permutation polynomials to construct new finite flag-transitive linear spaces. This talk will be an overview of the subject.

John Bamberg
University of Western Australia
John.Bamberg@uwa.edu.au

On the solvability of some special equations over finite fields

Ioulia N. Baoulina

We discuss the solvability in $\mathbb{F}_q^n$ of equations of the form

$$(a_1x_1^{m_1} + \cdots + a_nx_n^{m_n})^k = bx_1 \cdots x_n, \qquad (*)$$

where $a_1, \ldots, a_n, b \in \mathbb{F}_q^*$, $k, m_1, \ldots, m_n$ are positive integers. Since $(*)$ always has the trivial solution $(0, \ldots, 0)$, it is of interest to give conditions for the existence of a nontrivial solution and also for the existence of a solution with $x_1 \cdots x_n \neq 0$. Using the expression for the number of solutions in terms of some special character sums, we obtain such conditions. For some values of the exponents we give more precise results. In particular, for the generalized Markoff-Hurwitz equation

$$a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_n, \quad n \geq 3 \qquad (**)$$

our results are the following.

Theorem 1 *Equation $(**)$ always has a nontrivial solution unless $q = 3$, $n = 3$ and $a_1 = a_2 = a_3$.*

Theorem 2 *Equation $(**)$ is always solvable with $x_1 \cdots x_n \neq 0$ except in the following cases:*

- *$q = 2$ and n is even;*
- *$q = 3$ and 3 divides the difference between the numbers of squares and nonsquares among $a_1, \ldots, a_n$;*
- *$q = 5$, $n = 4$, a_1, a_2, a_3, a_4 are squares in $\mathbb{F}_q$ and $b^2/a_1a_2a_3a_4$ is not a 4th power in $\mathbb{F}_q$;*
- *$q = 5$, $n = 4$, a_1, a_2, a_3, a_4 are nonsquares in $\mathbb{F}_q$ and $b^2/a_1a_2a_3a_4$ is a 4th power in $\mathbb{F}_q$.*

Ioulia N. Baoulina
Indian Statistical Institute, Bangalore Centre
India

The Nucleus-Cloud Method for Simplifying Polynomial Systems mod 2

Gregory V. Bard

The recent subject of algebraic cryptanalysis consists of breaking ciphers via a two stage process. First, one converts the cipher system into a polynomial system of equations; second, one solves the system to get some secret information, usually the key. Often the coefficient field is the field of two elements, and the only solutions desired are those entirely inside the coefficient field. This paper presents a pre-processor for such polynomial systems, to enable standard methods to solve them faster.

The systems of equations are often sparse and highly structured, yet contain hundreds if not thousands of variables. In algebraic cryptanalysis, usually only the variables associated with the secret key are of interest. The values of the other variables convey no useful information. Accordingly, one might desire to divide the variables and equations into a "nucleus" N and a "cloud" C.

A "division" of a polynomial system of equations mod 2 is a partition of the set of variables V into two sets, N and C, as well as a partition of the set of equations into two sets, E_N and E_C, that meet the following criteria: that N and C are mutually exclusive and collectively exhaustive; E_N and E_C likewise; and that E_N uses variables only found in N.

The solution to the entire system can be obtained in a three-stage process: First, the equations E_N are solved for the variables in N. Second, these values are plugged back into the equations for E_C. Third, the equations E_C are solved for the variables in C. This can be done to test the correctness of the algorithm or to solve the entire system if desired. However, for algebraic cryptanalysis, one can stop after the first stage.

Naturally, it may be difficult to establish such a division, but we show heuristics that work quite well in practice, on several ciphers. The names for N and C come from the following properties. The nucleus is usually small, highly non-linear, and difficult (opaque) while the cloud is large, linear or containing a very small number of quadratic terms, and easy (transparent).

Gregory V. Bard
The University of Wisconsin—Stout Campus
Menomonie, WI, 54751, USA
gregory.bard@ieee.org

Efficient Finite Field Arithmetic for Pairing-Based Cryptography

Naomi Benger

(joint work with Selçuk Baktır)

Pairing-Based Cryptography (PBC) is a flourishing research area. Bilinear pairings have many uses in cryptography but, most notably, the only feasible way to implement ID-based cryptography is using pairings, as described in [3].

The implementation of protocols based on pairings requires *pairing-friendly* elliptic curves. Despite such curves being rare, research has gravitated towards the few families of pairing-friendly elliptic curves which satisfy some restraints and also admit some attractive qualities; namely, favoured curves have *embedding degrees* of a special form and admit higher order twists. Though the efficiency benefits of these two properties are undeniable, the curves receiving most of the focus are not suitable for all applications or security levels. In an attempt to rekindle interest in some of the less popular families of pairing-friendly elliptic curves, we examine the underlying arithmetic necessary for computing the pairing, namely arithmetic in $\mathbb{F}_{p^k}$. We argue that these curves certainly deserve more attention than they have been receiving and could be very handy for future implementations of pairing-based protocols. Building on the work of [1, 2] we present efficient representations of the required finite fields (constructed directly and quickly given the curve parameters) and efficient inversion and multiplication operations.

References

[1] S. BAKTIR AND B. SUNAR, *Optimal tower fields*, Computers, IEEE Transactions on, 53 (2004), pp. 1231 – 1243.

[2] N. BENGER AND M. SCOTT, *Constructing tower extensions of finite fields for implementation of pairing-based cryptography*, in Arithmetic of finite fields, vol. 6087 of Lecture Notes in Comput. Sci., Springer, Berlin, 2010, pp. 180–195.

[3] D. BONEH AND M. FRANKLIN, *Identity-based encryption from the Weil pairing*, in Advances in cryptology—CRYPTO 2001 (Santa Barbara, CA), vol. 2139 of Lecture Notes in Comput. Sci., Springer, Berlin, 2001, pp. 213–229.

Naomi Benger
Université de Versailles Saint-Quentin-en-Yvelines
naomi.benger@prism.uvsq.fr

Differential properties of $x \mapsto x^{2^t-1}$

Céline Blondeau

(joint work with Anne Canteaut and Pascale Charpin)

Differential cryptanalysis is the first statistical attack proposed for breaking iterated block ciphers. This security is quantified by the so-called *differential uniformity* [2] of the Substitution box used in the cipher. An *S-box* is viewed as a function F over $\mathbb{F}_{2^n}$. More generally, the *differential spectrum* of F can be of great interest [1]. For a power function $F(x) = x^d$, we have to consider the quantities $\delta(b) = \#\{x | x^d + (x+1)^d = b\}$ only, and the differential spectrum is

$$\{\omega_0, \omega_2, \ldots, \omega_{\delta(F)}\},\ \omega_i = \#\{b \in \mathbb{F}_{2^n} | \delta(b) = i\},\ i \text{ even},\ \delta(F) = \max_b\{\delta(b)\}.$$

We provide an extensive study of the differential properties of the functions $x \mapsto x^{2^t-1}$ over $\mathbb{F}_{2^n}$, for $1 < t < n$. For such functions, we exploit the fact that the differential spectrum is determined by the number of roots of the linear polynomials

$$x^{2^t} + bx^2 + (b+1)x,\ b \in \mathbb{F}_{2^n}.$$

We exhibit a general relationship between the differential spectrum of

$$x \mapsto x^{2^t-1} \text{ and } x \mapsto x^{2^{n-t+1}-1}.$$

Thus, we establish that the differential properties of the cube function and of the inverse function are strongly connected. We further study particular subclasses. Notably, we determine the whole differential spectrum of $x \mapsto x^7$, showing that it is expressed by means of some Kloosterman sums.

We also study the differential spectrum of $x \mapsto x^{2^t-1}$ for $t \in \{\lfloor n/2 \rfloor, n+1-\lfloor n/2 \rfloor, n-2\}$. Other problems concerning other subclasses are considered.

References

[1] C. BLONDEAU, P. CHARPIN, AND A. CANTEAUT, *Differential properties of power functions.*, Int. J. Inform. and Coding Theory, 1 (2010), pp. 149–170. Special Issue dedicated to Vera Pless.

[2] K. NYBERG, *Differentially uniform mappings for cryptography*, in Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993), vol. 765 of Lecture Notes in Comput. Sci., Springer, Berlin, 1994, pp. 55–64.

Céline Blondeau
SECRET project-team - INRIA Paris-Rocquencourt
celine.blondeau@inria.fr

Designs over Finite Fields—revisited

Michael Braun

Designs over finite fields arise from ordinary designs on sets by replacing the sets by vector spaces over finite fields and orders of sets by dimensions of vector spaces, i.e. a $t-(v,k,\lambda;q)$ design is a set $\mathcal{B}$ of k-subspaces of $\mathbb{F}_q^v$ such that each t-subspace of $\mathbb{F}_q^v$ is contained in exactly λ elements of $\mathcal{B}$.

Nearly 25 years have been gone, since Simon Thomas [1] published the first results on designs over finite fields. In this talk we provide the main results, describe recent results using a computer search and discuss the parameter sets of designs over finite fields which can be deduced from a given parameter set.

Especially, we consider the supplemented, reduced and derived designs over finite fields and finally discuss the issue of defining a complemented design over a finite field. It may turn out from experiments that there exist complemented designs over finite fields.

References

[1] S. THOMAS, *Designs over finite fields*, Geom. Dedicata, 24 (1987), pp. 237–242.

Michael Braun
University of Applied Sciences, Darmstadt, Germany
Faculty of Computer Science
m.braun@fbi.h-da.de

On the algebraic degree of iterated permutations

Anne Canteaut

(joint work with Christina Boura)

Estimating the algebraic degree (*i.e.*, the multivariate degree) of a composed function $G \circ F$ when F and G are two functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ is of great importance in cryptography. Actually, most symmetric primitives are constructed by iterating a single permutation several times, and a low degree of some parts of the primitive can be exploited in some attacks, like algebraic attacks, higher-order differential attacks or cube attacks. It is known that the trivial bound $\deg(G \circ F) \leq \deg G \deg F$ can be improved in several situations: when the Walsh coefficients of F are all divisible by a high power of 2, or when F consists of several parallel applications of a smaller function [1]. Here, we exhibit a new bound on $\deg(G \circ F)$ when F is a permutation, which involves the degree of F^{-1}.

Theorem 1 *For any function F from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$, and any integer $k \leq m$, let $\delta_k(F)$ denote the maximal degree of the product of any k output coordinates of F. Then, if F is a permutation of $\mathbb{F}_2^n$, $\delta_k(F) < n - \ell$ if and only if $\delta_\ell(F^{-1}) < n - k$.*

Corollary 2 *Let F be a permutation of $\mathbb{F}_2^n$ and G be any function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$. Then,*

$$\deg(G \circ F) \leq n - \left\lfloor \frac{\log_2(n - 1 - \deg G)}{\log_2(\deg F^{-1})} \right\rfloor .$$

For instance, $F(x) = x^d$ over $\mathbb{F}_2^{35}$ with $d = \sum_{i=0}^{17} 2^{2i}$, is the inverse of a quadratic power function. Then $\deg F = 18$ but, for any linear function L, $\deg(F \circ L \circ F) \leq 30$, while all previously known bounds do not provide any relevant information. Moreover, when F consists of several parallel applications of a smaller function F_0, Theorem 1 applied to F_0 can be combined with the result of [1]. It leads to improved bounds on the degree of the inner permutations of some block ciphers and of some cryptographic hash functions submitted to the SHA-3 competition, such as ECHO and JH. For instance, we show that the degree of 4 rounds of the AES is at most 124, while it was believed that the maximum value (*i.e.*, 127) is reached after 3 rounds.

References

[1] C. BOURA, A. CANTEAUT, AND C. DE CANNIÈRE, *Higher-order differential properties of keccak and luffa*, in Fast Software Encryption, 18th International Workshop, FSE 2011 (Lyngby, 2011), vol. 6733 of Lecture Notes in Comput. Sci., Springer, 2011, p. to appear.

Anne Canteaut
INRIA Paris-Rocquencourt, project-team SECRET
Anne.Canteaut@inria.fr

On certain forms related to symplectic dual polar spaces in characteristic 2

Ilaria Cardinali

(joint work with A. Pasini)

Let V be a $2n$-dimensional vector space over a field $\mathbb{F}$ and ξ a non-degenerate alternating form defined on V. Let Δ be the building of type C_n formed by the totally ξ-isotropic subspaces of V and, for $1 \leq k \leq n$, let $\mathcal{G}_k$ and Δ_k be the k-grassmannians of $\mathrm{PG}(V)$ and Δ, embedded in $W_k = \wedge^k V$ and in a subspace $V_k \subseteq W_k$ respectively, where $\dim(V_k) = \binom{2n}{k} - \binom{2n}{k-2}$.

Focusing on the case $k = n$ and $\mathrm{char}(\mathbb{F}) = 2$, we consider two forms α and β related to the notion of 'being at non maximal distance' in $\mathcal{G}_n$ and Δ_n and we study the subspace $\mathcal{D}$ of W_n formed by vectors v such that $\alpha(v, x) = \beta(v, x)$ for every $x \in W_n$. We show how properties of $\mathcal{D}$ can be exploited to investigate the poset of $\mathrm{Sp}(2n, \mathbb{F})$-invariant subspaces of V_k for $k = n - 2i$ and $1 \leq i \leq \lfloor n/2 \rfloor$.

Ilaria Cardinali
University of Siena
cardinali3@unisi.it

Exact Divisibility of Exponential Sums over $\mathbb{F}_p$

Francis N. Castro

(joint work with Raúl Figueroa)

In this paper we compute the exact divisibility of some exponential sums in one variable over $\mathbb{F}_p$. As a by-product, we obtain families of polynomials that cannot be permutation polynomials. In particular, we compute the exact divisibility of exponential sums of the type

$$\sum_{x\in\mathbb{F}_p} \psi(ax^d + bx^{d_1})$$

$$\sum_{x\in\mathbb{F}_p} \psi(ax^d + bx^2 + cx)$$

under some natural conditions.

Francis N. Castro
Department of Mathematics, University of Puerto Rico
franciscastr@gmail.com

On the minimum number of rational points in the union of lines on the plane

Eun Ju Cheon

(joint work with Seon Jeong Kim)

Let $\mathbb{F}_q$ be the finite field of order q, q be a prime power and $PG(2,q)$ be the projective plane over $\mathbb{F}_q$. Let θ_r be the number of points in $PG(r,q)$, i.e., $\theta_r = q^r + \cdots + q + 1$. Thus we have $\theta_2 = q^2 + q + 1$ and $\theta_1 = q + 1$. We consider the interesting problem of counting the number of points on the lines in $PG(2,q)$. First we define m_k as follows: For $1 \leq k \leq \theta_2$,

$$m_k = \min\{^{\#}\left(\cup_{i=1}^{k} l_i\right) : l_1, \ldots, l_k \text{ are distinct lines}\}.$$

We can easily see $m_1 = q + 1$, $m_2 = 2q + 1$, $m_3 = 3q$ and $m_{\theta_2} = \theta_2$. By convention, we let $m_0 = 0$ and $\theta_0 = 1$. In this talk, we determine the exact values of m_k for $0 \leq k \leq \theta_2$ and $2 \leq q \leq 8$. We prove the following theorem.

Theorem 1 *For any k, $0 \leq k \leq \theta_2$, we have*

$$m_k = \theta_2 - \max\{i : m_i \leq \theta_2 - k\}.$$

By considering the dual of Theorem 8.5 in [1], we have the following.

Lemma 2 *([1, Theorem 8.5])* (1) For q odd, there are $q + 1$ distinct lines satisfying that any three of them are not concurrent.
(2) For q even, there are $q + 2$ distinct lines satisfying that any three of them are not concurrent.

By the above theorem and lemma, we can determine the exact values of m_k for $q = 2, 3$ and 4. Therefore, we concentrate on the cases $q = 5, 7$ and 8.

References

[1] J. W. P. HIRSCHFELD, *Projective geometries over finite fields*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, second ed., 1998.

Eun Ju Cheon
Research Institute of Natural Science
Gyeongsang National University, South Korea

Fast vector arithmetic over $\mathrm{GF}(3)$

Kris Coolsaet

It is common practice to use binary machine instructions to implement fast vector operations over finite fields of characteristic 2. It is less well known that the same binary machine instructions can be used to implement vector arithmetic over the field of 3 elements.

We shall discuss two ways in which this can be done. One technique uses two bit strings to represent a single vector over $\mathrm{GF}(3)$, another one uses three bit strings for every vector, sacrificing memory usage for speed. Apart from the standard operations of addition, subtraction and (scalar) multiplication, we shall also consider combined addition and subtraction (useful when generating all vectors generated by a given base) and iteration over all vectors of a given dimension. Our methods should be useful when manipulating ternary codes.

It is not so difficult to extend the same principles to other small algebraic structures, e.g., $\mathrm{GF}(5)$ or the ring $\mathbb{Z}/4\mathbb{Z}$, but the speed advantages rapidly diminish with the size of the structure.

Kris Coolsaet
Department of Applied Mathematics and Computer Science
Ghent University
Krijgslaan 281–S9, B–9000 Gent, Belgium
Kris.Coolsaet@UGent.be

On classifying planar monomials over fields of square order

Robert Coulter

(joint work with Felix Lazebnik)

Let $q = p^e$ with $p \geq 5$ a prime. For a natural number n, the monomial X^n is *planar* over $\mathbb{F}_q$ if and only if $(X+1)^n - X^n$ is a permutation polynomial over $\mathbb{F}_q$.

The problem of classifying planar monomials remains open: it is conjectured that the only n for which X^n is planar satisfy $n \equiv p^i + p^j \bmod (q-1)$. This has only been confirmed for fields of prime order or prime squared order.

In this talk, we will discuss some recent results on the classification problem for fields of square order. In particular, we prove the conjecture is true for fields of order p^4.

Robert Coulter
Department of Mathematical Sciences
University of Delaware
coulter@math.udel.edu

Additive subgroups of a finite field with large inverse-closed subsets

Bence Csajbók

For a subset S of a finite field $\mathrm{GF}(q)$ with $q = p^h$ and $p \geq 2$ prime, let $S^{-1} = \{s^{-1} \mid s \in S,\, s \neq 0\}$. If $S^{-1} \subseteq S$, S is called inverse-closed. S. Mattarei proved that an inverse-closed additive subgroup S in $\mathrm{GF}(q)$ is either a subfield or it consists of all elements $x \in \mathrm{GF}(q)$ such that $x^{p^d} + x = 0$ for some $1 \leq d < h$, see [2].

In this talk we show that an additive subgroup of $\mathrm{GF}(q)$ with a large inverse-closed subset is actually inverse-closed at all. More precisely, we give a proof of the following theorems.

Theorem 1 *Let A be an additive subgroup of $\mathrm{GF}(p^n)$. If $|A \cap A^{-1}| > \frac{2}{p}|A| - 2$, then A is inverse-closed.*

When the characteristic is 2, then the following also holds:

Theorem 2 *Let A be an additive subgroup of $\mathrm{GF}(2^n)$. If $|A \cap A^{-1}| > \frac{3}{4}|A| - 1$, then A is a subfield of $\mathrm{GF}(2^n)$.*

Examples show the sharpness of Theorem 1 when $|A| = p^2$. The proof is independent and it requires computations with certain linearized polynomials. Large inverse-closed subsets in additive subgroups play an important role in the recent study of sharply focused arcs connected with cryptography, see [1].

References

[1] G. KORCHMÁROS, V. LANZONE, AND A. SONNINO, *Projective k-arcs and 2-level secret-sharing schemes*, Des. Codes Cryptogr., (to appear).

[2] S. MATTAREI, *Inverse-closed additive subgroups of fields*, Israel J. Math., 159 (2007), pp. 343–347.

Bence Csajbók
University of Basilicata
csajbok.bence@gmail.com

Functional codes of quadrics and Hermitian varieties

Maarten De Boeck

(joint work with D. Bartoli, S. Fanali and L. Storme)

Definition 1 *([4]) Let $\mathcal{X}$ be a fixed algebraic variety in $\mathrm{PG}(n,q)$, with point set $\{P_1,\ldots,P_N\}$, where we normalize the coordinates of the points with respect tot the leftmost non-zero coordinate. Let $\mathcal{F}_h$, resp. $\mathcal{F}_{Herm}$, be the set of the homogeneous polynomials in the variables $X_0,\ldots,X_n$, of degree h, resp. of the form $(X_0\ \ldots\ X_n)A(X_0^q\ \ldots\ X_n^q)^t$ with A a Hermitian matrix, over the finite field $\mathbb{F}_q$. The functional codes $C_h(\mathcal{X})$ and $C_{Herm}(\mathcal{X})$ are given by*

$$C_h(\mathcal{X}) = \{(f(P_1),\ldots,f(P_N)) \mid f \in \mathcal{F}_h\} \cup \{0\},$$
$$C_{Herm}(\mathcal{X}) = \{(f(P_1),\ldots,f(P_N)) \mid f \in \mathcal{F}_{Herm}\} \cup \{0\}.$$

In general it is easy to determine the dimension of these functional codes. Most research about these codes hence focuses on the minimum distance.

The functional codes $C_2(\mathcal{Q})$, with $\mathcal{Q}$ a non-singular quadric, and $C_{Herm}(\mathcal{H})$, with $\mathcal{H}$ a non-singular Hermitian variety, are the functional codes that were studied first (e.g in [2]). Recently, in [3], also the code $C_2(\mathcal{H})$ was studied.

In this talk, based on [1], we present new results about the code $C_2(\mathcal{H})$ and also study the code $C_{Herm}(\mathcal{Q})$, with $\mathcal{Q}$ a non-singular quadric.

References

[1] D. Bartoli, M. De Boeck, S. Fanali, and L. Storme, *On functional codes defined by quadrics and hermitian varieties*. preprint.

[2] F. A. B. Edoukou, *Codes correcteurs d'erreurs construits à partir des variétés algébriques*, PhD thesis, Université de la Méditerranée, Aix Marseille II, 2007.

[3] A. Hallez and L. Storme, *Functional codes arising from quadric intersections with Hermitian varieties*, Finite Fields Appl., 16 (2010), pp. 27–35.

[4] G. Lachaud, *Number of points of plane sections and linear codes defined on algebraic varieties*, in Arithmetic, geometry and coding theory (Luminy, 1993), de Gruyter, Berlin, 1996, pp. 77–104.

Maarten De Boeck
Ghent University
mdeboeck@cage.ugent.be

Nonclassical hyperplanes of $\mathrm{DW}(5,q)$

Bart De Bruyn

The subspaces of the projective space $\mathrm{PG}(5,q)$ that are totally isotropic with respect to a given symplectic polarity define a polar space $\mathrm{W}(5,q)$. We denote by $\mathrm{DW}(5,q)$ the dual polar space associated with $\mathrm{W}(5,q)$. The points and lines of $\mathrm{DW}(5,q)$ are the planes and lines of $\mathrm{W}(5,q)$, with incidence being reverse containment. A *hyperplane* of $\mathrm{DW}(5,q)$ is a proper set of points of $\mathrm{DW}(5,q)$ meeting each line of $\mathrm{DW}(5,q)$ in either a singleton or the whole line. A hyperplane of $\mathrm{DW}(5,q)$ is called *classical* if it is of the form $e^{-1}(e(\mathrm{DW}(5,q)) \cap \Pi)$, where $e : \mathrm{DW}(5,q) \to \Sigma$ is a full projective embedding of $\mathrm{DW}(5,q)$ into a projective space Σ and Π is a hyperplane of Σ.

In my talk, I will present a rather complete classification for the nonclassical hyperplanes of the dual polar space $\mathrm{DW}(5,q)$.

Bart De Bruyn
Ghent University
bdb@cage.ugent.be

Linear groups and primitive polynomials over $\mathbb{F}_p$

Jean-Yves Degos

In [3], René Guitart described the group $\mathrm{GL}_3(\mathbb{F}_2)$ as a borromean group, which means that he found generators for $\mathrm{GL}_3(\mathbb{F}_2)$ which deduce themselves from each others by a circular permutation of order 3.

In this talk, we will give new generators, by means of a general method. We also introduce the notion of a n-cyclable group (see [1] and [2]) which generalizes both the notion of a cyclic group and the notion of a borromean group, and we state that the groups $\mathrm{SL}_n(\mathbb{F}_p), \mathrm{PSL}_n(\mathbb{F}_p), \mathrm{GL}_n(\mathbb{F}_p)$ and $\mathrm{PGL}_n(\mathbb{F}_p)$ are n-cyclable groups, for all $n \geq 3$ and p prime.

Finally, we formulate and discuss two conjectures:

- Conjecture A, which should characterize primitive polynomials over $\mathbb{F}_p[X]$;
- Conjecture B, which should enable to construct a n-cyclable structure for $\mathrm{GL}_n(\mathbb{F}_p)$ from a primitive polynomial over $\mathbb{F}_p[X]$ of degree n, for $(n, p) \neq (2, 2)$.

References

[1] J.-Y. DEGOS, *A table for* $\mathrm{GL}_3(\mathbb{F}_2)$, 2010, `http://jean-yves.degos.pagesperso-orange.fr/tablegl3f2.pdf`.

[2] J.-Y. DEGOS, *Linear groups over $\mathbb{F}_p$ as cyclable groups and primitive polynomials over $\mathbb{F}_p[X]$*, 2011, submitted.

[3] R. GUITART, *Klein's group as a Borromean object*, Cah. Topol. Géom. Différ. Catég., 50 (2009), pp. 144–155.

Jean-Yves Degos
Université Bordeaux I
50, rue Jouis
33400 Talence
France
jean-yves.degos@wanadoo.fr

The probability that a $\mathbb{F}_q$-hypersurface is smooth

Jeroen Demeyer

Consider the projective space $\mathbb{P}^n$ over a finite field $\mathbb{F}_q$. A *hypersurface* is defined by one homogenous equation with coefficients in $\mathbb{F}_q$. For d going to infinity, we show that the probability that a hypersurface of degree d is non-singular approaches $1/\zeta_{\mathbb{P}^n}(n+1)$. This is analogous to the well-known fact that the probability that an integer is squarefree equals $1/\zeta(2) = 6/\pi^2$.

This is a special case of the results in Bjorn Poonen's paper "Bertini Theorems over Finite Fields", where he computes the probability that the intersection of a given variety and a random hypersurface is smooth. Poonen uses the full power of algebraic geometry, whereas the special case can be proven using only elementary linear algebra and properties of finite fields.

Jeroen Demeyer
Ghent University
jdemeyer@cage.ugent.be

On quasiprimitive rank 3 permutation groups

Alice Devillers

(joint work with Michael Giudici, Cai Heng Li, Geoffrey Pearce and Cheryl E. Praeger)

While studying quotients of locally s-distance transitive groups, we encountered the following question: which multipartite complete graphs $\Gamma = K_{n[m]}$ ($n \geq 3$) and automorphism group G of Γ are such that G acts distance-transitively on Γ and the only quotients of Γ by nontrivial normal subgroups of G are trivial. That implies that G is rank 3 on the set of vertices of Γ and quasiprimitive. This led us to look for a classification of rank 3 group actions which are quasiprimitive but not primitive.

Our classification is achieved by first showing that G must be almost simple and then by classifying imprimitive almost simple permutation groups which induce a 2-transitive action on a block system and for which a block stabiliser acts 2-transitively on the block. Some of the cases involve a detailed study of classical matrix groups over finite fields.

There are two infinite families and a finite number of individual imprimitive examples. All examples but one involve projective linear groups.

When combined with earlier work of Bannai, Kantor, Liebler, Liebeck and Saxl, this yields a classification of all quasiprimitive rank 3 permutation groups.

This work will be published in the Journal of the London Mathematical Society.

Alice Devillers
The University of Western Australia
alice.devillers@uwa.edu.au

Characterization theorems for a subclass of Buekenhout-Metz unitals in $\mathrm{PG}(2, q^2)$

Nicola Durante

(joint work with Giorgio Donati and Alessandro Siciliano)

Definition 1 *([2]) A unital $\mathcal{U}$ in $\mathrm{PG}(2, q^2)$ is a set of $q^3 + 1$ points intersecting every line either in 1 or $q + 1$ points.*

The ovoidal Buekenhout-Metz unitals obtained from an ovoidal cone of $\mathrm{PG}(4, q)$ in the André/Bruck-Bose representation of $\mathrm{PG}(2, q^2)$ into $\mathrm{PG}(4, q)$ are the unique class of unitals known in $\mathrm{PG}(2, q^2)$ (see [2]). Among these unitals, there are some important subclasses such as the non-degenerate Hermitian curves and the unitals union of conics of BEHS-type constructed independently by Baker and Ebert [1] and Hirschfeld and Szőnyi [5]. In this talk, we present two characterization theorems for the Buekenhout-Metz unitals of BEHS-type.

Theorem 2 *([3]) Let G be the group of projectivities stabilizing a unital $\mathcal{U}$ in $\mathrm{PG}(2, q^2)$. If there exists a point A of $\mathcal{U}$ such that the stabilizer of A in G contains an elementary abelian p-group of order q^2 with no non-identity elations, then q is odd and $\mathcal{U}$ is a Buekenhout-Metz unital of BEHS-type.*

Theorem 3 *([4]) If a unital $\mathcal{U}$ in $\mathrm{PG}(2, q^2)$ contains three non-degenerate conics, then q is odd and $\mathcal{U}$ is a Buekenhout-Metz unital of BEHS-type.*

References

[1] R. D. Baker and G. L. Ebert, *Intersection of unitals in the Desarguesian plane*, in Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1989), vol. 70, 1990, pp. 87–94.

[2] S. Barwick and G. Ebert, *Unitals in projective planes*, Springer Monographs in Mathematics, Springer, New York, 2008.

[3] G. Donati and N. Durante, *A group theoretic characterization of buekenhout-metz unitals in* $\mathrm{PG}(2, q^2)$. submitted.

[4] N. Durante and A. Siciliano, *Unitals in* $\mathrm{PG}(2, q^2)$ *containing conics*. preprint.

[5] J. W. P. Hirschfeld and T. Szőnyi, *Sets in a finite plane with few intersection numbers and a distinguished point*, Discrete Math., 97 (1991), pp. 229–242.

Nicola Durante
University of Naples "Federico II"
ndurante@unina.it

Generating of Menon Designs and Self-dual Codes

Mariya Dzhumalieva-Stoeva

(joint work with Iliya Bouyukliev and Venelin Monev)

Some self-dual codes can be constructed via Menon designs, namely $2-(4m^2, 2m^2-m, m^2-m)$ designs, $m \in \mathcal{N}$. There exists a Menon design if and only if there exists a regular Hadamard matrix of order $4m^2$. An Hadamard matrix is regular if the sum of the elements in each row and column is constant. 20 million inequivalent Hadamard matrices of order 36 are known, but the exact number is still a matter of question ([1]).

Theorem 1 *([2]) Let A be an incidence matrix of a symmetric $2-(v,k,\lambda)$ design and $k-\lambda$ is an odd number. If $k \equiv 3(mod\ 4)$, then the code with generator matrix (I, A) is double-even self-dual $[2v, v]$ code.*

Hadamard matrices and Menon designs of order 36 give a possible construction of self-dual $[72, 36]_2$ codes. All known $[72, 36]_2$ codes have minimum distance ≤ 12. Does a $[72, 36, 16]_2$ code exist?

Our aim is to generate and classify Menon designs of order 36 and check the minimum distances of the obtained self-dual $[72, 36]_2$ codes. If minimum distance $d = 16$ is not found, at least codes with $d = 12$ could be obtained.

We generate incidence matrices of Menon designs using an orderly generation algorithm to reject isomorphic solutions. This method consists of carefully selecting a canonical representative from every isomorphism class of nodes in the search tree, and then considering only nodes in canonical form. An heuristic algorithm for finding canonical representative of $\{0,1\} - matrices$ is implemented in the process of generation. Moreover, the minimum distance condition for the corresponding codes is also implemented in the process, so that only objects of interest are generated.

References

[1] J. SEBERRY AND M. MITROULI, *Some remarks on Hadamard matrices*, Cryptogr. Commun., 2 (2010), pp. 293–306.

[2] V. TONCHEV, *Kombinatorni konfiguratsii*, Nauka i Izkustvo, Sofia, 1984. Dizaini, kodove, grafi. [Designs, codes and graphs].

Mariya Dzhumalieva-Stoeva
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
mdzhumalieva@gmail.com

An Extension Field Approach to the Twin Primes Problem over $\mathbb{F}_2$

Gove Effinger

Using the idea of "irreducibility-preserving substitutions" it is not too hard to show that over every finite field $\mathbb{F}_q$ there are infinitely many "twin" monic irreducible polynomials *provided that* $q > 2$. (For $q > 2$, two monic irreducibles are called *twins* if they differ only in their constant term.) This then settles the "Twin Primes Conjecture over Finite Fields" for all fields but $\mathbb{F}_2$. (See, for example, [1].) However, over $\mathbb{F}_2$ twins differ in their linear and quadratic terms rather than constant term, rendering the technique used for all other fields useless in this case.

We discuss here an approach, using extension fields, to the "twin primes problem over $\mathbb{F}_2$" which may prove fruitful. Let $P = x^n + d_{n-1}x^{n-1} + ... + d_1x + 1$ be an irreducible polynomial of degree n over $\mathbb{F}_2$. The extension field $\mathbb{F}_{2^n}$ can be realized as $\mathbb{F}_2[x]/ < P >$, i.e., as all polynomials of degree less than n with all operations mod P. If $\alpha \in \mathbb{F}_{2^n}$ (i.e., α is realized as a polynomial) and if $\mathbf{M}$ is the n by $n+1$ matrix $\{1, \alpha, \alpha^2, ..., \alpha^n\}$, then row reduction of $\mathbf{M}$ will result in a final column $\{c_0, c_1, ..., c_{n-1}\}$ which is the coefficients of a new monic polynomial Q over $\mathbb{F}_2$ one of whose roots is α. In particular if α lies in no proper subfields of $\mathbb{F}_{2^n}$, then Q will itself be irreducible.

We consider now the special case $\alpha = x + 1$. Since α lies in no proper subfields of $\mathbb{F}_{2^n}$ (if it did, then so would $x = (x + 1) + 1$, and then P would not be irreducible), Q is irreducible. Moreover, as a result of the row reduction process we have each coefficient c_i of Q written as a linear combination of the coefficients $\{1, d_1, d_2, ..., d_{n-1}\}$ of P. This then sets up a "twin primes over $\mathbb{F}_2$" system of linear equations $d_1 = c_1 + 1, d_2 = c_2 + 1, d_3 = c_3, d_4 = c_4, ..., d_{n-1} = c_{n-1}$. If this system has a solution, then P and Q are irreducible twins. We investigate in particular the cases $n = 2^k$ since in those cases the matrix $\mathbf{M}$ is particularly simple.

References

[1] G. EFFINGER, *Toward a complete twin primes theorem for polynomials over finite fields*, in Finite fields and applications, vol. 461 of Contemp. Math., Amer. Math. Soc., Providence, RI, 2008, pp. 103–110.

[2] G. EFFINGER, K. HICKS, AND G. L. MULLEN, *Twin irreducible polynomials over finite fields*, in Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), Springer, Berlin, 2002, pp. 94–111.

[3] ——, *Integers and polynomials: comparing the close cousins* $\mathbf{Z}$ *and* $\mathbf{F}_q[x]$, Math. Intelligencer, 27 (2005), pp. 26–34.

[4] R. LIDL AND H. NIEDERREITER, *Finite fields*, vol. 20 of Encyclopedia of Mathematics and its Applications, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn.

Gove Effinger
Skidmore College
effinger@skidmore.edu

$\mathrm{GF}(2^n)$ parallel multipliers

Haining Fan

(joint work with Prof. Yiqi Dai (Tsinghua University) &
Prof. M.A. Hasan (University of Waterloo))

Efficient $\mathrm{GF}(2^n)$ arithmetic blocks are highly desired in two fields: error-control coding and cryptosystems, especially the latter. Compared to the addition operation in $\mathrm{GF}(2^n)$, which is equivalent to a simple bitwise logical Exclusive OR operation, the multiplication operation requires a larger and a slower hardware. The existing bit parallel $\mathrm{GF}(2^n)$ multipliers may be classified into the following two categories on the basis of the number of gates used: quadratic and subquadratic space complexity multipliers. Quadratic multipliers often use the school-book multiplication algorithm, and subquadratic multipliers often use the subquadratic algorithm, e.g., Karatsuba' algorithm.

In this talk, I will summarize our work on $\mathrm{GF}(2^n)$ multipliers from 2005 to 2010. They are, to the best of our knowledge, the best results currently.

First, I will introduce the definition of the Shifted Polynomial Bases (SPB). Unlike other bases, e.g., polynomial, normal and dual bases of $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2)$ (people found these bases many years ago from pure mathematical point-of-view), the motivation for finding SPB was purely to design fast $\mathrm{GF}(2^n)$ multipliers. SPB is a good example of the balance principle of algorithm design methodology, and we have designed the fastest bit-parallel quadratic multipliers for 5 NIST-recommended binary fields for the elliptic curve digital signature algorithm (ECDSA).

Furthermore, by establishing isomorphisms between the Montgomery and the SPB multipliers, we proved that the $\mathrm{GF}(2^n)$ Montgomery algorithm can be used to perform the SPB multiplication without any changes and vice versa.

Finally, I will introduce our work on $\mathrm{GF}(2^n)$ subquadratic multipliers, including the multipliers based on the Toeplitz matrix-vector product and an improvement to Karatsuba' approach. These are also the best results currently.

Haining Fan
School of Software, Tsinghua University
China
fhn@tsinghua.edu.cn

Isometry and Automorphisms of Constant Dimension Codes

Thomas Feulner

(joint work with Anna-Lena Trautmann)

Let $\mathcal{G}(k,n)$ be the set of all subspaces of $\mathbb{F}_q^n$ of dimension k, called the Grassmannian. Constant dimension codes were introduced by Kötter and Kschischang [2] to be subsets of the Grassmanian. A constant dimension code $\mathcal{C} = \{\mathcal{U}_1, \ldots, \mathcal{U}_m\} \subset \mathcal{G}(k,n)$ is linearly isometric to another constant dimension code $\mathcal{C}'$ if there is a matrix $A \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $\{\mathcal{U}_1 A, \ldots, \mathcal{U}_m A\} = \mathcal{C}'$.

From a coding theoretical point of view one is only interested in representatives of these isometry classes. The aim of this contribution is to present an algorithm that computes a canonical form for a given linear code, i.e. a unique representative within the linear isometry class of this given code. As a byproduct, the algorithm provides the automorphism group of the code, i.e. the stabilizer of the code $\mathcal{C}$ under the group action of $\mathrm{GL}_n(\mathbb{F}_q)$.

Like many other automorphism group algorithms, cf. [3], the method is based on the partition and refinement idea and is formulated in the language of finite group actions. The approach is a generalization of the algorithm for classical linear codes, see [1]. Furthermore, the resulting algorithm could also be applied to the computation of the canonical form and the automorphism group of an additive code.

References

[1] T. FEULNER, *The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes*, Adv. Math. Commun., 3 (2009), pp. 363–383.

[2] R. KÖTTER AND F. R. KSCHISCHANG, *Coding for errors and erasures in random network coding*, IEEE Trans. Inform. Theory, 54 (2008), pp. 3579–3591.

[3] B. D. MCKAY, *Practical graph isomorphism*, Congr. Numer., 30 (1981), pp. 45–87.

Thomas Feulner
University of Bayreuth
Germany
Thomas.Feulner@uni-bayreuth.de

A General Construction for Multi-Structured Designs

Ryoh Fuji-Hara

There are several kinds of block designs each block of which have further structures. Combinatorial conditions of the further structure are delicately different depend on applications. These designs was named independently, nested design, row-and-column design, splitting design, balanced or orthogonal array, etc. The constructions have been independently researched for long time, but often used the similar techniques. A thousand and one papers for constructions of those designs have been published. We like to call the class of these designs *multi-structured designs* [1] and denote them $MD_{\mathcal{S},\mathcal{R}}$, where $\mathcal{S}$ and $\mathcal{R}$ are condition sets for its super design and sub-designs, respectively. To construct various types of multi-structued designs, the theory of cyclotomy over a finite field or some configurations on a finite geometry are commonly used offen . In the conference, we like to discus the "breaking up blocks" recursive construction which was used for PBD construction by Wilson(1972). The recursive construction works for all multi-structured designs.

References

[1] R. FUJI-HARA AND Y. MIAO, *Multi-structured designs and their applications*, in Information Security, Coding Theory and Related Combinatorics, NATO Science for Peace and Security Series - D: Information and Communication Security, D. Crnković and V. Tonchev, eds., vol. 29, IOS Press, Amsterdam, 2011, pp. 326–362.

Ryoh Fuji-Hara
University of Tsukuba
Ibaraki, Japan
fujihara@sk.tsukuba.ac.jp

Counting decompositions of additive polynomials

Mark Giesbrecht

(joint work with Joachim von zur Gathen)

We consider the problem of counting decompositions of r-additive (or linearized) polynomials over a finite field $\mathbb{F}_q$, for q a power of a prime power r. The r-additive polynomials in $\mathbb{F}_q[x]$ have the form $f = \sum_{0\le i\le d} f_i x^{r^i}$. We count the number of distinct functional decompositions of r-additive polynomials with a right component of degree r (all such components must be r-additive):

$$C(f) = \#\left\{a \in \mathbb{F}_q : \ f = g \circ (x^r + ax)\right\},$$
$$R(d) = \left\{C(f) : f \in \mathbb{F}_q[x] \text{ monic, squarefree, } r\text{-additive of degree } r^d\right\}.$$

For f as above, $C(f)$ also equals the number of roots in $\mathbb{F}_q$ of the (generalized) projective polynomial $\sum_{0\le i\le d} f_i x^{(r^i-1)/(r-1)}$ (Abhyankar, 1997). We determine $R(d)$ for all d, and in particular $R(2) = \{0, 1, 2, r+1\}$ and $R(3) = \{0, 1, 2, 3, r+1, r+2, r^2+r+1\}$. This result for $R(2)$ is consistent with the work of Bluher (2004), who also considers the inverse problem of finding formulas for the number of polynomials in each class. I.e., for given d find

$$A_i^{(d)} = \#\left\{f \in \mathbb{F}_q[x] \text{ monic, squarefree, } r\text{-additive of degree } r^d,\ C(f) = i\right\}.$$

Bluher gives formulas for $d = 2$. Using elementary and explicit methods, we demonstrate analogous formulae for $d = 3$ as follows:

$$A_0^{(3)} = \frac{\left(q^3-1\right)(r+1)\,r}{3r^2+r+1}, \qquad A_{r+1}^{(3)} = \frac{q\,(q-1)\,(q-r)}{r^3\,(r-1)},$$
$$A_1^{(3)} = \frac{(q-1)\left(q^2r^3 - r^3 + 2q^2r + 2q^2\right)}{2r^2\,(r+1)}, \qquad A_{r+2}^{(3)} = \frac{(q-1)^2\,(q-r)\,(r-2)}{r\,(r^2-1)\,(r-1)},$$
$$A_2^{(3)} = \frac{q\,(q-1)^2\,(r-2)}{r\,(r-1)}, \qquad A_{r^2+r+1}^{(3)} = \frac{\left(q-r^2\right)(q-r)\,(q-1)}{r^3\,(r-1)\,(r^2-1)\,(r^2+r+1)},$$
$$A_3^{(3)} = \frac{(q-1)^3\,(r-2)\,(r-3)}{6\,(r-1)^2}, \qquad A_i^{(3)} = 0 \text{ otherwise.}$$

We then discuss the inverse problem for more general d. For all these problems we provide computable constructions and fast algorithms (requiring time polynomial in d and $\log q$).

Mark Giesbrecht
Cheriton School of Computer Science
University of Waterloo
Waterloo, Canada
mwg@uwaterloo.ca

Ternary Kloosterman sums modulo 4

Faruk Göloğlu

(joint work with Gary McGuire and Richard Moloney)

Let $q = p^m$ and $\zeta = e^{\frac{2\pi i}{p}}$. The p-ary Kloosterman sum is defined as $\mathcal{K}(a) := \sum_{x\in\mathbb{F}_q} \chi(x^{-1} + ax)$ for any $a \in \mathbb{F}_q$, where χ is the canonical additive character of $\mathbb{F}_q$, i.e., $\chi(x) := \zeta^{\mathsf{tr}(x)}$.

In [1], Garaschuk and Lisoněk initiated the characterization of ternary Kloosterman sums (i.e., $q = 3^m$) modulo 4. They proved:

Theorem 1 *Let $q = 3^m$. The ternary Kloosterman sum on $\mathbb{F}_q$ satisfies*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod 2 & \text{if } a = 0 \text{ or } a = b^2 \text{ with } \mathsf{tr}(b) \neq 0, \\ 2m+3 \pmod 4 & \text{if } a = t^2 - t^3 \text{ for some } t \in \mathbb{F}_q \setminus \{0,1\} \\ & \text{and at least one of } t, 1-t \text{ is a square}, \\ 2m+1 \pmod 4 & \text{if } a = t^2 - t^3 \text{ for some } t \in \mathbb{F}_q \setminus \{0,1\} \\ & \text{and none of } t, 1-t \text{ is a square}. \end{cases}$$

We complete the characterization:

Theorem 2 *Let $q = 3^m$. The ternary Kloosterman sum on $\mathbb{F}_q$ satisfies*

$$\mathcal{K}(a) \equiv \begin{cases} 0 \pmod 4 & \text{if } a = 0 \text{ or } a = b^2 \text{ with } \mathsf{tr}(b) = 1 \text{ and } -b \text{ is not a square}, \\ 2 \pmod 4 & \text{if } a = b^2 \text{ with } \mathsf{tr}(b) = 1 \text{ and } -b \text{ is a square}. \end{cases}$$

We will also give similar modular results for minimal polynomials of p-ary Kloosterman sums over rational numbers where $p > 3$ (and hence $\mathcal{K}(a)$ is not necessarily an integer). For instance:

Theorem 3 *Let p be an odd prime, and let $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol. Then*

$$\prod_{i=1}^{\frac{p-1}{2}} \mathcal{K}_q(i^2 a) \equiv p \left(\frac{\mathsf{tr}(a)}{p}\right) \pmod{p^2}.$$

References

[1] K. Garaschuk and P. Lisoněk, *On ternary Kloosterman sums modulo 12*, Finite Fields Appl., 14 (2008), pp. 1083–1090.

Faruk Göloğlu
Claude Shannon Institute
University College Dublin
farukgologlu@gmail.com

On the Linear Complexity and K-Error Linear Complexity over $\mathbb{F}_p$ of the Legendre-Sidelnikov Sequences

Domingo Gomez

Let p be a prime and $\mathbb{F}_p$ be the finite field of p elements. The linear complexity (LC) of a T-periodic sequence (u_n) over $\mathbb{F}_p$ is the length L of the shortest linear recurrence

$$u_{n+L} = a_{L-1}u_{n+L-1} + \cdots + a_1u_{n+1} + a_0u_n, \qquad n \geq 0$$

The measure therefore speaks to the difficulty of generating – and perhaps analyzing – a particular sequence. This is specially important in cryptography, where unpredictability is a requisite. In [1], Stamp and Martin proposed another stronger measure of complexity, the $k-$error linear complexity, which is defined by

$$L_k(u_n) = \min_{(v_n)} L(v_n)$$

where the minimum is taken over all T-periodic sequences (v_n) which are different in at most k elements of the original sequence. The *Legendre-Sidelnikov sequence*, which was introduced in [2], is defined by

$$s_n = \begin{cases} 1 & \text{if } p|n, \\ 0 & \text{if } g^n \equiv -1 \mod p \text{ and } p \not| n, \\ \frac{1-((g^n+1)n)^{(p-1)/2}}{2} & \text{otherwise,} \end{cases}$$

where $g \in \mathbb{F}_p$ is an element of order $p-1$. In this talk, we will give the exact value for the linear complexity of the sequence and also a lower bound for the $k-$error linear complexity over $\mathbb{F}_p$.

References

[1] M. STAMP AND C. F. MARTIN, *An algorithm for the k-error linear complexity of binary sequences with period* 2^n, IEEE Trans. Inform. Theory, 39 (1993), pp. 1398–1401.

[2] M. SU AND A. WINTERHOF, *Autocorrelation of Legendre-Sidelnikov sequences*, IEEE Trans. Inform. Theory, 56 (2010), pp. 1714–1718.

Domingo Gomez
University of Cantabria
gomezd@unican.es

Counting Nilpotent Matrices over Finite Fields

Rod Gow

(Joint work with John Sheekey)

In this talk, we describe a method to determine the number of nilpotent $n \times n$ matrices over a finite field. The key idea employed is the Fitting decomposition. The main result, due originally to Philip Hall (1955), is not new, but the method seems different. It is straightforward to extend the use the Fitting decomposition to obtain recursive formulae for the number of nilpotent symmetric, skew-symmetric and hermitian matrices over a finite field, but explicit formulae for these numbers are harder to obtain. We decribe a conjectured formula for the number of nilpotent symmetric matrices over a finite field, which we believe is new.

Rod Gow
School of Mathematical Sciences
University College Dublin
Ireland
rod.gow@ucd.ie

Unitals in $\mathrm{PG}(2, q^2)$ with a large 2-point stabiliser

Luca Giuzzi

(Joint work with G. Korchmáros)

Let $\mathcal{U}$ be any unital embedded in the Desarguesian projective plane $\mathrm{PG}(2, q^2)$ and denote by M the subgroup of $\mathrm{PGL}(3, q^2)$ consisting of all linear collineations preserving $\mathcal{U}$. We prove the following result.

Theorem 1 *The unital $\mathcal{U}$ is classical if, and only if, there exist two points $P, Q \in \mathcal{U}$ such that the stabiliser $G = M_{P,Q}$ has order $q^2 - 1$.*

This settles a recent conjecture presented by G. Donati and N. Durante at Combinatorics 2010.

Luca Giuzzi
Università degli Studi di Brescia
giuzzi@ing.unibs.it

General fibre products of Kummer covers with many rational points

Burcu Gülmez Temür

(joint work with Ferruh Özbudak)

In our previous work, we studied the fibre products of two Kummer curves and calculated the number of rational points exactly and we found an example which was a record and one which was a new entry for the "Table of curves with many points" of van der Geer. In this work, we study the general fibre products of Kummer covers over finite fields with many rational points. We exactly find the number of rational points for the fibre products of Kummer covers over finite fields. We will present examples of such curves over some finite fields. The examples with fibre product of three Kummer curves are really interesting as nobody found an example of fibre product of three Kummer curves before. Some of the examples are new entries and one of them is a record for the table in the website "manypoints.org". The curves in the examples are generally used in cryptography and coding theory, that is why they are so important.

References

[1] A. GARCIA AND A. GARZON, *On Kummer covers with many rational points over finite fields*, J. Pure Appl. Algebra, 185 (2003), pp. 177–192.

[2] M. Q. KAWAKITA, *Kummer curves and their fibre products with many rational points*, Appl. Algebra Engrg. Comm. Comput., 14 (2003), pp. 55–64.

[3] F. ÖZBUDAK AND B. G. TEMÜR, *Fibre products of Kummer covers and curves with many points*, Appl. Algebra Engrg. Comm. Comput., 18 (2007), pp. 433–443.

[4] H. STICHTENOTH, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

Burcu Gülmez Temür
bgtemur@atilim.edu.tr

Pólya permanent determinant conversion problem over finite fields and beyond

Alexander Guterman

(joint work with Gregor Dolinar, Bojan Kuzma and Marko Orel)

Two important functions in matrix theory, determinant and permanent, look very similar:

$$\det A = \sum_{\sigma \in S_n} (-1)^{\sigma} a_{1\sigma(1)} \cdots a_{n\sigma(n)} \quad \text{and} \quad \operatorname{per} A = \sum_{\sigma \in S_n} a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

here $A = (a_{ij}) \in M_n(\mathbb{F})$ is an $n \times n$ matrix and S_n denotes the set of all permutations of the set $\{1, \ldots, n\}$.

While the computation of the determinant can be done in a polynomial time, it is still an open question, if there are such algorithms to compute the permanent. Due to this reason, starting from the work by Pólya, 1913, different approaches to convert the permanent into the determinant were under the intensive investigation.

A transformation T on a certain matrix set S is called a *converter on* S if $\operatorname{per} A = \det T(A)$ for all $A \in S$. A single matrix A is called *sign-convertible* if there exists a $(+1, -1)$ matrix X such that $\operatorname{per} A = \det(X \circ A)$, where $X \circ A$ is the entrywise product of matrices.

Among our results we prove the following theorem:

Theorem 1 *Suppose $n \geq 3$, and let $\mathbb{F}$ be a finite field with $\operatorname{char} \mathbb{F} \neq 2$ and of sufficiently large cardinality (which depends only on n). Then, no bijective map $T : M_n(\mathbb{F}) \to M_n(\mathbb{F})$ satisfies $\operatorname{per} A = \det T(A)$. When $n = 3$ the conclusion holds for any finite field with $\operatorname{char} \mathbb{F} \neq 2$. ([1])*

Also we investigate Gibson barriers (the maximal and minimal numbers of non-zero elements) for convertible $(0, 1)$-matrices and solve several related problems on different matrix subspaces.

Our results are illustrated by the number of examples.

References

[1] G. Dolinar, A. E. Guterman, B. Kuzma, and M. Orel, *On the Polya permanent problem over finite fields*, European J. Combin., 32 (2011), pp. 116–132.

Alexander Guterman
Moscow State University
guterman@list.ru

The limit of the Dedekind sums in function fields

Yoshinori Hamahata

Given relatively prime rational integers $c > 0$ and a, the classical Dedekind sum is defined as

$$s(a,c) = \frac{1}{4c}\sum_{k=1}^{c-1} \cot\left(\frac{\pi k}{c}\right)\cot\left(\frac{\pi k a}{c}\right).$$

It satisfies a famous relation called the reciprocity law

$$s(a,c) + s(c,a) = \frac{a^2+c^2+1-3ac}{12ac} \quad (a>0).$$

A higher generalization for the Dedekind sums is done by Zagier [2]. He established the reciprocity law for his Dedekind sums.

The purpose of my talk is to introduce some sequences of the Dedekind sums in function fields. Our Dedekind sums are very similar to ordinary Dedekind sums and higher dimensional Dedekind ones in the classical case. We establish the reciprocity law for our Dedekind sums. We also prove that the limit of a sequence of the Dedekind sums is another type of the Dedekind sum which is introduced in [1].

References

[1] A. BAYAD AND Y. HAMAHATA, *Higher dimensional dedekind sums in function fields*. preprint.

[2] D. ZAGIER, *Higher dimensional Dedekind sums*, Math. Ann., 202 (1973), pp. 149–172.

Yoshinori Hamahata
Faculty of Engineering Science
Kansai University
3-3-35 Yamate-cho, Suita-shi, Osaka 564-8680, Japan
t114001@kansai-u.ac.jp

Numbers of Latin squares of prime power orders with orthogonal mates

Kenneth Hicks

(joint work with Josh Kaisen and Gary Mullen)

The number of Latin squares (LS) of order n is known for $n \leq 11$, made possible using computers to count automorphisms [3]. Other researchers have searched for maximal sets of mutually orthogonal Latin squares (MOLS) [1], which are known for n a prime, but still unknown for other orders such as $n = 10$. There are few direct searches for the exact number of distinct sets of MOLS of a given order. This is due to the increasing complexity of algorithmic searches for sets of MOLS. One such search was published by Hedayat and Federer [2] where limits were established from embedding subsquares of order m into a LS of order $n > m$. These limits were compared with numerical counts from Norton up to order 7.

For p an odd prime, using permutations over the finite field F_p, we construct $(p-2)!$ distinct complete sets of MOLS of order p, and we conjecture that this is the maximum number of distinct complete sets of MOLS of order p. In addition, we present numerical counts for sets of MOLS of order up to $n = 8$ and show that Norton's count at order 7 is incorrect. We also present an algorithm that will allow exact numerical counts up to higher orders.

References

[1] D. A. DRAKE, G. H. J. VAN REES, AND W. D. WALLIS, *Maximal sets of mutually orthogonal Latin squares*, Discrete Math., 194 (1999), pp. 87–94.

[2] A. HEDAYAT AND W. T. FEDERER, *On embedding and enumeration of orthogonal Latin squares*, Ann. Math. Statist., 42 (1971), pp. 509–516.

[3] B. D. MCKAY AND I. M. WANLESS, *On the number of latin squares*. preprint. (`http://arXiv:0909.2101`).

Kenneth Hicks
Ohio University
hicks@ohio.edu

A bound on the number of points of a curve in projective space over a finite field

Masaaki Homma

We expand a formula we used in the first step of our proof of the modified Sziklai conjecture for plane curves [1, 2, 3] into ones in higher dimensional projective space.

Let C be a nondegenerate irreducible curve of degree d in $\mathbb{P}^r$ over $\mathbb{F}_q$, and $N_q(C)$ the number of $\mathbb{F}_q$-points of C. Then

$$N_q(C) \leq \frac{(q-1)(q^{r+1}-1)}{q(q^r-1)-r(q-1)}d.$$

When $r = 2$, this bound coincides with that in [1, Theorem 2.1].

The order-sequence is the main ingredient of the proof of this formula, like Stöhr-Voloch's theory [4], but our formula does not involve the genus of C.

References

[1] M. HOMMA AND S. J. KIM, *Around Sziklai's conjecture on the number of points of a plane curve over a finite field*, Finite Fields Appl., 15 (2009), pp. 468–474.

[2] ——, *Sziklai's conjecture on the number of points of a plane curve over a finite field II*, in Finite fields: theory and applications, vol. 518 of Contemp. Math., Amer. Math. Soc., Providence, RI, 2010, pp. 225–234.

[3] ——, *Sziklai's conjecture on the number of points of a plane curve over a finite field III*, Finite Fields Appl., 16 (2010), pp. 315–319.

[4] K.-O. STÖHR AND J. F. VOLOCH, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3), 52 (1986), pp. 1–19.

Masaaki Homma
Department of Mathematics
Kanagawa University
Yokohama 221-8686
Japan
homma@kanagawa-u.ac.jp

Maximum Rank Distance Codes and Applications

Thomas Honold

(joint work with Shengtian Yang)

Suppose m, n, k are integers with $m \geq n \geq k \geq 1$. An (m, n, k) maximum rank distance (MRD) code over $\mathbb{F}_q$ is a set $\mathcal{C}$ of q^{mk} matrices in $\mathbb{F}_q^{m\times n}$ satisfying $\mathrm{rank}(\mathbf{A} - \mathbf{B}) \geq n - k + 1$ for all $\mathbf{A}, \mathbf{B} \in \mathcal{C}$ with $\mathbf{A} \neq \mathbf{B}$.

MRD codes were introduced (for different purposes and under different names) in [1, 2, 4]. They exist for all choices of the parameters m, n, k, q. The standard construction uses linearized polynomials and may be viewed as a q-analogue of the Reed-Solomon code construction. Recently, these codes have found an application in network coding [3].

In this talk, further applications of MRD codes are considered: The construction of random matrices over finite fields suitable for random coding arguments and having small support size, and the solution of a special case of the maximal arc problem in certain matrix geometries.

References

[1] P. DELSARTE, *Bilinear forms over a finite field, with applications to coding theory*, J. Combin. Theory Ser. A, 25 (1978), pp. 226–241.

[2] È. M. GABIDULIN, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii, 21 (1985), pp. 3–16.

[3] R. KÖTTER AND F. R. KSCHISCHANG, *Coding for errors and erasures in random network coding*, IEEE Trans. Inform. Theory, 54 (2008), pp. 3579–3591.

[4] R. M. ROTH, *Maximum-rank array codes and their application to crisscross error correction*, IEEE Trans. Inform. Theory, 37 (1991), pp. 328–336. Comments by E. M. Gabidulin and Author's Reply, ibid. 38 (1992), pp. 1183.

[5] Z.-X. WAN, *Geometry of matrices*, World Scientific Publishing Co. Inc., River Edge, NJ, 1996. In memory of Professor L. K. Hua (1910–1985).

[6] S. YANG AND T. HONOLD, *Good random matrices over finite fields*. submitted.

Thomas Honold
Zhejiang University, Hangzhou
honold@zju.edu.cn

On a uniformly distributed phenomenon in matrix groups

Su Hu

(joint work with Yan Li)

We show that a classical uniformly distributed phenomenon for an element and its inverse in $(\mathbb{Z}/n\mathbb{Z})^*$ also exists in $\mathrm{GL}_n(\mathbb{F}_p)$ and $\mathrm{SL}_n(\mathbb{F}_p)$. A $\mathrm{GL}_n(\mathbb{F}_p)$ analog of the uniform distribution on modular hyperbolas has also been considered.

References

[1] J. BECK AND M. R. KHAN, *On the uniform distribution of inverses modulo n*, Period. Math. Hungar., 44 (2002), pp. 147–155.

[2] M. DAMOTA AND R. TICHY, *Sequences, Discrepancies and Applications*, vol. 1652 of Lecture Notes in Mathematics, Springer-Verlag, 1997.

[3] R. FERGUSON, C. HOFFMAN, F. LUCA, A. OSTAFE, AND I. E. SHPARLINSKI, *Some additive combinatorics problems in matrix rings*, Rev. Mat. Complut., 23 (2010), pp. 501–513.

[4] K. FORD, M. R. KHAN, I. E. SHPARLINSKI, AND C. L. YANKOV, *On the maximal difference between an element and its inverse in residue rings*, Proc. Amer. Math. Soc., 133 (2005), pp. 3463–3468.

[5] M. R. KHAN AND I. E. SHPARLINSKI, *On the maximal difference between an element and its inverse modulo n*, Period. Math. Hungar., 47 (2003), pp. 111–117.

[6] E. KOWALSKI, *Some aspects and applications of the Riemann hypothesis over finite fields*, Milan J. Math., 78 (2010), pp. 179–220.

[7] I. E. SHPARLINSKI, *Modular hyperbolas*. arXiv:1103.2879.

[8] I. E. SHPARLINSKI AND A. WINTERHOF, *On the number of distances between the coordinates of points on modular hyperbolas*, J. Number Theory, 128 (2008), pp. 1224–1230.

[9] M.-F. TSAI AND A. ZAHARESCU, *On the action of permutations on distances between values of rational functions modulo p*, Finite Fields Appl., (to appear).

[10] Z. WENPENG, *On the distribution of inverses modulo n*, J. Number Theory, 61 (1996), pp. 301–310.

[11] W. ZHANG, *On the distribution of primitive roots modulo p*, Publ. Math. Debrecen, 53 (1998), pp. 245–255.

Su Hu
Department of Mathematics
Korea Advanced Institute of Science and Technology (KAIST)
Daejeon 305-701, South Korea
suhu1982@gmail.com

Codes in LRTJ-Spaces

Sapna Jain

In [4], Jain introduced a new metric viz. LRTJ-metric on the space $Mat_{m\times s}(\mathbf{Z}_q)$, the module space of all $m \times s$ matrices with entries from the finite ring $\mathbf{Z}_q(q \geq 2)$ generalizing the classical one dimensional Lee metric [7] and the two-dimensional RT-metric [8] which further appeared in [1]. In this talk, we discuss linear codes in LRTJ spaces [4] and obtain various bounds on the parameters of array codes in LRTJ-spaces for the correction of random array errors and usual and CT-burst array errors [4, 2, 6, 3].

We also introduce the complete weight enumerator for codes in LRTJ-spaces and obtain a MacWilliams type identity [5] for the complete weight enumerator of the dual code of an array code in LRTJ-spaces.

References

[1] M. M. DEZA AND E. DEZA, *Encyclopedia of distances*, Springer-Verlag, Berlin, 2009. With 1 CD-ROM (Windows, Macintosh and UNIX).

[2] S. JAIN, *On the generalized-Lee-RT-pseudo-metric (the GLRTP-metric) array codes correcting burst errors*, Asian-Eur. J. Math., 1 (2008), pp. 121–130.

[3] ——, *Sufficient conditions for burst error identification and correction in LRTJ-spaces*, (submitted).

[4] ——, *Array codes in the generalized-lee-rt-pseudo-metric (the GLRTP-metric)*, Algebra Colloq., (to appear).

[5] ——, *Macwilliams duality in LRTJ-spaces*, Ars Combin., (to appear).

[6] S. JAIN AND K. P. SHUM, *Correction of CT burst array errors in the generalized-Lee-RT spaces*, Acta Math. Sin. (Engl. Ser.), 26 (2010), pp. 1475–1484.

[7] C. Y. LEE, *Some properties of nonbinary error-correcting codes*, IRE Trans., IT-4 (1958), pp. 77–82.

[8] M. Y. ROZENBLYUM AND M. A. TSFASMAN, *Codes for the m-metric*, Problemy Peredachi Informatsii, 33 (1997), pp. 55–63. translation in Problems Inform. Transmission 33 (1997), no. 1, 45–52.

Sapna Jain
Department of Mathematics
University of Delhi 110007
India
sapnajain@gmx.com

Decompositions of the 2-design formed by the set of planes of $\mathrm{AG}(2n, q)$ for $q = 2, 3$

Masakazu Jimbo

(joint work with Miwako Mishima and Koji Momihara)

It is well known that for a prime power q and a positive integer m, the set of t-flats in $\mathrm{AG}(m, q)$ forms a 2-design. In this talk, we are interested in just the case $t = 2$, i.e., the 2-$(q^m, q^2, \frac{q^{m-1}-1}{q-1})$ design $(V, \mathcal{B})$ formed by the set of planes (2-flats) in $\mathrm{AG}(m, q)$, where $V = \mathbb{F}_{q^m}$, the finite field of order q^m, is the set of points and $\mathcal{B}$ is the collection of blocks (planes).

For a primitive element α of $\mathbb{F}_{q^m}$, let $\sigma : x \mapsto \alpha x$ and $G = \langle \sigma \rangle$. Moreover, let $H = G \ltimes T$, where $T = \{\tau_a : x \mapsto x + a \mid a \in \mathbb{F}_{q^m}\}$ is the group of translation. Then $\mathcal{B}$ can be decomposed into block orbits $\mathcal{O}_i$ by the action of H. It is known that the 2-design formed by the set of 2-flats in $\mathrm{AG}(m, q)$ is decomposed into subdesigns $(V, \mathcal{O}_i)$ with $\lambda = 1$ or $q + 1$.

In the case of $q = 2$, Munemasa (*Geometriae Dedicata* **77** (1999), 209–213) counted the number of spreads by examining the condition that the orbits of lines of $\mathrm{PG}(2n - 1, 2)$ can be decomposed into three spreads by the action of $G_3 = \langle \sigma^3 \rangle$. His result implies that a certain kind of the above subdesigns $(V, \mathcal{O}_i)$ with $\lambda = q + 1$ can be further decomposed into subdesigns with $\lambda = 1$.

In this talk, we will show that the 3-design formed by the set of planes in $\mathrm{AG}(2n, 2)$ can be decomposed into more subdesigns than the result by Munemasa (1999).

Theorem 1 *Let $s \geq 1$ be the highest power of 3 in $2^{2n} - 1$. The 3-design formed by the set of 2-flats in $\mathrm{AG}(2n, 2)$ is decomposed into N 2-$(2^{2n}, 4, 1)$ designs and $(2^{2n-1} - 1 - N)/3$ 2-$(2^{2n}, 4, 3)$ designs, where*

$$N = \frac{(2^n + (-1)^{n+1})^2}{8} \left(1 - \left(\frac{1}{9}\right)^s\right).$$

These designs are disjoint.

Similarly, in the case of $q = 3$, we will count the number of subdesigns of the 2-design formed by the set of planes in $\mathrm{AG}(2n, 3)$ by examining the distribution of elements in cyclotomic classes by means of Jacobi sums.

Masakazu Jimbo
Nagoya University
jimbo@is.nagoya-u.ac.jp

Weight enumeration of codes from finite spaces

Relinde Jurrius

There are several variations on and generalizations of the weight enumerator of a linear code. Two of them are the set of generalized weight enumerators and the extended weight enumerator. Both completely determine each other, so it is natural to study them together.

We consider the columns of the generator matrix of a linear $[n, k]$ code as n points in a $(k-1)$-dimensional projective space. This gives us the projective system associated with the code. It does not depend on the choice of the generator matrix, and generalized equivalent codes have equivalent projective systems. This geometric structure can be used to determine the generalized weight enumerator of a code. We do this calculations for codes that have a projective system consisting of all the points in a finite affine of projective space. These codes are the q-ary Simplex code and the q-ary first order Reed-Muller code.

As a result from the geometric method we use for the weight enumeration, we also completely determine the set of supports of subcodes and words in an extension code. It turns out that the complements of supports are incidence vectors of points and finite subspaces. A similar result is known for the set of supports of higher order Reed-Muller codes. Therefore this result could be helpful in studying the dimension of a design or the weight enumeration of the higher order Reed-Muller codes.

References

[1] R. JURRIUS, *Weight enumeration of codes from finite spaces*. in preparation.

Relinde Jurrius
Eindhoven University of Technology
r.p.m.j.jurrius@tue.nl

On the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials

Giorgos N. Kapetanakis

(joint work with Theodoulos Garefalakis)

Let q be a power of an odd prime and let $\mathbb{F}_q$ be the finite field with q elements. A polynomial Q over $\mathbb{F}_q$ of degree m, satisfying $Q(X) = X^m Q(X^{-1})$ is called *self-reciprocal*. It is well-known, [1], that self-reciprocal irreducible polynomials are of even degree and are of the form $Q(X) = X^n P(X + X^{-1})$, where P is a monic irreducible polynomial of degree n, satisfying $(P|X^2 - 4) = -1$. Here $(\cdot|X^2 - 4)$ is the Jacobi symbol modulo $X^2 - 4$ in $\mathbb{F}_q[X]$.

We consider a Hansen-Mullen type problem for self-reciprocal irreducible polynomials. More precisely, given $n \geq 2$, $1 \leq k \leq n$ and $a \in \mathbb{F}_q$ we investigate the existence of a self-reciprocal monic irreducible polynomial of degree $2n$ over $\mathbb{F}_q$, with its k-th coefficient equal to a.

We use Carlitz's [1] characterization of such polynomials, and by extending Wan's [3] method and using a character sum estimate, proved in [2] we prove the following theorem.

Theorem 1 *Let $n, k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. There exists a monic, self-reciprocal irreducible polynomial Q, of degree $2n$, such that its k-th coefficient is a, if the following bound holds.*

$$q^{\frac{n-k-1}{2}} \geq \frac{16}{5}k(k+5) + \frac{1}{2}.$$

References

[1] L. CARLITZ, *Some theorems on irreducible reciprocal polynomials over a finite field*, J. Reine Angew. Math., 227 (1967), pp. 212–220.

[2] T. GAREFALAKIS, *Self-reciprocal irreducible polynomials with prescribed coefficients*, Finite Fields Appl., 17 (2011), pp. 183–193.

[3] D. WAN, *Generators and irreducible polynomials over finite fields*, Math. Comp., 66 (1997), pp. 1195–1212.

Giorgos N. Kapetanakis
University of Crete
gkapet@math.uoc.gr

A New Method for Calculating the Merit Factor of a Character Sequence

Daniel J. Katz

(joint work with Jonathan Jedwab and Kai-Uwe Schmidt)

Binary sequences with prescribed correlation properties are interesting both as mathematical objects and for applications to the theory of communications. If one identifies a sequence with the polynomial whose coefficients are the terms of that sequence, then the problem of finding binary sequences with small mean-squared aperiodic autocorrelation (large merit factor) is equivalent to the problem of finding Littlewood polynomials with small L^4 norm. There have been relatively few advances in this area in spite of repeated attacks by both pure and applied mathematicians for decades.

Sequences whose terms are given by characters over finite fields are of interest both because of their elegant construction and because they furnish families with exceptionally high asymptotic merit factor. The terms of maximal linear sequences (m-sequences) are given by additive characters over finite fields. It is known that the merit factor of an m-sequence approaches 3 as the length of the sequence tends to ∞. The terms of Legendre sequences and their cyclic shifts are given by the quadratic multiplicative characters over finite fields. Here the asymptotic merit factor is known to vary between $3/2$ and 6 as a function of the rotation; one obtains asymptotic merit factor 6 if the rotation, considered as a fraction of the length of the sequence, tends to $\pm 1/4$ as the length tends to ∞.

Recently, an appending procedure was described that, when applied to rotated Legendre sequences of moderate length, reliably produces sequences with merit factor considerably in excess of 6. Numerical evidence has been published that suggests that sequence families produced in this manner have asymptotic merit factor above $19/3$. Nevertheless, a proof that there are families of sequences with asymptotic merit factor exceeding 6 has remained elusive. Here a theoretical advance is presented which greatly simplifies this problem.

Daniel J. Katz
Department of Mathematics
Simon Fraser University
daniel_katz_2@sfu.ca

New Ring-Linear Codes from Geometric Dualization

Michael Kiermaier

(joint work with Johannes Zwanzger)

Several new constructions for ring-linear codes are given. The class of base rings are the Galois rings of characteristic 4, which include $\mathbb{Z}_4$ as its smallest and most important member. Associated with these rings are the Hjelmslev geometries, and the central tool for the construction is geometric dualization [1]. Applying it to the $\mathbb{Z}_4$-preimages of the Kerdock codes and a related class of codes we will call Teichmüller codes, we get two new infinite series of codes and compute their symmetrized weight enumerators. In some cases, residuals of these code give further interesting codes.

The generalized Gray map translates our codes into ordinary, generally non-linear block codes in the Hamming space. The obtained parameters include $(58, 2^7, 28)_2$, $(60, 2^8, 28)_2$, $(114, 2^8, 56)_2$, $(180, 2^9, 88)_2$, $(372, 2^{10}, 184)_2$ and $(1988, 2^{12}, 992)_2$ which provably have higher minimum distance than any linear code of equal size and length over an alphabet of the same size, as well as $(244, 2^9, 120)_2$, $(484, 2^{10}, 240)_2$ and $(504, 4^6, 376)_4$ where no comparable (in the above sense) linear code is known.

References

[1] T. HONOLD AND I. LANDJEV, *The dual construction for arcs in projective Hjelmslev spaces*, Adv. Math. Commun., 5 (2011), pp. 11–21.

Michael Kiermaier
Universität Bayreuth
michael.kiermaier@uni-bayreuth.de

A classification of plane curves with the maximal number of rational points

Seon Jeong Kim

(joint work with Masaaki Homma, Kanagawa University)

In [1] we proved the following

Theorem 1 [1, Theorem 3.1] *If C is a plane curve of degree $d \geq 2$ over $\mathbb{F}_q$ without $\mathbb{F}_q$-linear components, then the number of $\mathbb{F}_q$-points $N_q(C)$ is bounded by*

$$N_q(C) \leq (d-1)q + 1, \tag{1}$$

except for the curve over $\mathbb{F}_4$ defined by the equation

$$X^4 + Y^4 + Z^4 + X^2Y^2 + Y^2Z^2 + Z^2X^2 + X^2YZ + XY^2Z + XYZ^2 = 0 \tag{2}$$

In this talk, we fix a finite field $\mathbb{F}_q$ of q elements, and projective plane $\mathbb{P}^2$ over $\bar{\mathbb{F}}_q$. The set of $\mathbb{F}_q$-points of $\mathbb{P}^2$ is denoted by $\mathbb{P}^2(\mathbb{F}_q)$, and for a plane curve C, $C(\mathbb{F}_q)$ means $C \cap \mathbb{P}^2(\mathbb{F}_q)$. Our curve C may be reducible, but C has no $\mathbb{F}_q$-linear components.

It is natural to find the curves attaining the bound (1). In previous papers, we classified such curves of degree $d \geq q+1$.

In this talk, we will prove the uniqueness of a curve of degree q attaining the bound as follows;

Theorem 2 *Let $q \geq 2$ be a prime power. Let C be a plane curve over $\mathbb{F}_q$ of degree $d = q$ with $q(q-1)+1$ rational points. Then C is projectively equivalent to C_q defined by the equation*

$$C_q : \ X^q - XZ^{q-1} + X^{q-1}Y - Y^q = 0 \tag{3}$$

over $\mathbb{F}_q$.

Also we try to classify the curves of degree $q-1$ attaining the bound (1).

References

[1] M. HOMMA AND S. J. KIM, *Sziklai's conjecture on the number of points of a plane curve over a finite field III*, Finite Fields Appl., 16 (2010), pp. 315–319.

Seon Jeong Kim
Department of Mathematics and RINS
Gyeongsang National University
Jinju 660-701, Korea
skim@gnu.kr

Large 2-groups of automorphisms of curves with positive 2-rank

Gábor Korchmáros

(joint work with Massimo Giulietti)

In this talk, $\mathbb{K}$ is an algebraically closed field of characteristic 2, $\mathcal{X}$ a curve defined over $\mathbb{K}$ with genus $g \geq 2$ and 2-rank (Hasse-Witt invariant) γ, and S is a 2-subgroup of the $\mathbb{K}$-automorphism group $\mathrm{Aut}_{\mathbb{K}}(\mathcal{X})$ of $\mathcal{X}$. For $\gamma = 0$, the Stichtenoth bound is $|S| \leq 4pg^2/(p-1)$. Here, if $\mathrm{Aut}_{\mathbb{K}}(\mathcal{X})$ fixes no point of $\mathcal{X}$, then $|S| \leq pg/(p-1)$ apart from four exceptional curves, see [1]. For $\gamma > 0$, the Nakajima bound is $|S| \leq 4(g-1)$, see [3] and [2]. Let $\gamma > 0$. For every $n = 2^h \geq 8$ and $n = g - 1$, we construct a curve $\mathcal{X}$ attaining the Nakajima bound and determine its relevant properties: $\mathcal{X}$ is a bielliptic curve with $\gamma = g$, and $\mathrm{Aut}_{\mathbb{K}}(\mathcal{X})$ has a dihedral $\mathbb{K}$-automorphism group of order $4n$ which fixes no point in $\mathcal{X}$. Moreover, we provide a classification of 2-subgroups S of $\mathrm{Aut}_{\mathbb{K}}(\mathcal{X})$ with no fixed point in $\mathcal{X}$ and such that $|S| > 2(g-1)$. Finally we exhibit several related curves with explicit equations defined over a finite field.

References

[1] M. GIULIETTI AND G. KORCHMÁROS, *Algebraic curves with a large non-tame automorphism group fixing no point*, Trans. Amer. Math. Soc., 362 (2010), pp. 5983–6001.

[2] J. W. P. HIRSCHFELD, G. KORCHMÁROS, AND F. TORRES, *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008.

[3] S. NAKAJIMA, *p-ranks and automorphism groups of algebraic curves*, Trans. Amer. Math. Soc., 303 (1987), pp. 595–607.

Gábor Korchmáros
Dipartimento di Matematica e Informatica
Università degli Studi della Basilicata
Potenza (Italy)
gabor.korchmaros@unibas.it

Toward an alternate proof of a classification result in commutative semifields

Pamela Kosick

(Joint work with Robert Coulter)

A finite semifield is a non-associative division ring. Three sets associated with a semifield are the left, middle and right nuclei, the sets of elements from the semifield that associate on the left, middle or right, respectively. Semifields can be viewed as (one sided) vector spaces over any of their nuclei. Historically they have been studied in terms of their equivalent notion in projective geometry, that of Lenz-Barlotti type V planes, a special class of translation planes.

Our approach is purely algebraic; we study finite commutative semifields via polynomials over finite fields. Specifically, finite commutative semifields of odd order are in a one-to-one correspondence with planar Dembowski-Ostrom (DO) polynomials. It is well known that any proper commutative semifield dimension 2 over its middle nucleus and dimension 4 over its left nucleus is a Dickson semifield. Here we outline our work towards an alternate proof of this classification.

Pamela Kosick
Richard Stockton College of New Jersey
pamela.kosick@stockton.edu

Grothendieck dessins d'enfants over finite fields

Elena Kreĭnes

Grothendieck dessins d'enfants are connected embedded graphs of certain special structure on smooth oriented compact surfaces without the boundary, see [1, 2, 4] for the details. They are naturally connected with so-called Belyi pairs, i.e., non-constant meromorphic functions with at most 3 critical values defined on algebraic curves. Theory of Grothendieck dessins d'enfants provides new and non-trivial interrelations between various branches of mathematics and mathematical physics, see [3, 4], what attracts the attention to this subject. Belyi functions can be defined over algebraically closed fields of arbitrary characteristics, which gives raise to the notion of Grothendieck dessins d'enfants over finite fields. We plan to give some introduction to the theory containing the recent research results on dessins d'enfants over finite fields and their applications.

References

[1] E. M. KREĬNES, *Parasitic solutions of systems of equations for Belyĭ functions in Hurwitz spaces*, Uspekhi Mat. Nauk, 56 (2001), pp. 155–156. translation in *Russian Math. Surveys* 56 (2001), no. 6, 1168–1169.

[2] S. K. LANDO AND A. K. ZVONKIN, *Graphs on surfaces and their applications*, vol. 141 of Encyclopaedia of Mathematical Sciences, Springer-Verlag, Berlin, 2004. With an appendix by Don B. Zagier, Low-Dimensional Topology, II.

[3] E. LOOIJENGA, *Cellular decompositions of compactified moduli spaces of pointed curves*, in The moduli space of curves (Texel Island, 1994), vol. 129 of Progr. Math., Birkhäuser Boston, Boston, MA, 1995, pp. 369–400.

[4] G. B. SHABAT AND V. A. VOEVODSKY, *Drawing curves over number fields*, in The Grothendieck Festschrift, Vol. III, vol. 88 of Progr. Math., Birkhäuser Boston, Boston, MA, 1990, pp. 199–227.

Elena Kreĭnes
Moscow State University
elena.kreines@gmail.com

On monomial graphs and generalized quadrangles

Brian Kronenthal

Let $\mathbb{F}_q$ be a finite field, where $q = p^e$ for some odd prime p and $e \in \mathbb{N}$. Let $f, g \in \mathbb{F}_q[x, y]$ be monomials. The monomial graph $G_q(f, g)$ is a bipartite graph with vertex partition $P \cup L$, $P = \mathbb{F}_q^3 = L$, and $(x_1, x_2, x_3) \in P$ is adjacent to $[y_1, y_2, y_3] \in L$ if and only if $x_2 + y_2 = f(x_1, y_1)$ and $x_3 + y_3 = g(x_1, y_1)$.

In [2], we proved that for any $e \in \mathbb{N}$, there exists a lower bound $p_0 = p_0(e)$ such that for every prime $p \geq p_0$, all monomial graphs $G_q(f, g)$ of girth at least eight are isomorphic to $G_q(xy, xy^2)$. This bound depends only on the largest prime divisor of e, which we will denote by ϕ. For example, when $\phi = 3$, $p_0 = 5$; furthermore, $\phi = 5$ implies $p_0 = 7$, $\phi = 7$ implies $p_0 = 11$, and $\phi = 11$ implies $p_0 = 13$. The $\phi = 3$ case was proven by Dmytrenko, Lazebnik, and Williford in [1].

In this talk, I will discuss these results, as well as their impact on a potential strategy for constructing new generalized quadrangles.

References

[1] V. DMYTRENKO, F. LAZEBNIK, AND J. WILLIFORD, *On monomial graphs of girth eight*, Finite Fields Appl., 13 (2007), pp. 828–842.

[2] B. KRONENTHAL, *Monomial graphs and generalized quadrangles*, Finite Fields Appl., (submitted).

Brian Kronenthal
University of Delaware
kronenth@math.udel.edu

Explicit constructions of permutation polynomials

Gohar Kyureghyan

A non-zero element $\alpha \in \mathbb{F}_{q^n}$ is called a b-linear translator (or structure) for the mapping $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ if $f(x + u\alpha) - f(x) = ub$ holds for any $x \in \mathbb{F}_{q^n}, u \in \mathbb{F}_q$ and a fixed $b \in \mathbb{F}_q$. The following two theorems describe constructions of permutation on finite fields via linear translators.

Theorem 1 *Let $L : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-linear permutation of $\mathbb{F}_{q^n}$. Let $b \in \mathbb{F}_q$, $h : \mathbb{F}_q \to \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}$ be a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$. Then the mapping*

$$G(x) = L(x) + L(\gamma)\, h(f(x))$$

permutes $\mathbb{F}_{q^n}$ if and only if $g(u) = u + bh(u)$ permutes $\mathbb{F}_q$.

Note that Theorem 1 has two aspects: Firstly, it allows to lift a single permutation of $\mathbb{F}_q$ to a variety of permutations on an extension $\mathbb{F}_{q^n}$. Secondly, it gives a method to produce permutations from a given linear permutation of $\mathbb{F}_{q^n}$ by adding $\mathbb{F}_q$-valued mappings to it. Regarding the second aspect, it is natural to ask whether it is possible to obtain permutations starting with a non-bijective linear mapping. It is easy to see that, if the addition of an $\mathbb{F}_q$-valued mapping to an $\mathbb{F}_q$-linear mapping L yields a permutation on $\mathbb{F}_{q^n}$, then the kernel of L is at most one-dimensional. The next theorem describes permutations obtained from $\mathbb{F}_q$-linear mappings of $\mathbb{F}_{q^n}$ with one-dimensional kernels.

Theorem 2 *Let $L : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-linear mapping of $\mathbb{F}_{q^n}$ with kernel $\alpha\mathbb{F}_q$, $\alpha \neq 0$. Suppose α is a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $h : \mathbb{F}_q \to \mathbb{F}_q$ is a permutation of $\mathbb{F}_q$. Then the mapping*

$$G(x) = L(x) + \gamma\, h(f(x))$$

permutes $\mathbb{F}_{q^n}$ if and only if $b \neq 0$ and γ does not belong to the image set of L.

Theorems 1, 2 imply explicit constructions of permutation polynomials, which satisfy "additive" properties required in the applications like Cryptology or Finite Geometry.

Gohar Kyureghyan
Otto-von-Guericke University of Magdeburg
gohar.kyureghyan@ovgu.de

The Packing Problem in Projective Hjelmslev Spaces

Ivan Landjev

(joint work with Michael Kiermaier)

Let R be a finite chain ring with $|R| = q^m$ and $R/\operatorname{rad} R \cong \mathbb{F}_q$. Let $\Pi = \mathrm{PHG}(R_R^n)$ be the n-dimensional projective Hjelmslev space [1, 2]. A spread of Π of type $\lambda = (\lambda_1, \ldots, \lambda_n)$, $\lambda_1 = m$, $0 \leq \lambda_i \leq m$, is a partition of the point set of Π in subspaces of type λ. In particular, an r-spread of Π is a partition of the point set of Π in r-dimensional Hjelmslev subspaces. An r-spread of Π is called regular if its image under the natural homomorphism $\eta : R \to R/\operatorname{rad} R$ is a multiple of an r-spread of $\mathrm{PG}(n, q)$.

Similarly to the case of projective spaces over finite fields, r-spreads of Π do exist if and only if $r + 1$ divides $n + 1$ [3]. The known proofs of this result are constructive and produce regular spreads only.

In this talk, we give the first examples of non-regular line spreads of the Hjelmslev geometries over the chain rings $\mathbb{Z}_4$, $\mathbb{Z}_2[X]/(X^2)$, $\mathbb{Z}_9$, $\mathbb{Z}_3[X]/(X^2)$.

Furthermore, we consider the problem of partitioning the points of Π into subspaces that are not necessarily Hjelmslev subspaces. This is equivalent to the problem of partitioning the module R_R^n into *non-free* submodules of fixed type that meet trivially. We prove that for spreads of subspaces of certain type the necessary divisibility conditions are not sufficient.

References

[1] T. HONOLD AND I. LANDJEV, *Linear codes over finite chain rings and projective hjelmslev geometries*, in Codes over Rings. Proceedings of the CIMPA Summer School Ankara, Turkey, August 2008, P. Solé, ed., World Scientific, 2009, pp. 60–123.

[2] ——, *Codes over rings and ring geometries*, in Current Research Topics in Galois Geometry, J. De Beule and L. Storme, eds., Nova Science Publishers, 2011, pp. 159–184.

[3] I. LANDJEV, *Spreads in projective Hjelmslev geometries*, in Applied algebra, algebraic algorithms, and error-correcting codes, vol. 5527 of Lecture Notes in Comput. Sci., Springer, Berlin, 2009, pp. 186–194.

Ivan Landjev
New Bulgarian University, 21 Montevideo str,
1618 Sofia, BULGARIA
ivan@math.bas.bg

Subfield subcodes of generalized Reed–Solomon codes

Valeriy Lomakov

Let α be a primitive element of the finite field $GF(q)$, where $q = p^m$. The Fourier transform of $\mathbf{v} = (v_0, \ldots, v_{n-1})$ is the vector $\mathbf{V} = (V_0, \ldots, V_{n-1})$ whose components are given by $V_j = \sum_{i=0}^{n-1} v_i \alpha^{ij}$. The Fourier transform can be used for lower bounding the weight of $\mathbf{v}$ through the Schaub bound, the van Lint-Wilson bound. Another method for bounding is based on zeros $Z_{\mathbf{V}}$ in $\mathbf{V}$: the Roos bound, the Hartmann-Tzeng bound, and the BCH bound.

Reed-Solomon code over $GF(q)$ is $RS = \{\mathbf{c} \,|\, \mathbf{C}_j = 0,\, 0 \le j \le r-1\}$. RS has the minimum distance $d_{RS} = r+1$. A generalized Reed-Solomon code $GRS(\nu_i)$ is a code formed by componentwise multiplication of $\nu = (\nu_0, \ldots, \nu_{n-1})$ with each of the RS codewords, i.e., $GRS(\nu_i) = \{\mathbf{a} \,|\, a_i = \nu_i c_i\}$, where $\mathbf{c} \in RS$. The distance of $GRS(\nu_i)$ is the same as the distance of RS: $d_{GRS} = d_{RS}$. A subfield subcode of $GRS(\nu_i)$ is defined as follows: $A = \{\mathbf{a} = (a_0, \ldots, a_{n-1}) \mid a_i = \nu_i c_i\}$, where $a_i \in GF(p)$ and $\mathbf{c} \in RS$. Hence $d_A \ge d_{GRS} = d_{RS}$. The vector $\mathbf{a}$ is a linear combination of some basis codewords $\mathbf{a}^{<t>}$ of A, i. e., $\mathbf{a} = \sum_{t=1}^{k} \beta_t \mathbf{a}^{<t>}$.

Theorem 1 *Suppose* $\mathbf{a} = \sum_{t=1}^{k} \beta_t \mathbf{a}^{<t>} \in A$ *and suppose* $a_i^{<t>} = \nu_i c_i^{<t>}$*; then* $C_j = \sum_{t=1}^{k} \beta_t C_j^{<t>}$.

Given A, Theorem 1 provides a way to compute $\mathbf{C}$ and $Z_{\mathbf{C}}$ and gives the generator matrix of A over $GF(q)$ for algebraic encoding.

Theorem 2 *Suppose* d *is the Schaub bound or the Roos bound (or the less general bounds), which is calculated by using* $\mathbf{C}$ *or* $Z_{\mathbf{C}}$*; then* $d_A \ge d$.

In particular, Theorems 1 and 2 remain valid for alternant codes, including Goppa codes, and enable us improve the classical lower bound on the minimum distance of such a class of linear codes.

Valeriy Lomakov
Saint Petersburg State University of Aerospace Instrumentation,
Russia
vl@guap.ru

On isotopisms and strong isotopisms of commutative presemifields

Giuseppe Marino

(joint work with Olga Polverino)

Commutative presemifields in odd characteristic can be equivalently described by planar Dembowski–Ostrom (DO) polynomials and two planar DO polynomials are CCZ–equivalent if and only if the corresponding presemifields are strongly isotopic [2]. Moreover, in [3], it has been proven that two presemifields of order p^n, with p prime and n odd integer, are strongly isotopic if and only if they are isotopic. Whereas, for $n = 6$ and $p = 3$, Zhou in [5], by using MAGMA computations, has shown that the presemifields constructed in [4] and [2] are isotopic but not strongly isotopic.

In this talk, we prove that the $P(q, \ell)$ (q odd prime power and $\ell > 1$ odd) commutative semifields constructed by Bierbrauer in [1] are isotopic to some commutative presemifields constructed by Budaghyan and Helleseth in [2]. Also, we show that they are strongly isotopic if and only if $q \equiv 1 \pmod 4$. Consequently, for each $q \equiv -1 \pmod 4$ there exist isotopic commutative presemifields of order $q^{2\ell}$ ($\ell > 1$ odd) defining CCZ–inequivalent planar DO polynomials.

References

[1] J. BIERBRAUER, *Commutative semifields from projection mappings*, Des. Codes Cryptogr., (to appear).

[2] L. BUDAGHYAN AND T. HELLESETH, *New perfect nonlinear multinomials over $\mathbf{F}_{p^{2k}}$ for any odd prime p*, in Sequences and their applications—SETA 2008, vol. 5203 of Lecture Notes in Comput. Sci., Springer, Berlin, 2008, pp. 403–414.

[3] R. S. COULTER AND M. HENDERSON, *Commutative presemifields and semifields*, Adv. Math., 217 (2008), pp. 282–304.

[4] G. LUNARDON, G. MARINO, O. POLVERINO, AND R. TROMBETTI, *Symplectic semifield spreads of $pg(5, q)$ and the veronese surface*, Ricerche di Matematica, (to appear).

[5] Y. ZHOU, *A note on the isotopism of commutative semifield*, (submitted).

Giuseppe Marino
Seconda Università degli Studi di Napoli
giuseppe.marino@unina2.it

Vectorial Feedback with Carry Registers

Abdelaziz Marjane

(joint work with Mokrane Farid and Allailou Boufeldja)

In 2004[2], Mrugalski and al. have introduced the Ring mode for LFR (Linear Feedback Register). The transition function of the generated sequence $s(t)$ is given by an arbitrary square matrix T : $s(t+1) = s(t).T$. In 2009[1], Arnault and al adapted this mode to binary FCSR (Feedback with Carry Shift Register). In this paper, we introduce the ring mode for registers with carry over $\mathbb{F}_{2^n}$ and establish its basic properties. To be more precise, fix a primitive polynomial $P(X)$ of degree n over $\mathbb{F}_2$ and T a square $r \times r$ matrix with coefficients in the binary field $\mathbb{F}_{2^n} \cong \mathbb{F}_2[X]/(P(X))$. We define Feedback with Carry Registers over $\mathbb{F}_{2^n}$ of length r and transition matrix T as a sequence generator whose state is a pair $(a(t), m(t))$ where $a(t) = (a_0(t), \ldots, a_{r-1}(t)) \in (\mathbb{F}_{2^n})^r$ and $m(t) = (m_1(t), \ldots, m_r(t)) \in (\mathbb{Z}^n)^r$ and whose operation state change is given by $a(t+1) = \sigma(t)\mathtt{mod}2$ and $m(t+1) = \sigma(t)\mathtt{div}2$ where $\sigma(t) = a(t) \otimes \mathcal{T} \oplus m(t)$ with $\mathcal{T}$ a $nr \times nr$ square matrix with coefficients in $\mathbb{Z}$ associated to T in a canonical way and $\otimes$ is some matrix multiplication defined by using standard matrix multiplication and the ring structure of $\mathbb{Z}[X]/(P(X))$ (an order of the number field $\mathbb{Q}[X]/(P(X))$). We show the following structural theorem 1.

Theorem 1 *The 2-adic expansion* $\sum_{t=0}^{t=+\infty} c(t)2^t$ *where* $c(t)$ *is any binary component of* $a_i(t)$ *is equal to a rational number* $\frac{p}{q}$ *where* $q = \det(I_{rn} - 2\mathcal{T})$.

We illustrate the result with some simple examples in the quadratic case ($n = 2$) and compare with binary FCSR in Ring mode.

References

[1] F. ARNAULT, T. P. BERGER, C. LAURADOUX, M. MINIER, AND B. POUSSE, *A new approach to FCSRs*, in In Selected Areas in Cryptography - SAC 2009, vol. 5867 of Lecture Notes in Comput. Sci., 2009, pp. 433–448.

[2] G. MRUGALSKI, J. RAJSKI, AND J. TYSZER, *Ring generators - new devices for embedded test applications*, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 23 (2004), pp. 1306 – 1320.

Abdelaziz Marjane
LAGA, UMR CNRS 7539,
Université Paris 13, Villetaneuse
France
marjane@math.univ-paris13.fr

Small bias sets from extended norm-trace codes

Gretchen L. Matthews

(joint work with Justin D. Peachey)

As demonstrated by Naor and Naor [4] among others [1, 2], the construction of small bias probability spaces, or small bias sets, is connected to that of error-correcting codes. Small bias sets are probability spaces that in some sense approximate larger ones. Error-correcting codes have provided explicit constructions of such spaces. For instance, the concatenation of a Reed-Solomon code with a Hadamard code provides a now standard construction. Recently, Ben-Aroya and Ta-Shma used Hermitian codes to construct small bias sets [3]. In this talk, we consider small bias sets constructed from more general function fields and codes. Specifically, we employ the extended norm-trace function field $\mathbb{F}_{q^r}(x,y)/\mathbb{F}_{q^r}$ defined by

$$Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y) = x^u$$

where $u \in \mathbb{Z}$ is such that

$$x^u | N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x),$$

q is a power of a prime, and $r \geq 2$; here, $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}$ and $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}$ denote the trace and norm with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$. As special cases of the extended norm-trace function field, one may obtain the Hermitian function field $y^q + y = x^{q+1}$, its quotient $y^q + y = x^u$ where $u|q+1$, and the norm-trace function field given by $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y) = N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x)$. We detail the resulting small bias sets.

References

[1] N. ALON, J. BRUCK, J. NAOR, M. NAOR, AND R. ROTH, *Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs*, IEEE Transactions on Information Theory, 38 (1992), pp. 509 –516.

[2] N. ALON, O. GOLDREICH, J. HÅSTAD, AND R. PERALTA, *Simple constructions of almost k-wise independent random variables*, Random Structures Algorithms, 3 (1992), pp. 289–304.

[3] A. BEN-AROYA AND A. TA-SHMA, *Constructing small-bias sets from algebraic-geometric codes*, in 2009 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), IEEE Computer Soc., Los Alamitos, CA, 2009, pp. 191–197.

[4] J. NAOR AND M. NAOR, *Small-bias probability spaces: efficient constructions and applications*, SIAM J. Comput., 22 (1993), pp. 838–856.

Gretchen L. Matthews
Clemson University
gmatthe@clemson.edu

The Number of Rational Points On Genus 4 Hyperelliptic Supersingular Curves in Characteristic 2

Gary McGuire

(joint work with Alexey Zaytsev)

This talk concerns the possibilities for the number of $\mathbb{F}_q$-rational points N on hyperelliptic supersingular curves. The Serre refinement of the Hasse-Weil bound gives

$$|N - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor \tag{4}$$

which allows a wide range of possible values for N. The typical phenomenon for supersingular curves is that the number of points is far more restricted than the general theory allows.

To be more precise, for curves of genus less than 4, the following results are known.

Genus 1: The number of $\mathbb{F}_q$-rational points N on a supersingular genus 1 curve defined over $\mathbb{F}_q$ satisfies $N - (q+1) \in \{0, \pm\sqrt{2q}\}$, and all these occur.

Genus 2: The number of $\mathbb{F}_q$-rational points N on a hyperelliptic supersingular genus 2 curve defined over $\mathbb{F}_q$ satisfies $N - (q+1) \in \{0, \pm\sqrt{2q}\}$, and all these occur.

Genus 3: Oort showed that there are no hyperelliptic supersingular genus 3 curves in characteristic 2.

We prove the following theorem.

Theorem 1 *The number of $\mathbb{F}_q$-rational points N on a hyperelliptic supersingular genus 4 curve defined over $\mathbb{F}_q$ satisfies*

$$N - (q+1) \in \{0, \pm\sqrt{2q}, \pm 2\sqrt{2q}, \pm 4\sqrt{2q}\}$$

and all these occur.

Gary McGuire
Claude Shannon Institute
University College Dublin
gary.mcguire@ucd.ie

Linear Recurrences and Asymptotic Behavior of Exponential Sums of Symmetric Boolean Functions

Luis A. Medina

(joint work with Francis N. Castro)

The correlation between two Boolean functions of n inputs is defined as the number of times the functions agree minus the number of times they disagree all divided by 2^n, i.e.,

$$C(F_1, F_2) = \frac{1}{2^n} \sum_{x_1,\ldots,x_n \in \{0,1\}} (-1)^{F_1(x_1,\ldots,x_n)+F_2(x_1,\ldots,x_n)}.$$

In this paper we are interested in the case when F_1 and F_2 are symmetric boolean functions. Without loss of generality, we write $C(F)$ instead of $C(F_1, F_2)$, where F is a symmetric boolean function.

In [1], J. Cai et. al. computed a closed formula for the correlation between any two symmetric Boolean functions. This formula implies that $C(F)$ satisfies a homogeneous linear recurrence with integer coefficients and provides an upper bound for the degree of the minimal recurrence of this type that $C(F)$ satisfies. In this paper we give an improvement to the degree of the minimal homogeneous linear recurrence with integer coefficients satisfying by $C(F)$.

We also compute the asymptotic value of $C(F)$. In particular, we give infinite families of boolean functions that are asymptotically not balanced, i.e., $\lim_{n\to\infty} C(F) \neq 0$. In [2], T. Cusick et al. conjectured that there are no nonlinear balanced elementary symmetric polynomials except for the elementary symmetric boolean function of degree $k = 2^r$ in $2^r \cdot l - 1$ variables, where r and l are any positive integers. We prove that Cusick et al's conjecture holds for sufficiently large n. In particular, an elementary symmetric function is asymptotically not balanced if and only if its degree is not a power of 2. Finally, we study the asymtotic behavior of $C(F + G)$, where degree of G is less than 2.

References

[1] J.-Y. CAI, F. GREEN, AND T. THIERAUF, *On the correlation of symmetric functions*, Math. Systems Theory, 29 (1996), pp. 245–258.

[2] T. W. CUSICK, Y. LI, AND P. STĂNICĂ, *Balanced symmetric functions over* GF(p), IEEE Trans. Inform. Theory, 54 (2008), pp. 1304–1307.

Luis A. Medina
Department of Mathematics, University of Puerto Rico
luis.medina17@upr.edu

On a construction of p-ary bent functions

Wilfried Meidl

(joint work with Ayça Çeşmelioğlu)

A function f from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is called bent if its Fourier transform $\widehat{f}(u) = \sum_{x\in\mathbb{F}_p^n} \epsilon_p^{f(x)-u\cdot x}$, $\epsilon_p = e^{2\pi i/p}$, yields absolute value $p^{n/2}$ for all $u \in \mathbb{F}_p^n$. A function f from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is called s-plateaued if for all $u \in \mathbb{F}_p^n$ the Fourier coefficient $\widehat{f}(u)$ has absolute value $p^{(n+s)/2}$ or 0. In this presentation the following construction of bent functions from s-plateaued functions is introduced and analysed:
For each $\mathbf{a} = (a_1, a_2, \cdots, a_s) \in \mathbb{F}_p^s$, let $f_{\mathbf{a}}(x)$ be an s-plateaued function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. If $\widehat{f_{\mathbf{a}}}(u) \neq 0$ implies $\widehat{f_{\mathbf{b}}}(u) = 0$ for any $\mathbf{a}, \mathbf{b} \in \mathbb{F}_p^s, \mathbf{a} \neq \mathbf{b}$ and $u \in \mathbb{F}_p^n$, then the function $F(x, y_1, y_2, \cdots, y_s)$ from $\mathbb{F}_p^n \times \mathbb{F}_p^s = \mathbb{F}_p^{n+s}$ to $\mathbb{F}_p$ is bent, where

$$F(x, y_1, y_2, \cdots, y_s) = \sum_{\mathbf{a}\in\mathbb{F}_p^s} \frac{(-1)^s \prod_{i=1}^s y_i(y_i-1)\cdots(y_i-(p-1))}{(y_1-a_1)\cdots(y_s-a_s)} f_{\mathbf{a}}(x).$$

The analysis shows that this construction, which can be seen as a generalization of earlier ones for $p = 2$ and $s = 1$, is very fruitful in various aspects:
1. Using quadratic s-plateaued functions, (weakly) regular as well as non-weakly regular bent functions (see [1]) can be designed. In particular the first known infinite classes of non-weakly regular bent functions are obtained.
2. EA-equivalent functions have the same algebraic degree, and as we also can show, the sets of Fourier coefficients (seen as multisets) are the same, except that the multiplication of f by a nonsquare $c \in \mathbb{F}_p$ may change all signs. With these observations a large variety of inequivalent bent functions can be constructed.
3. The algebraic degree of a bent function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is upper bounded by $n(p-1)/2 + 1$ (Hou, 2004). With the above method, the first known construction of bent functions attaining this bound for $p = 3$ and odd n can be obtained.
4. From weakly regular bent functions with certain additional properties strongly regular graphs can be obtained. With the described construction, bent functions that enable the construction of strongly regular graphs can be designed.

References

[1] P. V. KUMAR, R. A. SCHOLTZ, AND L. R. WELCH, *Generalized bent functions and their properties*, J. Combin. Theory Ser. A, 40 (1985), pp. 90–107.

Wilfried Meidl
MDBF, Sabanci University Orhanli
Tuzla, 34956 Istanbul
Turkey
wmeidl@sabanciuniv.edu

Optimal Separable Codes from Projective Planes

Ying Miao

(joint work with Minquan Cheng and Lijun Ji)

Let n, M and q be positive integers, and $Q = \{0, 1, \ldots, q-1\}$. A set $\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_M\} \subseteq Q^n$ is called an (n, M, q) code and each $\mathbf{c}_i$ a codeword..

For any (n, M, q) code $\mathcal{C} \subseteq Q^n$, define

$$\mathcal{C}(i) = \{\mathbf{c}(i) \in Q \mid \mathbf{c} = (\mathbf{c}(1), \mathbf{c}(2), \ldots, \mathbf{c}(n))^T \in \mathcal{C}\}, \ \ 1 \le i \le n,$$

and for any subset of codewords $\mathcal{C}_0 \subseteq \mathcal{C}$, define the descendant code of $\mathcal{C}_0$ as

$$\mathsf{desc}(\mathcal{C}_0) = \{\mathbf{x} = (\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(n))^T \in Q^n \mid \mathbf{x}(i) \in \mathcal{C}_0(i), 1 \le i \le n\},$$

that is, $\mathsf{desc}(\mathcal{C}_0) = \mathcal{C}_0(1) \times \cdots \times \mathcal{C}_0(n)$.

Definition 1 ([2]) *Suppose that $\mathcal{C}$ is an (n, M, q) code and $t \ge 2$ is an integer. $\mathcal{C}$ is a $\overline{t}$-separable code, or $\overline{t}$-SC(n, M, q), if for any $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$ such that $|\mathcal{C}_1| \le t$, $|\mathcal{C}_2| \le t$ and $\mathcal{C}_1 \ne \mathcal{C}_2$, we have $\mathsf{desc}(\mathcal{C}_1) \ne \mathsf{desc}(\mathcal{C}_2)$.*

Separable codes are used in multimedia fingerprinting to construct fingerprints resistant to the averaging collusion attack on multimedia contents.

In this talk, we investigate the optimality of $\overline{2}$-separable codes of length $n = 2$. We show that finite projective planes can produce infinite families of optimal $\overline{2}$-separable codes of length 2.

Theorem 2 ([1]) *For any prime power p, there exist both an optimal $\overline{2}$-SC$(2, (p+1) \times (p^2 + p + 1), p^2 + p + 1)$ and an optimal $\overline{2}$-SC$(2, p^3 + 2p^2, p^2 + p)$.*

References

[1] M. CHENG, L. JI, AND Y. MIAO, *Separable codes*, IEEE Trans. Inform. Theory, (submitted).

[2] M. CHENG AND Y. MIAO, *On anti-collusion codes and detection algorithms for multimedia fingerprinting*, IEEE Trans. Inform. Theory, (to appear).

Ying Miao
Faculty of Systems and Information Engineering
University of Tsukuba, Tsukuba 305-8573, Japan
miao@sk.tsukuba.ac.jp

Multiplication groups of finite semifields and quasifields

Gábor P. Nagy

A *quasigroup* is a set Q endowed with a binary operation $x \cdot y$ such that two of the unknowns $x, y, z \in Q$ determine uniquely the third in the equation $x \cdot y = z$. *Loops* are quasigroups with a unit element. The *left and right multiplication maps* of a loop $(Q, \cdot)$ are the bijections $L_a : x \mapsto a \cdot x$ and $R_a : x \mapsto x \cdot a$, respectively. The group generated by the left and right (right) multiplication maps of a loop Q is the *(right) multiplication group*.

The set Q endowed with two binary operations $+, \cdot$ is called a right quasifield, if

(Q1) $(Q, +)$ is an abelian group with neutral element $0 \in Q$,

(Q2) $(Q \setminus \{0\}, \cdot)$ is a quasigroup,

(Q3) the right distributive law $(x + y)z = xz + yz$ holds, and,

(Q4) for each $a, b, c \in Q$ with $a \neq b$, there is a unique $x \in Q$ satisfying $xa = xb + c$.

If Q has a multiplicative unit and satisfies both distributive laws then it is called a *semifield*.

In my talk, I will present results about the structure of right multiplication groups of finite right quasifields, and, result about the structure of multiplication groups of finite semifields.

References

[1] G. P. NAGY, *On the multiplication groups of semifields*, European J. Combin., 31 (2010), pp. 18–24.

Gábor P. Nagy
University of Szeged, Hungary
nagyg@math.u-szeged.hu

On non-isomorphism problems of strongly regular graphs constructed by p-ary bent functions

Nobuo Nakagawa

We construct a graph $\Gamma(f,p)$ by using a p-ary bent function f from $GF(p^{2k})$ to $GF(p)$ in the following way. Let S be the set of non-zero squares of $GF(p)$. The vertiex set is $GF(p^{2k})$ and a vertex x is adjacent to a vertex y iff $f(x-y) \in S$.

Then it is proved that $\Gamma(f,p)$ is a strongly regular graph under some condition (A) by Chee, Tan and Zhang. Below we suppose $k=2$ and set $F := GF(p^4)$. Then $\Gamma(f,p)$ is SRG with parameters $(\frac{p(p^2+1)(p-1)}{2}, \frac{p(p^2+3)(p-2)}{4}, \frac{p(p^2-p+2)(p-1)}{4})$ if f satisfies (A) from above.

Now there are two interesting bent functions satisfying (A), one of them is $f_0(x) := Tr(x^2)$ and another one is $g_0(x) := Tr(x^2+x^{p^3+p^2-p+1})$ which is constructed by Helleseth and Kholosha.

Theorem 1 *Let p be an odd prime which is less than 20. Then the graph $\Gamma(f_0,p)$ is not isomorphic to the graph $\Gamma(g_0,p)$.*

The outline of the proof is the following. The automorphism groups of $\Gamma(f_0,p)$ and $\Gamma(g_0,p)$ contain the translation group $T := \{t_a | a \in F\}$ and the scalar multiplication group $M := \{m_\alpha | \alpha \in GF(p)^\times\}$ where $t_a(x) = x+a$ and $m_\alpha(x) = \alpha x$. Besides $Aut(\Gamma(f_0,p))$ contains the orthogonal group $G := O^-(F)$ of minus type with respect to a bilinear mapping $b(x,y) := Tr(xy)$. We note $f_0(x) = b(x,x)$. Then F has an orthogonal basis $\{u_i | 1 \le i \le 4\}$ such that $f_0(u_i) = 1$ for $i = 1,2,3$ and $f_0(u_4) = \gamma_0$ for a fixed $\gamma_0 \notin S$.

Set $\Omega(\alpha,\beta) := \{y = \sum_{i=1}^4 \beta_i u_i \in F | f_0(y) = \alpha,\ \beta = \beta_1\}$ for $\alpha \in S$ and $\beta \in F$. It holds that T is transitive on $F \cdots (1)$; $\langle G, M \rangle$ is transitive on the 1-st neighborhood of $0 \cdots (2)$; G_{u_1}(the stabilizer of u_1) is transitive on $\Omega(\alpha,\beta)$ for each $\alpha \in S,\ \beta \in F \cdots (3)$. For a triangle $\Delta(a,b,c)$, we denote the cardinality of $\{v \in F | v \text{ is adjacent to } a, b \text{ and } c\}$ by $N(\Delta(a,b,c))$. We take a triangle $\Delta(a',b',c')$ of $\Gamma(g_0,p)$. If there is an isomorphism ψ from $\Gamma(g_0,p)$ to $\Gamma(f_0,p)$, then we may asumme $\psi(a') = 0$ from (1), $\psi(b') = u_1$ from (2) and $\psi(c') = y_{\alpha,\beta}$ for $y_{\alpha,\beta} \in \Omega(\alpha,\beta)$ for some α and β from (3). Therefore if $N(\Delta(a',b',c')) \notin \{N(\Delta(0,u_1,y_{\alpha,\beta})) | \alpha \in S,\ \beta \in F\}$ for a certain $\Delta(a',b',c')$ of $\Gamma(g_0,p)$, it means the non-isomorphism between $\Gamma(f_0,p)$ and $\Gamma(g_0,p)$. We used Magma to compute $N(\Delta(0,u_1,y_{\alpha,\beta}))$ for each $\alpha \in S, \beta \in F$.

Nobuo Nakagawa
Department of Mathematics, Kinki University
nakagawa@math.kindai.ac.jp

Probabilistic Results on the Joint Linear Complexity of Multisequences

Harald Niederreiter

(joint work with M. Vielhaber and L.-P. Wang)

The joint linear complexity is a standard complexity measure for keystreams in parallelized versions of stream ciphers. The Nth joint linear complexity $L_N(\mathbf{S})$ of an m-fold multisequence $\mathbf{S} = (S_1, \ldots, S_m)$ over $\mathbb{F}_q$ is defined to be the least order of a linear recurrence relation over $\mathbb{F}_q$ that simultaneously generates the first N terms of each sequence S_j, $j = 1, \ldots, m$. In this talk we present probabilistic results on the behavior of $L_N(\mathbf{S})$ as $N \to \infty$ with respect to a canonical probability measure on the set of all m-fold multisequences over $\mathbb{F}_q$. For instance, for the expected value E_N of $L_N(\mathbf{S})$ we have

$$E_N = \frac{mN}{m+1} + O(1) \qquad \text{as } N \to \infty.$$

The results improve and generalize earlier work by Z.D. Dai, X.T. Feng, R.A. Rueppel, L.-P. Wang, and the speaker.

Harald Niederreiter
RICAM (Austria) and KFUPM (Saudi Arabia)
ghnied@gmail.com

On the Waring Problem with Dickson Polynomials in Finite Fields: a Combinatorial Approach

Alina Ostafe

(joint work with I. E. Shparlinski)

In this talk we present some recent improvements of the results of D. Gomez and A. Winterhof [2] on an analogue of the Waring problem for Dickson polynomials over $\mathbb{F}_q$, that is, the question of the existence and estimation of a positive integer s such that the equation

$$D_e(u_1, a) + \ldots + D_e(u_s, a) = c, \qquad u_1, \ldots, u_s \in \mathbb{F}_q,$$

is solvable for any $c \in \mathbb{F}_q$. In particular, we denote by $g_a(e, q)$ the smallest possible value of s with this property and put $g_a(e, q) = \infty$ if such s does not exist. The method of [2] is based on bounds of exponential sums, namely on the Weil bound and applies only when

$$\gcd(e, q^2 - 1) \le q^{1-\varepsilon}.$$

However, since recently it has become apparent that the methods of arithmetic combinatorics provide a very powerful tool for the Waring problem and lead to results which are not accessible by other methods. The question about the possibility of extending this technique to the Waring problem with Dickson polynomials has been posed in [2]. Our work [3] gives a positive answer to this. In [3] we use a result of A. Glibichuk and M. Rudnev [1] to get a fully explicit bound on $g_1(e, q)$ (note that the case of $a = 1$ is of principal interest in [2]) in arbitrary finite fields $\mathbb{F}_q$ provided that

$$\gcd(e, q^2 - 1) \le q^{2-\varepsilon}$$

and that at least one of the the following conditions is satisfied

$$\frac{q-1}{p^r - 1} \nmid e \text{ for all } r \ne m, \qquad p^{m/2} - 1 \nmid e \text{ if } k \ge 1, \qquad \frac{q+1}{(2, p+1)} \nmid e \text{ if } \ell > 1,$$

and

$$\frac{q+1}{(2, p+1)} \nmid e, \qquad \frac{q+1}{p^r + 1} \nmid e \text{ for all } r \mid m,\ r < m,\ m/r \text{ odd},$$

where $q = p^m$ for a prime p and $m = 2^k \ell$ with a nonnegative integer k and a an odd integer ℓ. These conditions always hold if $q = p$.

We conclude the talk with related problems and open questions related to the Waring's problem with arbitrary polynomials.

References

[1] A. GLIBICHUK AND M. RUDNEV, *On additive properties of product sets in an arbitrary finite field*, J. Anal. Math., 108 (2009), pp. 159–170.

[2] D. GOMEZ AND A. WINTERHOF, *Waring's problem in finite fields with Dickson polynomials*, in Finite fields: theory and applications, vol. 518 of Contemp. Math., Amer. Math. Soc., Providence, RI, 2010, pp. 185–192.

[3] A. OSTAFE AND I. E. SHPARLINSKI, *On the waring problem with dickson polynomials in finite fields*, Proc. Amer. Math. Soc., (to appear).

Alina Ostafe
Macquarie University, Sydney, Australia
alina.ostafe@mq.edu.au

Two new measures for permutations: ambiguity and deficiency

Daniel Panario

(joint work with Brett Stevens, Amin Sakzad and Qiang Wang)

We introduce the concepts of weighted ambiguity and deficiency for a mapping between two finite Abelian groups of the same size. Then, we study the optimum lower bounds of these measures for permutations of an Abelian group. A construction of permutations, by modifying some permutation functions over finite fields, is given. Their ambiguity and deficiency is investigated; most of these functions are APN permutations. We show that, when they are not optimal, the Mobius function in the multiplicative group of $\mathbb{F}_q$ is closer to being optimal in ambiguity than the inverse function in the additive group of $\mathbb{F}_q$. We note that the inverse function over $\mathbb{F}_{2^8}$ is used in AES. We conclude that a twisted permutation polynomial of a finite field is again closer to being optimal in ambiguity than the APN function employed in the SAFER cryptosystem. We briefly comment on the linearity of our twisted permutation polynomials.

Daniel Panario
Carleton University
daniel@math.carleton.ca

On difference sets in high exponent 2-groups

Mario Osvin Pavčević

(joint work with Kristijan Tabak)

We investigate the existence of difference sets in particular 2-groups. Being aware of the famous necessary conditions derived from Turyn's and Ma's theorems, we are able to prove here necessary conditions for the existence of $(2^{2d+2}, 2^{2d+1}-2^d, 2^{2d}-2^d)$ difference sets, for a large class of 2-groups which are in a way complementary to the ones described by Turyn and Ma. If a 2-group possesses a normal cyclic subgroup of order greater than 2^{d+3}, where the outer elements act on the cyclic subgroup similarly as in the dihedral, semidihedral, quaternion or modular groups, then there is no difference set in such a group. Another important case covered by our main result is related to groups possessing a direct cyclic factor of order greater than 2^{d+3}. Technically, we firstly prove a useful result on how sums of 2^n-roots of unity can be annulated. That result is crucial for introducing a new concept of norm invariance. This concept gives necessary conditions when a linear combination of 2^n-roots of unity remains unchanged under homomorphism actions in the sense of the norm.

Mario Osvin Pavčević
University of Zagreb
mario.pavcevic@fer.hr

Infinite families of twisted tensor product codes

Valentina Pepe

(joint work with L. Giuzzi)

In the last few years, linear codes derived from finite geometric structures (where "derived" may assume different meanings) have been widely studied by several authors: in many cases it is possible to directly translate geometric properties into properties of the code. In [1], constacyclic codes derived from twisted tensor products of lines $PG(1, q^3)$ and of conics of $PG(2, q^2)$ are presented. In this talk, we present some infinite families of constacyclic linear codes encompassing those constructed in [1], derived from twisted tensor products of lines $PG(1, q^t)$ and of normal rational curves of $PG(d, q)$ of degree d. Furthermore, we determine the dimension and the minimum distance for all of them, by exploiting the connection between the codewords of minimum weight and the sublines $PG(1, q)$ of $PG(1, q^t)$.

References

[1] A. BETTEN, *Twisted tensor product codes*, Des. Codes Cryptogr., 47 (2008), pp. 191–219.

[2] V. PEPE, *On the algebraic variety $\mathcal{V}_{r,t}$*, Finite Fields Appl., 17 (2011), pp. 343–349.

Valentina Pepe
Ghent University
valepepe@cage.ugent.be

Fano subplanes in finite Figueroa planes

Bryan Petrak

It has been conjectured that all non Desarguesian projective planes contain an embedded Fano subplane. The Figueroa planes are an family of non-translation planes that are defined for both infinite orders and finite order q^3 for $q > 2$ a prime power. We will restate the problem of finding an embedded Fano subplane in finite Figueroa planes as a simpler problem of finding a root of a polynomial over a finite field. Finally we will use this approach to prove that an embedded Fano subplane can be found in all finite Figueroa planes.

Bryan Petrak
University of Delaware
petrak@math.udel.edu

On Parameters and Decoding of Subfield Subcodes of Norm-Trace Codes

Fernando L. Piñero

(joint work with Heeralal Janwa)

We present Gröbner Basis algorithms to determine the parameters (such as dimension and minimum distance) of the subfield subcodes of Norm-Trace codes, and we also discuss a decoding algorithm for these codes that helps us also to determine their minimum distance. Our results improve bounds given by Stichtenoth and others. To compute the basis for the Subfield Subcodes of Norm-Trace Codes, we use the following Gröbner Basis algorithm, which is: Compute a monomial basis for the quotient ring of the ideal $\mathcal{NT}$, Compute all p^m powers of the elements in the monomial basis, Convert the monomials to vectors and Apply the Gaussian Elimination algorithm to find the dimensions.

Definition 1 *[2] For a natural number s, we define $\mathcal{M}(s) = \{x^i y^j \mid q^{r-1}i + \frac{q^r-1}{q-1}j \leq s, 0 \leq j \leq \frac{q^r-1}{q-1}, 0 \leq i \leq q^r - 1\}$. Let $P_1, P_2, \ldots, P_n$ denote the points in $GF(q^r)^2$ which are solutions to $x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y$. We define the space $L_D(A)|GF(p^m)$ as a subspace of $L(A)$ which generates $C_L(D, A)|GF(p^m)$.*

To decode $r = (r_1, r_2, \ldots, r_n)$, we find a non zero polynomial Q which satisfies $Q(y) = Q_0 + yQ_1 + y^2Q_2 + \cdots + y^lQ_l,\ Q_i \in L(A - iG)|GF(p^m)$ and $Q(y)$ has a zero of multiplicity s in $(P_j, r_j), j = 1, 2, \ldots, n$, where A satisfies: $C_L(D, A - sQ)|GF(p^m) = \langle 0\rangle, \forall 0 \leq Q \leq D, \deg Q \geq n - \tau$ and $\Sigma \dim C(D, L - iG)|GF(p^m) > \frac{ns(s+1)}{2}$.

Theorem 2 *[1] If the second condition on A is true, then a non zero Q polynomial which satisfies the conditions of the theorem exists. If less that τ errors ocurred then $Q(f) = 0$.*

References

[1] P. Beelen and T. Høholdt, *The decoding of algebraic geometry codes*, in Advances in algebraic geometry codes, vol. 5 of Ser. Coding Theory Cryptol., World Sci. Publ., Hackensack, NJ, 2008, pp. 49–98.

[2] O. Geil, *On codes from norm-trace curves*, Finite Fields Appl., 9 (2003), pp. 351–371.

Fernando L. Piñero
UPR-RP
pinerofernando@gmail.com

Geometrically Uniform Hyperbolic Codes Derived from Graphs over Quaternion Orders

Cátia Quilles

(joint work with Reginaldo Palazzo Jr)

The existence of geometrically uniform hyperbolic error-correcting codes (GUH codes) was shown in [1]. To the best of our knowledge, an algebraic characterization of such a class of codes was not provided previously. In this paper we present the construction of GUH codes derived from graphs over quotient rings of quaternion orders. These orders are related to arithmetic Fuchsian groups Γ_8 and Γ_{12}, whose elements are edge-pairing isometries of fundamental hyperbolic polygons with 8 and 12 edges, respectively, tiling the hyperbolic plane $\mathbb{D}^2$. We also present a constructive procedure for labeling the points generated by the $\{8, 8\}$ and $\{12, 12\}$ tessellations of the Poincaré disk, and we show the geometric representation of the aforementioned codes. The main contributions in this paper are described next.

When $g = 2$, $\mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ (a non-maximal order), and $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, we have:

Theorem 1 *Let $0 \neq \alpha \in \mathcal{O}$. If the reduced norm of α is such that $Nrd(\alpha) \in \mathbb{Z}$, then $\frac{\mathcal{O}}{<\alpha>}$ has $Nrd(\alpha)^4$ elements.*

Theorem 2 *If $\beta \in \mathcal{O}$ is a right divisor of α and $Nrd(\beta) \in \mathbb{Z}$, then the left ideal generated by β, $\langle\beta\rangle \subseteq \mathcal{O}$ has $\left\{\frac{Nrd(\alpha)}{Nrd(\beta)}\right\}^4$ elements.*

For the maximal order $\mathcal{O}' = (\sqrt{2}, -1)_R$, where $R = \{\frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\sqrt{2}],\ m \in \mathbb{N}\}$, we have:

Theorem 3 *Let $\alpha \in \mathcal{O}'$. If $Nrd_R(\alpha) = 2^n$, then $\frac{\mathcal{O}'}{\langle\alpha\rangle}$ has a single element.*

Theorem 4 *Let $\alpha \in \mathcal{O}'$. If $Nrd_R(\alpha) \neq 2^n$, then $\frac{\mathcal{O}'}{\langle\alpha\rangle}$ has $Nrd_R(\alpha)^4$ elements.*

When $g = 3$, $\mathcal{O} = (\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$, with $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ and $\mathcal{O}' = (\sqrt{3}, -1)_R$, where $R = \{\frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\sqrt{3}],\ m \in \mathbb{N}\}$ the previous four theorems still hold.

References

[1] H. LAZARI AND R. PALAZZO, JR., *Geometrically uniform hyperbolic codes*, Comput. Appl. Math., 24 (2005), pp. 173–192.

Cátia Quilles
Dept Telematics, State University of Campinas, SP, Brazil
catia_quilles@hotmail.com

Spectrum results on maximal partial line spreads on non-singular quadrics

Sara Rottey

(joint work with Leo Storme)

A *partial line spread* in $\mathrm{PG}(n,q)$ is a set of pairwise disjoint lines. A partial line spread is called *maximal* when it is not contained in a larger partial line spread.

In the literature, there are several articles on spectrum results on maximal partial line spreads in $\mathrm{PG}(n,q)$, i.e., for large intervals, it is proven that for every integer k in that interval, there exists a maximal partial line spread of size k in $\mathrm{PG}(n,q)$.

Heden performed extensive work on spectrum results for maximal partial line spreads in $\mathrm{PG}(3,q)$ [2], and Gács and Szőnyi proved spectrum results on maximal partial line spreads in $\mathrm{PG}(n,q)$, $n \geq 5$ [1].

The techniques of Gács and Szőnyi have been extended to prove spectrum results on maximal partial line spreads in non-singular quadrics of $\mathrm{PG}(n,q)$. In this talk, I will present these spectrum results.

References

[1] A. GÁCS AND T. SZŐNYI, *On maximal partial spreads in* $\mathrm{PG}(n,q)$, Des. Codes Cryptogr., 29 (2003), pp. 123–129.

[2] O. HEDEN, *Maximal partial spreads and the modular* n*-queen problem. III*, Discrete Math., 243 (2002), pp. 135–150.

Sara Rottey
Ghent University
sararottey@gmail.com

Some classes of permutation polynomials and their applications in public key cryptography

Bhaba Kumar Sarma

(joint work with Rajesh Pratap Singh and Anupam Saikia)

Let $B = \{\vartheta_0, \vartheta_1, \ldots, \vartheta_{n-1}\}$ be a fixed basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. We identify $x = \sum_{i=0}^{n-1} x_i\vartheta_i \in \mathbb{F}_{2^n}$ with $(x_0, x_1, \ldots, x_{n-1})$. For an element $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_{2^n}$ the polynomial $L_\alpha(x) = \sum_{i=0}^{n-1} \alpha_i x^{2^i}$ is a linearized polynomial over $\mathbb{F}_{2^n}$. The following theorems give two classes of permutation polynomials over $\mathbb{F}_{2^n}$.

Theorem 1 *Let n be an odd positive integer. Suppose $\beta \in \mathbb{F}_{2^n}$ is of even weight and that 0 and 1 are the only roots of $L_\beta(x)$ in $\mathbb{F}_{2^n}$. Suppose k_1 and k_2 are nonnegative integers such that $\gcd(2^{k_1} + 2^{k_2}, 2^n - 1) = 1$. Let ℓ be any positive integer with $(2^{k_1} + 2^{k_2}) \cdot \ell = 1 \bmod 2^n - 1$ and γ be an element of $\mathbb{F}_{2^n}$ with $Tr(\gamma) = 1$. Then*

$$f(x) = (L_\beta(x) + \gamma)^\ell + Tr(x)$$

is a permutation polynomial of $\mathbb{F}_{2^n}$.

Theorem 2 *The polynomial $g(x) = (x^{2^{k2^r}} + x^{2^r} + \alpha)^\ell + x$ is permutation polynomial of $\mathbb{F}_{2^n}$, if $Tr(\alpha) = 1$ and $(2^{k2^r} + 2^r) \cdot \ell = 1 \bmod 2^n - 1$.*

Using the permutation polynomials in Theorem 1 and Theorem 2, we propose an efficient multivariate public key cryptosystem, called *Poly-Dragon*. The complexity and efficiency of the proposed cryptosystem is comparable to Big Dragon of Patarin [1] and other multivariate public key cryptosystems. Moreover, it seems to have overcome the insecurity of Big Dragon. Here, decryption needs only four exponentiations in the finite field $\mathbb{F}_{2^n}$, which results in much faster decryption than in the existing multivariate public key cryptosystems.

References

[1] J. PATARIN, *Asymmetric cryptography with a hidden monomial and a candidate algorithm for $\simeq 64$ bits asymmetric signatures*, in Advances in cryptology—CRYPTO '96 (Santa Barbara, CA), vol. 1109 of Lecture Notes in Comput. Sci., Springer, Berlin, 1996, pp. 45–60.

Bhaba Kumar Sarma
Indian Institute of Technology Guwahati
Guwahati, India 781039
bks@iitg.ernet.in

Anti-Codes in Terms of Berlekamp's Switching Game

Uwe Schauz

We view a linear code (subspace) $C \leq \mathbb{F}_q^n$ as a light pattern on the n-dimensional *Berlekamp Board* $\mathbb{F}_q^n$ with q^n light bulbs. The lights corresponding to elements of C are *ON*, the others are *OFF*. Then we allow axis-parallel switches of complete rows, columns, etc. We show that the dual code $C^\perp$ has a full weight vector if and only if the light pattern C cannot be switched off. Generalizations of this allow us to describe anti-codes with maximal weight δ in a similar way, or, alternatively, in terms of a switching game in projective space.

We focuss on the existence of full weight vectors. Full weight vectors are of central interest with respect to graph colorings and nowhere-zero flows of graphs. Using this connection, we will see that a graph G has a nowhere-zero k-flow if and only if the $\mathbb{Z}_k$-bond space of G cannot be switched off. It has a vertex coloring with k colors if and only if a certain corresponding code over $\mathbb{Z}_k$ cannot be switched off. Similar statements hold for Tait colorings, and for nowhere-zero points of matrices.

Introducing normal forms to equivalence classes of light patterns, we obtain new equivalents for the existence of full weight vectors in $C^\perp$. This leads to new equivalents, e.g., for the Four Color Problem, Tutte's Flow Conjectures and Jaeger's Conjecture. Two of our equivalents for colorability and existence of nowhere zero flows of graphs include as special cases results by Matiyasevich, by Balzs Szegedy, and by Onn. Alon and Tarsi's sufficient condition for vertex colorability also arrives, remarkably, as a generalized full equivalent.

Uwe Schauz
King Fahd University of Petroleum and Minerals
P.O. Box 201, Dhahran 31261, Saudi Arabia
schauz@kfupm.edu.sa

Additive decompositions induced by multiplicative characters over finite fields

Davide Schipani

(joint work with Michele Elia)

In 1952, Perron [3] showed that the quadratic residues in a field of prime order satisfy certain additive properties. This result has been generalized in different directions by Winterhof [4] in 1998 and by Monico and Elia [1, 2] in 2006 and 2010. Our contribution is to provide a further generalization concerning multiplicative quadratic and cubic characters over any finite field. In particular, recalling that a character partitions the multiplicative group of the field into cosets with respect to its kernel, we will derive the number of representations of an element as a sum of two elements belonging to two, possibly equal, given cosets. The techniques used in the derivation, involving Gauss and Jacobi sums among others, provide also a more direct and interesting approach to obtain some of the above mentioned results from the literature.

Furthermore we will show a connection, a quasi-duality, with the problem of determining how many elements can be added to each element of a subset of a coset in such a way as to obtain elements still belonging to a subset of a coset. Exact solutions for this problem are explicitly obtained in some particular cases.

References

[1] C. MONICO AND M. ELIA, *Note on an additive characterization of quadratic residues modulo p*, J. Comb. Inf. Syst. Sci., 31 (2006), pp. 209–215.

[2] ——, *An additive characterization of fibers of characters on $\mathbb{F}_p^*$*, Int. J. Algebra, 4 (2010), pp. 109–117.

[3] O. PERRON, *Bemerkungen über die Verteilung der quadratischen Reste*, Math. Z., 56 (1952), pp. 122–130.

[4] A. WINTERHOF, *On the distribution of powers in finite fields*, Finite Fields Appl., 4 (1998), pp. 43–54.

Davide Schipani
University of Zurich, Switzerland
davide.schipani@math.uzh.ch

Davenport's constant for groups with a large cyclic factor

Jan-Christoph Schlage-Puchta

(joint work with G. Bhowmik)

For a finite abelian group G, define Davenport's constant $D(G)$ to be the least n such that for every sequence $g_1, \dots, g_n$ of elements in G, there exists a subsequence $g_{i_1}, \dots, g_{i_k}$ adding up to 0. Balasubramanian and Bhowmik [1] conjectured that $D(G) \leq \frac{|G|}{k} + k - 1$ with $k = \min(\lfloor\sqrt{|G|}\rfloor, \frac{|G|}{\exp(G)})$. Here we reduce this conjecture to a combinatorial problem for vector spaces over finite fields, and solve this problem for all but finitely many vector spaces.

References

[1] R. BALASUBRAMANIAN AND G. BHOWMIK, *Upper bounds for the Davenport constant*, in Combinatorial number theory, de Gruyter, Berlin, 2007, pp. 61–69.

Jan-Christoph Schlage-Puchta
Department of Mathematics
Universiteit Gent
Gent, Belgium
jcsp@cage.ugent.be

Constant rank subspaces of symmetric and hermitian matrices over finite fields

John Sheekey

(joint work with Rod Gow, Jean-Guillaume Dumas)

In this talk we consider $\mathbb{F}_q$-subspaces of the space of $n \times n$ matrices $M_n(\mathbb{F}_q)$, symmetric matrices $S_n(\mathbb{F}_q)$, and hermitian matrices $H_n(\mathbb{F}_{q^2})$, in which the rank of non-zero elements is restricted in some way. In particular, we investigate the maximum dimension of a *constant rank* r subspace, i.e. a subspace in which every non-zero element has rank r, and present the following result:

Theorem 1 *[1] Let U be an $\mathbb{F}_q$-subspace of $H_n(\mathbb{F}_{q^2})$, of constant rank r. then*

$$\dim(U) \leq \begin{cases} r & \text{if } r \text{ is odd} \\ 2n - r & \text{if } r \text{ is even} \end{cases}$$

and there exist subspaces meeting these bounds.

References

[1] J.-G. DUMAS, R. GOW, AND J. SHEEKEY, *Rank properties of subspaces of symmetric and hermitian matrices over finite fields*, Finite Fields Appl., (to appear).

John Sheekey
University College Dublin
johnsheekey@gmail.com

The p-rank of the Jacobian of cyclotomic function fields

Daisuke Shiomi

Let $\mathbb{F}_q$ be the finite field of characteristic p. Let $k = \mathbb{F}_q(T)$ be the rational function field over $\mathbb{F}_q$. For a monic polynomial $m \in \mathbb{F}_q[T]$, let K_m be the extension of k obtained by adjoining m-th torsion elements on the Carlitz module. This field K_m is a function field analogue of cyclotomic field over $\mathbb{Q}$. For this reson, K_m is often referred to as the m-th cyclotomic function field. In this talk, we shall study the structure of the Jacobian of K_m.

We denote by J_m the Jacobian of $K_m\bar{\mathbb{F}}_q$, where $\bar{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$. For a prime l, it is well-known that the l-primary subgroup $J_m(l)$ of J_m is isomorphic to the following group:

$$J_m(l) \simeq \begin{cases} \bigoplus_{i=1}^{2g_m} \mathbb{Q}_l/\mathbb{Z}_l & \text{if } l \neq p, \\ \\ \bigoplus_{i=1}^{\lambda_m} \mathbb{Q}_p/\mathbb{Z}_p & \text{if } l = p, \end{cases}$$

where g_m is the genus of K_m, and λ_m is called the Hasse-Witt invariant of K_m.

Hayes, Kida-Murabayashi gave explicit formulas for g_m for all monic polynomial m (cf. [1]). Hence we have the l-ranks ($l \neq p$) of J_m.

On the other hand, it is more difficult to determine λ_m. In the paper [2], the author showed that $\lambda_{Q^n} = 0$ for a monic polynomial Q of degree one, and $n \geq 0$. Conversely, in this talk, we shall study conditions of $\lambda_m = 0$. Our main theorem is the following result.

Theorem 1 *We assume that $p \neq 2, 3$. Then we have $\lambda_m = 0$ if and only if $m = Q^n$ where Q is a monic polynomial of degree one, and $n \geq 0$.*

As an application of the above theorem, we give a congruence relation for the class number of K_m.

References

[1] M. KIDA AND N. MURABAYASHI, *Cyclotomic function fields with divisor class number one*, Tokyo J. Math., 14 (1991), pp. 45–56.

[2] D. SHIOMI, *On the deuring-shafarevich formula*, Tokyo J. Math, (to appear).

Daisuke Shiomi
Graduate School of Mathematics, Nagoya University
m05019e@math.nagoya-u.ac.jp

On the Existence of Codes with Two Homogeneous Weights

Alison Sneyd

(joint work with Eimear Byrne and Michael Kiermaier)

It was first shown in [4] that for any projective linear code over a finite field $GF(p^r)$ with two nonzero Hamming weights $w_1 < w_2$, there exist positive integers u and s such that $w_1 = p^s u$ and $w_2 = p^s(u+1)$. Moreover, it was shown that the Cayley graph generated by the words of a given weight of such a code is strongly regular. In [3], it was shown that for any regular projective linear code C over a finite Frobenius ring with two integral nonzero homogeneous weights $w_1 < w_2$, there is a positive integer d, a divisor of $|C|$, and positive integer u such that $w_1 = du$ and $w_2 = d(u+1)$. This simultaneously gave a new proof of the known result, first proved in [2], that any such code yields a strongly regular graph. Here, with the aid of a computer search, we apply these results to existence questions on two-weight codes with reference to the tables [1].

References

[1] A. E. BROUWER, *Tables of parameters of strongly regular graphs*. `http://www.win.tue.nl/~aeb/graphs/srg/srgtab.html`.

[2] E. BYRNE, M. GREFERATH, AND T. HONOLD, *Ring geometries, two-weight codes, and strongly regular graphs*, Des. Codes Cryptogr., 48 (2008), pp. 1–16.

[3] E. BYRNE AND A. SNEYD, *On the parameters of codes with two homogeneous weights*, Des. Codes Cryptogr., (submitted).

[4] P. DELSARTE, *Weights of linear codes and strongly regular normed spaces*, Discrete Math., 3 (1972), pp. 47–64.

Alison Sneyd
University College Dublin
alison.sneyd@ucdconnect.ie

Factorization of a Class of Polynomials

Henning Stichtenoth

(joint work with Alev Topuzoğlu)

The well-known product formula

$$x^{q^r} - x = \prod \{\, p(x) \in \mathbb{F}_q[x] \mid p(x) \text{ is irreducible, monic and } \deg p(x) \mid r \,\} \qquad (5)$$

is the basis for counting the number of irreducible polynomials over $\mathbb{F}_q$ of given degree. A similar formula due to H. Meyn [2] holds for self-reciprocal monic irreducible (briefly *srim*) polynomials over $\mathbb{F}_q$:

$$x^{q^r+1} - 1 = \prod \{\, p(x) \in \mathbb{F}_q[x] \mid p(x) \text{ is srim, } \deg p = 2k,\ k \mid r \text{ and } r/k \text{ is odd} \,\} \qquad (6)$$

From this identity one obtains again a formula for the number of srim polynomials of given degree.

Our aim is to generalize these results to a wider class of polynomials over $\mathbb{F}_q$ as follows. For $a, b, c, d \in \mathbb{F}_q$ with $ad - bc \neq 0$, we define

$$F_r(x) := bx^{q^r+1} - ax^{q^r} + dx - c\,, \quad \text{for all } r \geq 0\,. \qquad (7)$$

Our results include that the irreducible factors of $F_r(x)$ can be characterized by an invariance property under an action of $\mathrm{PGL}(2, q)$ on irreducible polynomials. We also prove an asymptotic formula for the number of such invariant irreducibles of degree n as $n \to \infty$.

We note that some of our results have been obtained independently in the forthcoming paper [1] (where the case $b = 0$ in Eqn. (3) is considered). The binary case $q = 2$ was studied in [3].

References

[1] T. GAREFALAKIS, *On the action of* $\mathrm{GL}_2(\mathbb{F}_q)$ *on irreducible polynomials over* $\mathbb{F}_q$, J. Pure and Appl. Algebra, 215 (2011), pp. 1835–1843.

[2] H. MEYN, *On the construction of irreducible self-reciprocal polynomials over finite fields*, Appl. Algebra Engrg. Comm. Comput., 1 (1990), pp. 43–53.

[3] J. F. MICHON AND P. RAVACHE, *On different families of invariant irreducible polynomials over* $\mathbb{F}_2$, Finite Fields Appl., 16 (2010), pp. 163–174.

Henning Stichtenoth
Sabancı University, İstanbul, Turkey
henning@sabanciuniv.edu

A quotient of the d-dimensional Buratti-Del Fra dual hyperoval in $\mathrm{PG}(2d+1,2)$ with d even

Hiroaki Taniguchi

(joint work with Satoshi Yoshiara)

Let $d \geq 2$, and $K := F_{2^{d+1}}$ a finite field of 2^{d+1} elements.

Definition 1 *Let $m > d$. A family S of d-dimensional subspace of $\mathrm{PG}(m,2)$ is a d-dimensional dual hyperoval in $\mathrm{PG}(m,2)$ if it satisfies the following:*
(1) any two distinct members of S intersect in a projective point,
(2) any three mutually distinct members of S intersect trivially,
(3) all members of S generate $\mathrm{PG}(m,2)$,and
(4) there are exactly 2^{d+1} members of S.

From a certain collection of $(d+1)$-dimensional subspaces in $K \oplus K$ constructed from a bilinear map B on $K \cong F_{2^{d+1}}$, we have a d-dimensional dual hyperoval $S[B]$ in $\mathrm{PG}(2d+1,2)$. From a bilinear map $B_f(x,y) := f(x+y)+f(x)+f(y)+f(0)$ for a quadratic APN function f on K, we have an APN dual hyperoval $S[B_f]$. It is known that any APN dual hyperoval $S[B_f]$ is a quotient of the Huybrechts dual hyperoval in $\mathrm{PG}(2d+1,2)$, and the Buratti-Del Fra dual hyperoval is considered as a deformation of the Huybrechts dual hyperoval.

Theorem 2 *Let d even, and $B(x,y) := x^4y + xy^4 + xy + x^2y^2$. Then $S[B]$ is a quotient of the d-dimensional Buratti-Del Fra dual hyperoval in $\mathrm{PG}(2d+1,2)$.*

Let V be a 2^{d+1}-dimensiona vector space over F_2 with basis $\{e_x \mid x \in K\}$. Defining a certain incidence structure on V, we obtain a semibiplane Π, called the halved hypercube. The affine expansion $Af(S[B_f])$ for any APN dual hyperoval $S[B_f]$ is covered by the halved hypercube Π. ($Af(S[B_f]) \cong \Gamma_f := \langle (1, x, \bar{f}(x)) \rangle$ is covered by Π by the mapping $e_x \mapsto (1, x, \bar{f}(x))$ for any $x \in K$, where $\bar{f}(x) := f(x) + f(0)$.)

Theorem 3 *For any quotient S of the d-dimensional Buratti-Del Fra dual hyperoval, the affine expansion $Af(S)$ is covered by the halved hypercube Π.*

For the quotient $S[B]$ of the Buratti-Del Fra dual hyperoval in $\mathrm{PG}(2d+1,2)$, this suggests the existence of a graph Γ_g constructed from a function g on K such that $Af(S[B]) \cong \Gamma_g$, by investigating the explicit covering map of $S[B]$ by Π. Since the Buratti-Del Fra dual hyperoval is regarded as a deformation of the Huybrechts dual hyperoval, such a function g, if it exists, is considered as a deformation of an APN function.

Hiroaki Taniguchi
Kagawa National College of Technology
taniguchi@dg.kagawa-nct.ac.jp

Systematic Authentication Codes based on Bent functions and the Gray map on a Galois ring

Horacio Tapia-Recillas

(joint work with J.C. Ku-Cauich)

Lately, authentication codes have received attention by several authors. Authentication codes may be with secrecy and without secrecy and a subclass of the latter is the Systematic Authentication Codes (SACs). Several types of SACs have appeared in the literature, constructed using various concepts such as highly nonlinear functions over finite fields [1] or non-degenerated and rational functions on a Galois ring [2]. In this talk, by introducing a class of bent functions on a Galois ring of characteristic p^2 (p a prime) and using the Gray map on this ring, a class of SACs is described. If P_I denotes the maximum probability of the impersonation attack and $q = p^m$ is the cardinality of the residue field of the Galois ring, it is shown that P_I reaches the minimum value, $P_I = \frac{1}{q}$, for this class of SACs and a good bound is obtained for the maximum probability of the substitution attack. Some examples will be given to illustrate the main results.

References

[1] C. DING AND H. NIEDERREITER, *Systematic authentication codes from highly nonlinear functions*, IEEE Trans. Inform. Theory, 50 (2004), pp. 2421–2428.

[2] F. ÖZBUDAK AND Z. SAYGI, *Some constructions of systematic authentication codes using Galois rings*, Des. Codes Cryptogr., 41 (2006), pp. 343–357.

Horacio Tapia-Recillas
Departamento de Matemáticas
Universidad Autónoma Metropolitana-I
09340 México, D.F., MEXICO
htr@xanum.uam.mx

Swan-like results over finite fields

David Thomson

(joint work with B. Hanson and D. Panario)

The study of low-weight polynomials, polynomials with few non-zero terms, is critical for implementations of fast finite field arithmetic using a polynomial basis. Swan [2] applies a theorem of Stickelberger to give the parity of the number of irreducible factors of all trinomials (a polynomial with precisely three non-zero terms) over the binary field. Swan-like results have undergone a resurgence in the last decade. These results give the parity of the number of the irreducible factors of a polynomial, and can often give negative results to proving irreducibility when other methods fail. In particular, if the polynomial has an even number of factors, it is reducible.

In this talk, we give Swan-like results for any binomial over finite fields of odd characteristic and for trinomials $x^n + ax^k + b$ when the field characteristic divides n, k or $n - k$. Necessary and sufficient conditions for the irreducibility of binomials over any finite field $\mathbb{F}_q$ are known [1, Theorem 3.75], but require the factorization of $q - 1$, which may be quite large in principle. Our results give necessary conditions for irreducibility, but require only the evaluation of a quadratic character over $\mathbb{F}_q$. This talk will contain an outline of the general methods used for proving Swan-like conditions, and indicate the bottleneck of the current method. We will conclude with some open problems.

References

[1] R. LIDL AND H. NIEDERREITER, *Finite fields*, vol. 20 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, second ed., 1997. With a foreword by P. M. Cohn.

[2] R. G. SWAN, *Factorization of polynomials over finite fields*, Pacific J. Math., 12 (1962), pp. 1099–1106.

David Thomson
School of Mathematics and Statistics, Carleton University
Ottawa ON Canada
dthomson@math.carleton.ca

Decoding Spread Codes in Field Representation

Anna-Lena Trautmann

Constant dimension codes are defined to be subsets of the Grassmannian $G(k, n)$ over a finite field $\mathbb{F}_q$, and are of great interest since Kötter and Kschischang developed a theory of subspace codes for application in random network coding [1]. One class of these codes are so-called spread codes [2], i.e. optimal codes with maximal minimum distance.

One can use the isomorphism of the vector space $\mathbb{F}_q^n$ and the extension field $\mathbb{F}_{q^n}$ to represent the code words as sets of field elements. We want to introduce a decoding algorithm for spread codes using this field representation.

Since a spread code has distance $2k$ we can correct up to $k-1$ errors, where an error is either an erasure or an insertion of an arbitrary element. Hence we can decode a codeword with a $\lfloor \frac{k-1}{2} \rfloor$-dimensional erroneous subspace.

The complexity of this algorithm is dominated by $\mathcal{O}(k^{f+1})$ steps (each an inversion and a multiplication) over $\mathbb{F}_{q^n}$, where k is the dimension of the code words and f is the error-correction capability of the code.

References

[1] R. KÖTTER AND F. R. KSCHISCHANG, *Coding for errors and erasures in random network coding*, IEEE Trans. Inform. Theory, 54 (2008), pp. 3579–3591.

[2] F. MANGANIELLO, E. GORLA, AND J. ROSENTHAL, *Spread codes and spread decoding in network coding*, in Proceedings of the 2008 IEEE International Symposium on Information Theory, Toronto, Canada, 2008, pp. 851–855.

Anna-Lena Trautmann
University of Zurich
Switzerland
anna-lena.trautmann@math.uzh.ch

On fractional binary Knuth semifield planes

Rocco Trombetti

(joint work with Olga Polverino)

Let $\pi = \pi(\mathbb{S})$ be a semifield plane of order p^n and let π_0 be a subplane of π of order p^k coordinatized by a subsemifield of $\mathbb{S}$, we define $\frac{n}{k}$ to be the *dimension* of π with respect to π_0. The subplane dimension question for semifield planes concerns with asking if the existence of such a subplane π_0 of π must force the integer k to divide n. If this is not the case, $\pi(\mathbb{S})$ is said to be *fractional dimensional* with respect to such a subplane.

The question has a negative answer, in fact in [2] the author proved that the semifield plane $\pi(\mathbb{K}_{2^5})$ coordinatized by the binary Knuth semifield $\mathbb{K}_{2^5}$ of order 2^5, is fractional dimensional with respect to the Desarguesian plane of order 4. Also, in [1], Jha and Johnson proved that there are isotopes of the commutative binary Knuth semifields of orders 2^{tk}, for k odd and $t = 5$ or 7, that admit the subfield of order 4.
In this talk, we concentrate on planes coordinatized by the commutative binary Knuth semifields which are fractional dimensional with respect to $PG(2, 4)$ and prove that this class is, in fact, wider. Precisely, we show that semifield planes $\pi(\mathbb{K}_{2^m})$ coordinatized by the commutative binary Knuth semifield $\mathbb{K}_{2^m}$, $m = nk$ (m odd), are fractional dimensional with respect to a subplane isomorphic to $PG(2, 4)$ if either $n = 9$ or $n \not\equiv 0 \pmod 3$, and one of the trinomials $x^n + x^s + 1$, $s \in \{1, 2, 3, 5\}$, is irreducible over the Galois field $\mathbb{F}_2$.

References

[1] V. JHA AND N. L. JOHNSON, *The dimension of a subplane of a translation plane*, Bull. Belg. Math. Soc. Simon Stevin, 17 (2010), pp. 463–477.

[2] I. F. RÚA, *Primitive and non primitive finite semifields*, Comm. Algebra, 32 (2004), pp. 793–803.

Rocco Trombetti
Universitá degli Studi di Napoli Federico II
rtrombet@unina.it

A Generalization of the Hansen-Mullen Conjecture on Irreducible Polynomials

Georgios Tzanakis

(joint work with Daniel Panario)

Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. We examine the existence of irreducible polynomials with prescribed coefficients over $\mathbb{F}_q$. We focus on a conjecture by Hansen and Mullen (Math. Comp. 1992) which states that for $n \geq 3$, there exist irreducible polynomials over $\mathbb{F}_q$ of degree n, with any *one* coefficient prescribed to any element of $\mathbb{F}_q$ (this being nonzero when the constant coefficient is being prescribed) and was proved by Wan (Math. Comp. 1997). We introduce a variation of Wan's method to give restrictions subject to which this result can be extended to more than one prescribed coefficient. It also follows from our generalization the existence of irreducible polynomials with sequences of consecutive zero coefficients.

Georgios Tzanakis
Carleton University
gtzanaki@connect.carleton.ca

Graphs associated with the map $x \mapsto x + x^{-1}$ in a finite field of characteristic two

Simone Ugolini

The map which sends x to $x+x^{-1}$ in a finite field (with a point ∞ added to it) plays a role in various investigations. The so-called Q-transform depends on it, as it takes a polynomial f of degree n to the self-reciprocal polynomial $f^Q(x) = x^n f(x+x^{-1})$ of degree $2n$ (see [1]). Also, the possible correlation between the multiplicative orders of x and $x + x^{-1}$ was studied in [2].

Iteration of maps on finite fields are also important. For example, Pollard's integer factoring algorithm is based on the iteration of a quadratic map $x \mapsto x^2 + c \pmod N$, where $c \neq 0, -2$ is a randomly-chosen constant and N is the integer to be factored. See [3] for one of several studies on iterations of maps of this form in a finite field.

Our work focuses on iterations of the map $x \mapsto x + x^{-1}$ on the projective line $\bar{E} = E \cup \{\infty\}$, where E is a finite field. A directed graph on $\bar{E}$ is associated to the map in an obvious way. Each connected component consists of a cycle and directed binary trees entering the cycle at various points.

Experimental evidence has shown that such graphs present remarkable symmetries when E has characteristic two. In fact, it turns out that the map is closely related to the duplication map on a certain elliptic curve on E, the Koblitz curve $y^2 + xy = x^3 + 1$ over $\mathrm{GF}(2)$. Using this fact we give a precise description of the structure of such graphs, including the length of the cycles and the depth of the trees.

References

[1] D. JUNGNICKEL, *Finite fields*, Bibliographisches Institut, Mannheim, 1993. Structure and arithmetics.

[2] I. SHPARLINSKI, *On the multiplicative orders of γ and $\gamma + \gamma^{-1}$ over finite fields*, Finite Fields Appl., 7 (2001), pp. 327–331.

[3] T. VASIGA AND J. SHALLIT, *On the iteration of certain quadratic maps over* $\mathrm{GF}(p)$, Discrete Math., 277 (2004), pp. 219–240.

Simone Ugolini
University of Trento, Italy
sugolini@gmail.com

Stopping sets, sets without tangents, and exterior sets to a conic

Geertrui Van de Voorde

LDPC codes are a well-studied class of linear codes; they are defined by a sparse parity-check matrix. The performance of LDPC codes under iterative decoding over the binary erasure channel is entirely defined by combinatorial structures, called stopping sets (see [2]). In the case that the LDPC code is defined by the incidence matrix of a projective plane $\mathrm{PG}(2,q)$, the stopping sets correspond to the so-called *sets without tangents* in $\mathrm{PG}(2,q)$. A set without tangents is a set of points S such that no line meets S in exactly one point.

In this talk, we briefly review the connection between LDPC codes and stopping sets, and we repeat what is known about sets without tangents in $\mathrm{PG}(2,q)$, q odd (see [1]). In $\mathrm{PG}(2,5)$, the smallest set without tangents have size 10, and can be shown to be of two different types (up to isomorphism). The first type is the trivial example, obtained by taking the symmetric difference of two lines. The second type is obtained by taking the points on a conic $\mathcal{C}$ and 4 well-chosen external points to $\mathcal{C}$. The set of these four points $\mathcal{E}$ forms an exterior set to $\mathcal{C}$, i.e., all connecting lines do not meet $\mathcal{C}$. Moreover, $\mathcal{E}$ consists of the 3 exterior points on an external line L to $\mathcal{C}$, together with one special point. We will show that exterior sets consisting of the exterior points on an external line L, together with one extra point, not on L, exist in $\mathrm{PG}(2,q)$ if and only if $q = 1 \bmod 4$ [3].

References

[1] A. BLOKHUIS, Á. SERESS, AND H. A. WILBRINK, *On sets of points in* $\mathrm{PG}(2,q)$ *without tangents*, in Proceedings of the First International Conference on Blocking Sets (Giessen, 1989), no. 201, 1991, pp. 39–44.

[2] C. DI, D. PROIETTI, I. E. TELATAR, T. J. RICHARDSON, AND R. L. URBANKE, *Finite-length analysis of low-density parity-check codes on the binary erasure channel*, IEEE Trans. Inform. Theory, 48 (2002), pp. 1570–1579. Special issue on Shannon theory: perspective, trends, and applications.

[3] G. VAN DE VOORDE, *On sets without tangents and exterior sets of a conic*, (preprint).

Geertrui Van de Voorde
Vrije Universiteit Brussel
gvdevoor@vub.ac.be

A new class of $(q+t,t)$-arcs of type $(0,2,t)$

Peter Vandendriessche

Definition 1 *A $(q+t,t)$-arc of type $(0,2,t)$ in $\mathrm{PG}(2,q)$ is a set S of $q+t$ points for which every line ℓ meets S in either 0, 2 or t points.*

Definition 1 was introduced in [3] and it is proven there that $(q+t,t)$-arcs of type $(0,2,t)$, with $1<t<q$, can only exist if q is even. Moreover, t must be a divisor of q, i.e. $t=2^r$ with $r\leq h$. In [1], it is proven that the number of t-secants is $\frac{q}{t}+1$ and that they are concurrent; their concurrent point is called the t-nucleus. From now on, we will assume that q is even and t divides q.

In [3], a construction is given in the case that $h-r$ divides h, conjecturing existence for all proper divisors t of $q=2^h$. This conjecture has been open for more than 20 years now. In [1], the authors construct 3 infinite classes of such arcs for which $h-r$ is not a proper divisor of h. Some $(40,8)$-arcs of type $(0,2,8)$ in $\mathrm{PG}(2,32)$ were found by J. Limbupasiriporn and a $(36,4)$-arc of type $(0,2,4)$ in $\mathrm{PG}(2,32)$ was discovered in [2], both via randomized computer searches.

In this talk, we construct a new infinite class of $(q+q/4,q/4)$-arcs of type $(0,2,q/4)$, for all $q=2^h$, $h\geq 3$. This results in new arcs of previously unknown parameters. We mainly use arguments from coding theory, interpreting $\mathbb{F}_q$ as a vector space over $\mathbb{F}_2$. We also provide a detailed conjecture on the structure of the Desarguesian plane code, backed up by computer results.

References

[1] A. Gács and Z. Weiner, *On $(q+t,t)$-arcs of type $(0,2,t)$*, Des. Codes Cryptogr., 29 (2003), pp. 131–139.

[2] J. D. Key, T. P. McDonough, and V. C. Mavron, *An upper bound for the minimum weight of the dual codes of Desarguesian planes*, European J. Combin., 30 (2009), pp. 220–229.

[3] G. Korchmáros and F. Mazzocca, *On $(q+t)$-arcs of type $(0,2,t)$ in a Desarguesian plane of order q*, Math. Proc. Cambridge Philos. Soc., 108 (1990), pp. 445–459.

[4] P. van den Driessche, *Codes of desarguesian projective planes of even order, projective triads and $(q+t,t)$-arcs of type $(0,2,t)$*, Finite Fields Appl., (2011). doi:10.1016/j.ffa.2011.03.003.

Peter Vandendriessche
Ghent University, Belgium
peter.vandendriessche@gmail.com

Eigenvalue techniques for regular and extremal substructures in geometry

Frédéric Vanhove

Several types of geometries are studied in literature, such as projective geometries, polar spaces, generalized polygons,.... Although they have not been classified for many types, most of the well-known constructions make use of finite fields. Because of their highly regular structure, geometries often gives rise to combinatorial objects like association schemes and distance-regular graphs (see for instance [1]). A general theory on subsets in these objects has already been developed, which includes Delsarte theory (see [2, 3, 4]). In this talk, we will discuss how eigenvalue techniques can be applied to obtain either alternative proofs of known results or new results for several geometries.

References

[1] A. E. BROUWER, A. M. COHEN, AND A. NEUMAIER, *Distance-regular graphs*, vol. 18 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], Springer-Verlag, Berlin, 1989.

[2] P. DELSARTE, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl., (1973), pp. vi+97.

[3] ———, *Association schemes and t-designs in regular semilattices*, J. Combinatorial Theory Ser. A, 20 (1976), pp. 230–243.

[4] ———, *Pairs of vectors in the space of an association scheme*, Philips Res. Rep., 32 (1977), pp. 373–411.

Frédéric Vanhove
Ghent University (Belgium)
(`http://cage.ugent.be/~fvanhove/`)
fvanhove@cage.ugent.be

On self-orthogonal quaternary codes and quantum codes

Zlatko Varbanov

P.Shor [2] proved that there exists a randomized algorithm for integer factorization which runs in polynomial time on a quantum computer (on a classical computer, primality testing is 'easy' but factorization is 'hard'). A quantum analogue of a bit of information is called a qubit. It is the state of a system in a 2-dimensional Hilbert space $\mathbb{C}^2$, spanned by e_0 and e_1, where e_0 and e_1 are eigenvectors corresponding to the eigenvalues 0 and 1 of the qubit.

Definition 1 ([1]) *A quantum error-correcting codes (QECC) is defined to be a unitary mapping (encoding) of k qubits into a subspace of the quantum state space of n qubits such that if any t of the qubits undergo arbitrary decoherence, not necessarily independently, the resulting n qubits can be used to faithfully reconstruct the original quantum state of the k encoded qubits.*

The problem of finding QECCs can be transformed into the problem of finding linear self-orthogonal codes under a Hermitian inner product over the finite field $\mathrm{GF}(4)$.

Theorem 2 ([1]) *if C is a Hermitian self-orthogonal linear $[n, k]$ code over $\mathrm{GF}(4)$ such that there are no vectors of weight $< d$ in $C^{\perp}\backslash C$, (where $C^{\perp}$ is the Hermitian dual of C) then there exists a quantum error-correcting $[[n, n-2k, d]]$ code.*

In the present work we search for self-orthogonal codes over $\mathrm{GF}(4)$ with good parameters. We develop some constructive algorithms and by computer search we prove the existence of QECC with minimum distance $d > 4$.

References

[1] A. R. CALDERBANK, E. M. RAINS, P. W. SHOR, AND N. J. A. SLOANE, *Quantum error correction via codes over* $\mathrm{GF}(4)$, IEEE Trans. Inform. Theory, 44 (1998), pp. 1369–1387.

[2] P. W. SHOR, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput., 26 (1997), pp. 1484–1509.

Zlatko Varbanov
Department of Mathematics and Informatics,
University of Veliko Tarnovo, Bulgaria
vtgold@yahoo.com

Discrete logarithm like problems and linear recurring sequences

Hugo Villafañe

(joint work with Santos González, Llorenç Huguet and Consuelo Martínez)

Linear recurring sequences were used with public key cryptographic aims for the first time by H. Niederreiter ("Some new cryptosystems based on feedback shift register sequences", Math. J. Okayama Univ. 30, 121-149, 1988). [1] and [2] also used certain linear recurring sequences to develop public key protocols.

The security of these schemes relies on the hardness of discrete logarithm like problems linked to linear recurring sequences. Modulo a good choice of parameters, these problems coincide with the underlying problems in some public key constructions where elements in finite fields are replaced by their traces over smaller subfields (see, for example, [3]).

We have addressed the question of the hardness of the problems that arise in a context of linear recurring sequences from a point of view as general as possible. We have defined new discrete logarithm, Diffie-Hellman and decisional Diffie-Hellman problems for any linear recurring sequence σ in any finite field $\mathbb{F}_q$. We have proven that when the minimal polynomial of σ, $f(x)$, is irreducible in $\mathbb{F}_q[x]$, then the new problems defined for σ are polynomially equivalent to the discrete logarithm, Diffie-Hellman and decisional Diffie-Hellman problems in the subgroup generated by the roots of $f(x)$ in some extension field of $\mathbb{F}_q$. This result generalizes [3, Th. 5.21] and [1, Th. 2] and minor inaccuracies in the proofs of these results are corrected.

Thus, public key cryptographic protocols based on these problems are as secure as protocols based on the discrete logarithm related problems in multiplicative subgroups of finite fields.

References

[1] K. GIULIANI AND G. GONG, *New lfsr-based cryptosystems and the trace discrete logarithm problem (Trace-DLP)*, in Sequences and their applications—SETA 2004, vol. 3486 of Lecture Notes in Computer Science, Berlin, 2004, Springer, pp. 298–312.

[2] G. GONG AND L. HARN, *Public-key cryptosystems based on cubic finite field extensions*, IEEE Trans. Inform. Theory, 45 (1999), pp. 2601–2605.

[3] A. K. LENSTRA AND E. R. VERHEUL, *The XTR public key system*, in Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA), vol. 1880 of Lecture Notes in Comput. Sci., Springer, Berlin, 2000, pp. 1–19.

Hugo Villafañe
Universitat de les Illes Balears
hugo.villafane@uib.es

The Pontryagin dual group to $\overline{\mathbb{Z}(p)}$

Apostolos Vourdas

In recent work we have studied the Pontryagin dual group to $GF(p^{p^\infty})$ [1] (and also used it for harmonic analysis on $GF(p^{p^\infty})$ [2]). We now extend this work and we study the Pontryagin dual group to the additive group $\overline{\mathbb{Z}(p)}$ (the algebraic closure of $\mathbb{Z}(p)$). Here the mathematical structure is much more complex (the subgroups of $\overline{\mathbb{Z}(p)}$ form a lattice in contrast to the subgroups of $GF(p^{p^\infty})$ which simply form a chain). The work is at the 'edge' of the subject of finite fields, where the fields become infinite but they still have the structure of finite fields.

The $\overline{\mathbb{Z}(p)}$ is introduced as the direct limit of $GF(p^\ell)$. The lattice structure of the subfields of $\overline{\mathbb{Z}(p)}$, is studied. The Galois group of Frobenius automorphisms of $\overline{\mathbb{Z}(p)}$ which leave fixed the elements of the subfield $GF(p^n)$ (where n is a supernatural (Steinitz) number), is shown to be isomorphic to the profinite group $n\widehat{\mathbb{Z}}$ (where $\widehat{\mathbb{Z}} = \prod \mathbb{Z}_p$ and $\mathbb{Z}_p$ are the p-adic integers). The fundamental theorem of Galois theory in this context, is also discussed.

The profinite group $\mathfrak{S}$ is defined as the inverse limit of the $GF(p^\ell)$. Its elements are the sequences $\mathfrak{a} = (\alpha_1, \alpha_2, ...)$ where if $k|\ell$ then $\alpha_k = \mathrm{Tr}_{\ell|k}(\alpha_\ell)$. A proposition with several properties of these sequencies, is proved. The lattice structure of the subgroups of $\mathfrak{S}$ is studied.

Theorem 1 *$\overline{\mathbb{Z}(p)}$ and $\mathfrak{S}$ are Pontryagin dual groups to each other.*

Definition 2 *$\mathcal{A}_n(\mathfrak{S})$ (n a supernatural number), is the group of automorphisms of $\mathfrak{S}$ which induce the identity map on $\mathfrak{S}/\mathfrak{S}(n)$ ($\mathfrak{S}(n)$ will be defined in the talk).*

Theorem 3 $\mathcal{A}_n(\mathfrak{S}) \cong n\widehat{\mathbb{Z}}$

Theorem 4 *$\mathfrak{S}$ as a right topological $\overline{\mathbb{Z}(p)}$-module.*

References

[1] A. VOURDAS, *Harmonic analysis on* GF(p^{p^∞})*: Part I*, J. Math. Anal. Appl., 370 (2010), pp. 57–70.

[2] ——, *Harmonic analysis on* GF(p^{p^∞})*: Part II*, J. Math. Anal. Appl., 370 (2010), pp. 71–81.

Apostolos Vourdas
Department of Computing,
University of Bradford,
Bradford BD7 1DP, United Kingdom
A.Vourdas@bradford.ac.uk

Primitive block designs with automorphism group $\mathrm{PSL}\,(2,q)$

Tanja Vučičić

(joint work with Joško Mandić and Snježana Braić)

A block design we call primitive if it has an automorphism group acting primitively on both point and block set. Taking the projective line $X = \{\infty\} \cup \mathrm{GF}(q)$ as the set of points, our research aims to determine, up to isomorphism and complementation, all primitive block designs with $\mathrm{PSL}\,(2,q)$ as an automorphism group. The number of such designs we denote by $npd(q)$. In dealing with primitive permutation representations of almost simple groups with socle $\mathrm{PSL}\,(2,q)$ we make use of the study ([1]) of their maximal subgroups. The obtained desigs we describe by their base block (a union of orbits of a block stabilizer) and the full automorphism group.

Our results so far include completely solving the problem in case when a block stabilizer is not in the fifth Aschbacher's class (in particular, for q a prime), and assertions such as the following.

Lemma 1 *Let $q \geq 4$. Then $npd\,(q) = 0$ if and only if $q = 7, 11, 23$ or $q = 2^r$, r a prime.*

Lemma 2 *Let $q \geq 13$ and let there exist a block design D, the socle of $AutD$ being $\mathrm{PSL}_2\,(q)$. If the base block stabilizer is in the second Aschbacher's class, then $q \equiv 1\,(\mathrm{mod}4)$, D is $2 - \left(q+1, \frac{q-1}{2}, \frac{(q-1)(q-3)}{8}\right)$ design up to complementation, and $AutD = P\Sigma L_2\,(q)$.*

References

[1] M. GUIDICI, *Maximal subgroups of almost simple groups with socle* $\mathrm{PSL}(2,q)$. arXiv:math/0703685v1 [math.GR], 2007.

Tanja Vučičić
University of Split, Croatia
vucicic@pmfst.hr

5-Designs related to binary extremal self-dual codes of length $24m$

Wolfgang Willems

(joint work with Javier de la Cruz)

Let C be a binary extremal self-dual code of length $n = 24m$. According to Mallows and Sloane, the minimum distance of C satisfies $d = 4m + 4$. We put $\mathcal{P} = \{1, \ldots, 24m\}$ and define the blocks $B \in \mathcal{B}$ as the support of codewords of minimal weight. Due to a result of Assmus and Mattson, $\mathcal{D}_C = (\mathcal{P}, \mathcal{B})$ forms a self-orthogonal 5-$(24m, 4m + 4, \binom{5m-2}{m-1})$ design.

Conversely suppose that $\mathcal{D}$ is a self-orthogonal 5-$(24m, 4m + 4, \binom{5m-2}{m-1})$ design. The related binary code $C(\mathcal{D})$ is defined as the $\mathbb{F}_2$-linear span of the rows of the block-point incidence matrix of $\mathcal{D}$. Clearly, $C(\mathcal{D})$ is self-orthogonal since $\mathcal{D}$ is self-orthogonal.

Weak Conjecture $C(\mathcal{D})^\perp = C(\mathcal{D})$.

Strong Conjecture $C(\mathcal{D})$ is an extremal self-dual $[24m, 12m, 4m + 4]$ code.

Remark Note that for $m = 1$, there is exactly one binary extremal self-dual code, namely the $[24, 12, 8]$ extended Golay code and exactly one 5-$(24, 8, 1)$ design, a Steiner system, where the related code is the binary extended Golay code. For $m = 2$, there is again exactly one binary extremal self-dual code, namely the binary extended quadratic residue code and exactly one self-orthogonal 5-$(48, 12, 8)$ design, where the related code is the binary extended quadratic residue code.

In case $m = 3$ and $m = 4$, we do not know about the existence neither of binary extremal self-dual codes of length 72 or 96 nor of self-orthogonal 5-$(72, 16, 78)$ or 5-$(96, 20, 816)$ designs. However, according to results of Harada, Kitazume and Munemasa, the strong conjecture has an affirmative answer in both cases. For $m = 5$, we prove

Theorem Let $\mathcal{D}$ be a self-orthogonal 5-$(120, 24, 8855)$ design. Then $C(\mathcal{D}) = C(\mathcal{D})^\perp$ with minimum distance $d = 16$ or $d = 24$.

Finally, for the automorphism group of a binary extremal self-dual code and the automorphism group of its related 5-design, we get

Proposition Let C be a binary extremal self-dual $[24m, 12m, 4m+4]$ code with related self-orthogonal 5-$(24m, 4m + 4, \binom{5m-2}{m-1})$ design $\mathcal{D}_C$. If $C(\mathcal{D}_C)^\perp = C(\mathcal{D}_C)$, then

$$\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}_C).$$

Wolfgang Willems
Otto-von-Guericke Universität, Magdeburg, Germany
wolfmann@univ-tln.fr

Polynomial quotients

Arne Winterhof

(joint work with Zhixiong Chen)

Let R be a complete residue system modulo a prime p and $f(X)$ an integer polynomial with leading coefficient not divisible by p and define for any integer u,

$$f_p(u) \equiv f(u) \bmod p, \quad f_p(u) \in R.$$

We call

$$F(u) \equiv \frac{f(u) - f_p(u)}{p} \bmod p, \quad 0 \le F(u) < p,$$

polynomial quotients modulo p. A special case, the *Fermat quotients*

$$q_p(u) = \frac{u^{p-1} - u^{p(p-1)}}{p} \bmod p,$$

has been studied in a series of papers, see [2] and references therein.

In particular, Heath-Brown [1, Theorem2] proved that $q_p(u)/p \in [0,1)$ are asymptotically uniformly distributed for $u = M+1, \ldots, M+N$ for any integers M and $N \ge p^{1/2+\varepsilon}$. A different approach was used in [2] to study the distribution of the points

$$\left(\frac{q_p(u)}{p}, \ldots, \frac{q_p(u+s-1)}{p}\right), \quad u = M+1, \ldots, M+N,$$

with consecutive lags in $[0,1)^s$ for any dimension $s \ge 1$, which is nontrivial for $N \ge sp^{1+\varepsilon}$.

Using the Burgess bound, for all k we extend the first result to polynomial quotients of the form $f_k(u) \equiv \frac{u^k - u^{kp}}{p} \bmod p$ and the second to arbitrary polynomial quotients.

References

[1] D. R. HEATH-BROWN, *An estimate for Heilbronn's exponential sum*, in Analytic number theory, Vol. 2 (Allerton Park, IL, 1995), vol. 139 of Progr. Math., Birkhäuser Boston, Boston, MA, 1996, pp. 451–463.

[2] A. OSTAFE AND I. E. SHPARLINSKI, *Pseudorandomness and dynamics of Fermat quotients*, SIAM J. Discrete Math., 25 (2011), pp. 50–71.

Arne Winterhof
Austrian Academy of Sciences
arne.winterhof@oeaw.ac.at

On the access structures of hyperelliptic secret sharing schemes

Siman Yang

(joint work with Lei Li)

One of the main tasks in secret sharing is the characterization of the access structures. Chen and Cramer [1] proposed secret sharing schemes based on algebraic-geometric codes as a natural generalization of Shamir's scheme. However, algebraic-geometric secret sharing schemes are ramp schemes in the sense that there exists a gap of $2g$ between the size of the qualified subsets and the forbidden subsets, where g is the genus of the underlying curve. Chen, Ling and Xing [2] completely determined the access structures of the elliptic secret sharing schemes. In this work we generalize their method to the jacobians of hyperelliptic curves of any genus and we reduce the general gap from $2g$ to $g-1$.

We determine explicitly which subsets of the size in the range $[n-\deg(G), n-\deg(G)+g]$ are qualified for the hyperelliptic secret sharing schemes as follows.

Theorem 1 *Let X be a hyperelliptic curve over $\mathbb{F}_q$ of genus g. Let $\boldsymbol{D}=\{P_0,\ P_1,\ldots,\ P_n\}$ be a subset of nonzero elements of $X(\mathbb{F}_q)$ and let $G=mO$.*

Let $\boldsymbol{A}=\{P_{i_1},P_{i_2},\ldots,P_{i_t}\}$ be a subset of the player set $\boldsymbol{P}=\{P_1,\ P_2,\ldots,\ P_n\}$. Let the group sum of $\tilde{P}_{i_1}-O$, $\tilde{P}_{i_2}-O$, $\cdots$, $\tilde{P}_{i_t}-O$ in $\mathbb{J}_X(\mathbb{F}_q)$ be the reduced divisor $B-kO$ (where $\tilde{P}$ is image of the canonical involution map). Let $\boldsymbol{A}^c:=\boldsymbol{P}\setminus\boldsymbol{A}$ and Γ is the access structure of the secret sharing scheme from $\boldsymbol{C}=C_\Omega(D,G)$ associated with X, then we have the following:

1) If $\#\boldsymbol{A}^c\leqslant n-m-1$, then $\boldsymbol{A}^c\notin\Gamma$; and if $\#\boldsymbol{A}^c\geqslant n-m+2g$, then $\boldsymbol{A}^c\in\Gamma$;

2) Suppose $n-m\leqslant\#\boldsymbol{A}^c\leqslant n-m+g$. If $\boldsymbol{A}^c$ is a minimal qualified subset, then $supp(B)\cap\boldsymbol{D}\subset\boldsymbol{A}$ and $deg(B)\leqslant m-t$, and conversely, if $supp(B)\cap\boldsymbol{D}\subset\boldsymbol{A}$ and $deg(B)\leqslant m-t$, then $\boldsymbol{A}^c$ is a qualified subset.

References

[1] H. CHEN AND R. CRAMER, *Algebraic geometric secret sharing schemes and secure multi-party computations over small fields*, in Advances in cryptology—CRYPTO 2006, vol. 4117 of Lecture Notes in Comput. Sci., Springer, Berlin, 2006, pp. 521–536.

[2] H. CHEN, S. LING, AND C. XING, *Access structures of elliptic secret sharing schemes*, IEEE Trans. Inform. Theory, 54 (2008), pp. 850–852.

Siman Yang
Department of Mathematics, East China Normal University
smyang@math.ecnu.edu.cn

Commutative semifields, planar functions and a character approach

Yue Zhou

(joint work with Alexander Pott)

A *semifield* $\mathbb{S}$ is an algebraic structure satisfying all the axioms of a skewfield except (possibly) associativity. By Wedderburn's Theorem, in the finite case, associativity implies commutativity. Therefore, a non-associative finite commutative semifield is the closest algebraic structure to a finite field. A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called a *planar function*, if for each $a \in \mathbb{F}_{p^n}^*$, $f(x+a) - f(x)$ is a bijection on $\mathbb{F}_{p^n}$. It is easy to show that there is no planar function for $p = 2$. It is well-known that a planar polynomial with algebraic degree 2 is equivalent to a commutative presemifield with odd characteristic.

In this talk, we will present a class of commutative semifields with 2 parameters from [2]. Its left and middle nucleus are both determined. Furthermore, we prove that for any different pairs of parameters, these semifields are not isotopic. Its autotopism group is determined. It is also shown that, for some special parameters, one semifield in this family can lead to two inequivalent planar functions. We will also present an interesting character approach in [1], which characterize planar functions within a class of functions $\mathbb{F}_{p^{2m}} \to \mathbb{F}_{p^{2m}}$ via the planarity of functions $\mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$. It gives a surprising connection between the Ganley and the Coulter-Matthews semifields.

References

[1] A. POTT AND Y. ZHOU, *A character theoretic approach to planar functions*. accepted.

[2] Y. ZHOU AND A. POTT, *A new family of semifields with 2 parameters*. submitted.

Yue Zhou
Faculty of Mathematics, Otto-von-Guericke-University Magdeburg,
39106 Magdeburg, Germany
yue.zhou@st.ovgu.de