PARIS 2023

Book of abstracts

Table of contents

Theory of finite fields

Polynomials over finite fields

Boolean and vectorial (cryptographic) functions and related theory

Specific linear codes

Coding theory with the rank metric

Algebraic geometry and number theory approach

Finite geometry and designs

Combinatorial and geometric aspects for codes and graphs

Theory of finite fields

The functional graphs of generalized cyclotomic mappings of finite fields

Daniel Panario
Carleton University
(Joint work with Alexander Bors and Qiang Wang)

Abstract

When we iterate functions over finite structures, there is an underlying natural functional graph. For a function f over a finite field $\mathbb{F}_q$, this graph has q nodes and a directed edge from vertex a to vertex b if and only if $f(a) = b$. It is well known, combinatorially, that functional graphs are sets of connected components, components are directed cycles of nodes, and each of these nodes is the root of a directed tree.

The study of iterations of functions over a finite field and their corresponding functional graphs is a growing area of research, in part due to their applications in biology, cryptography, and integer factorization methods like Pollard rho algorithm.

We briefly survey the main problems addressed in this area so far [1]. Then, we comment on recent research on the functional graphs of generalized cyclotomic mappings of finite fields [2]. We study periodic points, cycle structure, and rooted trees attached to periodic points of these mappings.

Keywords: dynamics over finite fields, generalized cyclotomic mappings

References

[1] A survey on iterations of mappings over finite fields. R. Martins, D. Panario and C. Qureshi, Radon Series on Computational and Applied Mathematics de Gruyter, 23, 135-172, 2019.

[2] Functional graphs of generalized cyclotomic mappings of finite fields. A. Bors, D Panario and Q. Wang, `https://arxiv.org/abs/2304.00181`, 221 pages, 2023.

Rationality of four-valued families of Weil sums associated to power permutations

Daniel J. Katz

California State University, Northridge

(Joint work with Allison E. Wong)

Abstract

Consider the Weil sum $W_{F,d}(a) = \sum_{x \in F} \psi(x^d - ax)$, where F is a finite field, ψ is the canonical additive character of F, a is a nonzero element of F, and d is a positive integer such that $\gcd(d, |F| - 1) = 1$. This last condition makes $x \mapsto x^d$ a power permutation of F, that is, a power map that permutes F. The Weil spectrum for F and d is the multiset of values $W_{F,d}(a)$ as a runs through F^*. From the Weil spectrum one can determine the Walsh spectrum of $x \mapsto x^d$, which measures the nonlinearity of this power permutation and hence the resistance to linear cryptanalysis of protocols derived from it. The Weil spectrum also determines the crosscorrelation spectrum of pairs of maximal linear sequences and the weight distribution of certain error-correcting codes. Since one sums roots of unity in the complex plane to obtain the Weil spectrum values, these are always algebraic integers. They are rational integers when the characteristic of the underlying finite field F is 2 or 3, but this is not always the case in higher characteristics. A rational Weil spectrum is one whose values are all rational integers. A v-valued Weil spectrum is one that has precisely v distinct values. If one sets aside degenerate cases, Helleseth showed that all Weil spectra of power permutations have at least three distinct values [1], and it has been shown that all three-valued spectra are rational [2]. In this talk, we show that, with one exception, four-valued Weil spectra of power permutations are also always rational.

Keywords: Weil sum, character sum, Walsh spectrum, crosscorrelation, m-sequence

References:

[1] Helleseth, T., Some results about the cross-correlation function between two maximal linear sequences, *Discrete Math.*, **16**(3):209–232 (1976).

[2] Katz, D.J., Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth, *J. Combin. Theory Ser. A*, **119**(8):1644–1659 (2012).

Ranges and lower degree ranks of polynomials over finite prime fields.

Thomas Karam
University of Oxford

Abstract

Let p be a prime, and let $1 \leq e < p$ be an integer. The *degree-e rank* of a polynomial $\mathbb{F}_p^n \to \mathbb{F}_p$ was defined in 2007 by Green and Tao [1] as the smallest nonnegative integer k such that we can find polynomials $P_1, \ldots, P_k : \mathbb{F}_p^n \to \mathbb{F}_p$ all with degree at most e and a function $F : \mathbb{F}_p^k \to \mathbb{F}_p$ satisfying $P = F(P_1, \ldots, P_k)$.

As shown by Green and Tao, if $2 \leq d < p$ is an integer and P is a degree-d polynomial not approximately uniformly distributed on $\mathbb{F}_p^n$, then P must have bounded degree-$(d-1)$ rank. This conclusion was later strengthened to the existence of a decomposition

$$P = Q_1 R_1 + \ldots + Q_k R_k$$

for some bounded integer k and some polynomials Q_i, R_i such that $\deg Q_i < d, \deg R_i < d$ and $\deg Q_i + \deg R_i \leq d$ for each $1 \leq i \leq k$.

In this talk I shall explain how this refinement may be used to deduce from the range $P(\mathbb{F}_p^n)$ of a polynomial that it has bounded degree-e rank for smaller values of e than $d-1$, and discuss the relevant adjustments to be made if the assumption merely holds on the restriction $P(S^n)$ for some non-empty subset S of $\mathbb{F}_p$ (which may be thought of as $\{0,1\}$ to begin with).

Keywords: Polynomials, range, rank, equidistribution.

References

[1] B. Green and T. Tao, *The distribution of polynomials over finite fields, with applications to the Gowers norms.* Contr. Discr. Math., **4** (2009), no. 2, 1-36.

Number of Equivalence Classes of Rational Functions over Finite Fields

Xiang-dong Hou
Department of Mathematics and Statistics
University of South Florida, Tampa, FL 33620, USA
xhou@usf.edu

Abstract

Two rational functions $f, g \in \mathbb{F}_q(X)$ are called *equivalent* if and only if there exist $\phi, \psi \in \mathbb{F}_q(X)$ of degree one such that $g = \phi \circ f \circ \psi$. Many intrinsic properties of rational functions are preserved under equivalence. For example, the cardinality of the value set and the arithmetic monodromy group of a rational function are preserved under equivalence. The equivalence classes of rational function of a given degree n correspond to the orbits of the subfields of $\mathbb{F}_q(X)$ of degree n under the action of the Galois group of $\mathbb{F}_q(X)$ over $\mathbb{F}_q$.

Let $\mathfrak{N}(q, n)$ denote number of equivalence classes of rational functions of degree n over $\mathbb{F}_q$. Despite its obvious significance, this number was not known previously. In this talk, we determine the number $\mathfrak{N}(q, n)$ explicitly for all q and n. The formula is obtained through a careful study of the stabilizers of rational functions in $\mathbb{F}_q(X)$ under the actions of $\mathrm{PGL}(2, \mathbb{F}_q)$ and $\mathrm{PGL}(2, \mathbb{F}_{q^2})$. The first nontrivial case of the formula, when $n = 3$, gives

$$\mathfrak{N}(q, 3) = \begin{cases} 2(q+1) & \text{if } q \equiv 1, 4 \pmod 6, \\ 2q & \text{if } q \equiv 2, 5 \pmod 6, \\ 2q+1 & \text{if } q \equiv 3 \pmod 6. \end{cases}$$

Recently, there is a surge of interest in low degree rational functions over finite fields. The determination of $\mathfrak{N}(q, n)$ is an important step towards a better understanding of such functions.

Frobenius nonclassicality of $y^n = f(x)$ over $\mathbb{F}_{p^3}$

Herivelto Borges
Universidade de São Paulo
(Joint work with C. Gonçalves)

Abstract

Let $q = p^n$ be a prime power and $\mathbf{F}_q$ be the finite field with q elements. An irreducible curve $\mathcal{C}$ over $\mathbf{F}_q$ is called $\mathbf{F}_q$-Frobenius nonclassical if the image $Fr(P)$ of each simple point $P \in \mathcal{C}$ under the Frobenius map lies on the tangent line at P.

Frobenius nonclassical curves were introduced in the work of Stöhr and Voloch in [2] .These curves possess remarkable arithmetic and geometric properties, and their complete classification remains an open problem. It is well-known that if $q \leq p^2$, then up to $\mathbf{F}_q$-projectivity, the only $\mathbf{F}_q$-Frobenius nonclassical curve of the form $y^n = f(x)$ is the Hermitian curve given by $y^{p+1} = x^p + x$. In this case, we have $q = p^2$.

In this talk, we discuss the classification of $\mathbf{F}_{p^3}$-Frobenius nonclassical curves of type $y^n = f(x)$. Building on recent results on minimal value set polynomials [1], we will show that such curves can be reduced to three types, and important birational invariants such as genus, automorphism group, and p-rank can be determined for each type.

Keywords: Frobenius nonclassical curve, Minimal value set polynomial.

References

[1] Borges, H. and Reis, L., Minimal value set polynomials over fields of size p^3 . Proceedings of the American Mathematical Society, 149, 3639–3649, (2021).

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

The factorization of $X^n - a$ and $f(X^n)$ over $\mathbb{F}_q$

Anna-Maurin Graner
University of Rostock

Abstract

The polynomial $X^n - 1$ and its factorization over $\mathbb{F}_q$ have been studied for a long time. Many results on this, and the closely related problem of the factorization of the cyclotomic polynomials, exist. We study the factorization of the polynomial $X^n - a$ with $a \in \mathbb{F}_q^*$. If there exists an element $b \in \mathbb{F}_q$ such that $b^n = a$, the factorization of $X^n - a$ can easily be derived from the factorization of $X^n - 1$. We also consider the case that there does not exist such an element b. We use our results to factorize the composition $f(X^n)$, where f is an irreducible polynomial over $\mathbb{F}_q$. The factorization of $f(X^n)$ is known for the case $\gcd(n, \mathrm{ord}(f) \cdot \deg(f)) = 1$. Our results allow us to give the factorization of $f(X^n)$ in a more general setting.

Keywords: Factorization, irreducible polynomials, composition.

References

[1] Brochero Martinez, F.E., Giraldo Vergara, C.R., Batista de Oliveira, L.: Explicit factorization of $x^n - 1 \in \mathbb{F}_q[x]$. Designs, Codes and Cryptography 77, 277–286 (2015)

[2] Brochero-Martinez, F.E., Reis, L., Silva-Jesus, L.: Factorization of composed polynomials and applications. Discrete Mathematics 342(12), 111603 (2019)

[3] Wu, Y., Yue, Q., Fan, S.: Further factorization of $x^n - 1$ over a finite field. Finite Fields and Their Applications 54, 197–215 (2018)

[4] Wu, Y. and Yue, Q.: Further factorization of $x^n - 1$ over a finite field (II). Discrete Mathematics, Algorithms and Applications 13(06), 2150070 (2021)

Special Rational Transformations and their Connection to Invariant Polynomials

Max Schulz
University of Rostock

Abstract

Let K be a field, $K(x)$ the rational function field over K and $PGL_2(K)$ the projective general linear group over K. We write $[A]$ for the coset of $A \in GL_2(K)$ in $PGL_2(K)$. It is well-known that $PGL_2(K)$ is isomorphic to the group of K-automorphisms of $K(x)$. Let $G \leq PGL_2(K)$ be a finite subgroup and consider the fixed subfield under G:

$$K(x)^G := \left\{ Q(x) \in K(x) | Q(x) = Q\left(\frac{ax+b}{cx+d}\right) \text{ for all } \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \in G \right\}.$$

By basic Galois theory $[K(x) : K(x)^G] = |G|$ and with Lüroths Theorem there exists a rational function $Q_G(x) = g(x)/h(x)$ of degree $|G|$ such that $K(Q_G(x)) = K(x)^G$. Moreover, $Q_G = g/h$ can be normalized in such a way that $|G| = \deg(g) > \deg(h) \geq 0$, these rational functions are called *quotient map* for G. For a monic polynomial $F = x^n + \sum_{i=0}^{n-1} a_i x^i \in K[x]$ and a rational function $Q(x) = g(x)/h(x)$ we define the Q-transform of F as

$$F^Q(x) = h(x)^n \cdot F(Q_G(x)) = g(x)^n + \sum_{i=0}^{n-1} a_i g(x)^i h(x)^{n-i}.$$

The main goal of our talk is to explain the factorization of polynomials $F^{Q_G} \in K[x]$ where Q_G is a quotient map and $F \in K[x]$ is an irreducible polynomial, and how that is connected to a group action of G on monic polynomials. We discuss factorizations that correspond to cyclic subgroups of $PGL(\mathbb{F}_q)$. Additionally, we will look at the case that $G = PGL(\mathbb{F}_q)$ which will lead us to a beautiful polynomial identity over finite fields.

Keywords: Irreducible Polynomials, Factorization, Group Action

Existence of primitive triples over finite fields

Soniya Takshak
Indian Institute of Technology Delhi, India
(Joint work with R. K. Sharma - IIT Delhi)

Abstract

Let q be a prime power and $\mathbb{F}_q$ be a finite field with q elements. The set of non-zero elements of $\mathbb{F}_q$, denoted by $\mathbb{F}_q^*$, forms a cyclic group under multiplication. A generator of $\mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q$. In this article, we obtain a sufficient condition for the existence of primitive elements $\alpha, \beta \in \mathbb{F}_q$ such that $f(\alpha, \beta)$ is also primitive, where $f(x, y)$ be a polynomial over $\mathbb{F}_q$ in two variables.

Keywords: Finite Field; Primitive Element; Character.

References

[1] S. D. Cohen, *Pair of primitive elements in fields of even order*, Finite Fields Appl., **28**, 22-42, 2014.

[2] S. D. Cohen, Hariom Sharma, and R. K. Sharma, *Primitive values of rational functions at primitive elements of a finite field*, Journal of Number Theory, **219**, 237-246, 2021.

[3] L. Fu and D. Q. Wan, *A class of incomplete character sums*, Journal of Number Theory, **65**, 1195-1211, 2014.

[4] Hariom Sharma and R. K. Sharma, *Existence of primitive normal pairs with one prescribed trace over finite fields*, Designs, Codes and Cryptography, **89**(12), 2841-2855, 2021.

Further Improvements to the Chevalley-Warning Theorems

Rachel L. Petrik

Rose-Hulman Institute of Technology

(Joint work with David B. Leep)

Abstract

Let $\boldsymbol{f} = \{f_1, \ldots, f_r\}$ with $f_i \in \mathbb{F}_q[x_1, \ldots, x_n]$. Let $d_i = \deg(f_i)$ for $1 \leq i \leq r$. Define the degree of $\boldsymbol{f}$ to be $d := d_1 + \ldots + d_r$. Let $Z(\boldsymbol{f}, \mathbb{F}_q^n)$ be the set of zeros of $\boldsymbol{f}$ over $\mathbb{F}_q$ and let $N(\boldsymbol{f}, \mathbb{F}_q^n) = |Z(\boldsymbol{f}, \mathbb{F}_q^n)|$. The Chevalley–Warning Theorem states that if $N(\boldsymbol{f}, \mathbb{F}_q^n) \geq 1$, then $N(\boldsymbol{f}, \mathbb{F}_q^n) \geq q^{n-d}$. Examples exist showing this lower bound is optimal. In 2011, Heath-Brown showed that all examples meeting this lower bound have the property that the set of zeros forms an affine space of $\mathbb{F}_q^n$ and by excluding these examples improved the lower bound. In this talk, we improve Heath-Brown's lower bound. The main result is

Theorem 1. *Suppose that $n > d$, $Z(\boldsymbol{f}, \mathbb{F}_q^n)$ is non-empty, and $Z(\boldsymbol{f}, \mathbb{F}_q^n)$ is not an affine space of $\mathbb{F}_q^n$. Then the following statements hold.*

1. *For $q = 2$, $N(\boldsymbol{f}, \mathbb{F}_2^n) \geq 2^{n-d} + 2$.*
2. *For $q \geq 3$, $N(\boldsymbol{f}, \mathbb{F}_q^n) \geq 2q^{n-d}$.*
3. *For $q \geq 2$, $N(\boldsymbol{f}, \mathbb{F}_q^n) > \dfrac{q^{n+1-d} - 1}{q - 1} \cdot \dfrac{q}{n + 2 - d}$ provided that the polynomials $f_1, \ldots, f_r$ are homogeneous forms.*
4. *For $q \geq 3$, $N(\boldsymbol{f}, \mathbb{F}_q^n) \geq 2q^{n-d} + (q-2)q$ provided that the polynomials $f_1, \ldots, f_r$ are homogeneous forms.*

In addition, we provide results that show the bounds in Theorem 1 (1), (2), and (4) are optimal for particular values of q, d, and n. For example, our bound is optimal when $q = 2$ and $n \in \{d + 1, d + 2\}$.

Keywords: Chevalley-Warning Theorem, Finite Fields, Homogeneous Forms, Number of Zeros

On the preimage distribution of $x^2 + L(x)$ over $\mathbb{F}_{p^2}$

Li-An Chen
University of Delaware and Boise State University
(Joint work with Robert S. Coulter)

Abstract

Let f be a function on $\mathbb{F}_q$ and denote by $V(f)$ the cardinality of the image set of f. The function f is *planar* if for every nonzero $a \in \mathbb{F}_q$, the mapping $x \mapsto f(x+a) - f(x)$ is a bijection. An easy example is the function $x \mapsto x^2$, which is planar over any field of characteristic not 2.

Planar functions themselves cannot be bijections, and there are known lower and upper bounds established on $V(f)$ for planar functions. Since the planarity of a function (in the sense just defined) is invariant under the addition of linear transformations and constants, this means that for any planar function f we actually have

$$\frac{q+1}{2} \leq V(f+L) \leq q - \frac{2(q-1)}{1+\sqrt{4q-3}}$$

for any linear transformation L. The lower bound was established independently by Kyureghyan and Pott [3], and Qiu, Weng, Wang and Xiang [4], and later shown to be true for a much larger class of functions by Coulter and Matthews [1]. The upper bound was proved in [2] by Coulter and Senger. As an initial attempt to understand this phenomenon, we completely determine the preimage distribution of $x^2 + L(x)$ for linear transformations over fields of order p^2, where p is an odd prime.

Keywords: planar functions, linear transformations

References

[1] R.S. Coulter and R.W. Matthews, *On the number of distinct values of a class of functions over a finite field*, Finite Fields Appl. **17** (2011), 220–224.

[2] R.S. Coulter and S. Senger, *On the number of distinct values of a class of functions with finite domain*, Ann. Comb. **18** (2014), no. 2, 233–243.

[3] G.M. Kyureghyan and A. Pott, *Some theorems on planar mappings*, Arithmetic of Finite Fields: Proceedings of the 2nd International Workshop, WAIFI 2008 (J. von zur Gathen, J.L. Imanã, and C.K. Koç, eds.), Lecture Notes in Comput. Sci., vol. 5130, 2008, pp. 117–122.

[4] W. Qiu, G. Weng, Z. Wang, and Q. Xiang, *Pseudo-Paley graphs and skew Hadamard difference sets from presemifields*, Des. Codes Cryptogr. **44** (2007), 49–62.

Splitting subspaces of linear operators over finite fields

Divya Aggarwal
Indraprastha Institute of Information Technology Delhi
(Joint work with Samrith Ram)

Abstract

Let V be a vector space of dimension N over the finite field $\mathbb{F}_q$ and T be a linear operator on V. Given an integer m that divides N, an m-dimensional subspace W of V is T-splitting if $V = W \oplus TW \oplus \cdots \oplus T^{d-1}W$ where $d = N/m$. Let $\sigma(m, d; T)$ denote the number of m-dimensional T-splitting subspaces. Determining $\sigma(m, d; T)$ for an arbitrary operator T is an open problem. We prove that $\sigma(m, d; T)$ depends only on the similarity class type of T and give an explicit formula in the special case where T is cyclic and nilpotent. Denote by $\sigma_q(m, d; \tau)$ the number of m-dimensional splitting subspaces for a linear operator of similarity class type τ over an $\mathbb{F}_q$-vector space of dimension md. For fixed values of m, d and τ, we show that $\sigma_q(m, d; \tau)$ is a polynomial in q.

Keywords: splitting subspace, Krylov space, anti-invariant subspace, invariant subspace lattice, q-Vandermonde identity, finite field

References

[1] Lynne M. Butler. Subgroup lattices and symmetric functions. *Mem. Amer. Math. Soc.*, 112(539):vi+160, 1994.

[2] Eric Chen and Dennis Tseng. The splitting subspace conjecture. *Finite Fields Appl.*, 24:15–28, 2013.

[3] Sudhir R. Ghorpade and Samrith Ram. Enumeration of splitting subspaces over finite fields. In *Arithmetic, geometry, cryptography and coding theory*, volume 574 of *Contemp. Math.*, pages 49–58. Amer. Math. Soc., Providence, RI, 2012.

The complexity of elliptic normal bases

Mohamadou Sall
Université Cheikh Anta Diop of Dakar
(Joint work with D. Panario and Q. Wang, Carleton University)

Abstract

There are different ways of doing efficient finite field arithmetic using a normal basis; see [1, 3, 4]. The number of nonzero terms of the multiplication table of this basis, that is its complexity [1], plays a major role in some computations. The complexity $C_{\mathcal{N}}$ of a normal basis $\mathcal{N}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is bounded by

$$2n - 1 \leq C_{\mathcal{N}} \leq n^2 - n + 1.$$

The lower the complexity is, the more interesting these bases become. In this talk, we are interested in elliptic normal bases introduced by Couveignes and Lercier [2]. We give an upper bound on the complexity of those bases, and analyze the weight of some special vectors related to their multiplication table. This analysis leads to some perspectives on the construction of low complexity normal bases from elliptic periods.

Keywords: Normal basis, elliptic periods, complexity, weight.

References

[1] D. W. Ash, I. F. Blake and S. A. Vanstone. Low complexity normal bases. *Discrete Appl. Math.*, 25 (1989), no. 3, pp. 191-210.

[2] J.-M Couveignes and R. Lercier. Elliptic periods for finite fields. *Finite Fields Appl.*, 15 (2009), no. 1, pp. 1-22.

[3] T. Ezome and M. Sall, On finite field arithmetic in characteristic 2. *Finite Fields Appl.*, 68 (2020) 101739.

[4] S. Gao, J. von zur Gathen, D. Panario and V. Shoup. Algorithms for exponentiation in finite fields. *J. Symbolic Comput.*, (2000), pp. 879-889

On the non-existence of perfect codes in the NRT-metric

Claudio Qureshi
Universidad de la República, Uruguay
(Joint work with Viviana Gubitosi and Aldo Portela)

Abstract

In this work we consider codes in $\mathbb{F}_q^{s\times r}$ with packing radius R regarding the NRT-metric (i.e. when the underlying poset is a disjoint union of chains with the same length) and establish necessary condition on the parameters s, r and R for the existence of perfect codes. More explicitly, for $r, s \geq 2$ and $R \geq 1$ we prove that if there is a non-trivial perfect code then $(r+1)(R+1) \leq rs$. We also explore a connection to the knapsack problem and establish a correspondence between perfect codes with $r > R$ and those with $r = R$.

Keywords: Poset codes, perfect codes, MDS codes, NRT spaces

Sets of Latin cubes of order $q+1$ with high symmetry

Petr Lisoněk
Simon Fraser University, Burnaby, BC, Canada

Abstract

A Latin cube of order n is an $n \times n \times n$ array such that entries in each line of the cube (obtained by fixing any two of the three coordinates) form a permutation of the set $\{1, \ldots, n\}$. For a prime power q several direct constructions of (sets of) Latin cubes of order q are known. In this work we provide direct construction of a set of $q-2$ Latin cubes of order $q+1$, where q is a prime power; when q is an odd square we construct two such sets.

We provide two equivalent formulations of our construction: one of them uses formulas in closed form, whereas the other one uses the action of a sharply 3-transitive group of rational transformations (classified by Zassenhaus [2]) acting on the projective line $\mathrm{PG}(1,q) = \mathbb{F}_q \cup \{\infty\}$. The second formulation emphasizes the high degree of symmetry present in our construction.

We study some properties of our Latin cubes. For example, we study under what conditions will 2-dimensional slices of our cubes constitute a set of $q-2$ mutually nearly-orthogonal Latin squares of order $q+1$, studied previously by Droz [1]. We also study connections of our constructions with complete mappings on $\mathbb{F}_q$.

References

[1] D.R. Droz, *Orthogonal sets of Latin squares and class-r hypercubes generated by finite algebraic systems.* Ph.D. thesis, Pennsylvania State University, 2016.

[2] H. Zassenhaus, Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen. *Abh. Math. Sem. Univ. Hamburg* 11 (1935), 17–40.

Keywords: finite field; Latin cube; sharply transitive group

Polynomial over finite fields

Permutation and local permutation polynomials of maximum degree

Jaime Gutierrez
University of Cantabria, Spain
(Joint work with Jorge Jimenez Urroz)

Abstract

Let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q[x_1, \ldots, x_n]$ the ring of polynomials in n variables over $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is a *permutation polynomial* if the equation $f(x_1, \ldots, x_n) = a$ has q^{n-1} solutions in $\mathbb{F}_q^n$ for each $a \in \mathbb{F}_q$, and it is called a *local permutation polynomial* if for each i, $1 \leq i \leq n$, the polynomial $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n)$ is a permutation polynomial in $\mathbb{F}_q[x_i]$, for all choices of $(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \in \mathbb{F}_q^{n-1}$. On the other hand, it is well known that any map from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ can be uniquely represented as $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ such that $\deg_{x_i}(f) < q$ for all $i = 1, \ldots, n$, where $\deg_{x_i}(f)$ is the degree of f as a polynomial in the variable x_i (see [3]). In this paper we construct permutation polynomials of maximum degree $n(q-1)-1$ and local permutation polynomials of maximum degree $n(q-2)$ when $q > 3$ extending previous results ([1, 2]).

Keywords: Permutation multivariate polynomials, finite fields.

References

[1] W.S. Diestelkamp, S.G. Hartke, R.H. Kenney, On the degree of local permutation polynomials, J.Comb. Math. Comb. Comput. 50 (2004) 129–140.

[2] J. Gutierrez, J. J. Urroz, Local permutation polynomials and the action of e-Klenian groups, arXiv:2205.0015, 2022.

[3] R. Lidl, H. Niederreiter, Finite Fields, 2nd edn., Encyclopedia Math. Appl., vol.20, Cambridge University Press, Cambridge, 1997.

Permutation polynomials with fewer terms over finite fields

Sartaj Ul Hasan

Indian Institute of Technology Jammu

(Joint work with Kirpa Garg, Chunlei Li, Hridesh Kumar, Mohit Pal)

Abstract

Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements, where p is a prime and n is a positive integer. A polynomial $f(X) \in \mathbb{F}_q[X]$ is called a permutation polynomial if the induced map $c \mapsto f(c)$ is a bijection from $\mathbb{F}_q$ to itself. Permutation polynomials over finite fields are of great importance due to their applications in cryptography, coding theory, combinatorial designs, etc. From the implementation point of view, permutation polynomials, which have only a few terms, are quite significant. It may be noted that the classification of permutation polynomials derived from power maps is complete and well-known. However, the classification of permutation polynomials over finite fields that are binomials, trinomials, quadrinomials, and pentanomials is not yet completely understood and appears to be a challenging problem.

We construct some classes of permutation polynomials with fewer terms over the finite field $\mathbb{F}_{q^2}$ of the shape $X^r h(X^{q-1})$ arising from permutation rational functions that permute the projective line $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$, where r is a positive integer and $h(X) \in \mathbb{F}_{q^2}[X]$. In particular, we give a few classes of permutation binomials, permutation quadrinomials, and permutation pentanomials over the finite field $\mathbb{F}_{q^2}$.

Keywords: Finite fields, permutation polynomials

A General Construction of Permutation Polynomials of $\mathbb{F}_{q^2}$

Vincenzo Pallozzi Lavorante
University of South Florida
(Joint work with Xiang-dong Hou)

Abstract

Let r be a positive integer, $h(X) \in \mathbb{F}_{q^2}[X]$, and μ_{q+1} be the subgroup of order $q+1$ of $\mathbb{F}_{q^2}^*$. It is well known that $X^r h(X^{q-1})$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(r, q-1) = 1$ and $X^r h(X)^{q-1}$ permutes μ_{q+1}. There are many ad hoc constructions of permutation polynomials of $\mathbb{F}_{q^2}$ of this type such that $h(X)^{q-1}$ induces monomial functions on the cosets of a subgroup of μ_{q+1}. We give a general construction that can generate, through an algorithm, *all* permutation polynomials of $\mathbb{F}_{q^2}$ with this property, including many which are not known previously. The construction is illustrated explicitly for permutation binomials and trinomials.

Keywords: finite field, permutation polynomial, self-dual polynomial

Linearized polynomials: elimination and geometrization

Olivier Ruatta
XLIM-MATHIS UMR 7252 Université de Limoges - CNRS
(Joint work with Philippe Gaborit and Gaëtan Murat)

Abstract

Let q be a prime-power and $\mathbb{F}_{q^m}/\mathbb{F}_q$ be an extension fields of degree $m \in \mathbb{N}$ of the finite field $\mathbb{F}_q$ with q elements. We denote by $\mathbb{F}_{q^m}\langle X^q\rangle$ the $\mathbb{F}_q$-subvector space of $\mathbb{F}_q[X]$, $\left\{\sum_{i=0}^{d} a_i \cdot X^{q^i} \mid \mid d \in \mathbb{N}, a_i \in \mathbb{F}_{q^m} \text{ for } i \in \{0, \cdots, d\}\right\}$. Equipped with the composition $\circ$, the ring $(\mathbb{F}_{q^m}\langle X^q\rangle, +, \circ)$ is an non-commutative $\mathbb{F}_q$-algebra (since $X^q \circ (a \cdot X) = a^q \cdot X^q$ and $(a \cdot X) \circ X^q = a \cdot X^q$) and a special case of Öre algebra isomorphic to the skew polynomials $\mathbb{F}_{q^m}[X, \theta]$ where θ is the Frobenius of $\mathbb{F}_{q^m}/\mathbb{F}_q$. They are Euclidian rings, both on the right and the left. Still, if there is no notion of evaluation or geometry associated with skew polynomials, linearized polynomials are very related to the geometry of $\mathbb{F}_{q^m}$ as $\mathbb{F}_q$-vector space. We give a new resultant's formulation through the multiplication matrices setting generalizing companion matrices and many well-known results in the commutative case.

Keywords: Structure of finite fields, polynomials, algorithms and complexity, algebraic coding theory

References

[1] Oystein Ore. On a Special Class of Polynomials. Transactions of the American Mathematical Society, American Mathematical Society, 35(3):559–584, 1933.

[2] Olivier Ruatta. Polynômes : du discret (codes correcteurs et cryptographie basée sur les codes) et du continu (autour des trajectoires optimales). HDR 2022. https://hal.science/tel-04071349.

On Niho-type permutations

Faruk Göloğlu
Charles University Prague
(Joint work with Jiří Pavlů and Adolf Středa)

Abstract

Niho-type polynomials are polynomials of the form:

$$\sum_{s=0}^{q} A_s X^{s(q-1)+1} \in \mathbb{F}_{q^2}[X], \tag{1}$$

Many of these polynomials have cryptographically desirable properties (more specifically, low differential uniformity and high non-linearity) and one is naturally interested in determining necessary and sufficient conditions for them to be permutation polynomials.

We give a method to convert the problem of determining bijective properties of these polynomials to determining some permutation rational functions of $\mathbb{P}^1(\mathbb{F}_q)$. This method helps us prove several results that determine Niho-type permutation polynomials of many specific types.

This talk is based on the works [1, 2].

Keywords: Permutation Polynomials, Projective Polynomials

Acknowledgments: This research was supported by the GAUK Grant 397421.

References

[1] Faruk Göloğlu. Classification of fractional projective permutations over finite fields. *Finite Fields and Their Applications*, 81:102027, 2022.

[2] Faruk Göloğlu, Jiří Pavlů and Adolf Středa. On Niho-type permutation polynomials, (preprint), 2023.

A wreath product approach to study cycle structures of permutation polynomials

Qiang Wang
Carleton University
(Joint work with Alexander Bors)

Abstract

In this talk, we introduce a wreath product approach to study cycle structures of permutation polynomials. Through generalized cyclotomic mappings, permutation polynomials can be presented in wreath product forms and thus their cycle structures can be described using permutation group theory. Our approach is effective (i.e., we have algorithms for converting between the three forms: polynomial, cyclotomic, wreath product).

Keywords: cyclotomic mappings, permutation polynomials, cycle structure, wreath product

References

[1] Alexander Bors and Qiang Wang, Generalized cyclotomic mappings: switching between polynomial, cyclotomic, and wreath product form. Commun. Math. Res. 38, no. 2, 246-318, 2022.

[2] H. Fripertinger, Cycle indices of linear, affine, and projective groups, *Linear Algebra Appl.* **263**: 133–156, 1997.

[3] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

[4] W.-D. Wei and J.-Y. Xu, Cycle index of direct product of permutation groups and number of equivalence classes of subsets of Z_v, *Discrete Math.* **123**: 179–188, 1993.

Rédei permutations with the same cycle structure

Ariane Masuda
New York City College of Technology, CUNY
(Joint work with Juliane Capaverde and Virgínia Rodrigues)

Abstract

Permutation polynomials over finite fields have been extensively studied over the past few decades. Among the major challenges in this area are questions concerning their cycle structures, which capture relevant properties both theoretically and practically.

In this talk, we focus on a family of permutation polynomials known as the Rédei permutations. Although their cycle structures are known, there are other related questions that can be investigated. For example, when do two Rédei permutations have the same cycle structure? We provide a characterization of such pairs and present explicit families of Rédei permutations with the same cycle structure. We also discuss some results regarding Rédei permutations with a particularly simple cycle structure consisting of 1- and j-cycles only, where j is 4 or a prime number. The case where $j = 2$ is especially important in some applications. We completely describe Rédei involutions with a prescribed cycle structure and show that the only Rédei permutations with a unique cycle structure are the involutions.

Keywords: Permutation polynomial, involution, Rédei function, cycle structure.

References

[1] J. Capaverde, A. M. Masuda, and V. M. Rodrigues, Rédei permutations with cycles of the same length, *Des. Codes Cryptogr.*, **88** (2020), no. 12, 2561–2579.

[2] J. Capaverde, A. M. Masuda, and V. M. Rodrigues, Rédei permutations with the same cycle structure, *Finite Fields Appl.*, **81** (2022), 102046, 24 pp.

Smooth polynomials with several prescribed coefficients over finite fields

László Mérai
Austrian Academy of Sciences, Linz, Austria

Abstract

In 2015, Bourgain [1] investigated the distribution of primes with a positive proportion of preassigned bits. His method has been adapted in different settings, for example Ha [2] considered this question in the case of rational function fields over finite fields by studying the distribution of irreducible polynomials with preassigned coefficients.

In this talk, we explore this quesetion for smooth (or friable) polynomials [3]. We recall that a polynomial is m-smooth if all of its irreducible factors are of degree at most m.

Among others, we show that under some natural conditions, the number of m-smooth polynomials of degree n with r preassigned coefficients over the finite field of size q tends to

$$\rho(n/m)q^{n-r},$$

where ρ is the Dickman's ρ function.

Keywords: polynomials, irreducible polynomials, smooth polynomials

References

[1] J. Bourgain, Prescribing the binary digits of primes, II, Isr. J. Math. 206 (1) (2015) 165–182.

[2] J. Ha, Irreducible polynomials with several prescribed coefficients. Finite Fields Appl. 40 (2016), 10–25.

[3] L. Mérai, Smooth polynomials with several prescribed coefficients, preprint

Boolean and vectorial (cryptographic) functions
and related theory

Generalizations of almost perfect nonlinearity and sums of inverses over affine spaces of $\mathbb{F}_{2^n}$

Claude Carlet

University of Paris 8 and LAGA, France; University of Bergen, Norway

Abstract

We shall introduce two generalizations of almost perfect nonlinearity, that are related in a natural way to the (important) integral attack: given $2 \leq k \leq n$ and m, an (n, m)-function F is called kth-order-non-affine (resp. kth-order-sum-free) if, for every k-dimensional affine subspace A of $\mathbb{F}_2^n$, the restriction of F to A is not an affine function (resp. the sum of the values taken by this restriction is nonzero). APNness corresponds in both cases to $k = 2$.

We shall study the behavior of the multiplicative inverse function (important in cryptography) with respect to them. To this aim, we shall find rather simple expressions of sums of inverses over any affine subspace A of $\mathbb{F}_{2^n}$: one when 0 does not belong to A, and one when it does. The expression obtained in the former case shows that this sum never vanishes then (which is a remarkable property of the inverse function).

We shall show that, for every k not co-prime with n, the multiplicative inverse function sums to zero over at least one k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$. We shall study the behavior of the inverse function over direct sums of vector spaces and deduce that the property of the inverse function to sum to zero over at least one k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$ happens for k if and only if it happens for $n - k$, and derive several other results.

Keywords: Integral attack, Vectorial function, inverse function, affine space

References:

C. Carlet. Boolean Functions for Cryptography and Coding Theory. *Cambridge University Press*, 2021.

L. Knudsen and D. Wagner. Integral cryptanalysis. *Fast Software Encryption FSE 2002, Lecture Notes in Computer Science* vol. 2365, pp. 112127, 2002.

Iterated Power Functions: from Univariate Polynomial Representation to Multivariate Degree

Clémence Bouvier

Sorbonne Université, France & Inria, France

(Joint work with Anne Canteaut and Léo Perrin)

Abstract

Recently many symmetric primitives have been proposed for use in new contexts, such as Multi-Party Computation or Zero-Knowledge Proofs. Our aim is to investigate the security of MiMC [1] against *higher-order differential attacks* for which the complexity decreases with the *multivariate degree*. MiMC consists of many iterations of a simple round function: the addition of a key and round constants and a low-degree power permutation of $\mathbb{F}_{2^n}$, where $n \approx 129$.

In light of [2], we carefully study families of exponents appearing or not in the *univariate polynomial* representation of the block cipher. For instance, we show that for *Gold function* $x \mapsto x^d$, with $d = 2^j + 1$, the exponents are necessary equal to 0 or 1 modulo 2^j, leading to very sparse polynomials for large j. This observation then allows us to propose a more theoretical analysis of the multivariate degree. Overall, we provide a detailed comparison of different instances of MiMC and show that at least one fourth of the exponents never appear in the univariate representation of the cipher.

Keywords: cryptanalysis, univariate polynomial, algebraic degree, MiMC

References

[1] Albrecht, M.R., Grassi, L., Rechberger, C., Roy, A., & Tiessen, T. MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. In: Cheon, J.H., Takagi, T. (eds), *ASIACRYPT 2016, Part I*, LNCS, vol 10031, pp. 191–219. Springer, Heidelberg (2016).

[2] Bouvier, C., Canteaut, A., & Perrin, L. (2023). On the algebraic degree of iterated power functions. *Designs, Codes and Cryptography, 91(3)*, 997-1033.

On Vectorial Bent-Negabent Functions, Their Constructions and Bounds

Alexandr Polujan
Otto von Guericke University Magdeburg
(Joint work with Enes Pasalic, Sadmir Kudin and Alexander Pott)

Abstract

In this talk, we introduce the notion of vectorial bent-negabent functions, which generalizes the original concept of Boolean bent-negabent functions introduced originally in [1]. We show that in general for a vectorial bent-negabent function $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ we necessarily have that $k \leq m-1$. Using a set of linear complete mappings, we specify a class of vectorial bent-negabent functions of the maximal output dimension $m-1$. On the other hand, we propose several methods of specifying vector spaces of nonlinear complete mappings which then induce vectorial bent-negabent functions (whose dimension is not maximal) having a certain number of component functions outside the completed Maiorana-McFarland class. Finally, we derive an upper bound on the maximum number of bent-negabent components for mappings $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$, where $m \leq k \leq 2m$, and identify some families of these functions reaching this upper bound. This talk is based on the paper [2].

References

[1] M. G. Parker and A. Pott. "On Boolean Functions Which Are Bent and Negabent". In: Golomb, S.W., Gong, G., Helleseth, T., Song, HY. (eds) Sequences, Subsequences, and Consequences. LNCS, vol 4893. Springer, Berlin, Heidelberg, 2007.

[2] E. Pasalic, S. Kudin, A. Polujan and A. Pott, "Vectorial Bent-Negabent Functions—Their Constructions and Bounds". In IEEE Transactions on Information Theory, vol. 69, no. 4, pp. 2702-2712, April 2023.

Keywords: Bent-negabent function, maximum number of bent components, Maiorana-McFarland class, permutation polynomial, linear translator, complete mapping.

On Carlitz-like Decompositions of Vectorial Boolean Functions

Samuele Andreoli[1]

[1]University of Bergen, Norway; [2]KU Leuven, Belgium;

(Joint work with Enrico Piccione[1], Lilya Budaghyan[1], and Svetla Nikova[1,2])

Abstract

The algebraic degree of a vectorial Boolean function is one of the main parameters driving the cost of hardware implementations. Thus, finding decompositions of functions in $\mathbb{F}_{2^n}$ into sequences of functions of lower algebraic degrees has been explored as a way to reduce the cost of implementations. In [1], the authors approach the problem searching for decompositions of the inverse map into quadratic and linear power permutations for some small n, and use the Carlitz theorem to extend the result all permutations. Another approach to decomposition can be found in [2], focusing on decompositions into power permutations and linear polynomials $ax+b$. We use a number theoretic approach to the problem of finding decompositions of the first form, proving the existence of decompositions using quadratic and linear power permutations for all permutations, when 2^n-1 is a Mersenne prime, a family of values of n that is conjectured to be infinite. Furthermore, we use the Zolotoroff-Frobenius Lemma to characterize the parity of a power permutation x^k using its Jacobi Symbol $\left(\frac{k}{2^n-1}\right)$. We use this to prove that if $4 \nmid n$, then any permutation admits a decomposition into quadratic power functions and linear polynomials $ax+b$. and we find sufficient conditions on n for the existence of decompositions of any permutation into cubic and linear polynomials $ax+b$.

Keywords: power function, vectorial Boolean function, decomposition, permutation

References

[1] S. Nikova and V. Nikov and V. Rijmen, *Decomposition of permutations in a finite field*, Cryptogr. Commun. **11** (2019).

[2] P. Çomak and F. Özbudak, *On the Parity of Power Permutations*, IEEE Access **9** (2021).

Reducing and estimating the search space for the QAM method through linear equivalences

Nikolay Kaleyski
University of Bergen, Norway
(Joint work with Simon Berg)

Abstract

Almost perfect nonlinear (APN) functions are of interest thanks to connections to cryptography, algebra, combinatorics, etc. Many mathematical and computational methods have been developed to find new examples of such functions. The authors of [1] show how a quadratic $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be represented as a matrix $M_F \in \mathbb{F}_{2^n}^{n \times n}$; which M_F correspond to APN functions F; and how this can be used to search for new APN functions. This produced thousands of new APN functions over $\mathbb{F}_{2^8}$. In [2], additional restrictions on M_F were obtained when F has coefficients in $\mathbb{F}_2$, leading to a classification of all quadratic APN functions over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$ for $n \leq 9$.

We discuss conditions for $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ for coefficients in a subfield $\mathbb{F}_{2^m}$ for $m \mid n$ and adapt the search accordingly. We describe pre-computations based on the notion of linear equivalence allowing the search space to be significantly reduced, to the point that we are able to classify all quadratic APN functions over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^2}$. They fall into 27 CCZ-classes, one of which appears to be new. We describe a procedure for estimating the complexity of the search for any m and n, and discuss other promising choices of m and n.

References

[1] Yu Y, Wang M, Li Y. A matrix approach for constructing quadratic APN functions. Designs, codes and cryptography. 2014 Nov;73:587-600.

[2] Yu Y, Kaleyski N, Budaghyan L, Li Y. Classification of quadratic APN functions with coefficients in F2 for dimensions up to 9. Finite Fields and Their Applications. 2020 Dec 1;68:101733.

Keywords: APN function, QAM, differential uniformity

Restricting vectorial functions to affine spaces and deducing infinite families of 4-uniform permutations, in relation to the strong D-property

Enrico Piccione[1]

[1]University of Bergen, [2]University of Paris 8

(Joint work with Claude Carlet[1,2])

Abstract

We study those (N, M)-functions $\mathcal{F}$ which map at least one n-dimensional affine subspace $A \subseteq \mathbb{F}_2^N$ to (a subset of) an m-dimensional affine subspace $A' \subseteq \mathbb{F}_2^N$. This leads to (n, m)-functions $\mathcal{F}_A$. We study the cryptographic properties of $\mathcal{F}_A$ by means of the ones of $\mathcal{F}$. We then focus on the case $M = N = m + 1 = n + 1$, resulting in $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ (or $\psi(\mathcal{G}(x)) + x$) where ψ is a linear function with a kernel of dimension 1. We are interested in the case where $\mathcal{G}$ is *almost perfect nonlinear (APN)*. We say that $\mathcal{G}$ has the *strong D-property* if $\mathcal{G}_A$ has the *D-property* [1] for all affine hyperplanes A whose contrary allows the APNness of $\mathcal{F}_A$. We study the strong D-property for crooked functions and we prove that the Gold APN function has the strong D-property in large dimension. Then we give a partial result on the Dobbertin APN function. We then consider the case where $\mathcal{F}_A$ and $\mathcal{G}$ are permutations. We prove that some of the known families [2, 3] of 4-uniform permutations corresponding to this framework are not APN in even dimension. Then we present our own construction of 4-uniform complete permutations.

Keywords: vBf, APN, complete permutation, restriction

References

[1] H. Taniguchi, *D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$*, Cryptography and Communications (2023).

[2] Y. Li and M. Wang, *Constructing differentially 4-uniform permutations over GF(2^{2m}) from quadratic APN permutations over GF(2^{2m+1})*, Designs, codes and cryptography (2014).

[3] C. Carlet, *On known and new differentially uniform functions*, ACISP, 2011.

On the Functions Which are CCZ-equivalent but not EA-equivalent to Quadratic Functions

Soonhak Kwon

Dept. of Mathematics, Sungkyunkwan University, Suwon, Korea

(Joint work with Jaeseong Jeong and Namhun Koo)

Abstract

For every quadratic (n, n)-function F, we present functions which are CCZ-equivalent to F, and if suitable conditions are satisfied, the constructed functions are shown to be EA-inequivalent to F. As a consequence, for every quadratic function F on $\mathbb{F}_{2^n}$ $(n \geq 4)$ with nonlinearity > 0 and differential uniformity $\leq 2^{n-3}$, we explicitly construct functions which are CCZ-equivalent but EA-inequivalent to F. In particular, for every APN quadratic function F in Table 11.4 (p. 407) of [3], we have explicit examples of cubic APN functions which are CCZ equivalent but EA-inequivalent to F.

Keywords: EA-equivalence, CCZ-equivalence, differential uniformity, linear structure

References

[1] L. Budaghyan, C. Carlet, and A. Pott, *New classes of almost bent and almost perfect nonlinear functions*, IEEE Trans. Inform. Theory, Vol. 52, issue 3, pp. 1141-1152, 2006.

[2] A. Canteaut and L. Perrin, *On CCZ-equivalence, extended-affine equivalence, and function twisting*, Finite Fields Appl., Vol. 56, pp. 209-246, 2019.

[3] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, Cambridge, 2020.

[4] P. Charpin and G. M. Kyureghyan, *On a class of permutation polynomials over* $\mathbb{F}_{2^n}$, SETA 2008, LNCS 5203, pp. 368-376, 2008.

On a family of scattered binomials over finite fields

Giovanni Zini
University of Modena and Reggio Emilia
(Joint work with Olga Polverino, Ferdinando Zullo, Marco Timpanella)

Abstract

An $\mathbb{F}_q$-linearized polynomial $f(x)$ over a finite field $\mathbb{F}_{q^n}$ is said to be scattered when two pairs $(y, f(y)), (z, f(z)) \in \mathbb{F}_{q^n}^2$ are $\mathbb{F}_{q^n}$-proportional only if they are $\mathbb{F}_q$-proportional. Scattered polynomials, and more generally scattered $\mathbb{F}_q$-subspaces of an $\mathbb{F}_{q^n}$-vector space, have a number of connections within mathematics and applications in information theory; see [S]. In this talk we study the scattered property for $\mathbb{F}_q$-linearized binomials $(x) = x^{q^s} + \delta x^{q^{s+n/2}} \in \mathbb{F}_{q^n}[x]$, where n is even and s is coprime with $n/2$. To this aim, we investigate the rational points of suitable algebraic varieties attached to $f(x)$.

In recent years, several generalizations of scattered polynomials have been investigated in the literature through an algebraic-geometric approach, usually through the manipulation of certain curves or hypersurfaces over finite fields; see for instance [BMNV]. In this talk we make also use of higher dimensional and codimensional varieties. This is based on joint works with Olga Polverino and Ferdinando Zullo [PZZ], and with Marco Timpanella [TZ].

References

[BMNV] D. Bartoli, G. Marino, A. Neri and L. Vicino: Exceptional scattered sequences, arXiv:2211.11477.

[S] J. Sheekey: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* 10(3), 475–488 (2016).

[PZZ] O. Polverino, F. Zullo and G. Zini: On certain linearized polynomials with high degree and kernel of small dimension, *J. Pure Appl. Algebra* 225(2), 106491 (2021).

[TZ] M. Timpanella and G. Zini: On a family of linear MRD codes with parameters $[8 \times 8, 16, 7]_q$, *Des. Codes Cryptogr.* (2023).

Keywords: linearized polinomial, scattered polynomial, algebraic variety

Value distributions of perfect nonlinear functions

Lukas Kölsch
University of South Florida
(Joint work with Alexandr Polujan)

Abstract

Perfect nonlinear functions (also called bent functions) are in the most general sense mappings between two finite abelian groups that are "as far apart" from homomorphisms as possible. They have well known connections to cryptography, coding theory, and design theory. In this talk, I shall discuss the value distributions of bent functions, i.e., their image and preimage sizes. It turns out that very strong conditions on the sizes of the preimage sets can be derived. Moreover, many well known constructions of perfect nonlinear functions have in some sense an extremal value distribution. I will also present some complete classification results for value distributions of perfect nonlinear functions between specific groups, connections between value distributions and other properties of perfect nonlinear functions, and more specific results on special perfect nonlinear functions like planar functions.

The talk is based on the preprint [1].

Keywords: Perfect nonlinear functions, bent functions, value distributions, planar functions

References

[1] Kölsch, L., Polujan, A.: Value distributions of perfect nonlinear functions. https://arxiv.org/abs/2302.03121.

APN Functions over Finite Fields of Odd Characteristic

Mohit Pal

University of Bergen

(Joint work with Lilya Budaghyan)

Abstract

Recently, many cryptographic primitives such as homomorphic encryption (HE), multi-party computation (MPC) and zero-knowledge (ZK) protocols have been proposed in the literature which operate on prime field $\mathbb{F}_p$ for some large prime p. Primitives that are designed using such operations only are called *arithmetization-friendly* primitives. As the concept of arithmetization-friendly primitive is new, a rigorous cryptanalysis of such primitives is yet to be done. Therefore, it is important to understand the behaviour of some basic cryptanalysis techniques, such as differential cryptanalysis [**?**], when they are applied to arithmetization-friendly designs. The minimum differential uniformity that a permutation function can have over finite fields of odd characteristic is 2 and are called almost perfect nonlinear (APN) functions.

In this talk, we give a brief survey of known classes of APN functions over finite fields of odd characteristic. Since APN functions over prime fields are of particular interest, we investigate APN permutations in the CCZ-class of known classes of APN power maps. More precisely, we show that there is no APN permutation in the CCZ-class of known classes of APN power maps when $p \equiv 1 \pmod 3$. When $p \equiv 2 \pmod 3$ then the only APN permutations we obtain by applying CCZ-equivalence on the known classes of APN power maps, are affine equivalent to either x^3 or x^{p-2}; or to their compositional inverses.
Keywords: Finite fields, Differential uniformity, CCZ-equivalence

References

[1] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems.* J. Cryptol. 4 (1991) 3–72.

On the exceptionality of rational APN functions

Francesco Ghiandoni
University of Florence/University of Perugia/INdAM
(Joint work with Daniele Bartoli, Giuliana Fatabbi)

Abstract

Almost perfect nonlinear (APN) functions, and the exceptional ones in particular, have been also investigated in connection with algebraic varieties over finite fields. In this direction, non-existence results were obtained by means of estimates on the number of $\mathbb{F}_q$-rational points of such varieties, as Hasse-Weil or Lang-Weil bounds, which can be applied only if the degree of the polynomial under investigation is small enough. On the one hand, using such a machinery non-existence results were obtained only in small-degree regime or of so-called exceptional APN functions. On the other hand, not all the examples of APN functions are described in the literature by polynomials. In fact, the inverse map $x \mapsto x^{-1}$ is known to be APN on $\mathbb{F}_{2^n}$ with n odd, and thus it is also exceptional. Such a map, seen as a polynomial function, has large degree (the function coincides with x^{2^n-2}) and thus the previous machinery does not apply. Inspired by this example, we start the investigation of APN functions which can be represented as rational functions and we provide non-existence results exploiting the connection between these functions and specific algebraic varieties over finite fields. This approach allows to classify families of functions when previous approaches cannot be applied.

Keywords: APN functions, algebraic varieties, finite fields

References

[1] Y. Aubry, G. McGuire and F. Rodier. A few more functions that are not APN infinitely often, finite fields theory and applications. *Contemporary Math.*, 518:23–31, 2010.

[2] M. Delgado. The state of the art on the conjecture of exceptional APN functions. *Note Mat.*, 37(1):41–51, 2017.

On Dillon's property for vectorial Boolean functions

Irene Villa
University of Trento
(Joint work with Matteo Abbondati and Marco Calderini)

Abstract

Dillon observed that an APN function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $n > 2$ necessarily satisfies the condition $\{F(x)+F(y)+F(z)+F(x+y+z) : x, y, z \in \mathbb{F}_2^n\} = \mathbb{F}_2^n$. Recently, Taniguchi in [1] generalized this condition to functions defined from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, with $m > n$, calling it the D-property.

We further study the D-property for (n, m)-functions with $m \geq n$. We give some combinatorial bounds on the dimensions for the existence of such functions, that is, $n \leq m < 3n - 4$ and for the quadratic case $m < 2n - 2$. Then, we characterize the D-property in terms of the Walsh transform and for quadratic functions we give a characterization in terms of the ANF.

For a quadratic function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we simplify the verification of the D-property as follows: F satisfies the D-property if and only if $\{F(0) + F(\alpha) + F(\beta) + F(\alpha + \beta) : \alpha \in K, \beta \in \mathbb{F}_2^n\} = \mathbb{F}_2^m$, $K \subseteq \mathbb{F}_2^n$ a vector subspace of dimension $n-1$ over $\mathbb{F}_2$. This result permits to extend some of the APN families provided in [1]: over $\mathbb{F}_{2^{n+1}}$ the Gold APN function x^{2^i+1} (i coprime with $n+1$) and the APN function $x^3 + Tr(x^9)$ restricted to the trace-zero elements satisfy the D-property for every dimension $n + 1 = 17s, 19s, 21s, 23s, 25s$, $s > 0$.

We further focus on the class of the plateaued functions, providing conditions for the D-property. Moreover, we deduce that for plateaued functions the D-property is CCZ-invariant. This generalizes the result obtained by Taniguchi for the class of quadratic functions.

Keywords: Vectorial Boolean functions; D-property; APN functions

References

[1] Taniguchi, H. (2023). D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$. Cryptography and Communications.

Generalized spread bent partitions and LP-packings

Tekgül Kalaycı
Sabanci University, Istanbul
(Joint work with Sezel Alkan, Nurdagül Anbar and Wilfried Meidl)

Abstract

Recently, the concept of bent partitions is introduced by Anbar and Meidl, 2022, which are partitions of elementary abelian groups having similar properties as spreads. In particular, generalized semifield spreads are bent partitions obtained from (pre)semifields with a certain additional property, which enable us to construct p-ary bent functions, vectorial bent functions and bent functions into finite abelian groups in general.

Also recently, the concept of Latin square partial difference set packings (LP-packings) of finite abelian groups is introduced by Jedwab and Li, 2022. We point out that LP-packings induce bent partitions of finite abelian groups, and generalized semifield spreads form LP-packings of elementary abelian groups. We employ ternary bent functions in order to obtain examples of bent partitions, which do not form LP-packings. Moreover, we extend a recursive construction of LP-packings of non-elementary abelian groups from spreads to a recursive construction of LP-packings of finite abelian groups from some generalized spread bent partitions. This potentially yields bent partitions other than generalized semifield spreads.

Keywords: Bent function, bent partition, LP-packing, partial difference set, semifield, spread

References

[1] S. Alkan, N. Anbar, T. Kalaycı, W. Meidl: Bent partitions and LP-packings, preprint.

[2] N. Anbar, T. Kalaycı, W. Meidl: On generalized spread bent partitions, Cryptography and Communications, to appear.

Pseudo-Chebyshev functions over finite fields

Juliano B. Lima

Federal University of Pernambuco (UFPE), Brazil

(Joint work with Daniel Panario – Carleton University and José R. de Oliveira Neto – UFPE)

Abstract

In this talk, we introduce the notion of pseudo-Chebyshev functions over finite fields. In brief, such functions correspond to a generalization of the n-th Chebyshev polynomial, where n is not restricted to integer values, but can take on any rational value. Our approach is mainly based on concepts of trigonometry over finite fields, which have previously been used to describe the referred ordinary polynomials. To be more specific, the n-th pseudo-Chebyshev function over $\mathbb{F}_q$ is defined as

$$P_n(x)_{\zeta,a,b} = \cos_\zeta\left(\left(n+\frac{a}{b}\right)\arccos_\zeta(x)\right),$$

where ζ is an element of multiplicative order denoted by $\mathrm{ord}(\zeta)$, lying in a quadratic extension of $\mathbb{F}_q$ and satisfying some other particular requirements; $n, a, b \in \mathbb{N}$, $b \neq 0$; $\cos_\zeta(y) = 2^{-1}(\zeta^y + \zeta^{-y})$, $y \in \mathbb{Z}_{\mathrm{ord}(\zeta)}$, denotes the finite field cosine computed with respect to ζ, and; $\arccos_\zeta(y)$ denotes the inverse finite field cosine. Besides defining the pseudo-Chebyshev functions, we derive several of their properties and explain how they can be used to construct permutations. We briefly comment on potential applications of these functions.

Keywords: Chebyshev polynomials, Pseudo-Chebyshev functions, trigonometry over finite fields, permutations

Differential analysis of some modified functions: Refined measures

Alev Topuzoğlu
Sabanci University, Istanbul
(Joint work with Nurdagül Anbar and Tekgül Kalaycı)

Abstract

We use so-called *difference squares* to analyze the differential behavior of functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, in particular those obtained by modifying the inverse function.

We introduce a new concept, the *APN-defect*, which can be thought of as measuring the distance of a given function F to the set of almost perfect nonlinear (APN) functions, i.e., assessing how far F is from being APN. We describe the relations between the APN-defect and other recent concepts of similar nature, see for instance [1, 2]. We give upper and lower bounds for the values of APN-defect as well as its exact values for several classes of functions of interest, including Dembowski-Ostrom polynomials. We also determine the APN-defect of some modifications of the inverse function.

Keywords: APN-defect, difference squares, vanishing flats, (p_a)-property, partially APN functions, modifications of the inverse function

References

[1] Charpin, P., Kyureghyan, G.M.: On sets determining the differential spectrum of mappings. Internat. J. Inf. Coding Theory **4**(2-3), 170–184 (2017).

[2] Li, S., Meidl, W., Polujan, A., Pott, A., Riera, C., Stănică, P.: Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application. IEEE Trans. Inform. Theory **66**, no. 11, 7101–7112 (2020).

Specific Linear codes

Classification of RM(6,8)/RM(4,8)

Philippe Langevin
Imath, Université de Toulon
(Joint work with Valérie Gillot)

Abstract

In our previous work [2], we determined the covering radius of the Reed-Muller code $RM(4,8)$. The numerical result was obtained through several steps. Firstly, we classified the Reed-Muller space $RM(6,8)/RM(4,8)$, denoted as $B(5,6,8)$, and obtained a set of representatives. Details of the results used in obtaining this set are presented in this paper, and the 20748 functions corresponding to this classification are available on the project page [1]. In the second step, we estimated the nonlinearity of the representatives using probabilistic algorithms presented at the ALCOCRYPT conference in February 2023.In this talk, we will focus on the algorithms used to classify $B(5,6,8)$. To this end, we propose new theoretical results that can be used for the classification of quotient spaces of the form $RM(t,m)/RM(t-2,m)$ in general.

Keywords: Affine general linear group, Boolean function, Reed-Müller codes

References

[1] Valérie Gillot and Philippe Langevin. Classification of $B(5,6,8)$. `http://langevin.univ-tln.fr/project/agl8/aglclass.html`, 2023.

[2] Valérie Gillot and Philippe Langevin. Covering radius of $RM(4,8)$. `https://arxiv.org/pdf/2305.03493v1.pdf`, 2023.

*This work is partially supported by the French Agence Nationale de la Recherche through the SWAP project under Contract ANR-21-CE39-0012

The weight spectrum of certain Reed-Muller codes

Patrick Solé
Institut de Mathématiques de Marseille
(Joint work with Claude Carlet)

Abstract

We determine the weight spectrum (a.k.a. weight set) of three infinite families of Reed-Muller codes: $RM(m-3,m)$ for $m \geq 6$, $RM(m-4,m)$ for $m \geq 8$, and $RM(m-5,m)$ for $m \geq 9$. The technique used is induction on m based on Corollary 2 of (Shi et al. 2019).

Keywords: Reed Muller codes, Boolean functions, weight spectrum

Reed-Muller Codes and Minimal Free Resolutions

Rati Ludhani
Indian Institute of Technology Bombay
(Joint work with Sudhir R. Ghorpade)

Abstract

Johnsen and Verdure [2] associated to any linear code C, a set of invariants called the *Betti numbers* of C and showed that these determine the generalized Hamming weights of C. Computation of these Betti numbers becomes tractable if we know that the minimal free resolutions of certain Stanley-Reisner rings associated to C are *pure*. For instance, this is always the case for Reed-Solomon codes, and more generally, MDS codes.

We consider the case of (generalized) Reed-Muller codes and also projective Reed-Muller codes, which were introduced by Lachaud [3] and Sørensen [4]. For these families of codes, we give a complete characterization of the purity of minimal free resolutions of the corresponding Stanley-Reisner rings. This extends the results of Ghorpade and Singh [1] on certain Reed-Muller codes.

Keywords: Generalized Hamming weight, Betti number, Reed-Muller code.

References

[1] S. R. Ghorpade and P. Singh, Pure Resolutions, linear codes, and Betti numbers. *J. Pure Appl. Algebra* **224** (2020), no. 10, Art. 106385, 22 pp.

[2] T. Johnsen and H. Verdure, Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids, *Appl. Algebra Engrg. Comm. Comput.* **24** (2013), 73–93.

[3] G. Lachaud, Projective Reed-Muller codes, in: *Coding theory and Applications* (Cachan, France, 1986), Springer, Berlin, 1988, pp. 125–129.

[4] A. B. Sørensen, Projective Reed-Muller codes, *IEEE Trans. Inform. Theory* **37** (1991), 1567–1576.

Quasi-cyclic codes of index 2

K. Abdukhalikov
UAE University

Abstract

Quasi-cyclic codes are asymptotically good codes [4]. We study quasi-cyclic codes of index 2 over finite fields. We give a classification of such codes and investigate their duals with respect to Euclidean, symplectic and Hermitian inner products. We describe self-orthogonal and dual-containing codes. Lower bounds for minimum distances of quasi-cyclic codes are given. Quasi-cyclic code of index 2 is generated by at most two elements. We describe conditions when such code (or its dual) is generated by one element. Some special classes of quasi-cyclic codes of index 2 were studied in [1, 2, 3].

Keywords: Quasi-cyclic codes, dual codes, lower bounds, quantum error-correcting codes

References

[1] K. Abdukhalikov, T. Bag, D. Panario, One-generator quasi-cyclic codes and their dual codes. Discrete Math. 346 (2023), no. 6, Paper No. 113369

[2] C. Galindo, F. Hernando and R. Matsumoto, Quasi-cyclic constructions of quantum codes, Finite Fields their Appl. 52 (2018), 261–280.

[3] C. Guan, R. Li, L. Lu, L. Lu, Y. Yao, New binary quantum codes constructed from quasi-cyclic codes. Int J. Theor. Phys. 61, 172 (2022).

[4] T. Kasami, A Gilbert-Varshamov bound for quasi-cyclic codes of rate $\frac{1}{2}$, IEEE Trans. Inf. Theory 20, (2018), 679.

On the Classification of Distinct Maximal Flag Codes of a Prescribed Type and Related Results

Ferruh Özbudak
Sabanci University, Istanbul, Türkiye
(Joint work with Zeynelabidin Karakaş)

Abstract

Flag codes have applications in network coding and their algebraic and combinatorial structures have been an active research area in recent years. Classification of maximal flag codes of a given type and distance over a given ambient space is a very difficult problem. In this paper, we completely solve this problem for small parameters using also MAGMA. In our classification we also provide new maximal flag codes for some small parameters explicitly. We study a connection of the number of maximal flag codes for some types with the permanents of the projective plane of order q and we obtain some new results.

Keywords: Finite Fields , Coding Theory, Flag Codes, Permanents.

References

[1] Liebhold, D., Nebe, G. and Vazquez-Castro, A., Network coding with flags. Designs, Codes and Cryptography, 86(2), 269-284 (2018).

[2] Alonso-González, C., Miguel Ángel Navarro, P. and Xaro Soler, E., Flag codes from planar spreads in network coding. Finite Fields and Their Applications, 68, Article N. 101745 (2020).

[3] Kurz, S., Bounds for flag codes. Designs, Codes and Cryptography, 89(12), 2759-2785 (2021).

[4] Alonso-González, C., Miguel Ángel Navarro, P. and Xaro Soler, E., Optimum Distance Flag Codes from Spreads via Perfect Matchings in Graphs, Journal of Algebraic Combinatorics 54 1279-1297 (2021).

A new invariant for cyclic orbit flag codes

Clementa Alonso-González
University of Alicante (Spain)
(Joint work with Miguel Ángel Navarro-Pérez)

Abstract

In the context of network coding, fixed a prime power q, a *constant type flag code* is a set of nested sequences of $\mathbb{F}_q$-subspaces of the vector space $\mathbb{F}_q^n$ (flags), all of them sharing their *type*, that is, their increasing sequence of dimensions. A remarkable family of this kind of codes are the *cyclic orbit flag codes*, which are orbits under the action the cyclic group $\mathbb{F}_{q^n}^*$ over a flag. Among the parameters of this family, we highlight its *best friend*, which is the largest field over which all the subspaces in the generating flag are vector spaces. This invariant permits to compute the cardinality of the code and estimate its minimum distance. Nevertheless, the information provided by the best friend is not complete in many cases since it can be deployed in different ways. In this talk, we present a new invariant, the *best friend vector*, that captures the specific way the best friend can be unfolded. The strong underlying interaction between this invariant and other parameters such as the cardinality, the flag distance, or the type vector will be also exhibited.

Keywords: Vector spaces over finite fields, best friend of a vector space, flag codes.

References

[1] C. Alonso-González and M.A. Navarro-Pérez, *A New Invariant for Cyclic Orbit Flag Codes*, https://arxiv.org/abs/2304.12991 (preprint).

[2] C. Alonso-González and M.A. Navarro-Pérez, *Cyclic Orbit Flag Codes*, Designs, Codes and Cryptography, Vol. 89 (2021), 2331–2356.

[3] H. Gluesing-Luerssen, K. Morrison and C. Troha, *Cyclic Orbit Codes and Stabilizer Subfields*, Advances in Mathematics of Communications, 9 (2015), 2, 177-197.

Certain linear codes using simplicial complexes

Vidya Sagar
Department of Mathematics,
Indian Institute of Technology Delhi,
Hauz Khas, New Delhi-110016, India.
(Joint work with Ritumoni Sarma)

Abstract

We construct a subset D of $\mathbb{F}_{2^n}^m$ by using simplicial complexes and D, in turn, defines the linear code C_D over $\mathbb{F}_{2^n}$ that consists of $(v \cdot d)_{d \in D}$ for $v \in \mathbb{F}_{2^n}^m$. Here we deal with the case $n = 3$, that is, when C_D is an octanary code. We establish a relation between C_D and its binary subfield code $C_D^{(2)}$ with the help of generator matrix. For a given length and dimension, a code is called distance optimal if it has the highest possible distance. With respect to the Griesmer bound, a few infinite families of distance optimal codes are obtained, and sufficient conditions for certain linear codes to be minimal are established. For various choices of D, we establish sufficient conditions for $C_D^{(2)}$ to be self-orthogonal, where $C_D^{(2)}$ is a binary subfield code corresponding to the linear code C_D. This talk is partially based on our recent article [2]. We shall also present a few new results.

Keywords: octanary linear code, subfield code, Griesmer code, minimal code, self-orthogonality, simplicial complex

References

[1] Huffman W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge, (2003)

[2] Sagar, V., Sarma, R.: Octanary linear codes using simplicial complexes. Cryptogr. Commun. (2022), https://doi.org/10.1007/s12095-022-00617-z

Some results on Galois LCD codes over a finite non chain ring

Astha Agrawal
Indian Institute of Technology, Delhi
(Joint work with Gyanendra K. Verma and R. K. Sharma)

Abstract

In [1], Wu and Shi examined l-Galois LCD codes over the finite chain ring. We extend the findings in this work to the finite non-chain ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u$, $v^2 = v$ and $uv = vu$. We define a relationship between the l-Galois dual of linear codes over R and the l-Galois dual of its component codes over $\mathbb{F}_q$. Moreover, using linear codes over R, we construct Euclidean LCD and l-Galois LCD codes. This consequently leads us to prove that any linear code over R is equivalent to Euclidean ($q > 3$) and l-Galois LCD ($0 < l < e$, and $p^{e-l} + 1 | p^e - 1$) code over R.

Keywords: Linear codes, Euclidean LCD code, l-Galois LCD code, Gray map

References

[1] Rongsheng Wu and Minjia Shi, A note on k-Galois LCD codes over the ring Fq + uFq, *Bull. Aust. Math. Soc.*, 104(1):154–161, 2021

Non-existence of LCD MDS group codes over finite group algebra

Satya Bagchi
Department of Mathematics, NIT Durgapur, Burdwan, W.B, Pin-713209, India
(Joint work with Ankan Shaw)

Abstract

The purpose of the work is to characterize the support set of a generator of the LCD group code and to exhibit its importance in studying the existence and non-existence of LCD MDS group codes under specific scenarios. *Linear complementary dual* LCD code is a special class of code that has trivial intersection with their dual. We characterize the support of a generator of the LCD group code with a focus on the algebraic structure of the underlying group. We also explore the dimension and distance of the LCD group code under certain restrictions. The non-existence of LCD MDS group code is discussed under specific circumstances. Specifically, it is shown that there does not exist any LCD MDS group code in binary Dihedral group algebra. The utility of the results is exhibited through relevant examples.

Keywords: Group code; LCD code; MDS code

The search for the right support: better bounds for the Lee metric

Violetta Weger
Technical University of Munich
(Joint work with Jessica Bariffi)

Abstract

One of the most important bounds in coding theory is the Singleton bound, which for the classical case of the Hamming metric is derived via a simple puncturing argument. Codes which attain the Hamming-metric Singleton bound are called Maximum Distance Separable (MDS) codes and it is well known that for large finite fields MDS codes are dense.

This is fundamentally different to the current situation in the Lee metric, where the same puncturing argument leads to Shiromoto's bound [1]. This bound, however, can only be achieved by one non-trivial linear code living in one ambient space. This implies that optimal codes with respect to Shiromoto's bound are sparse, whether we let the length of the code or the size of the underlying ring grow [2]. The puncturing argument is thus not suitable for the Lee metric and an other technique is required. For this, we will turn to generalized weights. In order to define generalized Lee weights, we encounter several possibilities and discuss which definition of support will lead to good properties. This allows us to present a new Lee-metric Singleton bound, for which several optimal codes exist.

Keywords: Coding Theory, Generalized Weights, Singleton Bound, Lee Metric

References

[1] K. Shiromoto. Singleton bounds for codes over finite rings, In *Journal of Algebraic Combinatorics*, v.21, pp. 95–99, 2000.

[2] E. Byrne, V. Weger. Bounds in the Lee metric and optimal codes. In *Finite Fields and Their Applications*, v. 87, 2023.

Coding theory with the rank metric

Subspace designs and optimal codes in the sum-rank metric

Paolo Santonastaso

University of Campania "Luigi Vanvitelli"

(Joint work with Alessandro Neri, John Sheekey and Ferdinando Zullo)

Abstract

Recently, the geometric counterpart of linear sum-rank metric codes has been introduced in [1], where the connection with subspace designs was found. A collection of $\mathbb{F}_q$-subspaces $U_1, \dots, U_t \subseteq \mathbb{F}_{q^m}^k$ is called an $(s, A)_q$-**subspace design** if $\sum_{i=1}^t \dim_{\mathbb{F}_q}(U_i \cap W) \leq A$, for every $\mathbb{F}_{q^m}$-subspace $W \subseteq \mathbb{F}_{q^m}^k$ of dimension s. In this talk we will explore intertwined results of both geometric and coding theoretic flavour:

- Subspace design: construction and characterization of $(s, s)_q$-subspace designs in terms of their intersection properties with respect to hyperplanes.
- Sum-rank metric codes: construction and characterization of optimal $\mathbb{F}_{q^m}$-linear sum-rank metric codes in $\bigoplus_{i=1}^t \mathbb{F}_{q^m}^n$, when $n = \frac{mk}{2}$, for any m, k such that mk is even and $t \leq q - 1$.

Keywords: Sum-rank metric, subspace design, system

References

[1] A. Neri, P. Santonastaso, and F. Zullo: The geometry of one-weight codes in the sum-rank metric. *Journal of Combinatorial Theory, Series A*, 194:105703, 2023.

[2] P. Santonastaso and J. Sheekey: On h-designs, MSRD codes and disjoint maximum scattered linear sets (2023).

[3] P. Santonastaso and F. Zullo: On subspace designs. *To appear in EMS Surveys in Mathematical Sciences*.

Maximum weight codewords in the rank metric

Ferdinando Zullo
University of Campania "Luigi Vanvitelli"
(Joint work with Olga Polverino and Paolo Santonastaso)

Abstract

The problem of determining general bounds on the number of maximum weight codewords in the Hamming metric is a classical and challenging problem, which has been shown to be related to certain arcs in projective spaces. So, it is quite natural to see which kind of bounds and *optimal* constructions we can get in the rank metric. More precisely, we investigate this problem for $\mathbb{F}_{q^m}$-linear non-degenerate rank metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. In this talk we show some instances of the problem of determining the number $M(\mathcal{C})$ of codewords in $\mathcal{C}$ with maximum weight, that is $\min\{m, n\}$, and we will show some characterization results of the codes with the maximum and the minimum values of $M(\mathcal{C})$.

Keywords: Rank metric, maximum weight codeword, linear set

On the equivalence issue of a class of 2-dimensional linear Maximum Rank Metric codes

Somi Gupta
University of Naples Federico ii
(Joint work with G. Longobardi and R. Trombetti)

Abstract

The study of *Maximum Rank Metric* (or shortly MRD) *codes* plays a crucial role due to its applications in network coding, distributed storage, and post-quantum cryptography. It is well known that linear MRD codes with dimension 2 over the finite field $\mathbb{F}_{q^n}$ and minimum distance $n-1$ are linked to some geometrical structures in the projective line $\mathrm{PG}(1,q^n)$ called *maximum scattered linear sets*. For instance, the celebrated generalized Gabidulin codes with these parameters can be obtained from the so-called *pseudoregulus* linear set of $\mathrm{PG}(1,q^n)$.
Several other families of such MRD codes have been recently introduced and studied. The latest one is exhibited in [2], where the authors extended a family of codes in $\mathbb{F}_{q^n}^2$, $n=2t$, with minimum distance $2t-1$ first appeared in [1]. Also, in the former article, the authors dealt with the equivalence issue among codes of this family, solving it for $t \geq 5$.
In this talk, we will develop some methods which will allow us to complete the equivalence study for $t \in \{3,4\}$. Finally, we will show that for $t=4$, the linear sets of $\mathrm{PG}(1,q^8)$, ensuing from codes in the relevant family, are not equivalent to any sets known so far.

References

[1] G. Longobardi, G. Marino, R. Trombetti, Y. Zhou. A large family of maximum scattered linear sets of $\mathrm{PG}(1,q^n)$ and their associated MRD codes. *Combinatorica*, to appear, arXiv:2102.08287v3.

[2] A. Neri, P. Santonastaso, F. Zullo. Extending two families of maximum rank distance codes. *Finite Fields and Their Applications* **81** (2022).

Keywords: linearized polynomial, finite field, finite projective space, linear set, rank metric code

Two-weight rank metric codes and spreads

Rakhi Pratihar
Inria Saclay Research Centre (GRACE team)
(Joint work with Tovohery H. Randrianarisoa)

Abstract

A linear rank metric code $\mathcal{C}$ over $\mathbb{F}_{q^m}/\mathbb{F}_q$ of length n and dimension k is a k-dimensional $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$, where the rank weight of a codeword $c \in \mathcal{C}$ is defined as the $\mathbb{F}_q$-dimension of the space spanned by the coordinates of c. The code $\mathcal{C}$ is called two-weight code if any nonzero codeword of $\mathcal{C}$ has rank weight (i.e. $\mathbb{F}_q$-dimension of the space spanned by the coordinates) either d or d' with $d < d' \leq n$ and if one of the two weights is the length of the code, then we call it antipodal.

For Hamming metric, the study of structure and properties of two-weight linear codes is being studied at least for the last five decades. In this talk, we present the structure of generator matrices of antipodal two-weight rank metric codes. We show that the dimension of an ATW rank metric code is 2 and the minimum distance $d \geq n/2$. For $d = n/2$, we show that the codes are always induced by certain maximum rank distance (MRD) codes. For the general case, we present structural properties of generator matrices of ATW rank metric codes and their connection to (Desarguesian) spreads using q-systems. At the end, we discuss briefly the open questions.

This talk is based on a joint work (arXiv:2208.07295) with Tovohery H. Randrianarisoa.

Keywords: two-weight codes, q-systems, Desarguesian spreads, MRD codes.

References

[1] R. Pratihar and T. H. Randrianarisoa, *Antipodal two-weight rank metric codes*, arXiv: 2208.07295.

[2] O. Polverino, P. Santonastaso, J. Sheekey and F. Zullo, *Divisible linear rank metric codes*, IEEE Trans. Inform. Theory., 2023.

Saturating systems and covering radius in the (sum-)rank metric

Matteo Bonini
Aalborg University
(Joint work with M. Borello and E. Byrne)

Abstract

The relationship between linear codes and sets of points in finite geometries have long been exploited by researchers, in fact it is a standard approach (see [2]) to construct generator matrices or parity check matrix of a linear code from a set of projective points. In this context, the supports of the codewords correspond to complements of hyperplanes in a fixed projective set, and this can be used to construct codes with bounded covering radius, related to saturating sets in projective space.

The covering radius of a code is the least positive integer ρ such that the union of the spheres of radius ρ about each codeword equals the full ambient space. This fundamental coding theoretical parameter has been widely studied for codes in respect of the Hamming-metric.

In this talk, we introduce the notion of saturating systems and their properties [1]. In analogy with codes for the Hamming-metric, it turns out that a rank ρ-saturating system corresponds to a linear code of rank-metric covering radius ρ.

Finally, we will also show how this approach can be also extended to the sum-rank metric.

Keywords: Covering codes, saturating systems, rank metric, sum-rank metric

References

[1] M. Bonini, M. Borello, E. Byrne. *Saturating systems and the rank covering radius*, submitted (arXiv:2206.14740).

[2] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein. *Covering codes*, Elsevier (1997).

Weierstrass Semigroup, pure gaps and algebraic geometry codes

Luciane Quoos

Universidade Federal do Rio de Janeiro

(Joint work with Alonso S. Castellanos/UFU and Erik A. R. Mendoza/UFRJ)

Abstract

The central object of this work are Kummer extensions defined by the affine equation $y^m = \prod_{i=1}^{r}(x-\alpha_i)^{\lambda_i}$ where $\alpha_1, \ldots, \alpha_r$ are pairwise distinct elements in K the algebraic closure of $\mathbb{F}_q$, and $\gcd(m, \sum_{i=1}^{r}\lambda_i) = 1$. Let $F = \mathbb{F}_q(x,y) \mid \mathbb{F}_q$ be its function field. Kummer extensions where all the multiplicities $\lambda_1 = \lambda_2 = \cdots = \lambda_r$ are equal have been object of interest concerning the theory of semigroups and codes in the last years. Also, several of the well known maximal curves over $\mathbb{F}_{q^2}$ admit a plane realization in the projective space $\mathbb{P}^2(\mathbb{F}_q)$ as a Kummer extension.

We determine the Weierstrass semigroup $H(P_1) = \{s \in \mathbb{N} \mid (z)_\infty = sP_1 \text{ for some } z \in F\}$ at one rational place, and two rational places $H(P_1, P_2) = \{(s_1, s_2) \in \mathbb{N}^2 \mid (z)_\infty = s_1P_1 + s_2P_2 \text{ for some } z \in F\}$, where P_1, P_2 are two tottally ramified places in the extension $F \mid \mathbb{F}_q(x)$.

In 2001, Homma and Kim investigated two point codes over the Hermitian curve and introduced the concept of *pure gaps* which turned out to be very useful for the improvement of the minimum distance of an AG code. For an arbitrary function field, from the knowledge of the minimal generating set of the Weierstrass semigroup at two rational places, we characterize the set of pure gaps.

We apply the results to construct algebraic geometry codes over certain function fields with many rational places. In particular, for q even and $n \geq 3$, we obtain a family of codes over $\mathbb{F}_{q^{2n}}$ with singleton defect $q/2$.

Keywords: Kummer extensions, Weierstrass semigroup, Pure gaps, AG codes

Factoring is equivalent to counting points of elliptic curves

Jorge Jiménez Urroz

Abstract

The purpose of this talk is to prove that factorization is equivalent to counting points on elliptic curves. Concretaly

Theorem 1 *Assume the Generalized Riemann Hypothesis and let $\varepsilon > 0$. Then there exist an integer k and an algorithm such that given an squarefree integer n, and the number of points modulo n of $(\log n)^k$ elliptic curves, returns the factorization of n with probability $1 - \varepsilon$.*

Keywords— Factoring, Elliptic curves

References

[1] E. Bach and J. Shallit, Factoring with cyclotomic polynomials, Math. Comp., 185, 52, 201-219, 1989.

[2] L. Dieulefait and J. Urroz, Factorization and Malleability of RSA Moduli, and Counting Points on Elliptic Curves Modulo N, Mathematics, 12, 8, 2020.

[3] R. Drylo and J. Pomykala, Integer factoring problem and elliptic curves over the ring $\mathbf{Z}_n$, Colloq. Math., Volume = 159, 2, 259–284, 2020.

[4] N. Kunihiro and K. Koyama, Equivalence of counting the number of points on elliptic curve over the ring $\mathbf{Z}_n$ and factoring n, Advances in cryptology—EUROCRYPT '98 (Espoo), Lecture Notes in Comput. Sci., 1998.

[5] H. W. Lenstra, Jr., Factoring integers with elliptic curves, Ann. of Math., 126, 649–673, 1987.

[6] S. Martin and P. Morillo and J. L. Villar,Computing the order of points on an elliptic curve modulo N is as difficult as factoring N, Appl. Math. Lett., 14, 341–346, 2001.

A geometric construction of a family of non-linear MRD codes

Giovanni Giuseppe Grimaldi
Università degli Studi di Napoli Federico II - DMA R. Caccioppoli
(Joint work with Nicola Durante and Giovanni Longobardi)

Abstract

In the finite projective space $\mathrm{PG}(n-1,q^n)$, let $\mathcal{C}$ be a C_F^s-set of a $(n-k+1)$-dimensional subspace Λ with vertices A and B and $\Lambda^\star$ be a $(k-3)$-dimensional subspace skew with Λ. In [1], it is shown that $\mathcal{C}$ is the union of $\{A,B\}$ and $q-1$ pairwise disjoint scattered $\mathbb{F}_q$-linear sets of rank n, say $\mathcal{C}_a$ for any $a\in\mathbb{F}_q^*$. Moreover, the line AB can be partitioned in $\{A,B\}$ and $q-1$ scattered $\mathbb{F}_q$-linear sets of rank n, say J_a for any $a\in\mathbb{F}_q^*$. Denote by $\mathcal{K}(\Lambda^\star,\mathcal{E})$ the cone with vertex $\Lambda^\star$ and base the set

$$\mathcal{E}=(\mathcal{C}\setminus\bigcup_{a\in T}\mathcal{C}_a)\cup\bigcup_{a\in T}J_a,$$

with $T\subset\mathbb{F}_q^*$ and $T\ni 1$. Then $\mathcal{K}(\Lambda^\star,\mathcal{E})$ gives rise to a new family of non-linear $(n,n,q;d)$-MRD codes for any $n\geq 3$, $2\leq d\leq n-1$ and $d=n-k+1$. This new class of codes contains properly those constructed by Donati and Durante [1], and any its element is not equivalent to non-linear MRD codes constructed by Otal and Özbudak in [2].

Keywords: finite projective space, C_F^s-set, linear set, rank metric code, MRD-code

References

[1] G. Donati, N. Durante: *A generalization of the normal rational curve in* $\mathrm{PG}(d,q^n)$ *and its associated non-linear MRD codes*. Des. Codes Cryptogr. 86, 1175–1184 (2018).

[2] K. Otal, F. Özbudak: *Some new non-additive maximum rank distance codes*. Finite Fields and Their Applications 50, 293–303 (2018).

Short minimal rank-metric codes and scattered subspaces

G. Longobardi

University of Naples Federico II

(Joint work with S. Lia, G. Marino and R. Trombetti)

Abstract

As described in [1], the property for non-degenerate rank-metric codes being minimal can be expressed in terms of evasiveness of the associated q-system. By exploiting this connection, in this talk we will exhibit an infinite class of codes with parameters $[m+2, 3, m-2]_{q^m/q}$, $m \geq 5$ odd, constructing scattered subspaces of $\mathbb{F}_{q^m}^3$ with rank $m+2$. Moreover, we will show that a code in this class has rank weights belonging to $\{m-2, m-1, m\}$.

Keywords: Scattered subspaces, linear sets, cutting blocking sets, rank-metric codes

References

1. G. N. Alfarano, M. Borello, A. Neri, A. Ravagnani. Linear cutting blocking sets and minimal codes in the rank metric. *Journal of Combinatorial Theory, Series A,* 192: 105658, 2022.

Evasive subspaces, generalized rank weights and near MRD codes

Rocco Trombetti

University of Naples Federico II

(Joint work with D. Bartoli, B. Csajbók, G. Marino, and A. Neri)

Abstract

Let $V = \mathbb{F}_{q^m}^k$ be a k-dimensional vector space over $\mathbb{F}_{q^m}$. An $\mathbb{F}_q$-subspace U of V is (h,k)-evasive if it meets the h-dimensional subspaces of V in $\mathbb{F}_q$-subspaces of dimension at most k.

In this talk we will first show some results about the maximum size of such geometric objects. Then, we will study the duality relations among them and provide various constructions.

In addition to this, we will revisit and extend the well-known connections described by Randrianarisoa in [**?**] between $\mathbb{F}_{q^m}$-linear rank-metric codes with minimum distance d and q-systems, which are a special type of evasive $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}^k$; i.e., $(k-1, m-d)$-evasive subspaces. This will lead us to establish a unifying framework in which we prove how the parameters of a rank-metric code are related to special geometric properties of the associated evasive subspace. Finally, we will briefly show how this simplified point of view also leads us to get a geometric characterization of so-colled near MRD codes and a bound on their length.

Keywords: Rank-metric code; Evasive subspace; Scattered subspace

References

[1] T. H. Randrianarisoa A geometric approach to rank metric codes and a classification of constant weight codes. *Des. Codes Cryptogr.*, **88** (2020).

[2] D. Bartoli, B. Csajbók, G. Marino, R. Trombetti Evasive subspaces. *J. Combi, Des.*, **29**(8) (2021).

[3] A. Neri, G. Marino, R. Trombetti Evasive subspaces, generalized rank weights and near MRD codes. *arXiv preprint: 2204.11791.*, (2022).

MRD codes and algebraic varieties over finite fields

Daniele Bartoli
University of Perugia
(Joint work with G. Marino, A. Neri, L. Vicino)

Abstract

Minimal rank-metric codes or, equivalently, linear cutting blocking sets are characterized in terms of the second generalized rank weight, via their connection with evasiveness properties of the associated q-system. Using this result, we provide the first construction of a family of $\mathbb{F}_{q^m}$-linear MRD codes of length $2m$ that are not obtained as a direct sum of two smaller MRD codes. In addition, such a family has better parameters, since its codes possess generalized rank weights strictly larger than those of the previously known MRD codes. This shows that not all the MRD codes have the same generalized rank weights, in contrast to what happens in the Hamming metric setting.

Keywords: MRD codes, scattered subspaces, evasive subspaces, algebraic varieties

Algebraic geometry and number theory approach

Algebraic curves in positive characteristic and their invariants

Marco Timpanella

University of Perugia

(Joint work with Massimo Giulietti and Gábor Korchmáros)

Abstract

The foundation of the theory of algebraic curves over the complex field goes back to the Nineteenth century, and most of this theory holds true if $\mathbb{C}$ is replaced by any field of characteristic zero. However, significant differences arise in positive characteristic. One of the main features of algebraic curves in positive characteristic concerns the fact that they may have much larger automorphism groups (compared to their genus) than in the zero characteristic case. In this talk we will describe the interplay between automorphism groups and other birational invariants of an algebraic curve, such as the genus and the p-rank, and we will present some recent results.

Keywords: Algebraic curves, automorphism groups.

References

[1] M. Giulietti, G. Korchmáros, M. Timpanella. On the Dickson-Guralnick-Zieve curve. *Journal of Number Theory* **196**, 114–138 (2019).

[2] H. W. Henn. Funktionenkorper mit großer Automorphismengruppe. *J. Reine Angew. Math.* **302**, 96-115 (1978).

[3] S. Lia, M. Timpanella. Bound on the order of the decomposition groups of an algebraic curve in positive characteristic. *Finite Fields and Their Applications* **69**, 101771 (2021).

[4] S. Nakajima. p-ranks and automorphism groups of algebraic curves. *Transactions of the American Mathematical Society* **303**, 595-–607 (1987).

A NUMBER THEORETICAL APPROACH TO POLYNOMIALS OVER FINITE FIELDS

Neslihan Girgin

Mimar Sinan Fine Arts University

(Joint work with Alp Bassa, Emrah Sercan Yilmaz)

Abstract

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. The explicit constructions of irreducible polynomials over $\mathbb{F}_q$ of high degree is one of the main problems in the arithmetic of finite fields which has many applications in several areas such as coding theory and cryptography. In general, some recursive methods are preferred to do these constructions using rational transformations. In particular, we are interested in methods that are obtained by using quadratic transformations. For doing this, we will first classify and normalize the rational transformations of degree 2 using the behaviour of the ramified places in the corresponding rational function field extensions over the finite field $\mathbb{F}_q$. Then we will investigate the constructions using Galois theory and some basic observations in group theory. This approach helps to better understand the iterative constructions and gives various generalisations of them. It also enables to determine the requirements put on the initial polynomials.

Keywords: finite field; irreducible polynomial; iterative construction

References

[1] Bassa, A., Menares, R., The R-transform as power map and its generalisations to higher degree, arXiv:1909.02608.

[2] Cohen, S.,D., The explicit constructions of irreducible polynomials over finite fields, Des.Codes Cryptogr., V.2 pp.169-174, 1992.

[3] Kyuregyan, M., K., Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd char., Fin. Fields Appl. V.9,pp.39-58,200.

Galois subcovers of the Hermitian curve in characteristic p with respect to subgroups of order p^2

Barbara Gatti

University of Salento, Italy

(Joint work with Francesco Ghiandoni and Gábor Korchmáros)

Abstract

A (projective, geometrically irreducible, non-singular) curve $\mathcal{X}$ defined over a finite field $\mathbb{F}_{q^2}$ is *maximal* if the number N_{q^2} of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound, that is $N_{q^2} = q^2 + 2\mathfrak{g}q + 1$ where $\mathfrak{g}$ is the genus of $\mathcal{X}$. An important question, also motivated by applications to algebraic-geometry codes, is to find explicit equations for maximal curves. For curves which are Galois covered of the Hermitian curve, this has been done so far ad hoc, in particular in the cases where the Galois group has prime order. In this talk we show explicit equations of all Galois covers of the Hermitian curve with Galois group of order p^2 where p is the characteristic of $\mathbb{F}_{q^2}$.

Keywords: Maximal curves, function fields, Galois cover

References

[1] A. Cossidente, G. Korchmáros and F. Torres, Curves of large genus covered by the Hermitian curve, *Comm. Algebra* **28** (2000), 4707–4728.

Isomorphisms of maximal curves

Gábor Korchmáros
University of Basilicata, Italy
(Joint work with Barbara Gatti)

Abstract

A (projective, geometrically irreducible, non-singular) curve of genus $\mathfrak{g}$ defined over a finite field $\mathbb{F}_{q^2}$ is $\mathbb{F}_{q^2}$-*maximal* if the number of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound, that is, it equals $q^2 + 2\mathfrak{g}q + 1$. Two $\mathbb{F}_{q^2}$-maximal curves with the same genus with different $\mathbb{F}_{q^2}$-automorphism groups were given in [1]. The question arise whether there exist non-isomorphic $\mathbb{F}_{q^2}$-maximal curves with the same genus, $\mathbb{F}_{q^2}$-automorphism group, and Weierstrass semigroup at an $\mathbb{F}_{q^2}$-rational point. We show that the answer is affirmative for $\mathbb{F}_{q^2}$-maximal curves which are Galois covered of the Hermitian curve with respect to an automorphism group of order p^2 where p is the characteristic of $\mathbb{F}_{q^2}$.

Keywords: Maximal curves, finite fields, isomorphism

References

[1] A. Cossidente, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, On plane maximal curves, *Compositio Math.* **121** (2000), 163–181.

On the proof of a conjecture on arboreal Galois representations

Giacomo Micheli
University of South Florida
(Joint work with Andrea Ferraguti)

Abstract

In this talk we first recall the notion of arboreal Galois representation and then we develop a method [1] to effectively determine the set of primes p for which certain arboreal Galois representations are surjective modulo p. Our method is based on a combination of height bounds on integral points on elliptic curves over function fields in positive characteristic and the ABC theorem for function fields. Using this technique we prove Jones' conjecture on the surjectivity of the arboreal Galois representation attached to $f = x^2 + t$ [2, Conjecture 6.7].

Keywords: Finite Fields; Galois Representations; Iteration of Polynomials; ABC Theorem for Function Fields; Height Bounds.

References

[1] Andrea Ferraguti and Giacomo Micheli. An equivariant isomorphism theorem for mod p reductions of arboreal Galois representations. *Transactions of the American Mathematical Society*, 373(12):8525–8542, 2020.

[2] Rafe Jones. Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set. *Compositio Mathematica*, 143(5):1108–1126, 2007.

E_8-Lattice via Quaternion Divison Algebras over Quadratic Imaginary Number Fields

Carina Alves
São Paulo State University (UNESP), Brazil
(Joint work with P. G. Sicuti and A. J. Ferrari)

Abstract

Lattices can be applied in different areas of research, particularly, they can be applied in information theory and encryption schemes. In the recent years, communications over multiple-antenna fading channels has attracted the attention of many researchers. In this context quaternion structure has been used since the introduction of the Alamouti code for two transmit antennas. Space-Time Codes based on an order of a quaternion algebra such that the volume of the Dirichlet's polyhedron of the group of units is small, are better suited for decoding using the method of algebraic reduction since the approximation error is smaller [1]. The volume of this Dirichlet's polyhedron is given by the Tamagawa formula and is called the Tamagawa volume [2]. From the point of view of relating quaternion algebras with lattices, we present constructions of E_8-lattice as a left ideal of a maximal order associated to quaternion division algebras over some quadratic imaginary number fields with class number one and small Tamagawa volume.

Keywords: Lattices, Coding Theory, Quaternion Algebra

References

[1] L. Luzzi, G. R-B. Othman, J-C. Belfiore, Algebraic Reduction for the Golden Code, Advances in Mathematics of Communications, 6 (1) (2012) 1-26.

[2] C. Maclachlan, A. W. Reid, The Arithmetic of Hyperbolic 3-Manifolds, Springer, 2003.

Kani–Rosen theorem, a tool for finding maximal curves

Annamaria Iezzi
Università degli Studi Federico II
(Joint work with Motoko Qiu Kawakita and Marco Timpanella)

Abstract

A theorem by Kani and Rosen ([3, Theorem B]) allows to fully decompose the Jacobian of a curve, under certain assumptions on the automorphism group of the curve. In this talk, after reviewing the relevant mathematical background, we show how this theorem has been used in literature to find examples of curves defined over finite fields with many rational points. We then explain how we use this approach to provide new examples of curves of genus 6 or 10 attaining the Serre bound, inside the family of sextics introduced in [2] as a a generalization of the Wiman and Edge sextics [1, 4].

Keywords: Maximal curves, Automorphism group, Jacobian variety, Kani–Rosen theorem.

References

[1] W. L. Edge, A pencil of four-nodal plane sextics, Math. Proc. Cambridge Philos. Soc. **89**(3) (1981), 413–421.

[2] M. Q. Kawakita, Certain sextics with many rational points, Adv. Math.of Commun. **11**(2) (2017), 289–292.

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

[4] A. Wiman, Ueber eine einfache Gruppe von 360 ebenen Collineationen, Math. Ann. **47**(4) (1896), 531–556.

A study of certain sextic number fields with the help of finite fields

Sumandeep Kaur
Panjab University, Chandigarh
(Joint work with Sudesh Kaur Khanduja)

Abstract

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field, where θ is a root of an irreducible polynomial $f(x) = x^6 + ax + b$ belonging to $\mathbb{Z}[x]$. Let p be a prime number. In case of finite fields, the most common valuation function is the p-adic valuation v_p which is defined for any non-zero integer m to be the highest power of the prime p dividing m. The Newton polygon is a graphical tool that encodes information about the valuations of the coefficients of a polynomial. The slope of each segment of the Newton polygon corresponds to the p-adic valuation of a certain coefficient. With each edge of the Newton polygon, a polynomial with coefficients from the finite field $\mathbb{F}_q$, where q is a prime power is attached. In this talk, using theory of Newton polygons and valuations, we will find discriminant of K and integral basis of K. For each prime p dividing discriminant of $f(x)$, we will study the corresponding finite field $\mathbb{F}_p$, and then applying theory of Newton polygons and attaching some polynomials (known as residual polynomial) with coefficients from $\mathbb{F}_p$, we will see how we can find discriminant and integral basis of K. In this talk, we will see how finite fields can be helpful to study the properties of algebraic number fields. In the end, I will illustrate the results with examples.

Keywords: Valuation, finite fields, discriminant, number fields, Newton polygon

Finite geometry and designs

Small complete caps in PG$(4n+1,q)$

Giuseppe Marino
University of Naples Federico II
(Joint work with A. Cossidente, B. Csajbók and F. Pavese)

Abstract

Let PG(r,q) denote the r-dimensional projective space over F_q, the finite field with q elements. A *k-cap* in PG(r,q) is a set of k points no three of which are collinear. A k-cap in PG(r,q) is said to be *complete* if it is not contained in a $(k+1)$-cap in PG(r,q). The study of caps is not only of geometrical interest, indeed their concept arises from coding theory (cf. [3]).

One of the main issues in this area is to determine the spectrum of the sizes of complete caps in a given projective space and in particular to determine the size of the smallest and the largest complete caps. For the size $t_2(r,q)$ of the smallest complete cap in PG(r,q), the trivial lower bound is $t_2(r,q) > \sqrt{2}q^{\frac{r-1}{2}}$. If q is even and r is odd (see e.g. [4]) or if $r \geq 4$ is even and q is an even square (cf. [1]), such bound is substantially sharp.

In this talk we will show that the trivial lower bound on $t_2(4n+1,q)$ is essentially sharp, by constructing a complete cap of PG$(4n+1,q)$, $q>2$, of size $2(q^{2n}+\ldots+1)$.

Keywords: cap, linearized polynomial

References

[1] D. Bartoli, M. Giulietti, G. Marino, O. Polverino, Maximum scattered linear sets and complete caps in Galois spaces, *Combinatorica*, **38** (2018), 255–278.
[2] A. Cossidente, B. Csajbók, G. Marino, F. Pavese: Small complete caps in PG$(4n+1,q)$, *Bulletin London Math. Soc.*, **55(1)** (2023), 522-–535.
[3] E.M. Gabidulin, A.A. Davydov, L.M. Tombak, Linear codes with covering radius 2 and other new covering codes, *IEEE Trans. Inform. Theory*, **37** (1991), 219–224.
[4] F. Pambianco, L. Storme: Small complete caps in spaces of even characteristic, *J. Combin. Theory Ser. A*, **75** (1996), 70–84.

A Class of Cross Resolvable Designs

Charul Rajput
Department of ECE, Indian Institute of Science, Bengaluru, India
(Joint work with B. Sundar Rajan)

Abstract

Resolvable block designs are well-known and extensively studied in the literature. A design (X, A) consists of a set X and a collection A of non-empty subsets of X called blocks, where each block has the same size. A subset of disjoint blocks from A whose union is X is called a parallel class, and a partition of A into several parallel classes is called a resolution. If A has at least one resolution, the design (X, A) is called a resolvable design.

In [1: D. Katyal, P. N. Muralidhar, and B. S. Rajan,"Multi-access coded caching schemes from cross resolvable designs", IEEE Trans. Commun., 2021], authors introduced cross resolvable designs, and using these designs, they obtained a scheme for multi-access coded caching problem. Further, a class of cross resolvable designs was obtained from affine resolvable balanced incomplete block designs. In a resolvable design (X, A) with a resolution containing r parallel classes, if the cardinality of the intersection of i blocks drawn from any i distinct parallel classes remains constant for at least one $i \in \{2, 3, \ldots, r\}$, then (X, A) is called a Cross Resolvable Design (CRD). A CRD is called a maximal cross resolvable design if the given condition is satisfied for $i = r$.

A new class of CRDs was presented in [2: P. N. Muralidhar, and B. S. Rajan, "Multi-access coded caching from a new class of cross resolvable designs," IEEE Int. Symp. Inf. Theory, 2021], and it was shown that the multi-access coded caching schemes derived from these CRDs perform better than the previously existing schemes. We constructed a class of maximal CRDs. The parameters of the proposed class coincide with the parameter of CRDs given in [2], but the method of construction is different in both. In this talk, we start by defining CRDs and then present a construction of maximal CRDs with some examples. Then we discuss the application of CRDs in obtaining a multi-access coded caching scheme.

Keywords: Resolvable designs, Cross resolvable designs, Multi-access coded caching

Construction and equivalence of Sidon spaces and cyclic subspace codes

Olga Polverino

University of Campania "Luigi Vanvitelli"

(Joint work with Chiara Castello, Paolo Santonastaso and Ferdinando Zullo)

Abstract

A Sidon space V is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ such that if $ab = cd$, where $a, b, c, d \in V \setminus \{0\}$, then $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$. Sidon spaces have been introduced by Bachoc, Serra and Zémor in 2017 as the q-analogue of Sidon sets, classical objects widely studied in additive combinatorics. The interest on Sidon spaces has increased quickly, especially after the work of Roth, Raviv and Tamo in 2018, in which they highlighted the correspondence between Sidon spaces and cyclic subspace codes. In this talk we will mainly focus on Sidon spaces contained in the sum of two multiplicative cosets of a fixed subfield of $\mathbb{F}_{q^n}$, for which we will provide characterization results and we will construct some new examples, arising also from some well-known combinatorial objects. Moreover, we will give a quite natural definition of equivalence among Sidon spaces, which relies on the notion of equivalence of cyclic subspace codes and we will discuss about the equivalence of the known examples.

Keywords: Sidon space, cyclic subspace code, linearized polynomial

The line and the translate properties for r-primitive elements

Giorgos Kapetanakis
University of Thessaly
(Joint work with Stephen D. Cohen)

Abstract

Let $\mathbb{F}_q$ be the finite field of q elements and $\mathbb{F}_{q^n}$ its extension of degree n. An element of $\mathbb{F}_{q^n}^*$ of order $(q^n-1)/r$ is called *r-primitive*, while, if $r=1$, we simply call it *primitive*. If θ is such that $\mathbb{F}_{q^n}=\mathbb{F}_q(\theta)$, then

$$\mathcal{T}_\theta := \{\theta + x \,:\, x \in \mathbb{F}_q\}$$

is a *set of translates* and, if $\alpha \in \mathbb{F}_{q^n}^*$,

$$\mathcal{L}_{\alpha,\theta} := \{\alpha(\theta + x) \,:\, x \in \mathbb{F}_q\}$$

is a *line*. It is known that, given n, if q is large enough, every set of translates and every line contain a primitive element, while effective versions are known for a few small values of n. In this work, we extend the asymptotic results to r-primitive elements and provide effective results for the case $r=n=2$.

Keywords: Primitive elements; Line property; Translate property

References

[1] S.D. Cohen and G. Kapetanakis. Finite field extensions with the line or translate property for r-primitive elements. *J. Aust Math. Soc.*, 111(3):313–319, 2021.

[2] S.D. Cohen and G. Kapetanakis. The translate and line properties for 2-primitive elements in quadratic extensions. *Int. J. Number Theory*, 16(9):2029–2040, 2020.

Intersection distribution and non-hitting index

Shuxing Li
Simon Fraser University
(Joint work with Alexander Pott)

Abstract

For a point set in the classical projective plane $\mathrm{PG}(2,q)$, we introduce the concept of intersection distribution, which reflects how this point set interacts the lines of $\mathrm{PG}(2,q)$. We compute the intersection distributions of several families of point sets, which can be represented by monomials over finite fields. These intersection distributions lead to several infinite families of Kakeya sets in the classical affine planes with prescribed sizes.

Among the intersection distribution, a particularly interesting quantity is the so called non-hitting index, which equals the number of lines not intersecting with the point set. We characterize the point sets whose non-hitting indices are close to the lower or upper bounds.

Reference:

S. Li and A. Pott. Intersection distribution, non-hitting index and Kakeya sets in affine planes. *Finite Fields and Their Applications*, 2020.

Keywords: Point set in projective plane, intersection distribution, non-hitting index, ploynomial, Kakeya set

Avoiding intersections of given size in finite affine spaces $AG(n, 2)$

Zoltán Lóránt Nagy
Eötvös University, Budapest
(Joint work with Benedek Kovács)

Abstract

We study the set of intersection sizes of a k-dimensional affine subspace and a point set of size $m \in [0, 2^n]$ of the n dimensional binary affine space $AG(n, 2)$. Following the theme of Erdős, Füredi, Rothschild and T. Sós, we discuss the q-analogue problem and partially determine which local densities (i.e., set sizes t) in k-dimensional affine subspaces are unavoidable in all m-element point sets in the n-dimensional affine space.

We also show constructions of point sets for which the intersection sizes with k-dimensional affine subspaces takes values from a set of a small size compared to 2^k. These are built up from affine subspaces and so-called evasive sets. Along the lines we improve the best known upper bounds on *evasive sets* and apply results concerning the canonical signed-digit (CSD) representation of numbers. When $t = 2^\ell$ for some integer $1 < \ell \leq k$, we show that for almost all values of $m \in [0, 2^n]$, a k-dimensional affine subspace with t points induced by an m-set is unavoidable, and present a similar statement for $t = 0.75 \cdot 2^\ell$ as well.

Keywords: unavoidable patterns, affine subspaces, evasive sets, random methods, canonical signed-digit number system.

References

Erdős, P., Füredi, Z., Rothschild, B. L., Sós, V. T. (1999). Induced subgraphs of given sizes. Discrete mathematics, 200(1-3), 61-77.

Guruswami, V. (2011). Linear-algebraic list decoding of folded Reed-Solomon codes, in Proceedings of the 26th IEEE Conference on Computational Complexity.

Kovács, B., Nagy, Z. L. (2023). Avoiding intersections of given size in finite affine spaces $AG(n, 2)$, manuscript.

When a hermitian, a quadric, and a subgeometry walk into a bar...

Stefano Lia
University College Dublin
(Joint work with John Sheekey)

Abstract

Building on the representation of three-fold tensors as points of $\mathrm{PG}(n^2-1, q^n)$, we exploit a geometrical framework allowing us to provide an interesting geometrical interpretation of the non-singularity of tensors. As a consequence, constructions of new quasi-hermitian surfaces, classifications of non-singular four-fold tensors, and new results on semifields (incorporating a new geometrical proof of a classical result) are obtained.

This is a two-part talk with John Sheekey.

Keywords: semifields - nonsingular tensors - quasi-hermitian surfaces

References

[1] Landsberg, J. M. "Tensors: geometry and applications." Graduate Studies in Mathematics, 128. American Mathematical Society, Providence, RI, 2012.

[2] Lavrauw, M.; Polverino, O. "Finite Semifields and Galois Geometry." Chapter in "Current research topics in Galois Geometry", 2011.

[3] Lavrauw, M.; Sheekey, J. "Orbits of the stabiliser group of the Segre variety product of three projective lines." Finite Fields and Their Applications, 2014.

... does a quasi-hermitian surface always follow?

John Sheekey
University College Dublin
(Joint work with Stefano Lia)

Abstract

This talk will follow on from the talk of Stefano Lia. We will focus on the construction of new quasi-hermitian surfaces [2] arising from the study of a geometric description of non-singular tensors in $\mathrm{PG}(3, q^2)$. The construction shares some commonalities with [3], though it arises naturally from a different problem, namely a new framework to study the orbits of tensors described in [1].

Keywords: quasi-hermitian surfaces; semifield; nonsingular tensors

References

[1] Lavrauw, Michel; Sheekey, John: *Orbits of the stabiliser group of the Segre variety product of three projective lines*. Finite Fields Appl. 26 (2014), 1?6.

[2] Lia, Stefano; Sheekey, John: *in preparation*.

[3] Lavrauw, Michel; Lia, Stefano; Pavese, Francesco: *On the geometry of the Hermitian Veronese curve and its quasi-Hermitian surfaces*, arXiv:2303.01953.

Combinatorial and geometric aspects for codes and graphs

Decomposition of finite commutative semisimple group algebras over finite fields using the Combinatorial Nullstellensatz

Robert Christian Subroto
Radboud University

Abstract

We present a full decomposition of finite commutative semisimple group algebras of the form $\mathbb{F}_q[G]$, where G is a finite commutative group with order coprime to q. This was achieved by studying algebraic properties of coordinate rings of the form

$$R_{m_1,...,m_n}(\mathbb{F}_q) \coloneqq \mathbb{F}_q[X_1,...,X_n]/\langle X_1^{m_1}-1,...,X_n^{m_n}-1\rangle,$$

which omits the use of finding primitive idempotents and character theory. Since $\mathbb{F}_q$ is not algebraically closed, we cannot simply apply results from algebraic geometry like the Hilbert's Nullstellensatz. This was solved by using the Combinatorial Nullstellensatz together with Galois group actions on the vanishing set of the ideal $\langle X_1^{m_1}-1,...,X_n^{m_n}-1\rangle$. This approach establishes a direct relation between the decomposition and the structure of cyclotomic Galois groups, and it does apply to any field. Galois extensions of finite fields are well understood, from which we can extract a lot of information of the decomposition of $R_{m_1,...,m_n}(\mathbb{F}_q)$, like the following result:

Theorem 1. *Let $m_1,...,m_n$ be coprime to q. The number of simple components of $R_{m_1,...,m_n}(\mathbb{F}_q)$ equals*

$$\sum_{d_1|m_1} \cdots \sum_{d_n|m_n} \left(\frac{\prod_{i=1}^n \varphi(d_i)}{\Delta_{d_1,...,d_n}(q)} \right),$$

where φ is Euler's totient function, and $\Delta_{d_1,...,d_n}(q) \coloneqq \operatorname{lcm}_{i=1}^n(\operatorname{ord}_{d_i}(q))$ (we use the notation $\operatorname{ord}_{d_i}(q)$ for the multiplicative order of q in $(\mathbb{Z}/d_i\mathbb{Z})^*$).

Keywords: Semisimple group algebras, Combinatorial Nullstellensatz, Galois theory

Partial Difference Sets in nonabelian groups

James A. Davis
University of Richmond
(Joint work with John Polhill, Ken Smith, Eric Swartz)

Abstract

Partial difference sets (PDSs) are subsets of groups that can be used to construct strongly regular graphs (SRGs). Since Paley's original construction in 1933, many other constructions have been found. Often the first constructions for a particular parameter set came from using cyclotomy in a finite field, then other constructions were found in non-elementary abelian groups. Most often these new constructions were in abelian groups. In this talk, we explore some constructions in nonabelian groups. In three of the examples, the parameter set will not support a PDS in an abelian group. Other examples occur in parameter families with known examples of abelian PDSs, but the new examples correspond to SRGs that are not isomorphic to known examples. This preliminary report parallels recent work done in automorphism groups on symmetric designs, and these recent discoveries in symmetric designs indicate that the nonabelian world will produce vastly more nice combinatorial results (difference sets, PDSs) than the abelian world.

Keywords: partial difference set, strongly regular graph, nonabelian
S. L. Ma, Partial difference sets, Discrete Math. 52 (1984) 75-89.
K. Smith, Nonabelian hadamard difference sets, Journal of Combinatorial Theory, Series A, v. 70, 1995, 144-156.

Polynomials, spreads and flag-transitive linear spaces

Cian Jameson
University College Dublin
(Joint work with John Sheekey)

Abstract

There has been much progress towards classifying linear spaces that possess a flag-transitive automorphism group. A complete classification is not yet available, as the case in which the automorphism group is a subgroup of one-dimensional affine transformations remains open. The linear spaces having such an automorphism group that we consider are constructed from spreads possessing a transitive automorphism group.

In [1], Pauley and Bamberg constructed new flag-transitive linear spaces via spreads upon which a cyclic group acts transitively, and provided a condition for such spreads to exist in terms of an associated polynomial.

In this talk, we will present our work on describing and classifying the polynomials that give rise to the desired spreads and linear spaces. We will focus on the case of cubic polynomials, corresponding to cyclic line spreads in $\mathrm{PG}(5, q)$, for which a complete classification has been attained. We will also discuss connections with permutation polynomials explored by Feng and Lu (2023), as well as the classification of a family of permutation trinomials by Bartoli and Timpanella (2021) for which our cubic polynomial problem can coincide.

Keywords: linear space, flag-transitivity, spread, permutation polynomial

References

[1] M. Pauley, J. Bamberg. A construction of one-dimensional affine flag-transitive linear spaces, *Finite Fields and Their Applications* 14, 2008.

Minimal Codes and Strong Blocking Sets

Gianira N. Alfarano
Eindhoven University of Technology
(Joint work with Martino Borello and Alessandro Neri)

Abstract

A linear code is said to be minimal if the support of each of its codewords does not contain the support of any other independent codeword, namely, all its codewords are minimal. The study of minimal codewords arises from their applications to secret sharing schemes and to decoding strategies. They have recently been shown to correspond to strong blocking sets which are sets of projective points, such that their intersection with each hyperplane generates the hyperplane itself; see [1] and [2].

In this talk we introduce the concepts of *outer minimal codes* and *outer strong blocking sets*. These are codes whose concatenation with minimal codes is minimal and sets whose field reduction is a strong blocking set. We investigate their structure and provide bounds on their length/size. Finally, we present a geometric construction of small strong blocking sets, with low computational cost. This talk is based on [3].

Keywords: Minimal linear codes; strong blocking sets; concatenation.

References

[1] Gianira N. Alfarano, Martino Borello, Alessandro Neri. *A geometric characterization of minimal codes and their asymptotic performance.* Advances in Mathematics of Communications, **16.1**(2022):115–133.

[2] Chunming Tang, Yan Qiu, Qunying Liao, Zhengchun Zhou. *Full characterization of minimal linear codes as cutting blocking sets.* IEEE Transactions on Information Theory, **67.6**(2021):3690-3700.

[3] Gianira N. Alfarano, Martino Borello, Alessandro Neri. *Outer Strong Blocking Sets.* preprint.

On the graph and on the set of directions determined by functions over finite fields

Bence Csajbók
Polytechnic University of Bari, Italy
(Joint work with G. Marino, V. Pepe)

Abstract

Consider $\mathrm{PG}(r,q^n)$ as $\mathrm{AG}(r,q^n) \cup H_\infty$, where H_∞ is the hyperplane at infinity. The set of directions determined by an affine point set S of $\mathrm{AG}(r,q^n)$ is the set of ideal points $\mathrm{dir}(S) = \{\langle P,Q\rangle \cap H_\infty : P,Q \in S, P \neq Q\}$. For a function $f\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ the graph of f is the affine point set $U_f = \{(x,f(x)) : x \in \mathbb{F}_{q^n}\} \subseteq \mathrm{AG}(2,q^n)$. Assume that f (and hence U_f) is $\mathbb{F}_q$-linear. If ℓ is a line through the origin, then $|U_f \cap \ell| = q^i$, $i \in \mathbb{Z}_0^+$. Let w be maximal such that for each line ℓ through the origin either $U_f \cap \ell = \{(0,0)\}$, or $|U_f \cap \ell| \geqslant q^w$. By a result of Ball et al. $\mathbb{F}_{q^w}$ is the largest subfield of $\mathbb{F}_{q^n}$ such that U_f is an $\mathbb{F}_{q^w}$-subspace. With G. Marino and V. Pepe we proved the following generalisation.

Theorem 1. *Let U denote an m-dimensional $\mathbb{F}_q$-subspace of $\mathrm{AG}(r,q^n)$. Let w be maximal such that for each line ℓ through the origin either $U \cap \ell = \{(0,\dots,0)\}$ or $|U \cap \ell| \geqslant q^w$.*

(a) If $n \mid m$, then $w \mid n$ and $\mathbb{F}_{q^w}$ is the largest subfield of $\mathbb{F}_{q^n}$ such that U is $\mathbb{F}_{q^w}$-linear.

If $n \nmid m$ then U is not necessarily linear over a larger field, but it acts similarly:

(b) If $q \geqslant n$, then there exists an integer $d \geqslant w$, $d \mid n$, such that $\mathrm{dir}(U) = \mathrm{dir}(\langle U\rangle_{\mathbb{F}_{q^d}})$.

Keywords: graph of a function, direction problem, linear set

References

[1] B. Csajbók, G. Marino, V. Pepe: On the maximum field of linearity of linear sets, submitted manuscript.

A proof of the Etzion-Silberstein conjecture for strictly monotone Ferrers diagrams

Alessandro Neri
Ghent University
(Joint work with Mima Stanojkovski)

Abstract

Ferrers diagram rank-metric codes were first studied by Etzion and Silberstein in 2009 [1]. In their paper, they proposed a conjecture on the largest dimension of a space of matrices over a finite field whose nonzero elements are supported on a given Ferrers diagram and have all rank lower bounded by a fixed positive integer d. Over the last 14 years, their conjecture has been proved only in some cases, mostly including an assumption on the field size being large enough, or some restriction on the minimum rank d depending on the Ferrers diagram. As of today, this conjecture still remains widely open. In this talk we give a constructive proof of the celebrated Etzion-Silberstein conjecture for the class of strictly monotone Ferrers diagrams, which does not depend on the minimum rank d and holds over every finite field.

Keywords: Ferrers diagrams, Rank-metric codes, Etzion-Silberstein conjecture

References

[1] T. Etzion, N. Silberstein. *Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams.* IEEE Transactions on Information Theory, **55.7**(2009):2909–2919.

The Diagonals of Ferrers Diagrams

Giuseppe Cotardo
Virginia Tech
(Joint work with Anina Gruica and Alberto Ravagnani)

Abstract

In [2], Garsia and Remmel defined the q-rook polynomials for Ferrers diagrams. They showed that they share many properties with the rook numbers introduced by Riordan and Kaplansky. In [4], Haglund established connections between q-rook polynomials and matrices over finite fields.

In this talk, we reconstruct the theory of q-rook polynomials for Ferrers diagrams by focusing on the properties of their diagonals. We show that the diagonals define an equivalent relation on the set of Ferrers diagrams and we establish connections with the problem of counting matrices of given rank supported on a Ferrers diagram.

Keywords: Ferrers diagram, q-rook polynomial, matrix space

References

[1] T. Etzion and N. Silberstein, *Error-Correcting Codes in Projective Spaces via Rank-Metric Codes and Ferrers Diagrams*, IEEE Transactions On Information Theory **55** (2009), no. 7, 2909-2919.

[2] A. M. Garsia and J. B. Remmel, *Q-Counting Rook Configurations and a Formula of Frobenius*, Journal Of Combinatorial Theory, Series A **41** (1986), 246-275.

[3] A. Gruica and A. Ravagnani, *Rook Theory of the Etzion-Silberstein Conjecture*, arXiv preprint arXiv:2209.05114 (2022).

[4] J. Haglund, *q-Rook Polynomials and Matrices over Finite Fields*, Advances in Applied Mathematics **20** (1998), no. 4, 450-487.

Quasi-Cyclic Codes from Finite Euclidean Planes

Eduardo Brandani da Silva

Universidade Estadual de Maringá (UEM)

(Joint work with F.V. Batista, F.V — Inst. Federal do Norte de Minas Gerais (IFNMG))

Abstract

In this work, we show how it is possible to use finite Euclidean planes to obtain a family of quasi-cyclic binary codes whose parameters are of the form $[2^{2r}, k, d]$, where $k = d = 2^r$ or $k \leq 2^r - 1$ with $d = 2^{r+1}$, where r is a positive integer. For this, we will present elements of the theory of finite fields and linear codes, which in this case are the main tools to get the generating matrices of such codes. The proposal to use the finite Euclidean plane proved to be promising, since the linear codes that will be obtained have the property of being self-orthogonal both in relation to the Euclidean inner product, and in relation to the symplectic inner product. This fact makes the quasi-cyclic codes constructed from finite Euclidean planes natural candidates for the construction of CSS quantum error-correcting codes that belong to the class of stabilizer codes.

Keywords: finite Euclidean plane, quasi-cyclic codes, self-orthogonal codes, quantum error-correcting codes, stabilizer codes

References

[1] Celniker, N. et al. Is there life on finite upper half planes?. Cont. Math., v. 143, p. 65-88, 1993.

[2] Chimal-Dzul, H.; Lieb, J.; Rosenthal, J. Generator matrices of quasi-cyclic codes over extension fields obtained from gröbner basis. IFAC-PapersOnLine, v. 55, n. 30, p. 61–66, 2022.

[3] Silva, E. B.; Carneiro, M. G.; Castelani, E. V. New quasi-cyclic codes from finite upper half-planes. Int. J. Inf. Cod. Th. IJICOT, v. 5, n. 3/4, p. 239, 2020.

[4] Güneri, C.; Özdemir, F.; Solé, P. On the additive cyclic structure of quasi-cyclic codes. Discrete Math., v. 341, n. 10, p. 2735–2741, 2018.

[5] Medrano, A. et al. Finite analogues of Euclidean space. J. Comp. App. Math., v. 68, n. 1–2, p. 221–238, 1996.

[6] Terras, A. Harmonic analysis on symmetric spaces—euclidean space, the sphere, and the Poincaré upper half-plane. Springer, 2016.

Inside the binary Golay code for minima in discrete polarization energy problems

Peter Boyvalenkov

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences

(Joint work with P. Dragnev, D. Hardin, E. Saff, and M. Stoyanova)

Abstract

We use the rich structure of the binary Golay code $\mathcal{C}_{23}$ ("probably the most important of all codes, for both practical and theoretical reasons" by MacWilliams and Sloane) to show that it provides deep views into the properties of sharp spherical codes, this time for polarization problems. The Higman-Sims graph on 100 vertices and the MacLaughlin graph on 275 vertices are described via certain construction involving the 253 minimum weight codewords of $\mathcal{C}_{23}$. This facilitates our analysis of two further sharp codes (sub-constituents of the MacLaughlin graph) which, therefore, can be also viewed inside $\mathcal{C}_{23}$. The detailed description allows us to derive explicitly the points of minima for the polarization problem under consideration. In particular, for the optimal polarization, the Higman-Sims graph splits accordingly to two copies of the Hoffman-Singleton graph.

Moreover, and not unexpected, the binary Golay code is also crucial in our description of structures which are close to the Leech lattice and its ingredients. We therefore derive optimality of a few further sharp codes and describe them and their points of minima. In particular, we obtain optimality of the kissing configuration of the Leech lattice and its derived codes of 4600 and 891 points.

Keywords: Binary Golay code, Minimum weight codewords, Higman-Sims graph, MacLaughlin graph, Maxmin polarization problem for spherical codes

Internal and external partial difference families and cyclotomy

Sophie Huczynska
University of St Andrews
(Joint work with Laura Johnson)

Abstract

Difference families have been studied since the 1930s and external difference families (EDFs) were introduced in the early 2000s, motivated by cryptography ([4]). Partial difference sets (PDSs) have also been much-studied ([3]). In this talk, I will present two recently-introduced combinatorial structures which extend these concepts in a natural way [2] - disjoint partial difference families (DPDFs) and external partial difference families (EPDFs). I will show how cyclotomic techniques in finite fields (including uniform cyclotomy [1]) can be used to construct them, and present a cyclotomic framework which also encompasses and extends various previously-known results on PDSs and EDFs.

Keywords: cyclotomy, difference families, partial difference sets

References

[1] L.D. Baumert, W.H. Mills and R. L. Ward, Uniform cyclotomy. J. Number Theory, 14 (1982), 67-82

[2] S. Huczynska and L. Johnson, Internal and external partial difference families and cyclotomy, Discrete Math. 346 (2023) 24 p., 113295.

[3] S. Ma, A survey of partial difference sets, Des. Codes Cryptogr. 4 (1994), 221-261.

[4] W. Ogata, K. Kurosawa, D.R. Stinson and H. Saido, New combinatorial designs and their application to authentification codes and secret sharing schemes, Discrete Math. 279 (2004), 383-405.