Contributed Talks

Amir Akbary-Majdabadno, University of Lethbridge

On permutation polynomials of prescribed shape

We count permutation polynomials of $\mathbb{F}_q$ which are the sum of $m+1$ monomials of prescribed degrees. This allows us to prove certain results about existence of permutation polynomials of prescribed shape.

This is a joint work with Dragos Ghioca and Qiang Wang.

Frédéric A. B. Edoukou, Nanyang Technological University

Number of points in the intersection of two quadrics defined over finite fields

Division of Mathematical Sciences,
Nanyang Technological University,
21 Nanyang Link, Singapore 637371.
E.mail : abfedoukou@ntu.edu.sg

This is a joint work with San Ling (NTU, Singapore) and Chaoping Xing (NTU, Singapore).

We denote by $\mathbb{F}_q$ the field with q elements and $\mathbb{P}^n(\mathbb{F}_q)$ the projective space of n-dimension over $\mathbb{F}_q$ and $\pi_n = \#\mathbb{P}^n(\mathbb{F}_q) = q^n + q^{n-1} + \cdots + q + 1$
In 1975, W. M. Schmidt [7., Lemma 3C, p. 175], gave an explicit upper bound for the number of points in the intersection of two hypersurfaces by using some results on the theory of resultants. For $\mathcal{Q}_1$ and $\mathcal{Q}_2$ two arbitrary quadrics with no common hyperplane in $\mathbb{P}^n(\mathbb{F}_q)$, his estimation led to the following result:

$$\#(\mathcal{Q}_1 \cap \mathcal{Q}_2) \leq 2(4q^{n-2} + 4\pi_{n-3}) + \frac{7}{q-1}.$$

In 1992, inspired by the techniques of W. M. Schmidt and the upper bound for hypersurfaces of Tsfasman-Serre-Sørensen [8], [9, Chap.2, pp.7-10], Y. Aubry [1, Theorem 3, p. 11] improved the above bound:

$$\#(\mathcal{Q}_1 \cap \mathcal{Q}_2) \leq 2(4q^{n-2} + \pi_{n-3}) + \frac{1}{q-1}.$$

In 1999, D. B. Leep and L. M. Schueller [6, p.172] improved the result of Y. Aubry under the condition that the pair of quadrics have full order. This is a very restrictive condition.
In this talk, we give the best upper bound for the number of points in the intersection of two quadrics without any condition. Our result states that

$$\#(\mathcal{Q}_1 \cap \mathcal{Q}_2) \leq 4q^{n-2} + \pi_{n-3}.$$

This result inspires us to establish a new conjecture on the number of points of an arbitrary algebraic set $X \subset \mathbb{P}^n(\mathbb{F}_q)$ of dimension s and degree d:

$$\#X(\mathbb{F}_q) \leq dq^s + \pi_{s-1}.$$

References

[1] Y. Aubry, Reed-Muller codes associated to projective varieties. In "Coding Theory and Algebraic Geometry, Luminy, 1991," Lecture Notes in Math. Vol. 1518 Springer-Verlag, Berlin, (1992), 4-17.
[2] F. A. B. Edoukou, Codes correcteurs d'erreurs construits à partir des variétés algébriques. Ph.D Thesis, Université de la Méditerranée (Aix-Marseille II), France, (2007).
[3] F. A. B. Edoukou, Codes defined by forms of degree 2 on quadric surfaces. IEEE Trans. Inf. Vol 54 N0.(2), (2008), 860-864.
[4] F. A. B. Edoukou, Codes defined by forms of degree 2 on quadric varieties in $\mathbb{P}^4(\mathbb{F}_q)$. In "Arithmetic, Geometry, Cryptography and Coding Theory", (CIRM, Marseille, France, November 5-9, 2007), Contemporary Mathematics 487, (2009), 21-32.
[5] J. W. P. Hirschfeld, General Galois Geometries, Clarendon press. Oxford 1991.
[6] D. B. Leep and L. M. Schueller, Zeros of a pair of quadric forms defined over finite field. Finite Fields and Their Applications 5 (1999), 157-176.
[7] W. M. Schmidt, Equations over finite fields. An Elementary Approach, Lecture Notes in Maths 536 (1975).
[8] J. -P. Serre, Lettre à M. Tsfasman, In "Journées Arithmétiques de Luminy (1989)", Astérisque 198-199-200 (1991), 3511-353.
[9] A. B. Sørensen, Rational points on hypersurfaces, Reed-Muller codes and algebraic-geometric codes. Ph. D. Thesis, Aarhus, Denmark, 1991.

Kseniya Garaschuk, University of Victoria

Highly nonlinear functions and exponential sums

Due to their resistance to different types of attacks on certain cryptosystems, almost perfect nonlinear (APN) and almost bent (AB) functions are well-known and widely used in cryptography. However, they can also serve as a base for obtaining different combinatorial structures, such as distance regular graphs, symmetric association schemes, uniformly packed codes and binary caps with many free pairs of points. Different techniques from numerous areas can all be successfully used in the study of highly non-linear functions and objects associated with them. To showcase this and explore interesting connections between binary linear codes, elliptic curves, APN and AB functions, we consider certain exponential sums $K(a)$, known as Kloosterman sums, when $a \in GF(2^m)$ and $a \in GF(3^m)$. Starting with a system of equations that define an APN function, we derive a family of elliptic curves that allows us to characterize all $a \in$

$GF(2^m)$ for which $K(a)$ is divisible by 3. Via a result due to Charpin, Helleseth and Zinoviev, we then get a characterization of all elements $a \in GF(2^m)$ such that $Tr(a^{1/3}) = 0$ and further generalize it to the case $Tr(a^{1/(2k-1)}) = 0$. We also establish the exact spectrum of the number of coset leaders of cosets of weight 3 of the binary Melas code. By applying a similar technique in the ternary case, we classify and count those $a \in GF(3^m)$ for which $K(a) \equiv 0, 2 \pmod 4$.

Jing He, Carleton University

A Family of Binary Sequences from Interleaved Construction and their Cryptographic Properties

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

Joint work with D. Panario and S. Wang.

Behzad Omidi Koma, Carleton University

The Number of Irreducible Polynomials of Even Degree n over $\mathbb{F}_2$ with Four Given Coefficients

The problem of estimating the number of irreducible polynomials of degree n over the finite field $\mathbb{F}_q$ with some prescribed coefficients has been largely studied. In particular, several interesting results have been obtained for the number of irreducible polynomials of degree n over $\mathbb{F}_2$ with some number of prescribed coefficients. We study the number of irreducible polynomials of even degree n over the finite field $\mathbb{F}_2$ where the coefficients of the terms x^{n-1}, x^{n-2}, x^{n-3} and x^{n-4} are given. The problem in under progress and we give preliminary results.

Joint work with D. Panario.

Amin Sakzad, Amirkabir University of Technology

Self-Inverse Interleavers for Turbo Codes

In this talk we introduce a set of new interleavers based on permutation functions with known inverses over a finite field for using in turbo codes. We use Möbius and Rédei functions in order to find new interleavers. As a byproduct, the cycle structure of Rédei functions are investigated. Finally, self-inverse versions of permutation functions are used to construct interleavers. These interleavers are their own de-interleavers and are useful for turbo coding and turbo decoding. Experiments carried out for self-inverse interleavers show excellent agreement with our theoretical results.

Georgios Tzanakis, Carleton University

On a generalization of the Hansen-Mullen Conjecture for irreducible polynomials with a fixed coefficient

Let q be a prime power and F_q be the finite field with q elements. Hansen and Mullen [1] conjecture that, given integers $n > m \geq 0$ and $a \in F_q$, there exists a monic irreducible polynomial in $F_q[x]$ of degree n with the coefficient of x^m being a. Wan [2] proves the conjecture for all but a finite number of cases for q and n, and these are settled by Ham and Mullen [3] using computer-assisted calculations. Using a variation of Wan's method we obtain a generalization of the Hansen-Mullen Conjecture to more than one fixed coefficient. For example, it follows from this generalization that, given integers $n \geq m_1 > m_2 \geq 1$ and $a_1, a_2 \in F_q$, and if $m_2 \leq n/4 - R(n,q)$ or $m_1 \geq 3n/4 + R(n,q)$ where $R(n,q) = 7\log_q(\sqrt{n}) + \log_q(\sqrt{2}) + 3$, then there exists a monic irreducible polynomial in $F_q[x]$ of degree n with the coefficients of x^{m_1} and x^{m_2} being a_1 and a_2, respectively. Our method also yields existence results for irreducible polynomials with sequences of consecutive zero coefficients.