The 9th International Conference on Finite Fields and their Applications
University College Dublin, July 13-17, 2009.

Invited Talks

Sum-Product and Character Sums in finite fields

Mei-Chu Chang

University of California, Riverside

In this talk I will present estimates on incomplete character sums in finite fields, with special emphasize on the non-prime case. Some of the results are of the same strength as Burgess celebrated theorem for prime fields. The improvements are mainly based on arguments from arithmetic combinatorics providing new bounds on multiplicative energy and an improved amplification strategy. In particular, we improve on earlier work of Davenport-Lewis and Karacuba.

Primitive elements on lines in extensions

Stephen D Cohen

University of Glasgow

Davenport (1937) and Carlitz (1953) proved that *provided q is sufficiently large*, whenever θ generates the extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ (i.e., $\mathbb{F}_q(\theta) = \mathbb{F}_{q^n}$), then there exists an element $a \in \mathbb{F}_q$ such that $\theta + a$ is a primitive element of $\mathbb{F}_{q^n}$.

For *quadratic extensions*, following a more geometrical formulation and a conjecture by Giudici and Margaglio (1980), I proved (1983) a complete unconditional existence result, namely that for *any* finite field $\mathbb{F}_q$, *any* θ generating $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and *any* non-zero $\alpha \in \mathbb{F}_{q^2}$, there exists an element $a \in \mathbb{F}_q$ such that $\alpha(\theta + a)$ is a primitive element of $\mathbb{F}_{q^2}$.

As regards *cubic extensions*, in the $\mathbb{F}_q6$ conference proceedings Mills and McNay (2002) gave strong evidence supporting a (complete) conjecture on the existence of primitive elements of $\mathbb{F}_{q^3}$ of the form $\theta + a, a \in \mathbb{F}_q$ for any generating element θ. I have recently proved this conjecture and partially extended it to the existence of primitive elements on general lines.

For *quartic extensions* $\mathbb{F}_{q^4}$ is it realistic to hope to be able to establish analogous complete existence results?

The talk will review these results and associated techniques.

APN Polynomials: An Update

J. F. Dillon

National Security Agency
Fort George G. Meade, MD USA

A map $f : \mathrm{GF}(2^m) \to \mathrm{GF}(2^m)$ is *almost perfect nonlinear*, abbreviated APN, if $x \mapsto f(x+a)-f(x)$ is 2-to-1 for all nonzero a in $\mathrm{GF}(2^m)$. If $f(0) = 0$, then this condition is equivalent to the condition that the binary code of length $2^m - 1$ with parity-check matrix

$$H := \begin{bmatrix} \cdots & \omega^j & \cdots \\ \cdots & f(\omega^j) & \cdots \end{bmatrix}$$

is double-error-correcting, where ω is primitive in $\mathrm{GF}(2^m)$.

After setting the stage with an overview of these maps, their polynomials and their codes, we shall give an account of some recent developments, some of which illuminate long-standing open questions.

Zeta Functions in Number Theory and Combinatorics

Wen-Ching Winnie Li

Pennsylvania State University, U.S.A. and

National Center for Theoretical Sciences, Taiwan

Roughly speaking, a zeta function is a counting function. Well-known zeta functions in number theory include the Riemann zeta function and the zeta function attached to an algebraic variety defined over a finite field. The former counts integral ideals of a given norm, while the latter counts solutions over a finite field. On the combinatorics side, attached to a finite graph is the Ihara zeta function, which counts geodesic cycles of a given length. In a recent joint work with Ming-Hsuan Kang, we obtained the zeta function of a finite 2-dimensional complex arising from the Bruhat-Tits building of PGL_3 over a local field. Such a zeta function counts geodesic cycles of a given length up to homotopy. This is the first explicit zeta functions for complexes of dimension greater than one. Like graph zeta functions, a complex zeta function has the following features:

(1) It is a rational function;

(2) It provides topological and spectral information of the complex;

(3) It satisfies the Riemann Hypothesis if and only if the complex is spectrally optimal, called a Ramanujan complex.

In this survey talk I shall compare the zeta functions mentioned above and discuss the role of the Riemann Hypothesis, emphasizing connections between combinatorics and number theory. If time permits, comments on zeta functions of complexes arising from general PGL_n will be made.

Discrete logarithm assumptions in cryptography

Alfred Menezes

University of Waterloo

(Joint work with Neal Koblitz)

The search for mathematically rigorous proofs of security for public-key cryptographic protocols has been an important theme of researchers over the past twenty years. However, there are many issues that arise when interpreting these reductionist proofs. I will consider the case of security proofs that rely on the hardness of non-standard versions of the discrete logarithm problem.

The asymptotic theory of error-correcting codes

Harald Niederreiter

RICAM Linz and University of Salzburg

For a prime power q and $0 \leq \delta \leq 1$, let $\alpha_q(\delta)$ be the largest asymptotic information rate that can be achieved by a sequence of q-ary codes with increasing lengths and asymptotic relative minimum distance δ. It is known that $\alpha_q(0) = 1$ and $\alpha_q(\delta) = 0$ for $(q-1)/q \leq \delta \leq 1$. A fundamental problem in coding theory is to find lower bounds on $\alpha_q(\delta)$ in the remaining range $0 < \delta < (q-1)/q$. A classical lower bound is the asymptotic Gilbert-Varshamov bound, but in a spectacular breakthrough Tsfasman, Vlăduţ, and Zink showed in 1982 that one can beat this bound by using algebraic-geometry codes.

In recent years the Tsfasman-Vlăduţ-Zink bound was improved by several authors, including Elkies, Xing, Maharaj, Özbudak, and the speaker. These advances are based on constructions of new types of algebraic-geometry codes. The talk discusses these recent developments and also gives a general introduction to the area.

Contributed Talks

Multiplicative Order of Gauss Periods

Omran Ahmadi

Claude Shannon Institute, University College Dublin

(Joint work with I. E. Shparlinski and J. F. Voloch)

We obtain a lower bound on the multiplicative order of Gauss periods which generate normal bases over finite fields. This bound improves the previous bound of J. von zur Gathen and I. E. Shparlinski.

Let $r = 2n + 1$ be a prime number coprime with q, a prime power, and $\beta \in \mathbf{F}_{q^{2n}}$ be a primitive rth root of unity. Then the element

$$\alpha = \beta + \beta^{-1} \in \mathbf{F}_{q^n}$$

is called a Gauss period of type $(n, 2)$.

The following theorem establishes a lower bound on the multiplicative order of Gauss period of type $(n, 2)$ generating normal bases.

Theorem *Let p be the characteristic of $\mathbf{F}_q$ and let q be a primitive root modulo a prime $r = 2n+1$. Then, uniformly over q, the multiplicative order L_n of α, given above, satisfies the bound*

$$L_n \geq \exp((\pi\sqrt{\frac{2(p-1)}{3p}} + o(1))\sqrt{n}),$$

as $n \to \infty$.

Construction of New Toric Quantum Codes

Clarice Dias de Albuquerque

Universidade Estadual de Campinas

(Joint work with Reginaldo Palazzo Jr. and Eduardo Brandani Silva)

The use of properties from quantum mechanics theoretically allows faster quantum computation than classic computation to obtain solutions of certain computational problems. However, one of the difficulty to the construction of such computers is the existence of *decoherence* due to the interaction between the systems and the surrounding environment.

Research indicates that this problem may be solved by use of quantum error-correcting codes. Most of the codes available in the literature are based on *quantum stabilizer codes*. The *toric codes* are a class of stabilizer codes associated to the square lattices in the torus, [1], which the parameters depend on the topology of the torus.

In [2] it is proposed a new interpretation of the toric codes based on a different regular fundamental region, Lee spheres, that provides a significant improvement in the length of the code and, consequently, an improvement in the coding rate too.

In this paper, we propose to use the concept of polyomino in the construction of the fundamental region of a toric code which tessellates a corresponding square lattice by translations of this polynomino (fundamental region). The codes defined in this way keep the same properties of the Kitaev's toric codes. This construction reproduces known codes and generates countless new classes of toric quantum codes, for instance, the class $[[d^2, 2, d]]$, which is the best known so far, in terms of achieving the least codeword length.

References

[1] A. Yu Kitaev, *Fault-tolerant quantum computation by anyons*, Annals of Physics **303**, pp. 2, 2003.

[2] H. Bombin and M. A. J. Martin-Delgado, *Homological error correction: classical and quantum codes*, J. Math. Phys. **48**, pp. 052105, 2007.

Cycles Structure of Permutations Induced by Perfect Nonlinear Functions over Finite Fields

Hassan Aly

University of Cairo

(Joint work with Rasha Shaheen)

Let p be an odd prime and $q = p^n$ be a prime power with positive integer n. Let $\mathbf{F}_q$ be the finite field of order q and $\mathbf{F}_q^*$ is the nonzero elements in $\mathbf{F}_q$. A function $f : \mathbf{F}_q \to \mathbf{F}_q$ is called *a perfect nonlinear function* if its *difference function* $\Delta_f(x) = f(x + a) - f(x) - f(a)$ is a permutation over $\mathbf{F}_q$ for each $a \in \mathbf{F}_q^*$. This paper gives the complete cycles structures of the permutations $\Delta_f(x)$, for $a \in \mathbf{F}_p$ and $\gcd(n, p) = 1$, over $\mathbf{F}_q$ for the perfect nonlinear functions:

1. $f(x) = x^2$ over $\mathbf{F}_q$.
2. $f(x) = x^{p^k+1}$ over $\mathbf{F}_q$ where $n/\gcd(n, k)$ is odd and $k < \frac{n}{2}$,
3. $f(x) = x^{10} + x^6 - x^2$ over $\mathbf{F}_{3^n}$ where $n \geq 5$ is odd,
4. $f(x) = x^{10} - x^6 - x^2$ over $\mathbf{F}_{3^n}$ where $n \geq 5$ is odd.

An algorithm has been developed to compute the cycles structure of any difference permutation function $\Delta_f(x)$, for $a \in \mathbf{F}_p$ and $\gcd(n, p) = 1$, over $\mathbf{F}_q$, for any perfect nonlinear function f which is a Dembowski-Ostrom polynomial with coefficients in $\mathbf{F}_p$. Several examples have been obtained over small finite fields. Cycles of small lengthes of such permutations may be avoided in applications. Extending this algorithm to a Dembowski-Ostrom polynomial with coefficients in $\mathbf{F}_{p^n}$ is an open problem.

The main objective of studying such cycles is to find under which circumstances different permutations $\Delta_f(x)$ split up the finite field $\mathbf{F}_q$ into the same number of cycles of the same lengthes. In

this direction the paper shows that if $k_1 \equiv pk_2 \pmod{n}$ the permutations induced by the functions $x^{p^{k_1}+1}$ and $x^{p^{k_2}+1}$ have the same number of cycles of the same lengthes. As an example the permutations of the two functions x^{26} and x^{126} splits the finite field $\mathbf{F}_{5^7}$ into 1 cycle of length 1, 1 cycle of length 4, 72 cycles of length 217, and 72 cycles of length 868. This is taken place although k_1 and k_2 in this example have been chosen less than $\frac{n}{2}$, the condition required for the two functions to be unequivalent. Other examples are shown in the paper. We are working to find all possible values of $k \leq \frac{n}{2}$ that give this property. The work of this paper is based on the results of Mullen and Vaughan in [1].

References

[1] Gary L. Mullen and Theresa P. Vaughan, " Cycles of Linear Permutation Over a Finite Field," *Linear algebra and its Applications*, vol 108,pp. 63–82, 1988.

Error correcting codes arising from cubes

Sheng Bau

Fuzhou University

In this note, experimental results on binary nonlinear error correcting codes arising from special families of graphs will be reported. The graph Q_n of the n-dimensional cube provide binary nonlinear error correcting codes with high capacity of error correction. The codes are given by maximum induced forests of a specific type in cubes, obtained by deletion of a (minimum) decycling set. Many interesting problems remain open in this topic.

References

[1] S. Bau and L.W. Beineke: The decycling number of graphs, *Australasian Journal of Combinatorics* 25(2002), 285-298.

[2] S. Bau, L.W. Beineke, G-M. Du, Z-S. Liu and R.C. Vandell: Decycling cubes and grids, *Utilitas Mathematica* 59(2001), 129137.

[3] L.W. Beineke and R.C. Vandell: Decycling graphs, *Journal of Graph Theory* 25(1996), 59-77.

[4] P. Erdős, M. Saks and V.T. Sós: Maximum induced trees in graphs, *Journal of Combinatorial Theory* B41(1986), 61-79.

[5] J.H. van Lint: Introduction to Coding Theory, Springer Verlag, New York 1982.

[6] F.J. MacWilliams and N.J.A. Sloane: The Theory of Error Correcting Codes, North-Holland, Amsterdam 1978.

Subclass of non-binary comulative Goppa codes

Sergey Bezzateev

St.Petersburg University of Aerospace Instrumentation

(Joint work with Natalia Shekhunova)

A new subclass of non-binary comulative (L, G) -codes [1] with $L = \{\alpha \in GF(q^{2l}) : G(\alpha) \neq 0\}$ and $G(x) = g(x)^q$, where $g(x)$ - is a separable polynomial of one of the following forms:

$$\begin{aligned} g_1(x) &= x^{t+1} + 1, \\ g_2(x) &= x^t + x^{t-1} + 1, \\ g_3(x) &= x^t + x + 1, \\ g_4(x) &= x^{t-1} + 1, \quad \text{where} \quad t = q^l \end{aligned}$$

is considered. For these codes the improved bounds for dimension and minimal distance are obtained. The construction of the presented subclass is based on the approach used early for constructing the subclasses of the best known binary classical Goppa codes [2]. It is shown that q-ary Goppa codes from the new subclass can be represented as a chain of equivalent and truncated codes in the same way as it was done in the binary case before [2]. The main theorem about the dimension of the first code from the subclass gives us an improved estimation which is better than it is for q-ary BCH codes.

Theorem *Let us consider the q-ary comulative (L, G) code with length $n = t^2 - t - 1$ and $G_1(x) = (x^{t+1} + 1)^q$ and $L = \{GF(t^2) \setminus \{\alpha : G_1(\alpha) = 0\}\}$, where $t = q^l$. The dimension k of this code is estimated as*

$$k \geq n - 2l(q(t+1) - (t+1)) + 2l(\tfrac{(q-1)(q+3)}{2}).$$

Examples of codes from subclass for q= 3,5,7,11 are presented.

References

[1] V.D.Goppa, Rational representation of codes and (L,g)-codes, Probl.Peredachi Inform,7,No.3,pp.41-49, 1971

[2] S. Bezzateev , N. Shekhunova, Chain of Separable Binary Goppa Codes and their Minimal Distance, *IEEE Transaction on Information Theory* , Volume 54, Number 12, December 2008 , pp.5773-5778

Distinct difference configurations

Simon R. Blackburn

Royal Holloway, University of London

(Joint work with T. Etzion, K.M. Martin, M.B. Paterson)

We say that a set $\{v_1, v_2, \ldots, v_m\}$ of vectors in $\mathbb{Z}^2$ is a *distinct difference array with m dots and diameter d* if the following two conditions hold:

1. The $m(m-1)$ vectors $v_i - v_j$ (where $i \neq j$) are distinct.

2. The vectors $v_i - v_j$ have (Euclidean) length at most d.

Costas arrays and B_2 sequences are examples of distinct difference arrays.

We give some constructions and bounds for distinct difference arrays (from [1] and [2]), and show how these results settle (in the negative) an old conjecture of Golomb and Taylor [1] on the existence of infinitely many honeycomb arrays.

References

[1] S.R. Blackburn, Tuvi Etzion, Keith M. Martin and Maura B. Paterson, 'Two-Dimensional Patterns with Distinct Differences – Constructions, Bounds, and Maximal Anticodes', `http://arxiv.org/abs/0811.3832`.

[2] S.R. Blackburn, Tuvi Etzion, Keith M. Martin and Maura B. Paterson, 'Distinct difference configurations: Multihop paths and key predistribution in sensor networks'. See `http://arxiv.org/abs/0811.3896`.

[3] S. W. Golomb and H. Taylor 'Constructions and properties of Costas arrays', Proceedings of the IEEE, vol. 72, pp. 11431163, 1984.

The multi-Frobenius non-classical curves

Herivelto Borges

The University Texas at Austin

An irreducible curve $\mathcal{F}$ defined over $\mathbf{F}_q$ is called q-Frobenius non-classical if the image $Fr(P)$ of each simple point P of $\mathcal{F}$ under the Frobenius map lies on the tangent line at P.

Based on [2], Hefez and Voloch extended the study of the q-Frobenius non-classical curves in [1], where some interesting arithmetic and geometric properties of such curves were first pointed out.

In this talk, I will present and characterize all irreducible plane curves defined over $\mathbf{F}_q$ which are simultaneously Frobenius non-classical for different powers of q. Such characterization gives rise to many previously unknown curves which turn out to have some interesting properties. For instance, for $n \geq 3$ a plane curve which is both q- and q^n-Frobenius non-classical will have its number of $\mathbf{F}_{q^n}$-rational points attaining the Stöhr-Voloch bound.

References

[1] A. Hefez and J.F.Voloch, Frobenius non classical curves, Arch. Math. **54**, (1990) 263–273.

[2] Stöhr, K-O. and Voloch, J.F., Weierstrass Points and Curves over Finite Fields, Proc. London Math. Soc.(3) **52** (1986)1–19.

Multidimensional cyclic burst–error–correcting codes

Igor Boyarinov

Institute for System Analysis RAS

Let $F[x_1,\ldots,x_m]$ be the ring of polynomials $f(x_1,\ldots,x_m)$ over $GF(q)$ and $I_{n_1,\ldots,n_m} = \langle x^{n_1}-1,\ldots,x^{n_m}-1\rangle$ be the ideal of $F[x_1,\ldots,x_m]$. A m–dimensional cyclic code is defined as an ideal in the residue class ring $R(x_1,\ldots,x_m) = F[x_1,\ldots,x_m]/I_{n_1,\ldots,n_m}$. A polynomial $e(x_1,\ldots,x_m) \in R(x_1,\ldots,x_m)$ with the maximal degrees of variables $deg_{x_i}e(x_1,\ldots,x_m) < n_i,\ i=1,\ldots,m$ is a cyclic $b_1\times\ldots\times b_m-$burst if there exist a polynomial $b(x_1,\ldots,x_m)$ with the maximal degrees of variables $deg_{x_i}b(x_1,\ldots,x_m) < b_i$ such that the polynomials $e(x_1,\ldots,x_m)$ and $x^{u_1}\ldots x^{u_m}b(x_1,\ldots,x_m)$ belong to the same residue class in $R(x_1,\ldots,x_m)$ for some $0 \le u_i < n_i,\ i=1,\ldots,m$.

In this paper we consider m–dimensional cyclic codes correcting cyclic $b_1\times\ldots\times b_m-$bursts of errors. We generalize and develop the constructions of two–dimensional cyclic array codes correcting rectangular cyclic bursts of errors [1]. So m–dimensional cyclic Fire codes are described as follows.

Theorem *Let s, b_i be positive integers and p be a prime, $q=p^s$, $c_i \ge 2b_i-1$, $i=1,\ldots,m$. Also, let $p_i(x_i)$ be a irreducible polynomial over $GF(q)$ of degree $\nu_i \ge b_i$ and period ξ_i, $n_i = LCM(c_i,\xi_i)$, $i=1,\ldots,m$. Then the intersection of ideals $A_{c_1,\ldots,c_m} = \langle x_1^{c_1}-1,\ldots,x_m^{c_m}-1\rangle$ and $A_{p_1(x_i),\ldots,p_m(x_m)} = \langle p_1(x),\ldots,p_m(x_m)\rangle$ in the the residue class ring $R(x_1,\ldots,x_m) = F[x_1,\ldots,x_m]/I_{n_1,\ldots,n_m}$ is the m–dimensional cyclic code correcting cyclic $b_1\times\ldots\times b_m-$bursts of errors.*

References

[1] I.M.Boyarinov,"Two–dimensional array codes correcting rectangular burst errors," *Problems of Information Transmission*,vol. 42, No. 2,pp. 90–105, 2006.

Bounds on the Size of a Network Error Correcting Code

Eimear Byrne

University College Dublin

Versions of the Singelton, sphere-packing and Gilbert-Varshamov bounds for a particular model for error-correcting codes for coherent network coding were given in [1]. Here we extend the classical Plotkin and Elias bounds (cf. [2, Ch. 17]) for the same model. We assume an acyclic digraph with n edges, a single source node s and several sinks labelled by elements of a set T. The min-cut for each sink t is n_t, which we assume to be the number of edges incident with t. Network words are transmitted along the network via an invertible transfer matrix $F \in \mathbb{F}_q^{n\times n}$ and are projected to sink t by $F_t \in \mathbb{F}_q^{n\times n_t}$, a rank n_t submatrix of F. We define $K_t := \ker F_t \subset \mathbb{F}_q^n$ and $\ell_t := |\mathrm{supp}(K_t)|$. If $\mathbf{x}\in\mathbb{F}_q^n$ is transmitted and edges of the network are corrupted by an error vector $\mathbf{e}$ then the word received by t is $\mathbf{y}_t = (\mathbf{x}+\mathbf{e})F_t$. F_t induces a distance function on $\mathbb{F}_q^{n_t}$ by $\mathrm{d}_t(\mathbf{u},\mathbf{v}) := \min\{\mathrm{d}_H(\mathbf{x},\mathbf{y}) : \mathbf{x}F_t = \mathbf{u}, \mathbf{y}F_t = \mathbf{v}\}$, where d_H denotes the Hamming distance. We let $C_t \subset \{\mathbf{x}F_t \in \mathbb{F}_q^{n_t} : \mathbf{x}\in\mathbb{F}_q^n\} = \mathbb{F}^{n_t}$ denote an $(n_t, |C_t|, d_t)$ network for node t where $d_t := \mathrm{d}_t(C_t)$. A network code C is a collection $C := \{C_t : t\in T\}$ and we say that C is an $(n, \{(n_t, c_t, d_t) : t\in T\})$ network code. Let $\gamma := \frac{q-1}{q}$ $d := \min\{d_t : t\in T\}$, $\ell := \min\{\ell_t : t\in T\}$ and $c := \min\{|C_t|x : t\in T\}$.

Theorem *Let $d > \gamma n$. Then*

$$c \leq \min\left\{\frac{d_t - \gamma\ell_t}{d_t - \gamma n} : t \in T\right\} \leq \frac{d - \gamma\ell}{d - \gamma n}$$

Theorem *Let $d_t < \gamma n$ and let $r \leq \gamma n - \sqrt{\gamma(\gamma n - d_t)(n - \ell_t)}$ for each $t \in T$. Then*

$$c \leq \min\left\{\frac{(d_t - \gamma\ell_t)\gamma(n - \ell_t)q^{n-\ell_t}}{(r^2 - 2\gamma nr + \gamma^2\ell_t n + \gamma d_t(n - \ell_t))|B^{n-\ell_t}(r - \gamma\ell_t)|} : t \in T\right\}.$$

References

[1] S. Yang, R. Yeung, "Refined Coding Bounds for Network Error Correction", *IEEE Inform. Th. Workshop on Inform. Th. for Wireless Networks*, July 2007, pp. 1–5.

[2] F. J. MacWilliams, N.J.A Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

Structural weaknesses of differentially uniform mappings

Anne Canteaut

INRIA Paris-Rocquencourt, project-team SECRET

(Joint work with Maria Naya-Plasencia)

The resistance of a function $F : \mathbf{F}_2^n \to \mathbf{F}_2^n$ to differential cryptanalysis is quantified by Δ_F which is the maximal cardinality $|\{x \in \mathbf{F}_2^n, F(x + \alpha) + F(x) = \beta\}|$ for $\alpha, \beta \in (\mathbf{F}_2^n)^*$. Then, F is said to be differentially Δ_F-uniform [2]. While Δ_F must be as small as possible, we show that a small Δ_F introduces other weaknesses in a cryptosystem, due to the existence of a nonzero output difference δ such that the set $D(\delta) = \{\alpha \in \mathbf{F}_2^n, \exists x \in \mathbf{F}_2^n \text{ with } F(x + \alpha) + F(x) = \delta\}$ has a large cardinality. It can be shown that, if F is a differentially Δ-uniform permutation over $\mathbf{F}_2^n$, then $|D(\delta)| \geq 2^n\Delta^{-1}$ for any $\delta \in \mathbf{F}_2^n$. The algebraic structure of $D(\delta)$ is also of great importance, especially the existence of a large affine subspace V such that the proportion of elements in V which belong to $D(\delta)$ is high. The extreme situation, related to the crooked property [1], occurs in particular when F^{-1} is quadratic.

As an example, an internal collision attack on the hash function Maraca, submitted to the SHA-3 competition, is mounted if its inner permutation F is such that there exists $\delta \neq 0$ satisfying one of the following conditions, where h is the hash size: $|D(\delta)| > 2^{n-\frac{h}{2}}$ or there exists an affine subspace V such that $|D(\delta) \cap V| > 2^{n-h}$ and $|D(\delta) \cap V|/|V| > 2^{-\frac{h}{2}}$. For the concrete case of Maraca, we exploit the existence of some δ such that $D(\delta)$ is included in a subspace of dimension 640 of $\mathbf{F}_2^{1024}$. But, contrary to a recent attack by Indesteege which only holds for this very particular permutation, our result is very general and it exploits some structural properties which contradict the usual security criterion. For instance, the attack becomes even more efficient if the inner permutation is replaced by the inverse function over $\mathbf{F}_2^n$.

References

[1] T. Bending and D. Fon der Flass. Crooked functions, bent functions, and distance regular graphs. *Electron. J. Combin.*, 5(1), 1998. R34.

[2] K. Nyberg and L.R. Knudsen. Provable security against a differential attack. *Journal of Cryptology*, 8(1):27–37, 1995.

CCZ-equivalence and Boolean functions

Claude Carlet

University of Paris 8, LAGA

(Joint work with Lilya Budaghyan)

The notion of CCZ-equivalence of vectorial functions, introduced in [3], is the proper notion of equivalence for vectorial functions used as S-boxes in cryptosystems. It preserves the differential uniformity and the nonlinearity of a function (the properties which describe the resistance of the function to differential and linear attacks, respectively).

Previously, CCZ-equivalence of vectorial Boolean functions has been studied in [1, 2]. We study further CCZ-equivalence of Boolean (n, m)-functions and its relation to EA-equivalence. EA-equivalence is a very particular case of CCZ-equivalence which is easy to deal with. We prove that for Boolean functions (that is, for $m = 1$), CCZ-equivalence coincides with EA-equivalence. On the contrary, we show that for (n, m)-functions, CCZ-equivalence is strictly more general than EA-equivalence when $n \geq 5$ and m is greater or equal to the smallest positive divisor of n different from 1. Our result on Boolean functions allows us to study the natural generalization of CCZ-equivalence corresponding to the CCZ-equivalence of the indicators of the graphs of the functions. We show that it coincides with CCZ-equivalence.

References

[1] L. Budaghyan and C. Carlet. On CCZ-equivalence and its use in secondary constructions of bent functions. To appear in preproceedings of WCC 2009. Preprint available at IACR ePrint Archive, number 2009/042.

[2] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 1141-1152, March 2006.

[3] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2), pp. 125-156, 1998.

Determination of the minimal length of some linear codes

Eun Ju Cheon

Gyeongsang National University

Let F_q^n be the n-dimensional vector space over the finite field F_q of order q, where q is a prime power. A q-ary $[n,k,d]$ linear code $\mathcal{C}$, simply $[n,k,d]_q$ code is a k-dimensional linear subspace of F_q^n with minimum Hamming distance d. Here $d = \min\{d(x,y) \mid x,y \in C, x \neq y\}$ and $d(x,y)$ is the number of different coordinates in x and y.

The fundamental problem in coding theory is to optimize any one parameter among n, k and d when the other two are given. We consider the problem to find the smallest length n, denoted by $n_q(k,d)$ for which there exists an $[n,k,d]_q$ linear code for given k and d. ([1], [4])

A linear code is called (length) optimal if whose length is equal to $n_q(k,d)$.

For an $[n,k,d]_q$ linear code C, it holds that

$$n \geq g_q(k,d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. This is called the Griesmer bound. Obviously, we note $n_q(k,d) \geq g_q(k,d)$.

We prove that for $q \geq 5$, there does not exist a $[g_q(6,d),6,d]_q$ code with $q^5 - q^3 - q^2 - 2q + 1 \leq d \leq q^5 - q^3 - q^2 - q$, and we have $n_q(6,d) = g_q(6,d) + 1$ for $q^5 - q^3 - q^2 - 2q + 1 \leq d \leq q^5 - q^3 - q^2 - q$ and $q \geq 5$.

References

[1] E.J. Cheon, *A class of optimal linear codes of length one above the Griesmer bound*, Designs Codes and Cryptography, 51, pp.9–20, 2009.

[2] R. Hill, *Optimal linear codes*, Cryptography and Coding II (ed. C. Mitchell), Oxford Univ. Press, Oxford, pp.75–104, 1992.

On constructing non-associative commutative algebras of dimension 2 over a prime field

Robert Coulter

University of Delaware

(Joint work with Marie Henderson)

We discuss recent work on constructing all algebras of the title using a method for constructing rings introduced by Batten, Coulter and Henderson. There it was conjectured that the number of non-isomorphic non-associative commutative algebras of dimension 2 over a prime field $GF(p)$ is $p^2 + 3p + 6$ if $p > 3$ and $p^2 + 3p + 5$ if $p = 3$. Though we are unable, at this time, to establish the full conjecture, we do prove that the number of classes is at least p^2.

The construction method involves Dembowski-Ostrom (DO) polynomials, with the resulting isomorphism problem reducing to the problem of determining the distinct orbits of a suitable action of the group of all non-singular linear transformations (as linearised permutation polynomials) on the set of all DO polynomials.

In the original paper of Batten *et al*, it was shown there are precisely 6 distinct strong isotopism classes for such algebras, regardless of the odd characteristic of the underlying prime field. We take a

similar approach for the isomorphism problem, looking to provide an explicit representative for each orbit. The isomorphism problem is, in a sense, a fine tuning of the strong isotopism classification, so that one may attack each of the 6 strong isotopism classes separately. Unfortunately, the isomorphism problem is sufficiently more difficult, that even with this simplification of the problem, the full statement of the conjecture remains unproved.

References

[1] L.M. Batten, R.S. Coulter and M. Henderson, *Extending abelian groups to rings*, J. Austral. Math. Soc. **82** (2007), 297–313.

Galois Rings, DRADS, and 3-class association schemes with rank 4 automorphism groups

James Davis

University of Richmond

(Joint work with J. Polhill)

Doubly Regular Asymmetric Digraphs (DRAD) with rank 4 automorphism groups were previously thought to be rare. We exhibit difference sets in Galois Rings that can be used to construct an infinite family of DRADs with rank 4 automorphism groups. These DRADs can also be used to construct nonsymmetric 3-class imprimitive association schemes.

On $\mathcal{C}$-ultrahomogeneous graphs and digraphs

Italo J. Dejter

University of Puerto Rico

The notion of a $\mathcal{C}$-ultrahomogeneous graph, due to Isaksen et al., is adapted for digraphs and studied for the twelve cubic distance transitive graphs, with $\mathcal{C}$ formed by g-cycles and $(k-1)$-paths, where $g =$ girth and $k =$ arc-transitivity. Excluding the Petersen, Heawood and Foster (90 vertices) graphs, one can go further by considering the $(k-1)$-powers of g-cycles under orientation assignments provided by the initial approach. This allows the construction of fastened $\mathcal{C}$-ultrahomogeneous graphs, via applications of finite fields, with $\mathcal{C}$ formed by copies of K_3, K_4, C_7 and $L(Q_3)$, for the Pappus, Desargues, Coxeter and Biggs-Smith graphs.

In particular, the Biggs-Smith graph yields a connected edge-disjoint union of 102 copies of K_4 which is a non-line-graphical Menger graph of a self-dual (102_4)-configuration, a K_3-fastened $\{K_4, L(Q_3)\}$-ultrahomogeneous graph. This contrasts with the self-dual (42_4)-configuration of [1], whose non-line-graphical Menger graph is K_2-fastened $\{K_4, K_{2,2,2}\}$-ultrahomogeneous.

The construction of [1] and the fact that the Coxeter graph (28 vertices) yields the Klein graph (56 vertices) as a $\mathcal{C}$-ultrahomogeneous graph embedded in the torus of genus 3 (dressed in F. Klein's work as the quartic $x^3y + y^3z + z^3x = 0$) with faces delimited by the g-cycles ($g = 7$) depend on finite fields of characteristic 2, as it does also our final result on the existence of a strongly connected $\vec{C}_4$-ultrahomogeneous digraph on 168 vertices and 126 pairwise arc-disjoint 4-cycles, with regular indegree and outdegree 3 and no circuits of lengths 2 and 3.

References

[1] I. J. Dejter, *On a $\{K_4, K_{2,2,2}\}$-ultrahomogeneous graph*, to appear in the Australasian Journal of Combinatorics.

[2] D. C. Isaksen, C. Jankowski and S. Proctor, *On K_*-ultrahomogeneous graphs*, Ars Combinatoria, Volume LXXXII, (2007), 83–96.

Elliptic Periods and Torus-Based Cryptography

Clément Dunand

University of Rennes 1

(Joint work with R. Lercier)

This work aims at giving an efficient parameterization of algebraic tori using elliptic normal bases in finite fields extensions.

Usually, finite field discrete logarithm based cryptosystems make use, not of a full cyclic group $\mathbb{F}_{q^n}^\times$, but of a subgroup of order $\Phi_n(q)$, where Φ_n denotes the n-th cyclotomic polynomial. In terms of algebraic varieties, such subgroups have the structure of algebraic tori of dimension $\varphi(n)$ (*cf.* [3]). The question that we consider is to what extent we can efficiently parameterize elements of these tori with $\varphi(n)$-tuples, instead of n-tuples. This is an interesting feature in practical applications.

In [2], van Dijk and Woodruff exhibit an explicit algorithm for computing the following parameterization:

$$\Theta : T_n(\mathbb{F}_q) \times \prod_{\substack{d|n \\ \mu(n/d)=-1}} \mathbb{F}_{q^d}^\times \longrightarrow \prod_{\substack{d|n \\ \mu(n/d)=+1}} \mathbb{F}_{q^d}^\times .$$

They show that this requires $O(n^3 \log^2 q)$ elementary operations. We observe that the heaviest part of the complexity comes from exponentiations to powers with sparse decompositions in basis q and we succeed in speeding up the algorithm with the help of an efficient normal basis representation of $\mathbb{F}_{q^n}$, more precisely elliptic normal bases as recently introduced in [1].

In a torus cryptographic context, q is large and n is small, *i.e.* $n = o(q)$. When n is the product of two distinct primes, we prove that we can reduce the asymptotical cost by a $\log q$ factor. For more general n, we observe a similar improvement.

References

[1] J-M. Couveignes and R. Lercier. Elliptic Periods for Finite Fields. *Finite Fields and their Applications*, 15(2009), pp. 1–22.

[2] M. van Dijk, R. Granger, D. Page, K. Rubin, A. Silverberg, M. Stam, D. Woodruff. Practical Cryptography in High Dimensional Tori. *EUROCRYPT 2005*, LNCS **3494**, pp. 234-250.

[3] K. Rubin, A. Silverberg. Torus-Based Cryptography. *Crypto'03*, LNCS **2729**, pp. 349-365.

Excluded Norm Problems

Gary L. Ebert

University of Delware

In recent years there have been several instances of situations in finite geometry which eventually lead to questions about excluded norms in finite fields. By this, I mean problems of the following type:

1. Determine the elements in $S_1 = \mathbb{F}_q^* \setminus \{N_{q^6/q^2}(1+u) \mid u^{q^2-q+1} = 1\}$, for any odd prime power q.
2. Let $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that $u^3 = \sigma u + 1$. Determine the elements in $S_2 = \mathbb{F}_{q^3}^* \setminus \{N_{q^6/q^3}(a+bu+u^2) \mid a, b \in \mathbb{F}_{q^2}\}$, for any prime power q.

It should be noted that in the first problem $N_{q^6/q^2}(1+u) \in \mathbb{F}_q$ when $u \in \mathbb{F}_{q^6}$ is a $(q^2-q+1)^{st}$ root of unity.

The first problem arose when enumerating the odd order three-dimensional flag-transitive affine planes, and the second problem arose when constructing certain semifields of order q^6 which are 2-dimensional over their left nucleus and 6-dimensional over their center. The amazing answers to these two problems are the following:

1. $S_1 = \emptyset$ if $q \not\equiv 1 \pmod 3$, and $S_1 = \{-1\}$ if $q \equiv 1 \pmod 3$.
2. $S_2 = \{\sigma^2 + 9u + 3\sigma u^2\}$ if q is odd, and $S_2 = \emptyset$ if q is even.

The known proofs are lengthy and awkward, involving messy polynomial counts in the first case and a careful analysis of the $\mathbb{F}_q$-rational points on an algebraic plane curve in the second case. It would be nice to find a general context for proving such results, and to know how rare such results are.

New caps in $PG(k, 5)$

Yves Edel

Ghent University

(Joint work with J. Bierbrauer)

We give a new recursive construction for caps in $PG(k, q)$, which generalizes the construction that lead to the 66-cap in $PG(4, 5)$ [2]. Apart from giving a more elegant construction for the 66-cap we are able to construct a 195-cap in $PG(5, 5)$, which improves the former lower bound (186 of [2]) on the maximal size of a cap in $PG(5, 5)$.

With the methods of [1] we get, using the new 195-cap, also substantial improvements on lower bound on the maximal size of a cap in $PG(8, 5)$ and $PG(11, 5)$.

References

[1] Y. Edel and J. Bierbrauer, *Recursive constructions for large caps,* Bulletin of the Belgian Mathematical Society - Simon Stevin, vol. 6, pp. 249–258, 1999.

[2] Y. Edel and J. Bierbrauer, *Large caps in small spaces,* Designs, Codes and Cryptography, vol. 23, pp. 197–212, 2001.

Normal cyclotomic schemes over a Galois ring

Sergei Evdokimov

Steklov Institute of Mathematics at St.Petersburg

Let R be a finite commutative ring with identity and let $\mathcal{C} = \mathrm{Cyc}(K, R)$ where K is a subgroup of the multiplicative group $R^\times$ of the ring R, be a *cyclotomic scheme* over R (see e.g. [1]). Cyclotomic schemes were introduced in 1973 by Delsarte (for R a field) in connection with coding theory. Denote by $\mathrm{Aut}(\mathcal{C})$ the automorphism group of $\mathcal{C}$, i.e. the set of all permutations $f \in \mathrm{Sym}(R)$ such that $x-y \in rK$ implies $x^f - y^f \in rK$ for all $x, y, r \in R$. The scheme $\mathcal{C}$ is called *normal* if $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}_1(R)$. In [1] the problem of identifying the normal cyclotomic schemes over the ring R was reduced to that over the local components of R.

To identify the normal cyclotomic schemes over a local ring, first suppose that $R = \mathbf{F}_q$ is a field. If $K = \mathbf{F}_q^\times$, then $\mathrm{Aut}(\mathcal{C}) = \mathrm{Sym}(R)$ and it is easy to see that the scheme $\mathcal{C}$ is normal if and only if $q = 2, 3, 4$. On the other hand, a reformulation of an old number-theoretical result by McConnel (1963) shows that $\mathcal{C}$ is normal for all $K < \mathbf{F}_q^\times$.

Now let R be a Galois ring (see [2]). We observe that Galois rings are local rings that generalize both finite fields and prime power cardinality factors of the ring $\mathbf{Z}$. To formulate the main result we need the following definition. A group $K \leq R^\times$ is called *pure* (resp. *quasipure*) if the equality $K + I = K$ where I is an ideal of R, implies that $I = 0$ (resp. $I \subset \mathrm{ann}(\mathrm{rad}(R))$).

Theorem *Let R be a Galois ring with residue field $\mathbf{F}_q$, other than a field, and $K \leq R^\times$ a group. Then the scheme $\mathrm{Cyc}(K, R)$ is normal if and only if the group K is pure for $q > 2$ and quasipure for $q = 2$.*

The case of an odd q was earlier studied in [1].

References

[1] S. Evdokimov, I. Ponomarenko, *Normal cyclotomic schemes over a finite commutative ring*, Algebra and Analysis, 19 (2007), 59–85. English translation in St.Petersburg Math. J., 19 (2008), 911-929.

[2] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, Vol. 28, Marcel Dekker Inc., New York, 1974.

Geometrically Uniform Hyperbolic Signal Sets Generated by Arithmetic Fuchsian Groups

M. B. Faria

State University of Campinas

(Joint work with V. L. Vieira, R. Palazzo Jr.)

In this paper we consider hyperbolic tessellations $\{10\lambda, 2\lambda\}$ denser than the self-dual tessellations $\{4g, 4g\}$, and so giving rise to denser lattices, in order to construct geometrically uniform hyperbolic signal sets related to arithmetic Fuchsian groups, [1]. The relevance of the former tessellations for $\lambda = 2^n$, $n \in \mathbb{N}$, is the connection of the group $\Gamma_{10\lambda}$ with the group Γ_{4g}, for $g = 2^n$ and $g = 5 \cdot 2^n$, [2]. The difficulty that comes out as a consequence of the change from the tessellation $\{4g, 4g\}$ to the tessellation $\{p, q\}$, is to determine the values of p such that Γ_p is an arithmetic Fuchsian group (to determine the arithmetic Fuchsian group Γ_p, (a Fuchsian group associated with a fundamental region, polygon with p-edges) in the group $\Gamma(A, O)$ we need to determine the number field K and a ring R in K, such that the quaternion algebra be given by $\mathcal{A} = (a, b)_K$ and the maximal order be given by $\mathcal{O} = (a, b)_R$). The complexity involved consists not only in finding a standard form for the generator matrices of the group Γ_p (since we want to construct a quaternion division algebra $\mathcal{A}$ from Γ_p), but in finding explicitly the number field K and a ring $R \subset K$ such that $\mathcal{A} = (a, b)_K$ and $\mathcal{O} = (a, b)_R$. As an example of this difficulty and complexity, we mention the case of the group Γ_{18} associated with the tessellation $\{12g - 6, 3\}$, when $g = 2$. The search of a group Γ_p, or equivalently, the surface $\mathbb{H}^2/\Gamma_p$, with the aim at constructing a hyperbolic signal set derived from the tessellation $\{p, q\}$, is equivalent to searching a prime ideal $\mathfrak{p}$, conveniently chosen in the integer ring $\mathfrak{D}_K$ of a number field K, such that the Euclidean signal set, coming from the quotient ring $\mathfrak{D}_K/\mathfrak{p}$ has a field structure and this is finite since $\mathfrak{p}$ is the principal ideal with norm $\mathfrak{q}$, with $\mathfrak{q}$ prime, which follows the theory of algebraic numbers, that this quotient is a finite field with $\mathfrak{q}$ elements. In the construction of a signal set in the hyperbolic plane $\mathbb{H}^2$, we consider a Fuchsian group whereas in the construction of a signal set in the Euclidean plane we consider an Abelian group. In this paper we provide the necessary conditions to obtain an arithmetic Fuchsian group Γ_p from a given hyperbolic tessellation $\{p, q\}$, and from this to construct a geometrically uniform hyperbolic signal set, whose signals constitute a $G_{\mathfrak{p}}$-orbit of 0.

References

[1] K. Takeuchi, "A caracterization of arithmetic Fuchsian groups," *J. Math. Soc.*, Japan, vol. 27, pp. 600-612, 1975.

[2] V.L. Vieira, R. Palazzo Jr., and M.B. Faria, "On the arithmetic Fuchsian groups derived from quaternion orders," *IEEE-SBrT VI Intl Telecommunications Symposium*, (ITS2006), Brazil, pp.1-6, 2006.

Classification of Rosenbloom-Tsfasman block codes

M. Firer

State University of Campinas

(Joint work with M. M. A. Souza and L. Panek)

Poset and block metrics were introduced in recent years as alternative metrics to study error correcting codes. Poset-block codes were introduced in 2008, intervening both poset and block metrics. A family of such metrics is the Rosenbloom-Tsfasman block (RTB) metrics, that is defined as follows: let N be a positive integer, $N = \pi_1+\pi_2+\ldots+\pi_n$ a partition of N and $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ a vector space over the finite field $\mathbb{F}_q$, with $\dim V_i = \pi_i$. The **RTB weight** w_π (or simply the **π-weight**) of a non-zero vector $x = x_1 + x_2 + \ldots + x_n \in V$, with $x_i \in V_i$, is $w_\pi(x) := \max\{i : x_i \neq \mathbf{0}\}$ and $d_\pi(x, y) := w_\pi(x - y)$ is a metric. The metric space (V, d_π) is called the **π-RTB space**.

Invariants of codes, such as generalized Wei minimal weights d_r^π, are defined in RTB-spaces as in usual Hamming spaces, just exchanging the Hamming weight by the π-weight.

Our main result is the Classification Theorem, which asserts that a k-dimensional linear code C with π-weight hierarchy $(d_1^\pi, ..., d_k^\pi)$ is equivalent to a code generated by a matrix in a canonical form

$$\begin{pmatrix} \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \ldots & \widetilde{I}_{s_{i_m} t_{i_m}} & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \widetilde{I}_{s_{i_{m-1}} t_{i_{m-1}}} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \cdots & \widetilde{I}_{s_{i_1} t_{i_1}} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \end{pmatrix}$$

where $\widetilde{I}_{ij} = \left(I_{i\times i} | 0_{i\times(j-1)}\right)$, with $I_{i\times i}$ and $0_{i\times(j-1)}$ being respectively the identity and null matrices, $d_r^\pi(C) = i_j$ for $s_{i_1} + ... + s_{i_{j-1}} < r \leq s_{i_1} + ... + s_{i_{j-1}} + s_{i_j}$ and $s_{i_1} + \ldots + s_{i_m} = k$.

Beside this result, we develop much of the classical theory of error correcting codes for RTB-codes, including determination of packing and covering radius, classification of MDS, perfect codes and quasi-perfect codes and propose an algorithm for syndrome decoding, including precise description of syndrome leaders.

Metric Diophantine Approximation for Formal Laurent Series over Finite Fields

Michael Fuchs

National Chiao Tung University

Let $\mathbf{F}_q((T^{-1}))$ be the field of formal Laurent series endowed with the valuation $|\cdot|$ induced by the degree function. Consider the set

$$\mathbf{L} = \{f \in \mathbf{F}_q((T^{-1})) : \ |f| < 1\}$$

together with the Haar probability measure. Several recent studies investigated the diophantine approximation problem

$$\left| f - \frac{P}{Q} \right| < \frac{1}{q^{2n+l_n}}, \quad \deg Q = n, \quad \gcd(P, Q) = 1, \tag{1}$$

where $f \in \mathbf{L}$ and l_n is a sequence of non-negative integers.

For instance, in [1] a strong law of large numbers with error term for the number of pairs (P, Q) with (1) with $\deg Q \leq N$ was proved. Moreover, in [2] a similar result for (1) without the comprimeness assumption was established, however, under further assumptions on l_n and without an error term.

In this talk, we will discuss improvements of these results as well as generalizations to inhomogeneous Diophantine approximation, restricted Diophantine approximation, and simultaneous Diophantine approximation. A typical result which improves the main result in [2] reads as follows:

Theorem *The number of pairs (P, Q) satisfying (1) without the coprimeness condition and* $\deg Q \leq N$ *is almost surely given by*

$$\Psi(N) + \mathcal{O}\left((\Psi(N))^{1/2}(\log \Psi(N))^{2+\epsilon}\right),$$

where $\epsilon > 0$ *and* $\Psi(N) = \sum_{n \leq N} q^{-l_n}$.

References

[1] K. Inoue and H. Nakada (2003). On metric diophantine approximation in positive characteristic, *Acta Arith.*, **110**, 215-218.

[2] H. Nakada and R. Natsui (2006). Asymptotic behavior of the number of solutions for non-Archimedean Diophantine approximations, *Acta Arith.*, **125**, 203-214.

Perfect Hash Families PHF$(3; n, m, 3)$ from Quadrics Q$(4, q)$ and Hermitian Varieties H$(3, q^2)$

Ryoh Fuji-Hara

University of Tsukuba, Japan

(Joint work with Yuichiro Fujiwara and Ying Miao)

A *perfect hash family* PHF$(N; n, m, t)$ is an $N \times n$ array on m symbols with $m \geq t$ in which every $N \times t$ subarray (t is called the *strength*) contains at least one row comprised of distinct symbols. Perfect hash families have applications in information retrieval, cryptographic key distribution, secure frameproof codes, software testing, and so on. The most basic non-trivial case is PHFs with $N = t = 3$. R. A. Walker II and C. J. Colbourn [1] listed a table of existing PHFs for the case of $N = t = 3$, and expected $n = o(m^2)$. We are interested in constructing PHS$(3; n, m, 3)$ with n as large as possible. We show constructions of PHF$(3; q^2(q+1), q^2, 3)$ and PHF$(3; q^5, q^3, 3)$. The second construction claims $n = m^{5/3}$ for m a prime power, which exceeds all n in the table asymptotically. For the constructions of these PHFs, Quadrics Q$(4, q)$ in PG$(4, q)$ and Hermitian Varieties H$(3, q^2)$ in PG$(4, q^2)$ known as classical generalized quadrangles are effectively used.

Keywords: Perfect hash families, quadrics, Hermitian varieties.

References

[1] R. A. Walker II and C. J. Colbourn, Perfect Hash Families: Constructions and Existence, J. Math. Crypto. (2007), 12–37.

[2] K. Thas, Symmetry in Finite Generalized Quadrangles, Birkhäuser Verlag, 2004.

Classification of plane curves with infinitely many Galois points

Satoru Fukasawa

Waseda University

Let $C \subset \mathbf{P}^2$ be an irreducible plane curve of degree $d \geq 3$ over an algebraically closed field K of characteristic $p \geq 0$. In 1996, H. Yoshihara defined the notion of *Galois point*: If the function field extension induced from the point projection from a point $P \in \mathbf{P}^2$ is Galois, then P is said to be Galois. A Galois point P is said to be inner (resp. outer) if $P \in C$ (resp. $P \in \mathbf{P}^2 \setminus C$). We have a natural question: *How many Galois points are there?*

In many cases, the number of Galois points has been determined. For example, Yoshihara determined when $p = 0$ and C is smooth: The number of inner (resp. outer) Galois points is at most four (resp. three). In most of such settled cases, the number is finite. *Is there a case where C has infinitely many Galois points?*

Recently, T. Hasegawa and the author proved that the curve defined by $XZ^{q-1} - Y^q = 0$ where q is a power of p in $p > 0$ has infinitely many inner and outer Galois points, and that a plane curve with infinitely many inner Galois points (and $d \geq 4$) is projectively equivalent to the one. *How about the case where outer Galois points exist infinitely many?* We will have:

Theorem ([1]) *Let $\Delta'(C) \subset \mathbf{P}^2$ be the set of all outer Galois points for C. Then, the following conditions are equivalent:*

(1) $\Delta'(C)$ is an infinite set.

(2) C is a rational strange curve with a center Q and there exists a line L which contains Q and infinitely many outer Galois points.

(3) $p > 0$ and C is projectively equivalent to an irreducible plane curve whose equation is of the form

$$\alpha_e x^{p^e} + \alpha_{e-1} x^{p^{e-1}} + \cdots + \alpha_1 x^p + \alpha_0 x + \beta_e y^{p^e} + \cdots + \beta_1 y^p = 0.$$

References

[1] S. Fukasawa, *Classification of plane curves with infinitely many Galois points*, J. Math. Soc. Japan (to appear).

Unitary superperfect polynomials

Luis H. Gallardo

University of Brest

(Joint work with O. Rahavandrainy)

A divisor d of a binary polynomial $A \in \mathbb{F}_2[x]$ is *unitary* if $\gcd(d, A/d) = 1$. The notion is the same that over the integers. Set $\sigma^*(A) = \sum_{d \,|A,\, d \text{ unitary}} d$. If A is fixed by σ^* then A is *unitary perfect*. While if $\sigma^*(\sigma^*(A)) = A$ then A is *unitary superperfect*.

The object of the talk is to explain how to classify some unitary superperfect polynomials with a small number of prime divisors. This is done under some conditions on the number of prime factors of $\sigma^*(A)$. To do that unconditionally seems to be a very difficult task.

The analogue problem over the integers was initiated by Suryanarayana [1] and Kanold [2]. While Gallardo and Rahavandrainy [3] recently worked on unitary binary polynomials.

References

[1] D. Suryanarayana, *Super perfect numbers*, Elem. Math, 24, pp. 16–17, 1969.

[2] H.-J. Kanold, *Über "super perfect numbers"*, Elem. Math, 24, pp. 61–62, 1969.

[3] L. H. Gallardo, O. Rahavandrainy, On unitary perfect polynomials over finite fields, Preprint, 2009.

The number of decomposable multivariate polynomials

Joachim von zur Gathen

B-IT, Universität Bonn

A polynomial f (multivariate over a field) is *decomposable* if $f = g \circ h$ for some polynomials g and h, where g is univariate of degree at least 2. It is intuitively clear that the decomposable polynomials form a small minority among all polynomials. The goal in this work is to give a quantitative version of this intuition, namely an approximation to the number of decomposables over a finite field. The relative error in our approximation is exponentially decaying in the input size. Interestingly, we find a special case for bivariate polynomials where the intuition about the "most general decomposable polynomials" is incorrect.

We let $d_{r,n}$ be the number of decomposable polynomials of degree $n \geq 2$ in $r \geq 2$ variables over $\mathbb{F}_q$, and denote by l the smallest prime factor of n. We have to single out the following special case:

$$r = 2, n/l \text{ is prime and } n/l \leq 2l - 5. \tag{2}$$

The smallest examples are $n = l^2$ with $l \geq 5$, $n = 11 \cdot 13$, and $n = 11 \cdot 17$. Furthermore, let

$$\begin{aligned} m &= \begin{cases} n & \text{if (1) holds ,} \\ l & \text{otherwise,} \end{cases} \\ \alpha_{r,n} &= q^{\binom{r+n/m}{r}+m-1}(1 - q^{-\binom{r-1+n/m}{r-1}}), \\ c_{r,n} &= \tfrac{1}{2}\tbinom{r-1+n/l}{r-1} - 1, \\ \beta_{r,n} &= \tfrac{2q^{-c_{r,n}}}{1-q^{-1}}. \end{aligned}$$

Theorem *For all r, n as above we have*

$$|d_{r,n} - \alpha_{r,n}| \leq \alpha_{r,n} \cdot \beta_{r,n}.$$

Walsh spectrum of bent and almost bent functions

Faruk Göloğlu

University of Magdeburg

(Joint work with Alexander Pott)

We prove that any almost bent (AB) exponent is AB on the nonprime subfields. By using this, we compute $\mathcal{W}_d(1)$ for any AB exponent d. Where

$$\mathcal{W}_d(a) := \sum_{x\in\mathbb{F}} (-1)^{\mathsf{tr}(x^d+ax)},$$

where $a \in \mathbb{F}$.

Note that in [1], Lahtonen, McGuire and Ward compute $\mathcal{W}_d(1)$ when d is a Kasami exponent. It turns out that $\mathcal{W}_d(1)$ is the same for all AB exponents. We also prove similar results for quadratic AB functions with coefficients from the field $\mathbb{F}_2$. We also generalize the result that the Gold exponents restricted to some hyperplanes are bent, to any quadratic AB function with coefficients from $\mathbb{F}_2$. We also show that they are also bent on some smaller subspaces. For these functions we give a relation between extension- and base-field Walsh values.

The idea used to prove the above facts is based on elementary number theoretic restrictions on intersections of cyclotomic cosets. We apply these ideas also to bent functions to prove some properties of rotationally invariant Boolean functions, i.e. $f(x) = f(x^2)$ for all $x \in \mathbb{F}$.

If the exponent m of the field $\mathbb{F} = \mathbb{F}_{2^m}$ has a simple prime decomposition, e.g. m prime, prime power, etc., one can relate the balance of a rotationally invariant Boolean sequence to its linear complexity. We will also show this relation.

References

[1] Lahtonen, J., McGuire, G., and Ward, H. N. Gold and Kasami-Welch functions, quadratic forms, and bent functions. *Adv. Math. Commun. 1*, 2 (2007), 243–250.

Waring's Problem with Dickson Polynomials in Finite Fields

Domingo Gomez

University of Cantabria

(Joint work with A. Winterhof)

The family of *Dickson polynomials* $D_e(X, a) \in \mathbb{F}_q[X]$ is defined by the following recurrence relation

$$D_e(X, a) = XD_{e-1}(X, a) - aD_{e-2}(X, a), \quad e = 2, 3, \ldots,$$

with initial values

$$D_0(X, a) = 2, \quad D_1(X, a) = X,$$

where $a \in \mathbb{F}_q$. For background on Dickson polynomials we refer to the monograph [1].

It is easy to see that $D_e(X, 0) = X^e$, $e \geq 2$.

Let $g(e, q)$ be the smallest s such that every element of $y \in \mathbb{F}_q$ is a sum of s values of $D_e(X, a)$,

$$y = D_e(u_1, a) + D_e(u_2, a) + \cdots + D_e(u_s, a), \quad u_1, u_2, \ldots, u_s \in \mathbb{F}_q.$$

For $a = 0$ the problem of determining or estimating s is called *Waring's problem in* $\mathbb{F}_q$ and has been studied extensively in the literature, see [2] and references therein. Here we concentrate on the special case $a = 1$.

The number $g(e,q)$ doesn't exist if the value set of $D_e(X,1)$ is a subset of a proper subfield of $\mathbb{F}_q$. Our first result characterizes the pairs (e,q) such that $g(e,q)$ exists.

Moreover, we prove several upper bounds for $g(e,q)$ using either bounds of *exponential sums* or tools from additive number theory as the *Cauchy-Davenport Theorem.*

References

[1] Lidl, R.; Mullen, G. L.; Turnwald, G. Dickson polynomials. John Wiley & Sons, Inc., New York, 1993.

[2] Winterhof, Arne On Waring's problem in finite fields. Acta Arith. 87 (1998), no. 2, 171–177.

Evaluation Codes and Complete Bipartite Graphs

Manuel González Sarabia

UPIITA-IPN, México

(Joint work with C. Rentería Márquez)

Let $K_{m,n}$ be a complete bipartite graph. We can associate an evaluation linear code to the incidence matrix of this graph. Our goal is to determine the main parameters of these codes (length, dimension, minimum distance). Let X be the toric variety associated to this incidence matrix and F be a finite field with q elements. Let $F[Z_{00},\ldots,Z_{(m-1)(n-1)}]_d$ be the $d-$graded homogenous component of the corresponding polynomial ring. Let $s=\#(X)$ and consider the following evaluation map

$$\theta : F[Z_{00},\ldots,Z_{(m-1)(n-1)}]_d \to F^s$$
$$\theta(f) = (f(P_1),\ldots,f(P_s))$$

where $X=\{P_1,\ldots,P_s\}$. The evaluation code of order d, $C_X(d)$, associated to the incidence matrix of the complete bipartite graph $K_{m,n}$ is the image of the last evaluation map. The following theorem shows the main parameters of this kind of codes.

Theorem *The main parameters of the evaluation code $C_X(d)$ are given by*

1. *Length:* $s=(q-1)^{m+n-2}$
2. *Dimension:* $\dim C_X(d) = H_{X_1}(d)\cdot H_{X_2}(d)$
3. *Minimum Distance:* $\delta_X(d) = \delta_{X_1}(d)\cdot\delta_{X_2}(d)$

where $H_{X_i}(d)$ and $\delta_{X_i}(d)$ are the corresponding dimension and minimum distance of the generalized Reed-Solomon codes for $i=1,2$.

References

[1] M. González Sarabia and C. Rentería Márquez, *Evaluation Codes Associated to Complete Bipartite Graphs*, International Journal of Algebra, Hikari Ltd, Bulgaria, Vol. 2, No. 4, pp. 163-170, 2008.

The Ring of Additive Polynomials and Weights of Cyclic Codes

Cem Güneri

Sabancı University, İstanbul

(Joint work with F. Özbudak)

Trace representation of cyclic codes relates the weights of codewords to the number of solutions of certain equations over finite fields. Under certain assumptions on the cyclic code, these equations define Artin-Schreier type (irreducible) curves whose number of rational points can be estimated by the Hasse-Weil bound. Using this, Wolfmann gave a bound for the weights of a broad family of cyclic codes. In particular, his bound applies to any cyclic code over prime finite fields. However, if the cyclic code is defined over more general finite fields then related equations may define reducible curves, in which case Wolfmann's bound does not apply.

We prove the theorem below which helps us determine irreducible components of such reducible curves. Applying the Hasse-Weil bound on the irreducible components, we can write general bounds for the weights of any cyclic code. Our result reduces the estimation of the weights of a cyclic code to determination of the left greatest common divisor of certain polynomials in the ring of additive polynomials.

Theorem *Let K be a perfect field of positive characteristic p and $\mathcal{R}$ be the ring of additive polynomials in $K[T]$. Let $A, B_1, \ldots, B_t \in \mathcal{R}$ be nonzero additive polynomials such that A is monic, separable and splits in K. Let $L(T)$ be the left greatest common divisor of $A, B_1, \ldots, B_t$ in $\mathcal{R}$ and denote by W the set of roots of $L(T)$. Assume that $r_1, \ldots, r_t$ are distinct positive integers with $\gcd(p, r_i) = 1$, for all $1 \leq i \leq t$. Then,*

i) The polynomial $A(y) - \sum_{i=1}^{t} B_i(x^{r_i})$ is irreducible over $K(x)$ if and only if $L(T) = T$.

ii) Let $\circ$ denote the composition operation in $\mathcal{R}$. If

$$\begin{aligned} A(T) &= L(T) \circ \hat{A}(T) \\ B_i(T) &= L(T) \circ \hat{B}_i(T), \end{aligned}$$

then we have following factorization into irreducibles:

$$A(y) - \sum_{i=1}^{t} B_i(x^{r_i}) = \prod_{w \in W} \left(\hat{A}(y) - \sum_{i=1}^{t} \hat{B}_i(x^{r_i}) - w \right).$$

On the Jacobi sum $\sum \psi(x_1 \cdots x_t)$ over finite fields

S. Gurak

University of San Diego

Let $q = p^v$, a power of a prime p, and $\mathbf{F}_q$ denote the finite field of q elements. For any character ψ of $\mathbf{F}_q^*$, say of order s, define the special Jacobi sum

$$J_t(\psi) = \sum_{x_i \in F_q^*, x_1 + \cdots + x_t = 1} \psi(x_1 \cdots x_t).$$

Explicit values of $J_t(\psi)$ are known for ψ of small order $1 \leq s \leq 4$, but beyond that nothing seems to be determined. Here I show how to express $J_t(\psi)$ as a ratio of Eisenstein sums involving a power or lift of ψ. Using known evaluations of Eisenstein sums for characters of order 6, 8 and 12, I give a complete determination of the sums $J_t(\psi)$ whenever s divides 8 or 12. These results can be applied to the problem to determine the number of irreducible polynomials of fixed degree over $\mathbf{F}_q$ with prescribed trace and norm lying in a specified s-power coset of $\mathbf{F}_q^*$.

On the number of points of Jacobian and Prym varieties

Safia Haloui

Institut de Mathématiques de Toulon

(Joint work with Yves Aubry and Marc Perret)

Let A be an abelian variety of dimension d defined over ${}_{Fq}$. Weil proved that:

$$(q + 1 - 2\sqrt{q})^d \leq \sharp A({}_{Fq}) \leq (q + 1 + 2\sqrt{q})^d.$$

Moreover, if J_X is the jacobian of a curve X of genus g admitting a map of degree d onto ${}_P{}^1$, then Lachaud and Martin-Deschamps proved that:

$$\sharp J_X({}_{Fq}) \leq e(2g\sqrt{e})^{d-1} q^g.$$

Furthermore, Perret proved that:

$$\sharp J_X({}_{Fq}) \leq \Big(q + 1 + \frac{\sharp X({}_{Fq}) - (q+1)}{g}\Big)^g.$$

Let $\pi : Y \longrightarrow X$ be an unramified covering of degree 2 of smooth algebraic irreducible projective curves defined over ${}_{Fq}$ of odd characteristic. Let σ be the non-trivial involution of this covering and σ^* the induced involution on the jacobian J_Y of Y. If X has genus $g \geq 2$, the Prym variety Pr_π associated to π is defined as

$$Pr_\pi = Im(\sigma^* - id).$$

It is an abelian subvariety of J_Y of dimension $g - 1$ isogeneous to a direct factor of J_X in J_Y. Perret proved lower and upper bounds for such abelian varieties.

Our purpose is to give improvements of these bounds on jacobian and Prym varieties.

Crosscorrelation of Legendre Sequences of Different Periods

Jing (Jane) He

Carleton University

Families of pseudorandom sequences with low cross correlation have important applications in communications and cryptography. Among several known constructions of sequences with low cross correlations, interleaved constructions proposed by Gong uses two sequences of the same period with two-level autocorrelation. Recently, Wang and Qi used a similar idea to extend this construction to Legendre sequences of period p and $p+2$, respectively, where both p and $p+2$ are primes. Moreover, they studied the cross correlation of the interleaved sequences. In this paper, we study the cross-correlation of interleaved sequences of two Legendre sequences of periods p and q,respectively, where p and q are prime numbers.

Proof of a Conjecture on the Sequence of Exceptional Numbers, Classifying Cyclic Codes and APN functions

Fernando Hernando

University College Cork and Claude Shannon Institute

(Joint work with Gary McGuire)

The sequence of numbers of the form $2^i + 1$ or $4^i - 2^i + 1$ (where $i \geq 1$) is

$$3, 5, 9, 13, 17, 33, 57, 65, 129, 241, 257, 513, 993, 1025, \ldots.$$

This is sequence number A064386 in the On-Line Encyclopedia of Integer Sequences. It has been known for almost 40 years that these numbers are *exceptional* numbers, in the sense we will define shortly. No further exceptional numbers were found, and it was conjectured that this sequence is the complete list of exceptional numbers. We prove this conjecture.

This conjecture arises in two different ways, from cryptography and from coding theory. In the theory of APN (Almost Perfect Nonlinear) functions, an odd integer $t \geq 3$ is said to be exceptional if $f(x) = x^t$ is APN over $\mathbb{F}_{2^n}$ for infinitely many values of n. Equivalently, t is exceptional if the binary cyclic code of length $2^n - 1$ with two zeros ω, ω^t has minimum distance 5 for infinitely many values of n. We prove that every exceptional number has the form $2^i + 1$ or $4^i - 2^i + 1$.

Arcs in Galois ring planes invariant under a Singer cycle

Thomas Honold

Zhejiang University, Hangzhou

(Joint work with M. Kiermaier, University of Bayreuth)

Let $\mathbb{G}_q$ be the Galois ring of characteristic p^2 and order $q = p^r$. The incidence structure $\mathrm{PHG}(2, \mathbb{G}_q)$, whose points and lines are the free rank-one, respectively, free rank-two $\mathbb{G}_q$-submodules of $\mathbb{G}_q^3$ and whose incidence relation is set inclusion, is called the projective Hjelmslev plane over $\mathbb{G}_q$. A (k, n)-arc in $\mathrm{PHG}(2, \mathbb{G}_q)$ is a k-multiset of points meeting every line in at most n points. The study of such arcs and their higher-dimensional analogues is motivated by the following observation from [2, 3]: Just as in classical finite geometry, large (k, n)-arcs in projective Hjelmslev geometries over $\mathbb{G}_q$ correspond to good linear codes over $\mathbb{G}_q$.

We describe a method for constructing (k, n)-arcs in $\mathrm{PHG}(2, \mathbb{G}_q)$ from special point sets in the affine plane $\mathrm{AG}(2, \mathbb{F}_q)$. The resulting arcs are invariant under a (lifted) Singer cycle of $\mathrm{PHG}(2, \mathbb{G}_q)$. Examples are provided by the known hyperovals in the planes $\mathrm{PHG}(2, \mathbb{G}_q)$ with q even [4]. Using the new method, we construct two new infinite families of arcs with good parameters.

References

[1] T. Honold and M. Kiermaier. Singer arcs in uniform projective Hjelmslev planes over Galois rings. In preparation, Apr. 2009.

[2] T. Honold and I. Landjev. Linearly representable codes over chain rings. *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, 69:187–203, 1999.

[3] T. Honold and I. Landjev. Linear codes over finite chain rings. *Electronic Journal of Combinatorics*, 7:Research Paper 11, 22 pp. (electronic), 2000.

[4] T. Honold and I. Landjev. On maximal arcs in projective Hjelmslev planes over chain rings of even characteristic. *Finite Fields and their Applications*, 11(2):292–304, 2005.

The merit factor of binary sequence families constructed from m-sequences

Jonathan Jedwab

Simon Fraser University

(Joint work with Kai-Uwe Schmidt)

We consider a *sequence* A of length n to be an n-tuple $(a_0, a_1, \ldots, a_{n-1})$ for which each a_j takes the value $+1$ or -1. Given a sequence A of length $n > 1$, its *aperiodic autocorrelation* at shift u is $C_A(u) := \sum_{j=0}^{n-u-1} a_j a_{j+u}$ for $0 \le u < n$, and its *merit factor* is $F(A) := n^2/(2\sum_{u=0}^{n-1}[C_A(u)]^2)$.

The merit factor is important both practically and theoretically. The larger the merit factor of a sequence that is used to transmit information by modulating a carrier signal, the more uniformly the signal energy is distributed over the frequency range. The optimal value of the merit factor of a sequence is studied in complex analysis, in statistical mechanics, and in theoretical physics and theoretical chemistry. The asymptotic value of the merit factor is known for only a few infinite families of sequences, including Legendre sequences and m-sequences.

We study two product constructions that were analysed in [SJP09]. A first, "negaperiodic", construction inputs a length n sequence and outputs a length $2n$ sequence. A second, "periodic", construction inputs a length n sequence and outputs a length $4n$ sequence. We show that, in the case of an input m-sequence, both output sequences have the same asymptotic merit factor as the input

sequence at all rotations of sequence elements. A similar property was previously shown [SJP09] to hold for input Legendre sequences. However we show by example that this property does not appear to hold for a general input sequence.

References

[SJP09] K.-U. Schmidt, J. Jedwab, and M.G. Parker. Two binary sequence families with large merit factor. *Adv. Math. Commun.*, 2009. To appear.

Parallel Multiplication, Trivial Traces, and Conjugates in Order Dividing Extension Fields

Anna Johnston

Washington State University

An order dividing extension field has the form $\mathbb{F}_{P^q}$ where q divides the multiplicative order of the base field. They occur accidentally, as in quadratic extension fields with odd characteristic, or intentionally as in Cipolla's algorithm for computing q^{th} roots or in optimal extension fields for efficient elliptic curve operations.

These extension fields have an obvious computational advantage. If $\gamma \in \mathbb{F}_P$ is a q^{th} non-residue then $r(x) = (x^q - \gamma)$ is irreducible and $\mathbb{F}_{P^q} = \mathbb{F}_P[x]/(r(x))$. Using a two term modulus simplifies reduction and any multiplicative computations in the field.

Order dividing extension fields have another computational advantage. The rings $\mathbb{F}_P[x]/(x^q - 1)$ and $\mathbb{F}_P[x]/(x^{2q} - 1)$ are closely related to the representation of $\mathbb{F}_{P^q}$ by $\mathbb{F}_P[x]/(r(x))$. The rings $\mathbb{F}_P[x]/(x^q - 1)$ and $\mathbb{F}_P[x]/(x^q - 1)$ are the q and $2q$ discrete Fourier transform rings over $\mathbb{F}_P$. With these rings, multiplication can be reduced from q^2 multiplications down to $2q$, or a single parallel $2q$ vector multiplication.

Fast multiplication using a transform ring is not limited to order dividing extension fields. However only in order dividing extension fields can the relationship between the two term field modulus $r(x) = (x^q - \gamma)$ and the ring modulus $(x^{2q} - 1)$ be exploited.

This research focuses on two of the benefits of this relationship.

1. Although fast multiplication is possible using the transform ring, the computation saved is often wasted by the required field reduction. Using the relationship between $r(x)$ and $(x^{2q} - 1)$, a field reduction algorithm within the ring was designed which requires only $(q + 1)$ vector multiplications.

2. Field elements in their transformed state have the property that their conjugates are simply its cyclic shifts. A field element and all its conjugates can therefore be represented as a single cyclicly ordered list of q elements in $\mathbb{F}_P$. These conjugate sets were examined in relation to their trace and minimal polynomials.

The maximum number of rational points on plane curves over a finite field

Seon Jeong Kim

Gyeongsang National University

(Joint work with Masaaki Homma)

We consider the number of points on a curve C of degree d in the projective plane $\mathbb{P}^2$ over a finite field $\mathbb{F}_q$. We denote by $C(\mathbb{F}_q)$ the set of all $\mathbb{F}_q$-rational points of C. We are interested in the cardinality $N_q(C)$ of the set $C(\mathbb{F}_q)$. We suppose that our curve C contains no $\mathbb{F}_q$-line as a component. Let $M_q(d)$ be the maximum among the numbers in $\{N_q(C) \mid C \in \mathcal{C}_d(\mathbb{F}_q)\}$, where $\mathcal{C}_d(\mathbb{F}_q)$ is the set of all plane curves over $\mathbb{F}_q$ of degree d without an $\mathbb{F}_q$-line as a component.

We have an obvious bound $M_q(d) \leq q^2 + q + 1$, since $C(\mathbb{F}_q) \subseteq \mathbb{P}^2(\mathbb{F}_q)$, where $\mathbb{P}^2(\mathbb{F}_q)$ denotes the set of all $\mathbb{F}_q$-points of $\mathbb{P}^2$.

In [1], we proved that $M_q(d) = q^2 + q + 1$ for any $d \geq q + 2$.

In [2], Sziklai stated a conjecture

$$M_q(d) \leq (d-1)q + 1.$$

Note that $M_q(2) = q + 1$ is well-known.

In [1], we proved that the conjecture holds for $d = q+1$, and that it does not hold when $d = q = 4$.

In this talk, we prove that Sziklai's conjecture holds for the cases $d = q$ with $q \geq 5$. We prove the inequality $M_q(q) \leq (q-1)q + 1$ using algebraic and combinatorial methods and then construct a curve with exactly $(q-1)q + 1$ $\mathbb{F}_q$-rational points.

Also, we prove the inequality $N_q(C) \leq (d-1)q + 1$ for any nonsingular plane curve for degree d with $2 \leq d \leq q - 1$.

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*, to appear in Finite Fields and Their Applications, doi:10.1016/j.ffa.2009.02.008.

[2] P. Sziklai, *A bound on the number of points of a plane curve*, Finite Fields Appl. 14 (2008) 41–43.

Lower Bounds on Distances of Improved Two-Point Codes

Radoslav Kirov

University of Illinois, Urbana-Champaign

(Joint work with I.Duursma)

Improved algebraic geometric codes, due to a construction by Feng and Rao, improve on classical algebraic geometric codes by selectively adding parity checks. Parity checks are added only if needed to achieve a given designed distance. We extend and improve the Feng-Rao method for one-point codes to arbitrary codes. We apply our method to two-point codes on the Hermitian and Suzuki curves. For the Hermitian curve the obtained bounds are sharp. They improve classical two-point codes, studied by Homma and Kim, as well as improved one-point codes, studied by Bras-Amorós and O'Sullivan.

References

[1] M. Bras-Amorós, M. O'Sullivan, "On Semigroups Generated by Two Consecutive Integers and Improved Hermitian Codes", *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2560-2566, 2007.

[2] G.-L. Feng and T. R. N. Rao, "Improved geometric Goppa codes. I. basic theory, Special issue on algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 41, pt. 1, pp. 1678-1693, 1995.

[3] M. Homma and S. J. Kim. "The complete determination of the minimum distance of two-point codes on a Hermitian curve." *Des. Codes Cryptogr.*, 40(1):524, 2006.

Commutative semifields via Dembowski-Ostrom polynomials

Pamela Kosick

University of Delaware

(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. However, 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. Using this approach we give a partial classification of finite commutative semifields of order 3^5 and discuss the connections between finite commutative semifields and some combinatorial structures.

On a class of permutation polynomials

Gohar Kyureghyan

Otto-von-Guericke University of Magdeburg

(Joint work with Pascale Charpin)

We study permutation polynomials of the shape $G(X)+\gamma Tr(H(X))$ in $\mathbf{F}_{q^n}[X]$, where $Tr(X) = X + X^q + \ldots + X^{q^{n-1}}$ is the polynomial describing the relative trace mapping from $\mathbf{F}_{q^n}$ onto its subfield $\mathbf{F}_q$. We introduce several families of such permutation polynomials. In particular our results imply:

Theorem *Let $\gamma, \beta \in \mathbf{F}_{q^n}$ and $H(X) \in \mathbf{F}_{q^n}[X]$.*

(i) *Then the polynomial*

$$F(X) = X + \gamma\, Tr\left(H(X^q - \gamma^{q-1}X) + \beta X\right)$$

is a permutation polynomial if and only if $Tr(\beta\gamma) \neq -1$.

(ii) *Then the polynomial*

$$F(X) = X + \gamma\, Tr\left(\sum_{u\in\mathbf{F}_q} H(X+u\gamma) + \beta X\right)$$

is a permutation polynomial if and only if $Tr(\beta\gamma) \neq -1$.

We show also that the associated mappings to the polynomials from the above theorem are p-to-1 if $Tr(\beta\gamma) = -1$. Further we determine the inverse and the cycle structure of such a permutation.

References

[1] P. Charpin and G. Kyureghyan, *When does* $G(x) + \gamma Tr(H(x))$ *permute* $\mathbf{F}_{p^n}$?, a manuscript, 2008.

[2] G. Kyureghyan, *Remarks on a family of permutation polynomials*, arXiv:0903.0743 .

Inner metric bounds on the minimal Euclidean distance for arbitrary q-ary block codes

Efraim Laksman

Blekinge Institute of Technology

(Joint work with H. Lennerstad and M. Nilsson)

In this line of research general bounds on the minimal Euclidean distance for PSK block codes have been established as explicit functions of the code size $|C|$, block length n and alphabet size q. For several values of $|C|$, n and q, the bounds are optimal in the sense that there are known codes that fulfil the bound with equality, proving that these codes are the best possible. The bounds characterize a geometrical property of any subset of $\mathbf{Z}_q^n$: maximizing the minimal distance between two words in a subset C of $\mathbf{Z}_q^n$.

In all reports in this research, the problem is localized to an Elias sphere. Code words in an Elias sphere are written as rows in a matrix, and the results rely on finding worst case columns of this matrix. Limited to the case $q = 8$ the method has in recent papers adopted a more general approach: to consider a general inner metric inside the Elias sphere, and optimizing this metric to derive sharper bounds for the outer metric, which is Euclidean.

The present paper generalizes this approach to arbitrary q, while using $q = 6$, 7 and 9 as illustrating examples. It turns out that it is possible to find restrictions to worst case columns of an Elias sphere for general q.

References

[1] E. Laksman, H. Lennerstad and M. Nilsson, *Improving bounds on minimum Euclidean distance for block codes by inner metric optimization*, contribution to the conference Combinatorics 2008.

Blocking Sets of Rédei Type in Coordinate Geometries over Finite Chain Rings

Ivan Landjev

New Bulgarian University

Let R be a chain ring, $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, and let $\Pi = \mathrm{PHG}(R_R^3)$ be the (right) coordinate projective Hjelmslev plane over R. A (k, n)-blocking set in Π is defined as a set K with $|K| = k$, $|K \cap L| \geq n$ for any line L, and $|K \cap L_0| = n$ for at least one line L_0.

As in the classical case of projective planes over finite fields, the smallest $(k, 1)$-blocking set is a line and its cardinality is $k = q^{m-1}(q + 1)$. In case of chain rings R with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, the size of the second smallest irreducible $(k, 1)$-blocking set is $q^2 + q + 1$. All blocking sets with this cardinality can be characterized. It turns out that if $\operatorname{char} R = p$ there exist (up to isomorphism) two such sets. One of them is the Baer subplane and is not trivial in the sense that its image under the canonical epimorphism is not contained in a line. If $\operatorname{char} R = p^2$ we have only trivial irreducible $(q^2 + q + 1, 1)$-blocking sets. This raises the question of the construction of nontrivial blocking sets in planes over the Galois rings $\mathrm{GR}(q^2, p^2)$.

The goal of this talk is to introduce Rédei type blocking sets in projective Hjelmslev planes over finite chain rings. In Hjelmslev planes over chain rings of nilpotency index 2 that contain the residue field as a proper subring, we construct the Baer subplanes associated with this subring as Rédei type blocking sets. For planes over Galois rings, two further examples of Rédei type blocking sets are given generalizing familiar constructions in projective planes over finite fields.

Algebraic continued fractions in fields of power series over a finite base field

Alain Lasjaunias

University of Bordeaux

Given a finite field $\mathbf{F}_q$, we consider power series in $\mathbf{F}_q((T^{-1}))$ which are algebraic over $\mathbf{F}_q(T)$. In the case of algebraic real numbers the continued fraction expansion of an element is explicitely known if and only if this element is quadratic. In the case of power series over a finite field, due to the existence of the Frobenius isomorphism, the continued fraction expansion of an algebraic element may be explicitely given for many examples which are not quadratic. Indeed there exists a class of algebraic power series, called hyperquadratic, which for different reasons should be compared to the class of quadratic real numbers. In this talk we resume the properties of these algebraic elements and we present some explicit continued fraction expansions which have connections with recurrent sequences in a finite field.

References

[1] A. Lasjaunias, *Continued fractions for hyperquadratic power series over a finite field*, Finite Fields and Their Applications 14 (2008) 329-350.

[2] A. Lasjaunias, *Algebraic continued fractions in* $\mathbf{F}_q((T^{-1}))$ *and recurrent sequences in* $\mathbf{F}_q$, Acta Arithmetica 133.3 (2008) 251-265.

On monomial graphs of girth eight

Felix Lazebnik

University of Delaware

(Joint work with V. Dmytrenko and J. Williford)

Let e be a positive integer, p be a odd prime, $q = p^e$, and $\mathbf{F}_q$ be the finite field of q elements. Let $f_2, f_3 \in \mathbf{F}_q[x, y]$. The graph $G = G_q(f_2, f_3)$ is a bipartite graph with vertex partitions $P = \mathbf{F}_q^3$ and $L = \mathbf{F}_q^3$, and edges defined as follows: a vertex $(p) = (p_1, p_2, p_3) \in P$ is adjacent to a vertex $[l] = [l_1, l_2, l_3]$ if and only if

$$p_2 + l_2 = f_2(p_1, l_1) \quad \text{and} \quad p_3 + l_3 = f_3(p_1, l_1).$$

Motivated by some questions in finite geometry and extremal graph theory, we ask when G has no cycle of length less than eight, i.e., has girth at least eight. When f_2 and f_3 are monomials, we call G a monomial graph. We show that for $p \geq 5$, and $e = 2^a 3^b$, a monomial graph of girth at least eight has to be isomorphic to graph $G_q(xy, xy^2)$, which is an induced subgraph of the classical generalized quadrangle $W(q)$. For all other e, we show that a monomial graph is isomorphic to a graph $G_q(xy, x^k y^{2k})$, with $1 \leq k \leq (q-1)/2$ and satisfying several other strong conditions. These conditions imply that $k = 1$ for all $q \leq 10^{10}$. In particular, for a given positive integer k, graph $G_q(xy, x^k y^{2k})$ can be of girth eight only for finitely many odd characteristics p.

Double recurrence in finite fields and algebraic sets

Akos Magyar

University of British Columbia

(Joint work with Brian Cook)

Motivated by ergodic theory, we call a set $S \subset \mathbb{F}^n$, $\mathbb{F}$ being a finite field of q elements, a set of double recurrence; if for every set $A \subset \mathbb{F}^n$ of density $\alpha = |A|/q^n$ there exists an $s \in S$ ($s \neq 0$), such that $|A \cap (A+s) \cap (A+2s)| \geq c(\alpha)\, q^n$. Here $c(\alpha)$ is a positive number depending only on the density α.

We show that if S is an algebraic set, defined by a family of polynomials, such that the locus of the singular points of S has sufficiently large codimension with respect to α, then S is a set of double recurrence.

The proof uses some basic notions from additive combinatorics, such as that of quadratic uniformity, and elementary methods for counting the solutions of certain linear equations in algebraic sets.

Symplectic Spreads and Commutative Semifields

Giuseppe Marino

Seconda Università degli Studi di Napoli

(Joint work with Guglielmo Lunardon, Olga Polverino and Rocco Trombetti)

In this paper we face with the problem of constructing semifield spreads of projective spaces. To this aim we study the relationship between linear sets disjoint from the secant variety of a Segre variety $\mathcal{S}_{n,n}$ of $PG(n^2-1,q)$ and semifield spreads of $PG(2n-1,q)$ (see [2], [1] and [3]), focusing on the symplectic case. We prove that a semifield spread is symplectic if and only if the associated linear set is contained in a subspace of $PG(n^2-1,q)$ intersecting $\mathcal{S}_{n,n}$ in a quadric Veronesian. Moreover, for q odd, starting from a symplectic semifield spread $\mathcal{S}$ of $PG(5,q)$ we construct another symplectic semifield spread of $PG(5,q)$ called the *symplectic dual* of $\mathcal{S}$. Finally, we exhibit a new example of symplectic semifield spread of $PG(5,q^2)$, q odd, and, using the Knuth cubical array, we determine the associated commutative semifield of order q^6.

References

[1] I. Cardinali, O. Polverino, R. Trombetti, *Semifield planes of order q^4 with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$*, European J. Combin., **27** (2006), 940–961.

[2] G. Lunardon, *Translation ovoids*, J. Geom., **76** (2003), 200–215.

[3] M. Lavrauw, *Finite semifields with a large nucleus and higher secant varieties to Segre varieties*, submitted.

On the nonexistence of some q-ary linear codes meeting the Griesmer bound

Tatsuya Maruta

Osaka Prefecture University

(Joint work with Noboru Hamada)

Let $\mathbb{F}_q^n$ denote the vector space of n-tuples over the field of q elements $\mathbb{F}_q$. A k-dimensional subspace of $\mathbb{F}_q^n$ is called a q-ary linear code of length n with dimension k, or an $[n,k]_q$ *code*. An $[n,k,d]_q$ *code* is an $[n,k]_q$ code with minimum Hamming distance d. A fundamental problem in coding theory is to find $n_q(k,d)$, the minimum length n for which an $[n,k,d]_q$ code exists. There is a natural lower bound on $n_q(k,d)$, called the Griesmer bound:

$$n_q(k,d) \geq g_q(k,d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil, \tag{3}$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. It is known for all q that the equality in (1) holds for all d when $k = 1, 2$ and for $d \geq (k-2)q^{k-1} - (k-1)q^{k-2} + 1$ when $k \geq 3$, see [1]. As for the case when $d = (k-2)q^{k-1} - (k-1)q^{k-2}$, the following is known.

Theorem ([2]) *For $d = (k-2)q^{k-1} - (k-1)q^{k-2}$, it holds that $n_q(k,d) \geq g_q(k,d) + 1$ for $q \geq k$ when $k = 3, 4, 5$ and for $q \geq 2k-3$ when $k \geq 6$.*

We conjecture that the condition "$q \geq 2k-3$" for $k \geq 6$ could be improved to "$q > (3k-6)/2$". We shall show some results which corroborates our conjecture.

References

[1] R. Hill, Optimal linear codes, In: C. Mitchell, ed., Cryptography and Coding II, Oxford Univ. Press, Oxford (1992), 75–104.

[2] T. Maruta, On the achievement of the Griesmer bound, Des. Codes Cryptogr. **12** (1997) 83–87.

Riemann-Roch spaces of the norm-trace function field

Gretchen L. Matthews

Clemson University

(Joint work with Justin Peachey)

The norm-trace function field over the finite field $\mathbf{F}_{q^r}$ is given by $\mathbf{F}_{q^r}(x,y)/\mathbf{F}_{q^r}$ where $N_{\mathbf{F}_{q^r}/\mathbf{F}_q}(x) = Tr_{\mathbf{F}_{q^r}/\mathbf{F}_q}(y)$, that is, the norm of x is equal to the trace of y with respect to the extension $\mathbf{F}_{q^r}/\mathbf{F}_q$. It is a generalization of the Hermitian function field over $\mathbf{F}_{q^2}$, which is obtained when $r = 2$. The norm-trace function field has $q^{2r-1}+1$ places of degree one, including q^{r-1} places P_{0b} and a single place at infinity P_∞. In this talk, we discuss explicit bases for Riemann-Roch spaces $\mathcal{L}\left(a_0 P_\infty + a_1 P_{0b_1} + \cdots + a_m P_{0b_m}\right)$ where $1 \leq m \leq q^{r-1}$ and determine the Weierstrass semigroups of $(m+1)$-tuples of the form $(P_\infty, P_{0b_1}, \ldots, P_{0b_m})$.

On the calculation of the linear complexity of *un*-periodic sequences

Wilfried Meidl

Sabanci University Orhanli

(Joint work with Hassan Aly, Radwa Marzouk)

In [IEEE Trans. Inform. Theory 52 (2006), 5537–5539] H. Chen showed how to reduce the calculation of the linear complexity of a *un*-periodic sequence over a finite field $\mathbb{F}_{p^m}$ to the calculation of the linear complexities of u sequences of period n over $\mathbb{F}_{p^m}$, under the condition that u divides $p^m - 1$. In W.Meidl [DCC 46 (2008), 57–65], the main theorem of Chen has been combined with some further observations to point out how the condition that u divides $p^m - 1$ can be dropped. This makes it possible to apply Chen's result to sequences over small fields like to the important case of binary sequences. W. Meidl (2008) applied then Chen's result to construct algorithms for determining the linear complexity of $u2^v$-periodic binary sequences, u odd. Concrete algorithms were presented for $u = 3, 5, 7, 15$.

This presentation provides a more general approach: Based on a slight generalization of Chen's theorem and some results on multisequences we prove a general theorem that shows how to reduce the calculation of the linear complexity of a un-periodic sequence over a finite field $\mathbb{F}_p$ to a certain number of n-periodic sequences over $\mathbb{F}_p$, without the strong condition that u divides $p-1$. Instead, p, u, n solely have to satisfy the following conditions:

(I) There exists an integer m for which $u|p^m-1$ and $\gcd(p^m-1,n)=1$,

(II) if $n=(char(\mathbb{F}_p))^rT$, $r\geq 0$, $\gcd(p,T)=1$, and l is the order of p modulo T, then $\gcd(l,m)=1$.

Similarly to the result of Chen, our result can be combined with fast algorithms for n-periodic sequences known for certain integers n. As examples we discuss algorithms for binary sequences of period un with $n=2^n$, and un-periodic sequences over a prime field $\mathbb{F}_p$ with $n=q^v$ where q is a prime for which p is a primitive root modulo q^2. For simple concrete examples one may choose $u=3,5,7,15$ in the first case, in which one then obtains improvements of the algorithms of W. Meidl, DCC (2008). In the second case for $p=2$ for instance the pairs $(u,q)=(7,5),(7,11)$, and for $p=3$ the pairs $(u,q)=(13,5),(13,17)$ and $(2,q)$ for an arbitrary prime q for which 3 is a primitive root modulo q^2 satisfy the conditions (I), (II). Thus one can easily generate corresponding new algorithms for the linear complexity.

Equicharacteristic Galois representations of local function fields

Carl A. Miller

University of Michigan, Ann Arbor

The purpose of this talk is to present an equicharacteristic version of the Swan conductor.

Let G be the absolute Galois group of the field $\mathbb{F}_{p^r}((t))$, where p is prime. Let $\mathcal{I}$ be the inertia subgroup of G, and let $\mathcal{P}$ be the largest pro-p-subgroup of $\mathcal{I}$. Representations of G tend to be complex because $\mathcal{P}$ is large and nonabelian. Suppose that $\phi: G\rightarrow \mathrm{Aut}((\mathbb{F}_\ell)^n)$ is a representation, where ℓ denotes a prime different from p. The *Swan conductor* of ϕ measures the higher ramification of ϕ (i.e., the extent to which $\mathcal{P}$ acts nontrivially on $(\mathbb{F}_\ell)^n$).

Now suppose that $\psi\colon G\rightarrow \mathrm{Aut}((\mathbb{F}_p)^n)$ is an equicharacteristic representation. The definition of the Swan conductor cannot be carried over to this case. (The definition of the Swan conductor of ϕ relies on the fact that the representation $\phi_{|P}$ is semisimple. This is not true of $\psi_{|P}$.) However in this talk I will define a different invariant, the "minimal root index," which measures the ramification of an equicharacteristic representation.

The minimal root index serves a similar role to the Swan conductor in the subject of étale cohomology. Whereas the Swan conductor helps us to count $\mathbb{Q}_\ell$-étale cocycles on characteristic-p curves, the minimal root index helps us count $\mathbb{Q}_p$-étale cocycles on characteristic-p curves.

Division Polynomials for Twisted Edwards Curves

Richard Moloney

University College Dublin and Claude Shannon Institute

(Joint work with Gary McGuire)

The famous last entry in the diary of Gauss concerns the curve with equation

$$x^2 + y^2 + x^2y^2 = 1 \tag{4}$$

and its rational points over $\mathbb{F}_p$.

The idea of *division polynomials* on a curve with a group law on its points, is that we try to write down a formula for $[n]P$ in terms of the coordinates of P, where $[n]P$ denotes P added to itself n times under the group law. In some unpublished work, discovered after his death and subsequently published, Gauss wrote down such formulae for the curve (4), see Figure 1. Surprisingly, his formulae are not correct, although they are very close to being correct. In this paper we shall give the correct version, in the general context of twisted Edwards curves, of which (4) is a special case. We discuss work of Gauss and Eisenstein on the lemniscatic sine function.

Edwards [1] introduced an addition law on the curves $x^2 + y^2 = c^2(1 + x^2y^2)$ for $c \in k$, where k is a field of characteristic not equal to 2. He showed that every elliptic curve over k is birationally equivalent (over some extension of k) to a curve of this form.

In [2], Bernstein and Lange generalised this addition law to the curves $x^2 + y^2 = 1 + dx^2y^2$ for $d \in k \setminus \{0, 1\}$. More generally, they consider $x^2 + y^2 = c^2(1 + dx^2y^2)$, however, any such curve is isomorphic to one of the form $x^2 + y^2 = 1 + d'x^2y^2$ for some $d' \in k$, so we will assume $c = 1$. These curves are referred to as Edwards curves. Bernstein and Lange showed that if k is finite, a large class of elliptic curves over k (all those which have a point of order 4) can be represented in Edwards form. The case $d = -1$ gives the curve (4) considered by Gauss.

In [3], Bernstein et al. introduced the twisted Edwards curves $ax^2 + y^2 = 1 + dx^2y^2$ (where $a,\ d \in k$ are distinct and non-zero) and showed that every elliptic curve with a representation in Montgomery form is birationally equivalent to a twisted Edwards curve. Obviously, the case $a = 1$ of a twisted Edwards curve is an Edwards curve.

In this paper we describe a sequence of rational functions, and consequently a sequence of polynomials, defined on the function field of a twisted Edwards curve which are analogous to the division polynomials for elliptic curves in Weierstrass form. In particular, these polynomials characterise the n-torsion points of the twisted Edwards curve for a positive integer n. These twisted Edwards division polynomials are polynomials in y with coefficients in $\mathbb{Z}[a, d]$, and have degree in y less than $n^2/2$.

References

[1] H. M. Edwards, *A normal form for elliptic curves*, Bulletin of the American Mathematical Society 44 (2007), 393 - 422.

[2] D. Bernstein, T. Lange, *Faster addition and doubling on elliptic curves*, Advances in Cryptology - ASIACRYPT 2007, Springer Lecture Notes in Computer Science 4833, pp.29 - 50 (2007)

[3] D. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, *Twisted Edwards curves*, AFRICACRYPT 2008, Springer Lecture Notes in Computer Science, Springer 5023, pp. 389 - 405 (2008)

A new construction of cyclic relative difference families and related optical orthogonal codes

Koji Momihara

Nagoya University

Let H be a subgroup of order h of a finite group G of order v. A family of s k_i-subsets A_i, $1 \le i \le s$, of G is called a $(v, h, \{k_i \,|\, 1 \le i \le s\}, \lambda)$ *difference family (DF) over G relative to H* if the list

$$\{a - b \,|\, a, b \in A_i; a \neq b; 1 \le i \le s\}$$

of differences contains every element of $G - H$ exactly λ times but no element of H.

In this talk, we consider the case when G is cyclic and we identify G with $Z_v = Z/vZ$, the residue ring of rational integers modulo v. In this case, the subgroup H of order h is uniquely determined and hence we simply call the family as a cyclic $(v, h, \{k_i \,|\, 1 \le i \le s\}, \lambda)$-DF. A new series of such difference families is obtained by using the trace function and the logarithm function over a finite field. The following is our main theorem:

Theorem *Let q be a prime power and let n and m be positive integers satisfying* $\gcd(n, m) = 1$ *and $n \,|\, q - 1$. Let e be a positive integer such that* $\gcd(e, n) = 1$. *Then, there exists a cyclic $(\frac{q^m-1}{n}, \frac{q-1}{n}, \{k_i \,|\, 1 \le i \le \frac{q-1}{e}\}, \frac{q^{m-2}(q-1)}{en})$-DF, where each k_i is bounded by*

$$\frac{q^{m-1} - (n-1)q^{\frac{m-1}{2}}}{n} \le k_i \le \frac{q^{m-1} + (n-1)q^{\frac{m-1}{2}}}{n}.$$

Further, in relation to the theorem above, we also get a new family of optimal $(v, k, 1, 1)$ optical orthogonal codes.

References

[1] C. Ding, Optimal and perfect difference systems of sets, *J. Combin. Theory, Ser. A,* 116, pp. 109–119, (2009).

[2] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, (1997).

Duality for poset codes

Allan O. Moura

State University of Campinas

(Joint work with M. Firer)

Let $\mathbb{F}_q^n$ be an n-dimensional vector space over the field $\mathbb{F}_q$ and $P = ([n], \preceq_P)$ a partial order (*poset*) on the set of coordinates of $\mathbb{F}_q^n$, $[n] = \{1, 2, ..., n\}$. The *P-weight w_P of v* is $w_P(v) = |\langle supp(v) \rangle|$, where $supp(v) = \{ i \,;\, v_i \neq 0\}$, $\langle A \rangle$ is the smallest ideal of P containing A and $|X|$ is the cardinality of X. The P-weight defines a *P-distance* $d_P(u, v) := w_P(v - u)$ that generalizes the usual Hamming metric and the pair $\left(\mathbb{F}_q^n, d_P\right)$ is called a P-space. The study of error correcting codes in P-spaces, using the P-distance to define the metric invariants (such as weight hierarchy), started with works of Niederreiter [2] and Brualdi [1] and since then it is being developed in a way similar to that of classical Hamming spaces. Using multiset techniques, we generalize Wei's Duality Theorem [3] to P-spaces:

Theorem (Duality) *Let C be an $[n,k]_q$ P-code and $C^{\perp}$ the orthogonal code. Then the sets $X = wh_P(C) = \left\{d_1^P(C), d_2^P(C), ..., d_k^P(C)\right\}$ and $Y = \left\{n+1-d_1^{\overline{P}}\left(C^{\perp}\right), n+1-d_2^{\overline{P}}\left(C^{\perp}\right), ..., n+1-d_{n-k}^{\overline{P}}\right.$ are disjoint and $X \cup Y = \{1,2,...,n\}$, where $\overline{P}$ is the dual order of P, $d_i^P(C)$ and $d_i^{\overline{P}}\left(C^{\perp}\right)$ are Wei's i-th P and $\overline{P}$ weight of the codes C and $C^{\perp}$ respectively.*

From this result we derive some consequences relating the discrepancy and the chain property of a code C with the ones of its orthogonal $C^{\perp}$.

References

[1] R. A. Brualdi, J. S. Graves and K. Mark Lawrence, *Codes with a poset metric*, Discrete Math., 147:57-72, 1995.

[2] H. Niederreiter, *A combinatorial problem for vector spaces over finite fields*, Discrete Math. 96:221-228, 1991.

[3] V. K. Wei, *Generalized Hamming Weights for Linear Codes*, IEEE Trans. Inform. Theory, 37 n.o: 5:1412-1418, 1991.

Dickson Polynomials over Finite Fields: A Different Perspective

Gary L. Mullen

The Pennsylvania State University

If $a \in F_q$, the finite field of order q, the *Dickson polynomial of degree n and parameter a* is defined by

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}.$$

Dickson polynomials over finite fields have many very interesting properties. Some of these properties are related to questions of permutations of finite fields. For example, it is well known that if $a \in F_q^*$, then $D_n(x,a)$ induces a permutation on the field F_q if and only if $(n, q^2-1) = 1$.

In previous work, the parameter a has been fixed and the variable x then runs through the field F_q. In the current work, we reverse these roles, and fix $x \in F_q$, and then allow a to run through the elements of the field F_q. We will discuss some results concerning the permutational properties of these "reversed Dickson polynomials."It appears that once again, we have an interesting, though far from completely understood, class of polynomials. For example, these reversed Dickson polynomials lead to results concerning APN functions.

This is joint work with Xiang-dong Hou (S. Florida), James Sellers (Penn State) and Joseph Yucas (Southern Illinois).

Error-Block Codes and Poset Metrics

Marcelo Muniz S. Alves

Universidade Federal do Paraná

(Joint work with L. Panek and M. Firer)

In 1997 Niederreiter introduces a generalization of one of the main problems of coding theory, the problem of finding k-dimensional subspaces in $\mathbb{F}_q^n$ with the largest possible minimum distance, in terms of maximizing sets of vectors in $\mathbb{F}_q^{n-k}$ subject to some restrictions. In order to rewrite this question in terms of a metric, Brualdi, Graves and Lawrence introduced in [2] the concept of a poset metric. In brief, to each poset $P = (\{1, 2, \ldots, n\}, \leq)$ there corresponds a weight ω_P on $\mathbb{F}_q^n$, the Hamming weight being one of these. Some of the new problems put by this family of metrics are: (i) the classification of perfect codes; (ii) the description of the automorphisms and symmetries of each metric spaces; (iii) the inverse problem of fixing a code and classifying which metrics render this code perfect.

Another generalization of the classic Hamming distance was recently proposed by Feng, Xu and Hickernell, the so-called π-distance (or π-metric). We have obtained a construction that unites both kinds of metrics; we call it a *poset block metric* .

We give a complete description of the groups of linear isometries of these metric spaces in terms of a semi-direct product, which turns out to be similar to the case of poset metric spaces. We also describe poset block structures which turn the extended binary Hamming codes and the extended Golay code into perfect codes.

References

[1] M.Muniz S. Alves, L. Panek and M. Firer, *Error-block codes and poset metrics*, Advances in Mathematics of Communications V. 2, No. 1 (2008) 9511.

[2] R. Brualdi, J. S. Graves and M. Lawrence, *Codes with a poset metric*, Discrete Mathematics 147 (1995) 57-72.

[3] H. Niederreiter, *A combinatorial problem for vector spaces over finite fields*, Discrete Mathematics 96 (1991) 221-228.

Measures on quantum logics of idempotents matrices over finite fields

Daniar Mushtari

Kazan State University

Quantum logics are generalizations of Boolean algebras. They are orthomodular partially ordered sets with the least, 0, and the greatest, 1, elements. The set $\mathrm{P}(\mathcal{M})$ of all idempotents in an algebra $\mathcal{M}$ with unit is a quantum logic. Two elements, P and Q, in such a quantum logic are said to be *orthogonal* iff $PQ = QP = 0$. *Signed measures* $\mu : \mathrm{P}(\mathcal{M}) \to \mathbf{R}$ are defined by the relation

$$\mu\left(\bigvee_n P_n\right) = \sum_n \mu(P_n) \tag{5}$$

for any sequence of pairly orthogonal elements. The well-known Gleason theorem [1] asserts that every nonnegative measure μ on the quantum logic $\Pi(H)$ of all projections (Hermitian idempotents) on a Hilbert space H, $\dim H > 2$, admits representation

$$\mu(P) = tr(TP) \text{ for all } P \in \Pi(H). \tag{6}$$

The author had proved [2] such representation for the signed measures on the quantum logics of all continuous idempotents on a Hilbert space or of all rational idempotent $n \times n$-matrices, $\dim H > 2$. The proof of the second theorem used some computer calculations. The analogical presentation for F_2-valued measures on the set of all idempotent $n \times n$-matrices with values in the field F_4 used some computer calculations, too [3]. We will sketch a new proof of this result without computer calculations as well as some problems and results concerning representations of F_p-valued measures on the set of F_{p^s}-valued idempotent matrices where p is a prime and s is a natural.

References

[1] A.M. Gleason, *Measures on the closed subspaces of Hilbert space*, J. Math. Mech., 1957, **6**, no 6, p. 885-894.

[2] D. Mushtari, *Gleason-type theorems for signed measures on orthomodular posets of projections on linear spaces*, Int. J. Theor. Physics, 1995, **34**, p. 1627-1635.

[3] D. Mushtari, *Gleason-type theorem for linear spaces over the field of four elements*, Int. J. Theor. Physics, 1998, **34**, p. 127-130.

On the number of generalized quadratic APN functions

Nobuo Nakagawa

Kinki University

Generalized quadratic APN functions was defined by S.Yoshiara. Let F and R be vector spaces over $GF(2)$. A function f from F to R is called almost perfect nonlinear if $\sharp\{x \in F |\ f(x+a)+f(x) = b\ \} \leq 2$ for every $a \in F^{\times}$ and every $b \in R$. EA-equivalence of two APN functions from F to R is defined similarly as that of APN functions on $GF(2^n)$. A function f from F to R is called quadratic if $f(x+y+z)+f(x+y)+f(y+z)+f(z+x)+f(x)+f(y)+f(z)+f(0) = 0$ for all elements x, y, z of F. Define as $b_f(x,y) = f(x+y)+f(x)+f(y)+f(0)$. We denote the alternating tensor product of F by $F \wedge F$. A subspace W of $F \wedge F$ is called a nonpure subspace if $W \cap \{x \wedge y |\ x, y \in F\ \} = \{0\}$.

Theorem *(S. Yoshiara) Let $\{e_1, e_2, \cdots, e_n\}$ be a basis of F, a map γ be a linear function from $F \wedge F$ onto R such that* $\mathrm{Ker}(\gamma)$ *is a nonpure subspace and a map α be an affine map from F to R. Then the function $f := f_{\gamma,\alpha}$ defined by the following formula is a quadratic APN function. $f(\sum_{i=1}^n x_i e_i) := \sum_{0 \leq i < j \leq n} x_i x_j (e_i \wedge e_j)^{\gamma} + (\sum_{i=1}^n x_i e_i)^{\alpha}$. Conversely, for every quadratic APN function f from F to R such that b_f is surjective, there is a uniqe pair (γ, α) satisfying $f = f_{\gamma,\alpha}$ where γ is a linear map from $F \wedge F$ to R such that* $\mathrm{Ker}(\gamma)$ *is a nonpure subspace and α is an affine map from F to R.*

An automorphism $g \in GL(F)$ induces an automorphism $\hat{g}$ of $F \wedge F$ defined as $\hat{g}(\sum a_{i,j} e_i \wedge e_j) := \sum a_{i,j} g(e_i) \wedge g(e_j)$. Put $\widehat{G} := \{\ \hat{g} \mid g \in GL(F)\}$. For subspaces W_1, W_2 of $F \wedge F$, we define W_1 is $\widehat{G}$-equivalent to W_2 iff $W_2 = \hat{g}(W_1)$ for an automorphism $g \in GL(F)$.

Theorem *Suppose that f and g are quadratic APN functions from F to R such that $f = f_{\gamma,\alpha}$ and $g = f_{\gamma',\alpha'}$ for γ, γ' are linear maps from $F \wedge F$ to R whose kernels are nonpure subspaces and α, α' are affine maps from F to R. Then f is EA-equivalent to g iff* $\mathrm{Ker}(\gamma)$ *is* $\widehat{G}$*-equivalent to* $\mathrm{Ker}(\gamma')$.

We can calculate the explicit inequivalent number of quadratic APN functions from F to R for $\dim(R) = \frac{n(n-1)}{2} - i$ and $i = 0, 1, 2$ from theorem 1 and theorem 2, moreover the explicit inequivalent number of quadratic APN functions on $GF(2^n)$ by counting nonpure subspaces of $GF(2^n) \wedge GF(2^n)$ with dimension $\frac{n(n-3)}{2}$ for $n = 3, 4, 5$, probably $n = 6$.

Folded Algebraic Geometric Codes from Galois Extensions

Anand Kumar Narayanan

University of Southern California

(Joint work with Ming-Deh Huang)

We describe a new class of list decodable codes based on Galois extensions of function fields and present a list decoding algorithm. These codes are obtained as a result of folding the set of rational places of a function field using certain automorphisms from the Galois group of the extension. This work is an extension of Folded Reed Solomon codes to the setting of Algebraic Geometric codes. We describe two constructions based on this framework depending on if the order of the automorphism used to fold the code is large or small compared to the block length. When the automorphism is of large order, the codes have polynomially bounded list size in the worst case. This construction gives codes of rate R over an alphabet of size independent of block length that can correct a fraction of $1 - R - \epsilon$ errors subject to the existence of asymptotically good towers of function fields with large automorphisms. The second construction addresses the case when the order of the element used to fold is small compared to the block length. We describe a decoding algorithm by reducing it to a root finding problem over the local completion at a place where the automorphism acts as the Frobenius. In this case, with a heuristic analysis we argue that the list size and the running time of the decoding algorithm are bounded by a polynomial in the block length. The heuristic is that a certain multivariate polynomial induced by the received word and the decoding algorithm is not of a very special form. When applied to the Garcia-Stichtenoth tower, this yields codes of rate R over an alphabet of size $(\frac{1}{\epsilon^2})^{O(\frac{1}{\epsilon})}$, that can correct a fraction of $1 - R - \epsilon$ errors. If the worst case list size bound can be proven without this heuristic, this construction leads to explicit codes over a constant alphabet achieving the list decoding capacity. This work is a step towards that goal.

References

[1] Huang M and Narayanan A, "Folded Algebraic Geometric Codes from Galois Extensions". `http://arxiv.org/abs/0901.1162`.(early version)

An upper bound for the number of certain f- sequences

J. Eurico Nogueira

Universidade Nova de Lisboa

(Joint work with Owen J. Brison, Universidade de Lisboa)

Let $\mathbf{F} \subseteq \mathbf{L}$ be finite fields and let $f(t) = t^2 - \sigma t - \rho \in \mathbf{F}[t]$, $\rho \neq 0$. An f-sequence in $\mathbf{L}$ is a sequence $(\mu_i)_{i \in \mathbf{Z}}$ where $\mu_i \in \mathbf{L}$ such that $\mu_{i+2} = \sigma \mu_{i+1} + \rho \mu_i$ for all i. An f-subgroup is a subgroup $M = \{s_0, \cdots, s_{|M|-1}\} \leq \mathbf{L}^*$ such that M may be written as an f-sequence $(\cdots, s_0 = 1, s_1, \ldots, s_{|M|-1}, \cdots)$ of least period $|M|$. In this situation we say that $(s_i)_{i \in \mathbf{Z}}$ represents M.

Here, for certain special cases, we give an upper bound on the number of ways it is possible to write given subgroups as f-sequences.

Results in [1] and [2] imply:

Theorem *Let p be an odd prime and $n \in \mathbf{N}$. Let $f(t) \in \mathbf{F}_{p^n}$ be irreducible of degree 2 with restricted period $p^k + 1$ where k is a proper divisor of n such that n/k is odd. Let $M \leq \mathbf{F}_{p^{2n}}$ be an f-subgroup of order m. Then M admits at least $p^k(p^k - 1)$ representing f-sequences.*

We prove

Theorem *Let p be an odd prime and $n \in \mathbf{N}$. Let $f(t) \in \mathbf{F}_{p^n}$ be irreducible of degree 2 with restricted period $p^k + 1$ where k is a proper divisor of n such that n/k is odd. Let $M \leq \mathbf{F}_{p^{2n}}$ be an f-subgroup of order m. Then M admits at most $p^k(p^k - 1)$ representing f-sequences.*

References

[1] O.J. Brison and J.E. Nogueira, Linear recurring sequence subgroups in finite fields. Finite Fields Appl. 9 (2003) 413-422.

[2] O.J. Brison and J.E. Nogueira, Second order linear sequence subgroups in finite fields. Finite Fields Appl. 14 (2008) 277-290.

The Number of Irreducible Polynomials of Degree n over $\mathbb{F}_q$ with Given Trace and Constant Terms

Behzad Omidi Koma

Carleton University

(Joint work with D. Panario, and Q. Wang)

The problem of estimating the number of irreducible polynomials of degree n over the finite field $\mathbb{F}_q$ with some prescribed coefficients has been largely studied. In particular, several interesting results have been obtained for the number of irreducible polynomials of degree n over $\mathbb{F}_q$ with any given trace and any arbitrary constant term. We use elementary techniques to study the largest number of irreducible polynomials of degree n with given trace and constant terms, and give bounds of it. We also obtain a simple and precise formula for the number of irreducible polynomials of degree $q-1$ over $\mathbb{F}_q$ with given primitive constant term.

References

[1] R. Lidl and H. Niederreiter, "Finite Fields", Cambridge Univ. Press, Cambridge, second edition, 1994.

[2] M. Moisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, *Acta Artith*, **132** (2008), 329-350.

[3] J. L. Yucas, Irreducible polynomials over finite fields with prescribed trace/prescribed constant term, *Finite Fields and Their Applications*, **12** (2006), 211-221.

[4] J. L. Yucas and G. L. Mullen, Irreducible polynomials over GF(2) with prescribed coefficients, *Discrete Mathematics*, **274** (2004), 265-279.

[5] D. Wan, Generators and irreducible polynomials over finite fields, *Math. Comp.*, **66** (1997), 1195-1212.

Finite Field Multiplication via Number-Theoretic Transforms

Edusmildo Orozco

University of Puerto Rico at Rio Piedras

(Joint work with D. Bollman and E. Ferrer)

The convolution theorem can be used to reduce the number of operations needed to multiply two m-degree polynomials over the field of complex numbers from $O(m^2)$ to $O(m \log m)$. It is thus natural to apply the same technique to the multiplication of elements in a finite field $GF(p^m)$ represented in the polynomial basis. However, the problem in $GF(p^m)$ is that there is a second step, namely reduction modulo the irreducible polynomial that defines the field.

In this work we show that for a certain family of finite fields $GF(p^m)$, multiplication, including the reduction step, can be expressed in terms of convolution, thus reducing the number of operations from $O(m^2)$ to $O(m \log m)$. This result is achieved by showing that a variant of the Mastrovito matrix can be embedded in a circulant matrix and then using the fact that the product of a circulant matrix and a vector can be expressed as a convolution.

References

[1] S. Baktir and B. Sunar, *Achieving Efficient Polynomial Multiplication in Fermat Fields Using the Fast Fourier Transform*, ACM Southeast Regional Conference Proceedings of the 44th annual Southeast regional conference, pp 549-554, ACM Press, 2006.

[2] S. Baktir and B. Sunar, *Frequency Domain Finite Field Arithmetic for Elliptic Curve Cryptography*, ece.wpi.edu/sunar/preprints/jmbpaper.pdf.

[3] L. S. Cheng, A. Min, and T. H. Yeap, *Efficient FPGA Implementation of FFT Based Multipliers*, Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Saskatoon, Canada, pp 1300-1303, May 2005.

Interval Partitions and Polynomial Factorization

Daniel Panario

Carleton University

(Joint work with Joachim von zur Gathen and Bruce Richmond)

The fastest algorithms for factoring a univariate polynomial f of degree n over a finite field use a baby-step/giant-step approach. The set $\{1, \ldots, n\}$ of potential factor degrees is partitioned into intervals. In a first stage, for each interval the product of all irreducible factors with degree in the interval is determined, generalizing the method of Cantor and Zassenhaus. In a second stage, each polynomial corresponding to a *multi-factor interval* (that is, an interval containing two or more irreducible factors) is completely factored.

The goal in this work is to analyze the behavior of this algorithm on uniformly random squarefree input polynomials, for various partitions. To this end, we study several parameters such as:

- the expected number of multi-factor intervals,
- the expected number of irreducible factors with degrees lying in multi-factor intervals,
- the number of gcds executed in the factoring process,
- the expected total degree among the irreducible factors with degrees in multi-factor intervals, and
- the probability of a polynomial having no multi-factor interval.

We concentrate on partitions with polynomially growing interval sizes, and determine the partition that minimizes the expected number of gcds.

Paley partial difference sets in groups of order n^4 and $9n^4$ for all odd n

John Polhill

Bloomsburg University of Pennsylvania

A partial difference set with parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$ is said to be of Paley type. In this presentation we give a recursive theorem that, for all odd n, constructs Paley partial difference sets in certain groups of order n^4 and $9n^4$. The theorem makes use of building sets constructed using the structure of the fields $GF(p^{4t})$ for an odd prime p and any positive integer t. These are the same building sets used in the construction of Hadamard (Menon) difference sets. The main result is as follows:

Theorem *Let* $G = \mathbb{Z}_{p_1}{}^{4t_1} \times \mathbb{Z}_{p_2}{}^{4t_2} \times \mathbb{Z}_{p_3}{}^{4t_3} \times \cdots \times \mathbb{Z}_{p_k}{}^{4t_k}$ *and* $G' = Z_3{}^2 \times \mathbb{Z}_{p_1}{}^{4t_1} \times \mathbb{Z}_{p_2}{}^{4t_2} \times \mathbb{Z}_{p_3}{}^{4t_3} \times \cdots \times \mathbb{Z}_{p_k}{}^{4t_k}$ *where the* p_i *are odd primes and* t_i *are positive integers. Then* G *and* G' *both contain Paley partial difference sets.*

We are also able to construct Paley-Hadamard difference sets of the Stanton-Sprott family in groups of order $n^4(n^4 \pm 2)$ when $n^4 \pm 2$ is a prime power and $9n^4(9n^4 \pm 2)$ when $9n^4 \pm 2$ is a prime power. These are new parameters for such difference sets.

Minimum Polynomials and Trace Forms for Cyclic Extensions

Rachel Quinlan

National University of Ireland, Galway

Let L/K be a cyclic Galois extension (for example any extension of finite fields) of degree n, with Galois group generated by σ. From Artin's theorem on linear independence of characters it follows that every K-linear endomorphism of L has a unique expression of the form

$$a_0\mathrm{id} + a_1\sigma + \cdots + a_{n-1}\sigma^{n-1}.$$

Thus the K-linear endomorphisms of L can be identified with "polynomial-type" expressions of degree at most $n-1$ in σ. If $p(\sigma)$ is such an expression, we show that the kernel of the endomorphism corresponding to $p(\sigma)$ is at most equal to the degree of $p(\sigma)$. Furthermore, if $V = \langle a_1, a_2, \ldots a_k\rangle$, we show that up to multiplication by an element of $L^\times$ there is a unique polynomial of degree k in σ that annihilates exactly V. Such a polynomial is given by

$$m_V(\sigma) = \det \begin{pmatrix} a_1 & a_2 & \ldots & a_k & \mathrm{id} \\ \sigma(a_1) & \sigma(a_2) & \ldots & \sigma(a_k) & \sigma \\ \vdots & \vdots & & \vdots & \vdots \\ \sigma^k(a_1) & \sigma^k(a_2) & \ldots & \sigma^k(a_k) & \sigma^k \end{pmatrix}$$

Thus $m_V(\sigma)$ may be considered to be a *minimum polynomial* for the K-subspace V of L. We will show that if $f(\sigma)$ is any polynomial annihilating V, then $f(\sigma)$ is a left multiple of $m_V(\sigma)$ in the K-endomorphism ring of V.

The *trace form* on L is the nondegenerate symmetric form τ defined by $\tau(x,y) = \mathrm{Trace}_{L/K}(xy)$. If T denotes the kernel of the trace mapping from L to K, then T is a K-hyperplane of L, and the orthogonal complement of the K-subspace $V = \langle a_1, a_2, \ldots, a_k\rangle$ of L can be described as follows as the intersection of k hyperplanes of L :

$$V^\perp = \bigcap_{i=1}^{k} a_i^{-1}T.$$

If W is a subspace of L of codimension m, and W is described as above as the intersection of m K-hyperplanes of L, we can use this description to describe an alternative construction for the minimum polynomial $m_W(\sigma)$ of W. By comparing the two polynomial constructions, we can give an explicit description of the orthogonal complement with respect to the trace form of a given K-subspace of L.

On Maximal Curves

Luciane Quoos

Universidade Federal do Rio de Janeiro

(Joint work with M. Abdon and J. Bezerra)

In the last twenty years, curves over Finite Fields have been studied intensely, due in part to their application to coding theory coming from Goppa's construction of codes arising from algebraic curves. A projective nonsingular algebraic curve X, of genus g defined over a Finite Field $\mathbb{F}_{q^2}$ with q^2 elements and irreducible over the algebraic closure, is *maximal* over $\mathbb{F}_{q^2}$, if the cardinality of the set $X(\mathbb{F}_{q^2})$ of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound: $\sharp X(\mathbb{F}_{q^2}) = q2 + 1 + 2gq$. We prove that the following family of curves is maximal and, in some cases, is covered by the Hermitian Curve:

Theorem *The curve $X(q;n)$ defined over $X(\mathbb{F}_{q^{2n}})$ by:*

$$y^{q^2} - y = x^{\frac{q^n+1}{q+1}},$$

with $n \geq 3$ and odd; is maximal.

These curves generalize Garcia and Stichtenoth's curves $y^{q^2} - y = x^{s^2-s+1}$; over $\mathbb{F}_{q^2}$ and $q = s^3$ [1], and the curve introduced in Serre's lecture at AGCT-10 $y^4 + y = x^3$ over $\mathbb{F}_{64}$. For $s = 3$ the curve is not Galois-covered by the Hermitian curve, while for $s = 2$ it is Galois-covered by the Hermitian curve [2]. Recently [3], Giulietti and Korchmaros gave the first example of a maximal curve which is not covered by the Hermitian Curve over $\mathbb{F}_{q^6}$, for $q > 8$.

References

[1] A. Garcia, F. Torres, *On unramified coverings of maximal curves* , Proceedings AGCT-10, Semin. Congr., to appear.

[2] A. Garcia, H. Stichtenoth,*A maximal curve which is not a Galois subcover of the Hermitian curve*, Bulletin of the Brazilian Mathematical Society 37 (2006), 139 - 152.

[3] M. Giulietti, G. Korchmaros,*A new family of maximal curves over a Finite Field*, arXiv:0711.0445v1.

Irreducible Cyclic Codes

Asha Rao

RMIT University

Finding the weights of irreducible cyclic codes is a recurring problem in the literature. Even determining the weights of two-weight irreducible cyclic codes is still an open problem. The important early work in this area includes [1, 2] but in recent years there has been a number of papers revisiting this problem, for example [3, 4].

Let p be a prime number and $K = GF(p, 1)$ the finite field of p elements. Let $L = GF(p, m)$ be the extension of degree m over K. Let n be a divisor of $p^m - 1$ and write $\lambda = (p^m - 1)/n$, (making λ and p coprime). Let ω be a primitive n^{th} root of unity in L. Then $c(p, m, \lambda) := \{c(y) := (Tr(y\omega^i))_{i=0}^{n-1} | y \in L\}$ is called an irreducible cyclic code over K, where Tr is the trace of L over K. The dimension of $c(p, m, \lambda)$ is $ord_n(p)$, the multiplicative order of p modulo n.

Schmidt and White conjecture in [4] that an irreducible cyclic code is a two-weight code if and only if it is a subfield code or a semiprimitive code or it is one of 11 exceptional cases, which they give in Table 1, page 9 of their paper. We discuss this conjecture in the light of recent papers and present a family of two-weight irreducible cyclic codes that are neither subfield codes nor semiprimitive.

References

[1] L. D. Baumert and R. J. McEliece. Weights of irreducible cyclic codes. Inform. and Control, 20:158175, 1972.

[2] L. D. Baumert and J. Mykkeltveit. Weight distributions of some irreducible cyclic codes. DSN Progr. Rep., 16:128131, 1973.

[3] C. Ding. The weight distribution of some irreducible cyclic codes. IEEE Trans. Info. Th., 55:955960, 2009.

[4] Bernhard Schmidt and Clinton White. All two-weight irreducible cyclic codes? Finite Fields and Their Applications, 8(1):1 17, 2002.

A Multilinear Generalization of the Tate Pairing

Wayne Raskind

Arizona State University

(Joint work with Ming-Deh Huang)

We consider a multilinear generalization of the Tate pairing that is of interest in cryptography, especially in the case of a principally polarized abelian variety over a finite field. More generally, Let V be an $\mathbb{F}_\ell$ vector space of even dimension $2g$ that is a subgroup of a group variety defined over a finite field $\mathbb{F}_q$. Let φ be the geometric Frobenius and put $N = 1 - \varphi$. Suppose V is also defined over $\mathbb{F}_q$ in the sense that $\varphi V = V$, and suppose moreover that the action of N is maximally nilpotent on V. That is, $N^{2g} = 0$, but $N^{2g-1} \neq 0$. In particular, $V(\mathbb{F}_q)$, the subgroup of $\mathbb{F}_q$-points in V, is of $\mathbb{F}_\ell$-dimension one. For $i = 0$, ..., $d = 2g-1$, let $V_{2i-d} = \ker N^{i+1}$, and $Gr_{2i-d} = \ker N^{i+1}/\ker N^i$. Let $I = \{d,\ d-2,\ ...,\ -d\}$ and $I_+ = \{d, d-2,\ ...,\ 1\}$. Then (1) For all $i \in I$, $Gr_i V$ is of $\mathbb{F}_\ell$-dimension one and is $\mathbb{F}_q$-rational in the sense that $\varphi x = x$ for $x \in Gr_i V$. (2) A non-trivial $2g$-linear alternating pairing on V taking values in a group G which is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ induces a non-trivial multilinear pairing:

$$Gr_d V \times Gr_{d-2} V \times ... \times Gr_{-d} V \to G.$$

(3) Moreover if $<,>: V \times V \to G$ is a non-degenerate bilinear pairing, then the bilinear pairing induces a perfect pairing between Gr_i and Gr_{-i} for $i \in I_+$, and the $(2g)$-linear pairing $Gr_d V \times ... \times Gr_{-d} V \to G$ sending $v_i \in V_i$ to $(\prod_{i \in I_+} b_i)t$, where t is a generator of G and $b_i t =< v_i, v_{-i} >$, is identical, up to a constant factor, to the multilinear pairing in (2).

In the case where $g = d = 1$, E is an elliptic curve over $\mathbb{F}_q$ and $V = E[\ell]$, the points of order ℓ defined over an algebraic closure of $\mathbb{F}_q$, the condition on N amounts to Frobenius trace being 2 modulo ℓ and $V(\mathbb{F}_q)$ being of $\mathbb{F}_\ell$ dimension one. The pairing resulting from the filtration $V_1 \supset V_{-1}$ is essentially the Tate pairing. In the case of the Jacobian of a curve, the perfect pairing between Gr_d and Gr_{-d} is again essentially the Tate pairing. We will also discuss computational problems in multilinear algebra that are related to and motivated by this construction.

References

[1] D. Boneh and A. Silverberg, Applications of Multilinear Forms to Cryptography, *Contemporary Mathematics* Vol. 324, American Mathematical Society, pp. 71-90, 2003.

Polynomials on $\mathbb{F}_{2^m}$ with good resistance to cryptanalysis

Francois Rodier

Institut de Mathématiques de Luminy

(Joint work with Y. Aubry, G. McGuire)

Vectorial Boolean functions are useful in private key cryptography for designing block ciphers. Two main attacks on block ciphers are differential attacks and linear attacks. An important criterion on Boolean functions is a high resistance to the differential cryptanalysis. K. Nyberg has introduced the notion of differential uniformity δ to characterize those functions which have the better resistance to differential attacks. Boolean functions with small δ are highly appreciated for cryptographic purpose. Such functions with $\delta = 2$ are called almost perfect nonlinear (APN). Up to now, the study of APN functions was especially devoted to the power func- tions. Recently, Budaghyan and al. showed that certain binomial quadratic functions were APN. Recently it has been shown by Hernando and McGuire that the Gold and Kasami functions are the only monomials where d is odd and which give APN functions for an infinity of values of m. G. McGuire conjectured that the Gold and Kasami functions are the only APN functions which are APN on infinitely many extensions of their field of definition. We prove some results toward this conjecture. We use some results about surfaces on finite fields. H. Janwa showed, by using Weils bound, that certain cyclic codes could not correct two errors. A. Canteaut showed by using the same method that certain power functions were not APN for a too large value of the exponent. We could generalize this result to all the polynomials. We prove that when one fixes the degree of a polynomial then, under some condition, the corresponding function can have a low differential uniformity only finitely many often.

The second weight of Generalized Reed-Muller Codes in most cases

Robert Rolland

Institut de Mathématiques de Luminy

Let $\mathbb{F}_q$ be the finite field with q elements and $n \geq 1$ an integer. Let d be an integer such that $1 \leq d < n(q-1)$. The generalized Reed-Muller code of order d is the following subspace of the space $\mathbb{F}_q^{(q^n)}$:

$$\mathrm{RM}_q(d,n) = \left\{ \left(f(x)\right)_{x \in \mathbb{F}_q^n} \mid f \in \mathbb{F}_q[X_1, \cdots, X_n] \text{ and } \deg(f) \leq d \right\}.$$

Let us denote by a and b the quotient and the remainder in the Euclidian division of d by $q-1$, namely

$$d = a(q-1) + b \text{ and } 0 \leq b < q-1.$$

Let us denote by W_2, the second weight, namely the weight just above the minimal distance. In this talk, we determine for $n \geq 3$, $q \geq 3$ and $b \neq 1$ the second weight W_2 (or the second number of points of a hypersurface $N_2 = q^n - W_2$) of the generalized Reed-Muller code and for $b = 1$ we give a lower bound on this second weight. This work is done for all the other values of d not yet handled, namely $q \leq d \leq (n-1)(q-1)$ for $q \geq 3$. The proof which follows the method introduced by O. Geil is based on Gröbner basis technics.

Moreover, for $b \neq 1$ we determine hyperplane arrangements reaching the second weight, but we don't prove that these words are the only words reaching this value.

Solvability of systems of polynomial equations over finite fields

Ivelisse Rubio

University of Puerto Rico at Río Piedras

(Joint work with F. Castro)

In this work we determine the solvability of families of systems of polynomial equations over finite fields by computing the exact divisibility of the exponential sums associated to the systems. This generalizes a theorem of Carlitz to systems of equations. In some cases, our result gives an upper bound for the Waring number of systems of diagonal equations. Also, as a by-product, we obtain information about the p-divisibility of the number of solutions of the systems for cases for which the well known results of Chevalley-Warning and Katz do not give any information.

On the Second Order Nonlinearity of a Cubic Maiorana-McFarland Bent Function

Sumanta Sarkar

Projet SECRET, INRIA Rocquencourt

(Joint work with Sugata Gangopadhyay)

In this paper we study a new class of cubic Maiorana-McFarland bent functions which is based on a permutation constructed by Dobbertin [2]. First we show that this function can not have an affine derivative. Then we determine a lower bound of the second order nonlinearity of this function.

Let $n = 2t$, where $t = 2m + 1$ and $m \geq 2$. We define the cubic Maiorana-McFarland function $\phi_n : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_2$ as $\phi_n(x, y) = Tr_1^t(x(y^{2^{m+1}+1} + y^3 + y))$, where $y \mapsto y^{2^{m+1}+1} + y^3 + y$ is a permutation over $\mathbb{F}_{2^t}$ [2].

Theorem *The function ϕ_n does not possess affine derivatives.*

Using Carlet's result (Corollary 2, [1]), we derive the following lower bound of the second order nonlinearity ($nl_2(\phi_n)$) of the function ϕ_n. To do this we also use the result of Theorem .

Theorem *The lower bound of the second order nonlinearity of ϕ_n is given as*

$$\begin{aligned} nl_2(\phi_n) &\geq 2^{n-1} - \tfrac{1}{2}\sqrt{(2^n - 1)2^{\frac{n+t}{2}+3} + 2^n} \\ &\approx 2^{n-1} - 2^{\frac{7n+4}{8}}. \end{aligned}$$

For larger n, this lower bound of second order nonlinearity of ϕ_n is better than the lower bound given in [1] for a general n-variable Boolean function which does not possess affine derivatives.

References

[1] C. Carlet. *Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications*, IEEE Transactions on Information Theory, Vol. 54(3), pp. 1262–1272, March 2008.

[2] H. Dobbertin. *Almost Perfect Nonlinear Power Functions on GF(2^n): The Welch Case*. IEEE Transactions on Information Theory, Vol. 45, No. 4, May 1999.

On finite semifields of prime degree and the equivalence classification of subspaces of invertible matrices

John Sheekey

University College Dublin and Claude Shannon Institute

(Joint work with Rod Gow)

Let q be a power of a prime, n be a positive integer, and let A and B be n-dimensional subspaces of $n \times n$ matrices over $\mathbf{F}_q$ in which each non-zero element is invertible. We say that A and B are equivalent if there exist invertible $n \times n$ matrices X and Y, say, with

$$XAY = B.$$

We can show that the number of equivalence classes of such subspaces equals the number of isotopy classes of semifields of degree n over $\mathbf{F}_q$. When $n = 3$, results of Menichetti allow us to enumerate the number of equivalence classes, as semifields of degree 3 are classified. When $n = r$ is a prime, a theorem of Weil and Lang enables us to prove that when q is sufficiently large, a semifield of degree r over $\mathbf{F}_q$ always has a primitive element. Moreover, we can in principle enumerate the number of equivalence classes of subspaces of r-dimensional subspaces of $r \times r$ invertible matrices.

On the Distribution of the Number of Points on Elliptic Curves in a Tower of Extentions of Finite Fields

Igor E. Shparlinski

Macquarie University

(Joint work with Omran Ahmadi)

Let E be an elliptic curve defined over $\mathbf{F}_q$, a finite field of q elements. By the Hasse-Weil theorem, the number $\#E(\mathbf{F}_q)$ of $\mathbf{F}_q$-rational points on E satisfies $\#E(\mathbf{F}_q) = q+1-a_q$ with $|a_q| \le 2q^{1/2}$, see [1].

The distribution of $\#E(\mathbf{F}_p)$, where E is defined over $\mathbf{Q}$ and reduced modulo consecutive primes p (that is, $q = p$) is described in the *Sato–Tate conjecture*, which has been recently proven [2]. In particular, the proportion of primes p for which $a_p/2p^{1/2} \in [\beta, \gamma]$ is approximated given by

$$\mu_{ST}(\beta, \gamma) = \frac{2}{\pi} \int_{\beta}^{\gamma} \sqrt{1 - \alpha^2} d\,\alpha.$$

Here we fix an ordinary curve E over $\mathbf{F}_q$, consider it in the tower of extensions, that is, the sets $E(\mathbf{F}_{q^n})$, and study the ratios $a_{q^n}/2q^{n/2}$, $n = 1, 2, \ldots$. In particular, we show that their distribution is not governed by $\mu_{ST}(\beta, \gamma)$ but by a different distribution function

$$\lambda(\beta, \gamma) = \frac{1}{\pi} \int_{\beta}^{\gamma} (1 - \alpha^2)^{-1/2} d\,\alpha.$$

We also discuss some open problems, in particular the possibility of generalising this result to curves of higher genus, where two possible interpretations are possible: related to the number of points on a curve and on its Jacobian, respectively.

References

[1] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.

[2] R. Taylor, 'Automorphy for some l-adic lifts of automorphic mod$l$ representations, II', *Pub. Math. IHES*, **108** (2008), 183–239.

Classification of arcs of size $\frac{q+7}{2}$ with a conical subset of size $\frac{q+3}{2}$

Heide Sticker

Ghent University

(Joint work with K. Coolsaet)

Consider the Desarguesian projective plane $\mathrm{PG}(2, q)$ for odd q. Define a k-arc of $\mathrm{PG}(2, q)$ to be a set S of points, with $|S| = k$, such that no three elements of S are collinear. It is easily proved that a k-arc which is not part of a conic can intersect a conic in at most $(q + 3)/2$ points. Arcs of this type with size $(q + 5)/2$ must necessarily contain an external point to the conic and are easily described.

For the next case, of two extra points, i.e., arcs of this type of size $|S| = (q + 7)/2$, we present an explicit complete classification, up to PGL-equivalence.

Our methods are very similar to those of Korchmáros and Sonnino [1], but instead of using the group structure of a cyclic affine plane of order q, we use the properties of the cyclic group of all norm 1 elements of the field $\mathrm{GF}(q^2)$. This has the advantage that the classification can be formulated without the use of groups, making it very straightforward (and efficient) to use in further computer programs.

We have applied this representation in computer searches for arcs of this type of size larger than $(q + 7)/2$, of which currently only a few examples are known.

References

[1] G. Korchmáros and A. Sonnino, *On arcs sharing the maximum number of points with ovals in cyclic affine planes of odd order*, to appear in Journal of Combinatorial Designs, DOI: 10.1002/jcd.20220

On Projective Planes and Ternary Rings, and their Applications

Klara Stokes

Universitat Rovira i Virgili

(Joint work with Maria Bras-Amorós)

A new construction of projective planes from ternary rings is presented. Explicit constructions of projective planes are usually given in coordinates. It is however possible to give an explicit construction of a projective plane without coordinates, enumerating the points of the planes from 1 to n, where n is the cardinality of the plane.

This construction of projective planes was invented in order to give projective planes for configurations used in P2P UPIR (Peer To Peer User-Private Information Retrieval). In the search for optimal configurations for P2P UPIR we found and proved that these optimal configuration were exactly the projective planes. When defining projective planes for P2P UPIR it makes no sense introducing coordinates, since the points and the lines of the plane correspond to users and communication spaces, and these do not have any underlying structure before the introduction of the projective plane.

References

[1] Bras-Amorós, M. and Stokes K., Optimal Configurations for Peer-to-Peer User-Private Information Retrieval, Submitted, 2009.

[2] Colbourn,C.J. and Dinitz,J. H., Handbook Of Combinatorial Designs, 2007, Chapman and Hall/CRC, Kenneth H. Rosen.

[3] Domingo-Ferrer, J. and Bras-Amorós, M. and Wu, Q. and Manjón, J., *Private Information Retrieval Based on a Peer-to-Peer Community*, Data and Knowledge Engineering, Elsevier, 2009.

[4] Hall, M., *The theory of groups*, New York : Macmillan, cop. 1959.

A study of $(x(q+1), x; 2, q)$-minihypers

Leo Storme

Ghent University

(Joint work with I. Landjev)

We study the weighted $(x(q+1), x; 2, q)$-minihypers. These are weighted sets of $x(q+1)$ points in $\mathrm{PG}(2, q)$ intersecting every line in at least x points. We investigate the decomposability of these minihypers, and define a switching construction which associates to an $(x(q+1), x; 2, q)$-minihyper, with $x \leq q^2 - q$, not decomposable in the sum of an other minihyper and a line, a $(j(q+1), j; 2, q)$-minihyper, where $j = q^2 - q - x$, again not decomposable into the sum of an other minihyper and a line. We also characterize particular $(x(q+1), x; 2, q)$-minihypers. Additionally, we show that $(x(q+1), x; 2, q)$-minihypers can be described as rational sums of lines. In this way, this work continues the research on $(x(q+1), x; 2, q)$-minihypers by Hill and Ward [1], giving many new results on these minihypers.

References

[1] R. Hill and H.A. Ward, Geometric approach to classifying Griesmer codes. *Des. Codes Cryptogr.* **44** (2007), no. 1-3, 169–196.

[2] I. Landjev and L. Storme, A study of $(x(q+1)x; 2, q)$-minihypers. *Des. Codes Cryptogr.*, submitted.

A characterization of the linearity of the Gray image of a linear code over a Galois ring

H. Tapia-Recillas

Universidad Autónoma Metropolitana-I

(Joint work with C.A. López-Andrade)

In [1] it is shown that some non-linear binary codes, including the Kerdock and Preparata codes, are the image of $\mathbf{Z}_4$-linear codes under the Gray map defined on the ring $\mathbf{Z}_4$. Several interesting questions arise not just on codes over this ring but over the ring $\mathbf{Z}_{p^k}$ where p is any prime and k a positive integer, Galois rings, and, more generally, over finite chain rings.

If Φ is the (classical) Gray map over $\mathbf{Z}_4^n$, in [1] (Section II, Theorem 5, pag. 305) the following relation is proved

$$\Phi(\mathbf{a}) + \Phi(\mathbf{b}) + \Phi(\mathbf{a}+\mathbf{b}) = \Phi(2(\mathbf{a}_0 * \mathbf{b}_0)) \quad (*),$$

and used to give a characterization of the linearity of the Gray image of a linear code.

Several generalizations of the the Gray map have appeared in the literature on rings that include $\mathbf{Z}_{p^k}$, and more broadly, finite chain rings in which the class of Galois rings is included. A generalization of the above relation for the ring $\mathbf{Z}_{p^2}$ has appeared in the literature and a similar result about the linearity of the Gray image of a linear code defined over this ring is proved.

By using the Witt ring of (truncated) vectors over the residue field of the Galois ring $R = GR(p^2, m)$ a relation similar to $(*)$ is obtained and used to give a characterization of the linearity of the Gray image of a R-linear code. Examples of Galois rings include $\mathbf{Z}_{p^k}$ and finite fields. If $GR(p^2, m) = \mathbf{Z}_4$, i.e., $p = 2$ and $m = 1$, the relation $(*)$ given in [1] is recovered.

References

[1] A.R. Jr. Hammonds, P.V. Kummar, R. Calderbank, N.J.A. Sloane, and P. Solé, "The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes." IEEE Trans. Inf. Theory, vol.40, pp. 301-319, (1994).

Gauss periods as low complexity normal bases

David Thomson

Carleton University

(Joint work with M. Christopoulou, T. Garefalakis and D. Panario)

An element $\alpha \in \mathbb{F}_{q^n}$ is called *normal* over $\mathbb{F}_q$ if $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is linearly independent. We call N a *normal basis*. Normal bases are used in communications systems where fast exponentiation is highly required. The bottleneck when using a normal basis is in the efficiency of the multiplier. This efficiency is directly related to the *complexity* of the normal basis.

Let q be a prime power and let n, k be integers such that $r = nk + 1$ is a prime not dividing q. Let β be a primitive rth root of unity in $\mathbb{F}_{q^{kn}}$ and let τ be a primitive kth root of unity in $\mathbb{Z}_r$. Then $\alpha = \sum_{i=0}^{k-1} \beta^{\tau^i} \in \mathbb{F}_{q^n}$ is a Gauss period of type (n, k) [1]. Let e be the order of q in $\mathbb{Z}_r$, then α generates a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $\gcd(nk/e, n) = 1$. Normal bases obtained by Gauss periods of type $(n, 1)$ for any q and $(n, 2)$ for $q = 2$ define the *optimal* normal bases with the minimum possible complexity $2n - 1$.

We generalize the result of [2] to give an upper bound on the complexity of the normal basis generated by the trace of a (not necessarily optimal) normal element. This bound depends only on the number of non-zero elements in each row of the multiplication table of the original basis.

We also study the multiplication tables of normal bases obtained by Gauss periods for small values of n and k. We expand on the results in [2] to give the complexity of a normal basis generated by the trace of a Gauss period normal basis for small values of n and k.

References

[1] D. W. Ash, I. F. Blake and S. A. Vanstone, Low complexity normal bases, *Discrete applied mathematics*, **25** (1989), 191-210.

[2] M. Christopoulou, T. Garefalakis, D. Panario, D. Thomson, The trace of an optimal normal element and low complexity normal bases, *Designs, codes and cryptography*, **49** (2008), 199-215.

Some remarks on permutation polynomials

Alev Topuzoğlu

Sabancı University

This talk intends to give a short survey of results which appeared in three recent papers [1, 2, 3], and present new results on their applications.

A well-known result of Carlitz, that any permutation polynomial $\wp(x)$ of a finite field $\mathbf{F}_q$ is a composition of linear polynomials and the monomial x^{q-2}, implies that any $\wp(x)$ can be represented by a polynomial $\mathcal{P}_n(x) = (\ldots((a_0x + a_1)^{q-2} + a_2)^{q-2} \ldots + a_n)^{q-2} + a_{n+1}$, for some $n \geq 0$. Results on the cycle structure of $\mathcal{P}_n(x)$ will be given. Evaluation of the smallest integer n, such that $\mathcal{P}_n(x)$ represents $\wp(x)$ is of interest. This integer n, which we define to be the *Carlitz rank* of $\wp(x)$ is, of course, the least number of "*inversions*" x^{q-2}, needed to obtain $\wp(x)$. A method for determining the

Carlitz rank and results on the enumeration of permutations of $\mathbf{F}_q$ with a fixed Carlitz rank will be presented.

Some new applications in coding theory and pseudorandom number generation will also be discussed.

This is joint work with E. Aksoy, A. Çeşmelioğlu, and W. Meidl.

References

[1] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, On the cycle structure of permutation polynomials, *Finite Fields Appl.* 14 (2008), 593–614.

[2] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, Enumeration of a class of sequences generated by inversions, Proceedings of the Int. Workshop on Coding and Cryptology, Fujian, China, (June 2007) (Y.Q Li et *al*, Eds), (2008), 44–57.

[3] E. Aksoy, A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, On the Carlitz rank of permutation polynomials, *Finite Fields Appl.*, (2009), appeared on line.

$\mathbb{F}_q$–pseudoreguli of $PG(3,q^3)$ and semifields of order q^6

Rocco Trombetti

Universitá di Napoli Federico II

(Joint work with Michel Lavrauw, Giuseppe Marino and Olga Polverino)

In [1] and [2], the finite semifields of order q^6 which are two–dimensional over their left nucleus and six–dimensional over their center have been geometrically partitioned into several non–isotopic classes by using the associated linear sets in $\mathbb{P} = PG(3,q^3)$. Nevertheless, in the same paper a connection between semifields belonging to one of these classes (precisely, class $\mathcal{F}_5$) and an other geometric object of $\mathbb{P}$ called $\mathbb{F}_q$–pseudoregulus, has been discovered. So far, the known examples of semifields belonging to the class $\mathcal{F}_5$ are some Knuth semifields and some Generalized Twisted Fields. In [1], these examples have been characterized in terms of the associated $\mathbb{F}_q$–pseudoreguli. Taking into account these results, in this conference, starting from the study of an $\mathbb{F}_q$–pseudoregulus of $\mathbb{P}$ and exploiting the above mentioned connection we derive, up to the isotopy relation, the multiplication of some semifields belonging to the class $\mathcal{F}_5$. We present several computer-generated examples of new semifields belonging to this class; finally, we are able to generalize some of these to an infinite family belonging to $\mathcal{F}_5$. This family turns out to be a new infinite family of semifields.

References

[1] G. Marino, O. Polverino, R. Trombetti, *$\mathbb{F}_q$–linear sets of $PG(3,q^3)$ and semifields*, J. Comb. Theory Ser. A, **114** (2007), 769–788.

[2] N.L. Johnson, G. Marino, O. Polverino and R. Trombetti, *Semifields of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$*, Finite Fields and Their Applications, **14** n.2 (2008), 456–469.

The intersection of a subline and an $\mathbb{F}_q$-linear set

Geertrui Van de Voorde

Ghent University

(Joint work with Michel Lavrauw)

Let $\mathrm{PG}(n,q)$ be the n-dimensional projective space over the finite field $\mathbb{F}_q$ with q elements. A linear pointset in $\mathrm{PG}(n,q)$ can be defined in several equivalent ways. We use the following geometrical definition.

Suppose $q=q_0^t$, with $t\geq 1$. By "field reduction", the points of $\mathrm{PG}(n,q)$ correspond to $(t-1)$-dimensional subspaces of $\mathrm{PG}((n+1)t-1,q_0)$, since a point of $\mathrm{PG}(n,q)$ is a 1-dimensional vector space over $\mathbb{F}_q$, and so a t-dimensional vector space over $\mathbb{F}_{q_0}$. In this way, we obtain a partition $\mathcal{D}$ of the pointset of $\mathrm{PG}((n+1)t-1,q_0)$ by $(t-1)$-dimensional subspaces, which forms a *Desarguesian spread*. Let $\mathcal{D}$ be the Desarguesian $(t-1)$-spread of $\mathrm{PG}((n+1)t-1,q_0)$. If U is a subset of $\mathrm{PG}((n+1)t-1,q_0)$, then we define $\mathcal{B}(U):=\{R\in\mathcal{D}||U\cap R\neq\emptyset\}$, and we identify the elements of $\mathcal{B}(U)$ with the corresponding points of $\mathrm{PG}(n,q_0^t)$. If U is subspace of projective dimension k of $\mathrm{PG}((n+1)t-1,q_0)$, then $\mathcal{B}(U)$ is an $\mathbb{F}_{q_0}$-*linear set of rank* $k+1$.

Using this representation, we investigate the intersection of $\mathbb{F}_q$-linear sets. For example, we show that a subline, i.e. an $\mathbb{F}_q$-linear set of rank 2, intersects an $\mathbb{F}_q$-linear set of rank 3 in $0,1,2,3$ or $q+1$ points.

On permutation polynomials of prescribed shape

Qiang Wang

Carleton University

(Joint work with A. Akbary and D. Ghioca)

Enumerating permutation polynomials over finite fields by degrees is one of open problems proposed by Lidl and Mullen in 1988. When the field is prime field $\mathbf{F}_p$ and the degree is $p-2$, Das gave an asymptotic formula and explicit bounds of the number of these permutation polynomials in 2002. His result was later extended to any field $\mathbf{F}_q$ and degree $q-2$ by Konyagin and Pappalardi. Moreover, Konyagin and Pappalardi studied the number of permutation polynomials which have no monomials of prescribed degrees. Here we count permutation polynomials of $\mathbf{F}_q$ which are sums of monomials of prescribed degrees. This allows us to prove certain results about existence of permutation polynomials of prescribed shape, which also generalize some recent results on permutation binomials obtained by Laigle-Chapuy, Masuda and Zieve respectively.

Primitive normal polynomials over finite fields with a prescribed coefficient for $11\leq n\leq 14$

Xiaozhe Wang

China National Digital Switching System Engineering and Technological Research Center

(Joint work with Shuqin Fan)

This thesis concerns of the existence of a primitive normal polynomial with any coefficient arbitrarily prescribed.Let $n = 11, 12, 13, 14$, and q a prime power.We obtain that for any element $a \in F_q$ and any $1 < m < n$, there exists a primitive normal polynomial $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^{n-1}\sigma_{n-1}x + (-1)^n\sigma_n$ of degree n with $\sigma_m = a$ except $\sigma_1 = 0$. This has been proved for $n \geq 15$ by Fan et.al[3],but was unestablished for $n \leq 14$.

In this work, we obtain new estimates for the number of primitive normal polynomials of degree n over F_q with any coefficient arbitrarily prescribed.We improve upon the estimates of [3] by rewriting the system of trace equations. With this new estimate and a new variation of Cohen's sieve techniques[4] which makes the computation easier,we achieve the following theorem:

Theorem *Let $n = 11, 12, 13, 14$,q a prime power. For any given $a \in F_q$ and any integer $1 < m < n$, there exists a primitive normal polynomial $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^{n-1}\sigma_{n-1}x + (-1)^n\sigma_n$ of degree n over F_q with $\sigma_m = a$ with exceptions: $(m, a) = (1, 0)$.*

References

[1] S.D.Cohen, *Primitvie polynomials with a prescribed coefficient*, Finite Fields and Their Applications,12(2006),425-491.

[2] Mateja Prešern, *Existence problems of primitive polynomials over finite fields*, A thesis for the degree of Doctor of Philosophy of the University of Glasgow,2007

[3] SQ.Fan, XZ.Wang, *Primitive normal polynomials with a prescribed coefficient*,Submitted

[4] S.Fan, X.Wang, *Primitive normal polynomials with the last two coefficients*,Discrete Mathematics(2009),Accepted

---

Legendre-Sidelnikov Sequences

Arne Winterhof

Austrian Academy of Sciences

(Joint work with D. Gomez and M. Su)

Several sequences with nice pseudorandomness properties in view of applications in wireless communication and cryptography have been defined using the *quadratic character* of a finite field, see the survey [1] and references therein. Among these sequences are the *Legendre sequence*, the *Sidelnikov sequence* and the *two-prime generator*.

Here we introduce and analyze a new sequence combining the concepts of these three sequences.

Let p be an odd prime and q the power of an odd prime such that $\gcd(p, q-1) = 1$. We consider the $p(q-1)$-periodic binary sequence (s_i) defined by

$$s_i = \begin{cases} 1, & \text{if } p \mid i, \\ 0, & \text{if } i \equiv (q-1)/2 \bmod q-1,\ p \not| i, \\ \frac{1-\left(\frac{i}{p}\right)\eta(g^i+1)}{2}, & \text{otherwise,} \end{cases} \quad i \geq 0,$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, $\eta(.)$ is the quadratic character of $\mathbb{F}_q$, and g is a primitive element of $\mathbb{F}_q$.

We provide a formula for the number of 1s in a period of (s_i) which shows that (s_i) is *balanced* if $p = q$. We determine the exact values of the *periodic autocorrelation* and an upper bound on the absolute value of the *aperiodic autocorrelation*. Moreover, we analyze the *linear complexity* of (s_i) and related measures.

The proofs are mainly based on results on *character sums* over finite fields.

References

[1] A. Topuzoğlu, A. Winterhof, "Pseudorandom sequences", *Topics in geometry, coding theory and cryptography*, 135–166, Algebr. Appl., 6, Springer, Dordrecht, 2007.

New parameters for Bent Functions

Jacques Wolfmann

IMATH(GRIM), Université du Sud Toulon-Var

k-boolean fuctions are the maps from $\mathbb{F}_2^k$ into $\mathbb{F}_2$. Bent functions are the boolean functions whose Walsh coefficients have constant magnitude and they only exist if k is an odd number. They are interesting for Coding Theory, Cryptology and well-correlated binary sequences.

Let $k = 2t$, $n = 2^{2t-1} - 1$. $\mathcal{B}(k)$ is the set of k-bent functions.
A simple way to classify bent functions is to consider their degrees and their weights. On the other hand, $\mathcal{B}(k)$ is invariant under the action of the affine linear group of $\mathbb{F}_2^k$ and under the action of the group of translations of affine boolean functions. The corresponding partition into orbits define a classification in $\mathcal{B}(k)$ and the corresponding "affine equivalence".

Two infinite families of bent functions are known but nobody knows if every bent function is affine equivalent to a member of these families.

In this work, we first restrict the study at a particular subset $\mathcal{B}_0(k)$ of bent functions, without loss of generality. Every member of $\mathcal{B}_0(k)$ is then described by means of two $(k-1)$-boolean functions f_p and f_q. Several properties of these functions are given. The Mattson-Solomon polynomials of f_p, f_q, $f_p + f_q$ in $\mathbb{F}_2[x]/(x^n - 1)$ are specified as members of particular binary cyclic codes. This leads to introduce two integers $\mathfrak{i}$ and $\mathfrak{s}$ as new parameters for every k-bent function of $\mathcal{B}(k)$ This gives rise to a new classification which is more sharp that the one defined only by degrees and weights or by affine equivalence.

In order to illustrate this fact we present examples of bent functions having the same degree and the same weight but different new parameters $\mathfrak{i}, \mathfrak{s}$ and also examples of affine equivalent bent functions with different new parameters. Furthermore, we give several additional properties of the new parameters and we specify the classification for the case $k = 6$.

An Algebraic Characterization of q-ary Images of q^n-ary Codes Invariant under a Permutation

Isaac Woungang

Ryerson University

(Joint work with H-C. Chao, M. K. Denko, S. Misra, and F. Huang)

An algebraic characterization of the q-ary images of linear codes of length m over F_{q^n} which are invariant under the action of a permutation σ (σ-codes), is introduced for the first time. To this effect, We consider σ a permutation of $\{0, 1, \ldots, m-1\}$ as a product of p disjoint cycles c_i, and we define $\underline{\tilde{\sigma}}$ a linear mapping on F_q^{nm} induced by σ. Then, we derive the following result:

Theorem *If $C \subseteq F_{q^n}^m$ is a $\underline{\sigma}$-code (code invariant under $\underline{\sigma}$), then $D_{\underline{\alpha}}(C) \subseteq F_q^{nm}$, the q-ary image of C with respect to $\underline{\alpha}$, a basis of F_{q^n} over F_q, is a $\underline{\tilde{\sigma}}$-code.*

To characterize the class of codes $\{D_{\underline{\alpha}}(C), C \subseteq F_{q^n}^m \text{ a } \underline{\sigma}\text{-code}\}$, let Γ be the subspace generated by the matrices of $(\gamma)_m$ and $\underline{\tilde{\sigma}}$ relatively to the canonical basis of F_q^{mn}, where $(\gamma)_m = D_{\underline{\alpha}} \circ \Phi_\gamma \circ D_{\underline{\alpha}}^{-1}$ and $\Phi_\gamma : F_{q^n}^m \to F_{q^n}^m$ is defined by $\Phi_\gamma(X_0, \ldots, X_{m-1}) = (\gamma X_0, \ldots, \gamma X_{m-1})$, $\gamma \in F_{q^n} = F_q(\beta)$. We get:

Theorem *Let $W \subseteq F_q^{mn}$ be a F_q-subvector space of F_q^{mn}, W is the q-ary image of a $\underline{\sigma}$-code $C \subseteq F_{q^n}^m$ if and only if W is a Γ-submodule of F_q^{mn}.*

To characterize in-depth the above submodules, we investigate the structure of the matrices $\mathcal{Q}^k$, $k > 0$, where $\mathcal{Q}$ is the matrix of $\underline{\tilde{\sigma}}^{-1} \circ (\beta)_m$ relatively to the canonical basis of F_q^{mn}. Based on this, we obtain the main theorem.

Theorem *(1) If there exists a polynomial $f(X) \in F_q[X]$ such that $P = f(\mathcal{Q})$, then the $F_q[X]$-submodules of F_q^{nm} for the action induced by $\mathcal{Q}$ are the q-ary images, with respect to $\underline{\alpha}$, of $\underline{\sigma}$-codes in $F_{q^n}^m$. (2) If $F_q(\beta) = F_q(\beta^l)$, where $l = l.c.m_{0 \le i < p}(l_i)$, l_i the order of the cycle c_i, then there exists a polynomial $f(X) \in F_q[X]$ such that $P = f(\mathcal{Q})$.*

References

[1] J. Lacan, E. Delpeyroux, *The q-ary image of some q^m-ary cyclic codes: permutation group and soft-decision decoding*, IEEE Transactions on Information Theory, Vol. 48 i.7, no 7, pp. 20692078, 2002.

Zeta functions of an optimal tower of function fields

Alexey Zaytsev

University College Dublin and Claude Shannon Institute

(Joint work with Gary McGuire)

A recursive formula for the L-polynomial of each step in the second Garcia-Stichtenoth tower is obtained. Additionally we prove that the Galois closure of the second Garcia-Stichtenoth tower (cf. [3]) is an ordinary tower and hence the initial tower is also ordinary. In particular, the L-polynomials up to step 6 were computed.

More precisely, let $T_1 := \mathbf{F}_4(x_1)$ be a rational function field. Then the tower is defined by (cf. [1])

$$T_n := \mathbf{F}_4(x_1, \ldots, x_n), \text{ where } \qquad x_i^2 + x_i = \frac{x_{i-1}^3}{x_{i-1}^2 + x_{i-1}}.$$

After applying some observations (which are easy for this specific case) and the Kani-Rosen decomposition (cf. [2]) of Jacobians we obtain the following theorem.

Theorem *For the tower of the function field mentioned above, we have the following decomposition of the L-polynomials:*

$$\begin{aligned}
&\mathrm{L}_{T_2} = 1 + 3T + 4T^2 \\
&\mathrm{L}_{T_3} = (1 + 3T + 4T^2)^3 \\
&\mathrm{L}_{T_4} = (1 - T + 4T^2)^2(1 + 3T + 4T^2)^7 \\
&\mathrm{L}_{T_5} = (1 - T + 4T^2)^4(1 + 3T + 4T^2)^{11}(1 + T + 4T^2)^2(1 + 2T + T^2 + 8T^2 + 16T^4)^2.
\end{aligned}$$

In general, if $n \geq 6$ *then*

$$\begin{aligned}
&L_{T_n} = (1 + T + 4T^2)^{2n-8}(1 + 3T + 4T^2)^{12n-49}(1 - T + 4T^2)^{6n-26} \\
&(1 + 2T + T^2 + 8T^3 + 16T^4)^{6n-24}(1 + T - T^2 + 3T^3 - 4T^4 + 16T^5 + 64T^6)^{2n-10} \\
&L_{Y_{5,1}}^{2n-12} \dots L_{Y_{n-2,1}}^2,
\end{aligned}$$

where $L_{Y_{i,1}}$ *is a quotient of the L-polynomial of a function field*

$$\mathbf{F}_4(x_2, \dots, x_i, u + 1/x_1)$$

by the L-polynomial of T_{i-1} *and* u *is a root of* $T^2 + T + \dfrac{x_i^4}{(x_i + 1)(1 + \gamma^2 x_i^2)}$.

References

[1] Arnaldo Garcia and Henning Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory*, 61(2):248–273, 1996.

[2] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.

[3] A. Zaytsev. The Galois closure of the Garcia-Stichtenoth tower. *J. Finite Fields and Their Applications*, 13(4):751–761, 2007.