Invited Talks

Constructing genus 2 curves over finite fields

KIRSTEN EISENTRÄGER (The Pennsylvania State University, USA)

We present an algorithm for constructing genus 2 curves over a finite field with a given number of points on its Jacobian. This has important applications in cryptography, where groups of prime order are used as the basis for discrete-log based cryptosystems. For a quartic CM field K with primitive CM type, we compute the Igusa class polynomials modulo p for certain small primes p and then use the Chinese remainder theorem and a bound on the denominators to construct the class polynomials. One part of the algorithm requires determining the endomorphism ring of Jacobians of genus 2 curves over finite fields. We will discuss some recent improvements to this.

A simplified setting for discrete logarithms in small characteristic finite fields

ANTOINE JOUX (Paris, France)

The hardness of computing discrete logarithms in finite field has served as a foundation for many public key cryptosystems. In the last two years, tremendous progress have been made in the case of small characteristic finite fields.
In this talk, we present a simplified description of the algorithmic framework that has been developed to solve this problem faster. This framework is an index calculus approach that relies on two main ingredients, the definition of the extension field and the generation of multiplicative relations in this field. Given a base field $\mathbb{F}_q$ we construct its extension field $\mathbb{F}_{q^k}$ in the following way: we find two polynomials of low degree h_0 and h_1 with coefficients in $\mathbb{F}_q$ such that $x^q h_1(x) - h_0(x)$ has an irreducible factor of degree k over $\mathbb{F}_q$.
To generate relations, we start from the well-known identity:

$$X^q - X = \prod_{c \in \mathbb{F}_q} (X - c).$$

Combining substitution of X by a fraction in the identity with the field definition, we easily obtain many multiplicative relations. This is enough to obtain the logarithms of a factor base of small degree elements in polynomial time.
Once this is done, we use a descent procedure to recursively express any element of the finite field $\mathbb{F}_q$ into elements represented by polynomials of lower degree. This procedure is quite complex but ultimately leads to a quasi-polynomial time algorithm for the discrete logarithm problem in small characteristic finite fields.
The simplified description presented in this talk is a joint work with Cécile Pierrot and also improves the complexity of the polynomial time pre-computation.

Special Monomial Maps: Examples, Classification, Open Problems

GOHAR M. KYUREGHYAN (Magdeburg, Germany)

Numerous objects in coding theory, combinatorics or cryptology can be described as (or constructed from) special types of maps on finite fields. The first step in understanding maps with particular properties is the study of such monomial maps, which surprisingly often yield even optimal solutions.

In this talk we describe monomial maps which were used to construct Kakeya sets in finite vector spaces. Further we survey progress on classification and constructions of monomial maps satisfying certain non-linearity criteria like being APN, crooked or planar.

Scattered spaces in Galois geometry

MICHEL LAVRAUW (Università di Padova, Italy)

By $\mathrm{PG}(n-1,q)$ we denote the $(n-1)$-dimensional projective space associated with the vectorspace $\mathrm{GF}(q)^n$. A *spread* in projective space is a partition of the set of points by subspaces of constant dimension. A typical example is a line spread in $\mathrm{PG}(3,q)$, in which case the set of points is partitioned by a set of q^2+1 lines. With respect to a spread $\mathcal{S}$, a subspace U is called *scattered* if U intersects each element of $\mathcal{S}$ in at most a point. In the case of a line spread in $\mathrm{PG}(3,q)$ it is straightforward to see that there exist scattered lines, but there do not exist scattered planes: every plane contains a line from $\mathcal{S}$ (exactly one to be precise). So in this case the maximal dimension of a scattered space is 1. In general the situation is obviously more complicated. A scattered space meeting the upper bound on the dimension of scattered spaces is called *maximum scattered*. In a paper with A. Blokhuis from 2000 upper and lower bounds were proved for the dimension of a maximum scattered space, and new classes of two-intersection sets (and hence two-weight codes) were constructed using scattered spaces. The study of scattered spaces was at that time motivated by the theory of blocking sets: in a paper with S. Ball and A. Blokhuis a scattered space was constructed in order to obtain a blocking set which is not the union of Baer subplanes, but of size close to the bound by Blokhuis, Storme and Szőnyi. Recently, many other applications of scattered spaces in Galois geometry have emerged. In this talk I intend to survey old and new results, and elaborate on these (and possible future) applications.

L-Polynomials of Curves over Finite Fields

GARY MCGUIRE (University College Dublin, Ireland)

We will give a gentle introduction to the topic of curves over finite fields and their L-polynomials. We consider the issue of when the L-polynomial of one curve divides the L-polynomial of another curve. Previous results in this direction use theorems of Kleiman-Serre and Kani-Rosen. We will present some new results relating this divisibility property directly to the number of rational points on the two curves. For one proof we use the theory of linear recurring sequences, which we will also introduce and summarize.

(Joint work with Omran Ahmadi and Antonio Rojas Leon)

Some Open Problems Arising from my Recent Finite Field Research

GARY L. MULLEN (The Pennsylvania State University, USA)

We will discuss a number of my favorite open problems and conjectures which have arisen in my recent research related to finite fields. These discussions will focus on a variety of areas including some theoretical topics as well as some topics from combinatorics and coding theory.

Hyperelliptic Curve Arithmetic

RENATE SCHEIDLER (University of Calgary, Canada)

Elliptic and low genus hyperelliptic curves represent a very suitable setting for public key cryptography, due to their small space requirements, efficient arithmetic and excellent security properties. Elliptic curve cryptography, for example, provides information protection in the Blackberry smartphone, Bluray technology, and other

real world applications. The points on an elliptic curve, together with the point at infinity (which functions as the identity element), form an abelian group by virtue of the cord & tangent law that declares any three collinear points on the curve to sum to zero.
While elliptic curves support simpler and faster arithmetic than their hyperelliptic counterparts, this is offset by the fact genus 2 hyperelliptic curves achieve the same level of security with a base field that is half the size of that used for elliptic curves. The cord & tangent law no longer works on curves of higher genus, such as hyperelliptic curves. Instead, the appropriate hyperelliptic generalization of the group of points on an elliptic curve is the degree zero divisor class group (aka the Jacobian variety) of the hyperelliptic curve. Classes in the Jacobian can be represented uniquely by their reduced representatives, which in turn are given in terms of their Mumford representation consisting of a pair of polynomials of small degree. This is a computationally highly useful representation that supports an efficient two-stage arithmetic comprised of addition and reduction.
This talk will provide a survey on hyperelliptic curve class group arithmetic.

Value sets of rational functions

MICHAEL ZIEVE (University of Michigan, USA)

I will present all possibilities for the approximate size of $f(\mathbf{F}_q)$ when $f(x) \in \mathbf{F}_q(x)$ is a rational function of prime degree. I will then give partial analogues for rational functions of composite degree.

Contributed Talks

Equivalence of mutually unbiased bases

KANAT ABDUKHALIKOV (UAE University)

The notion of mutually unbiased bases (MUBs) is one of the basic concepts of quantum information theory and plays an important role in quantum tomography and state reconstruction. MUBs have very close relations to other problems in various parts of mathematics, such as algebraic combinatorics, finite geometry, coding theory, Lie algebras, sequences, and spherical codes. All these branches have problems similar to MUBs, and all these problems were developed independently from others. MUBs can be constructed with the help of planar functions, commutative and symplectic semifields, and symplectic spreads [1]. We will discuss equivalence of MUBs obtained from these constructions, and their generalizations.

[1] K. Abdukhalikov, Symplectic spreads, planar functions and mutually unbiased bases, J. Algebraic Combin. (2015). http://dx.doi.org/10.1007/s10801-014-0565-y

Intersection sets, two-character multisets and associated codes

ANGELA AGUGLIA (Politecnico di Bari, Italy)

We provide a new construction of minimal intersection sets in $AG(r, q^2)$ with respect to hyperplanes, of size q^{2r-1}, sporting three intersection numbers with hyperplanes; we then use these sets to obtain linear error correcting codes with just few weights whose weight enumerator we also determine.

Furthermore, for any odd q we get a new family of two-character multisets in $PG(3, q^2)$ and we also compute the weight distribution of the two-weight codes associated to them.
The essential idea is to investigate some point-sets in $AG(r, q^2)$ satisfying the opposite of the algebraic conditions required in [1] for quasi–Hermitian varieties.

This is joint work with Luca Giuzzi.

[1] A. Aguglia, A. Cossidente, G. Korchmáros, *On quasi-Hermitian varieties*, J. Combin. Des. 20 (2012), no. 10, 433–447.

A characterization of the Artin-Mumford curve

NAZAR ARAKELIAN (University of Campinas, Brazil)

Let $\mathcal{M}$ be the Artin-Mumford curve over the finite prime field $\mathbb{F}_p$ with $p > 2$, i.e.,

$$\mathcal{M} : (x^p - x)(y^p - y) = c \in \mathbb{F}_p^*.$$

By a result of Valentini and Madan, $\mathrm{Aut}_{\mathbb{F}_p}(\mathcal{M}) \cong H$ with $H = (C_p \times C_p) \rtimes D_{p-1}$, where C_p is a cyclic group of order p and D_{p-1} is a dihedral group of order $2(p-1)$. We prove that if $\mathcal{X}$ is an algebraic curve of genus $\mathsf{g} = (p-1)^2$ defined over $\mathbb{F}_p$ such that $\mathrm{Aut}_{\mathbb{F}_p}(\mathcal{X})$ contains a subgroup isomorphic to H then $\mathcal{X}$ is birationally equivalent over $\mathbb{F}_p$ to the Artin-Mumford curve $\mathcal{M}$.

Stopping sets of Hermitian codes

SARAH E. ANDERSON (Clemson University, USA)

Stopping sets are combinatorial structures that are useful in analyzing the performance of a linear code when coupled with an iterative decoding algorithm over an erasure channel. Stopping sets have been studied for a number of codes, including Hamming codes, Reed-Muller codes, and array codes. The study of stopping sets of algebraic geometric codes was initiated by Zhang, Fu, and Wan where they demonstrate that Riemann-Roch spaces may be used to determine if a set of column indices of a parity-check matrix whose rows are precisely the nonzero codewords of the dual is a stopping set. Using these ideas, they consider algebraic geometric codes from function fields of low genus, such as the rational function field and elliptic function fields. In this talk, we consider stopping sets of Hermitian codes, the best understood class of algebraic geometric codes beyond Reed-Solomon codes.

This is joint work with Gretchen Matthews.

Randomness Properties of Some Vector Sequences Generated by Multivariate Polynomial Iterations

PINAR BALIKÇIOĞLU (Middle East Technical University Ankara, Turkey)

We examine the method of pseudorandom vector sequence generation proposed by Ostafe and Shparlinski, which is described as follows: Let p be a prime number and $F_1, ..., F_m \in \mathbb{F}_p[x_1, ..., x_m]$ be m polynomials in m variables over a finite field of p elements. For each $i = 1, ..., m$, the k-th iteration of the polynomial F_i is defined by the recurrence relation, $f_i^{(k+1)} = F_i(f_1^{(k)}, ..., f_m^{(k)}) \forall k$, where $f_i^{(0)} = X_i$. In the series of papers [1]-[4], multivariate polynomial systems $F_1, ..., F_m$ of m polynomials in m variables over a finite field $\mathbb{F}_p$ have been considered, having the "triangular" form $F_1(X) = X_1 G_1(X_2, ..., X_m) + H_1(X_2, ..., X_m)$, ..., $F_{m-1}(X) = X_{m-1} G_{m-1}(X_m) + H_{m-1}(X_m)$, $F_m(X) = g_m X_m + h_m$, with $G_i, H_i \in \mathbb{F}_p[X_{i+1}, ..., X_m]$,

$i = 1, ..., m-1$ and $g_m, h_m \in \mathbb{F}_p$, $g_m \neq 0$. In order to obtain fast pseudorandom generators, some choices for the polynomials are proposed by the same authors. For the system above, a first degree G_i polynomial with a constant H_i (Choice 1 in [1]), a second degree G_i polynomial with a constant H_i (Choice 2 in [2]), a constant G_i polynomial (with a constant H_i in Choice 3(a) [3] and with a first degree H_i in Choice 3(b) [3]) and $G_i = 1$ with "degree of $H_i = (m-i)(p-1)$" (Choice 4 in [4]). Choice 4 sequences have the maximum period p^m.
In the first part of our study, we have performed an exhaustive search in order to obtain the period distribution of the generated vector sequences generated by the first three polynomial choices for prime field sizes up to $p = 13$ and vector sizes $m = 2, 3$. For more than half of the possible sequences, we observe that the period of the vector sequence is less than p. In addition, for Choice 1, 3(a) and 3(b), there is no maximum-period sequence of period p^m. Choice 2 is more promising since sequences with period p^m do exist, although their existence probability is less than 3% for $p > 3$. Choice 2 also has smaller percentage of low-period sequences than other choices. Additionally, our exhaustive search indicates that the sequence period T_v is equal to the product of m terms, each of which can be equal either to the multiplicative order p or to a factor of the additive order $p-1$.
In the second part, we have analysed the randomness of the generated sequences with respect to their linear complexity for prime field sizes up to 31. We have observed that with very low probabilities, Choice 1 and 2 can generate sequences having high linear complexities. Changing the number of polynomials, m, does not affect the linear complexities of the sequences generated by Choice 1 and 2; however, for the sequences produced by Choice 3(a) and 3(b), rising m causes an increase in the linear complexity. We have also observed that because of having simple minimal polynomials, the sequences generated by Choice 4 have extremely low linear complexity, which is decreasing while the number of polynomials is increasing.

[1] A. Ostafe and I. E. Shparlinski, On The Degree Growth In Some Polynomial Dynamical Systems And Non-linear Pseudorandom Number Generators, 2010.

[2] A. Ostafe, Multivariate Permutation Polynomial Systems and Non-linear Pseudorandom Number Generators, 2010.

[3] A. Ostafe, Pseudorandom Vector Sequences Derived from Triangular Polynomial Systems with Constant Multipliers, 2010.

[4] A. Ostafe, Pseudorandom Vector Sequences of Maximal Period Generated by Triangular Polynomial Dynamical Systems, 2011.

Algebraic curves and Random Network Codes

DANIELE BARTOLI (Universiteit Gent, Belgium)

In their seminal paper [1], Koetter and Kschischang introduced a metric on the set of vector spaces and showed that if the dimension of the intersections of the vector spaces is large enough then a minimal distance decoder for this metric achieves correct decoding. In particular, given an r-dimensional vector space V over $\mathbb{F}_q$, the set $\mathcal{S}(V)$ of all subspaces of V forms a metric space with respect to the subspace distance defined by

$$d(U, U') = \dim(U + U') - \dim(U \cap U').$$

In this context the main problem asks for the determination of the larger size of codes in the space $(\mathcal{S}(V), d)$ with given minimum distance. Recently, Hansen [2] presented a construction of random network codes based on Riemann-Roch spaces associated to algebraic curves, describing the parameters of these codes.
We generalize this construction and we obtain new infinite families of random network codes from algebraic curves.

This is a joint work with Matteo Bonini and Massimo Giulietti.

[1] R. Koetter, F.R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory* **54**(8), (2008) 3579–3591.
[2] J.P. Hansen. Riemann-Roch spaces and linear network codes, http://arxiv.org/abs/1503.02386.

Montes Algorithm In Global Function Fields

JENS-DIETRICH BAUCH (Technische Universiteit Eindhoven, The Netherlands)

Let $A = \mathbb{F}_q[t]$ be the polynomial ring and $f \in A[x]$ a monic irreducible separable polynomial. Denote by $F/\mathbb{F}_q$ the function field determined by f and consider a given non-zero prime ideal $\mathfrak{p}$ of A. The Montes algorithm determines a new representation, so called OM-representation, of the prime ideals of the (finite) maximal order of F lying over $\mathfrak{p}$. This yields a new representation of places of function fields. In this talk we summarize briefly some applications of this new representation; that are the computation of the genus, the computation of the maximal order, and the improvement of the computation of Riemann-Roch spaces.

Right Angles in $\mathbb{F}_q^d$

MICHAEL BENNETT (University of Rochester, USA)

Here we examine an Erdős-Falconer-type problem in vector spaces over finite fields involving "right angles". Our main goal is to show that a subset $A \subset \mathbb{F}_q^d$ of size $\gg q^{\frac{d+2}{3}}$ contains three points a, b, c so that $(a-b)\cdot(c-b) = 0$. We will then define "spread", which is the finite field analog to Euclidean angle measure, and provide additional extremal results for nonzero spread. At the end we will present some sharpness examples.

The Cardinality of Sets of k-Independent Vectors over Finite Fields and their Connection to Matroids

DANIEL CAPODILUPO (University of Michigan, USA)

A matroid is a combinatorial object that generalizes the notion of independence. In this talk, we study the cardinality of sets of vectors over finite fields $\mathbb{F}_q$, where q is a power of a prime and examine how this circle of ideas relate to matroids.

This is joint work with Steven Damelin (Mathematical Reviews and the University of Michigan), Samuel Freedman (University of Michigan), Michael Hua (University of Michigan), Jeffrey Sun (University of Michigan) and Ming Yu (Australia National University).

More $\mathcal{PS}$ and $\mathcal{H}$-like bent functions

CLAUDE CARLET (University of Paris 8 and Paris 13, France)

Two general classes (constructions) of bent functions are derived from the notion of spread. The first class, $\mathcal{PS}$, gives a useful framework for designing bent functions which are constant (except maybe at 0) on each of the m-dimensional subspaces of $\mathbb{F}_{2^{2m}}$ belonging to a partial spread. Explicit expressions (which may be used for applications) of bent functions by means of the trace can be derived for subclasses corresponding to some partial spreads, for instance the $\mathcal{PS}_{ap}$ class. Many more can be. The second general class, H, later slightly modified into a class called $\mathcal{H}$ so as to relate it to the so-called Niho bent functions, is (up to addition of affine functions) the set of bent functions whose restrictions to the subspaces of the Desarguesian spread (the spread of all multiplicative cosets of $\mathbb{F}_{2^m}^*$, added with 0, in $\mathbb{F}_{2^{2m}}^*$) are linear. It has been observed that the functions in $\mathcal{H}$

are related to o-polynomials, and this has led to several classes of bent functions in bivariate trace form. In this paper, after briefly looking at the $\mathcal{PS}$ functions related to the André spreads, and giving the trace representation of the $\mathcal{PS}$ corresponding bent functions and of their duals, we show (as Çeşmelioglu, Meidl and Pott also do independently in a paper to appear) that it is easy to characterize those bent functions whose restrictions to the subspaces of a spread are linear, but that it leads to a notion extending that of o-polynomial, for which it seems a hard task to find examples. We illustrate this with the André spreads and also study three other cases of $\mathcal{H}$-like functions (related to other spreads).

Acknowledgement We are indebted to William Kantor who gave very useful information on spreads.

On Reed-Muller type codes defined over a rational normal scroll

CÍCERO CARVALHO (Universidade Federal de Uberlândia, Brazil)

In this talk we would like to present some results on codes obtained by the evaluation of homogeneous polynomials of a fixed degree on the points of a projective variety, namely a rational normal scroll. The scroll is a projective surface S which may be defined as

$$S = \left\{ (x_0 : \cdots : x_\ell) \in \mathbf{P}^\ell(\mathbf{F}_q) \mid \operatorname{rank} \begin{pmatrix} x_0 & \cdots & x_{n-1} & x_{n+1} & \cdots & x_{\ell-1} \\ x_1 & \cdots & x_n & x_{n+2} & \cdots & x_\ell \end{pmatrix} = 1 \right\},$$

where n and ℓ are positive integers with $n \leq \ell - 2$, and $\mathbf{F}_q$ is a finite field with q elements. Let I_S be ideal of the set of points $P_1, \ldots, P_N$ of the scroll. For a fixed nonnegative integer d denote by $\mathbf{F}_q[\mathbf{X}]_d$ the $\mathbf{F}_q$-vector space of homogeneous polynomials of degree d in $\mathbf{F}_q[X_0, \ldots, X_\ell]$ and let $I_S(d) = I_S \cap \mathbf{F}_q[\mathbf{X}]_d$. Let $C(d)$ be the image of the evaluation morphism $\varphi : \mathbf{F}_q[\mathbf{X}]_d / I_S(d) \to \mathbf{F}_q^N$ defined by $\varphi(f + I_S(d)) = (f(P_1), \ldots, f(P_N))$. We will show how to determine the length, the dimension and a lower bound for the minimum distance of the code $C(d)$, and in many cases we will present the exact value of the minimum distance. These results were obtained by adapting a method that has been successfully used to determine the parameters of certain affine variety codes, and uses tools coming from Gröbner bases theory.

The talk will be based on a joint work with Victor G.L. Neumann, to appear in Finite Fields and Their Applications.

Using Permutation Polynomials to Coordinatize Finite Projective Planes

CHRIS CASTILLO (University of Delaware, USA)

We will show that certain finite projective planes, including type II.2 planes, always possess a coordinatization where multiplication is represented by a bivariate polynomial over a finite field which arises from a certain construction method. This method can also be used to construct groups of (univariate) permutation polynomials, and there is some amount of translation between the structure of the group and the structure of the polynomials representing it.

On a Generalization of Cusick-Li-Stănică's Conjecture about Balanced Elementary Symmetric Boolean Functions to Finite Fields of Odd Characteristic

FRANCIS N. CASTRO (University of Puerto Rico)

In this work we give an affirmative answer to some of the open cases of Cusick-Li-Stănică's conjecture about balanced elementary symmetric Boolean Functions. Also, we state a generalization of Cusick-Li-Stănică's

conjecture about balanced elementary symmetric functions for finite fields of characteristic $p > 2$. In particular, we prove that this conjecture is true for many families.

This work is jointly with: R. Arce, O. Gonzalez, L. Medina, R. Negrón and I. Rubio

Coordinatising projective planes using finite fields

ROBERT COULTER (University of Delaware, USA)

We revisit the method of coordinatising projective planes, which produces a planar ternary ring (PTR), a three-variabled function defined on the labelling set, containing the algebraic properties of the plane. For planes of prime power order q, the finite field $\mathbb{F}_q$ can be used as the labelling set. This leads to the concept of a PTR polynomial. Restrictions on the general form of a PTR polynomial are then derived from the properties a PTR function must exhibit. With further assumptions on the plane, further restrictions on the PTR polynomial can be derived.

On scattered linear sets of pseudoregulus type in $\mathrm{PG}(1, q^t)$

BENCE CSAJBÓK (University of Padova, Italy)

Linear sets of a finite projective space generalize the concept of a subgeometry. In the recent years they have been used to construct or characterize various objects in finite geometry, such as blocking sets, two-intersection sets in finite projective spaces, translation spreads of the Cayley Generalized Hexagon, translation ovoids of polar spaces, semifield flocks, semifield spreads and finite semifields. A point set $L \subseteq \mathrm{PG}_{q^t}(\mathbb{F}_{q^t}^r) = \mathrm{PG}(r-1, q^t)$ is said to be $\mathbb{F}_q$-*linear* (or simply *linear*) *of rank* n if an n-dimensional $\mathbb{F}_q$-space S of $\mathbb{F}_{q^t}^r$ exists such that

$$L = \{\mathrm{PG}_{q^t}(T)\colon\ T \text{ is a one-dimensional } \mathbb{F}_{q^t}\text{-space of } \mathbb{F}_{q^t}^r \text{ and } T \cap S \neq \{0\}\}.$$

Lunardon and Polverino characterized linear sets as projections of canonical subgeometries. Let $\Sigma \cong \mathrm{PG}(n-1, q)$ be a canonical subgeometry of $\Sigma^* = \mathrm{PG}(n-1, q^t)$. Let $\Gamma \subset \Sigma^* \setminus \Sigma$ be an $(n-1-r)$-space and let $\Lambda \subset \Sigma^* \setminus \Gamma$ be an $(r-1)$-space of Σ^*. Denote the projection of Σ from *center* Γ to *axis* Λ by $L = p_{\Gamma,\Lambda}(\Sigma) := \{\langle \Gamma, P\rangle \cap \Lambda\colon\ P \in \Sigma\}$.
The result of Lunardon and Polverino states that L is an $\mathbb{F}_q$-linear set of rank n with $\langle L\rangle = \Lambda$, and conversely, if L is an $\mathbb{F}_q$-linear set of rank n of $\Lambda = \mathrm{PG}(r-1, q^t) \subset \Sigma^*$ with $\langle L\rangle = \Lambda$, then there is an $(n-1-r)$-space Γ disjoint from Λ and a canonical subgeometry $\Sigma \cong \mathrm{PG}(n-1, q)$ disjoint from Γ such that $L = p_{\Gamma,\Lambda}(\Sigma)$.
The maximum size of an $\mathbb{F}_q$-linear set of rank n is the number of points of $\mathrm{PG}(n-1, q)$. A linear set is called *scattered*, if its size attains this upper bound. In $\mathrm{PG}(1, q^3)$ there is a unique scattered linear set of rank 3 up to projective equivalence. This linear set is *of pseudoregulus type*, which is a family of scattered linear sets of rank tn in $\mathrm{PG}(2n-1, q^t)$, $n \geq 1$, $t \geq 3$, defined by Lunardon, Marino, Polverino and Trombetti; and by Lavrauw and Van de Voorde.
In this talk we give a geometric characterization of the projecting configurations (Γ, Σ), such that $L := p_{\Gamma,\Lambda}(\Sigma)$ is a linear set of pseudoregulus type in the line Λ. We show that the preimage $p_{\Gamma,\Lambda}^{-1}(r)$ of any q-order subline $r \subseteq L$ is a rational normal curve in Σ. This extends a result of Lavrauw and Van de Voorde who proved the same in $\mathrm{PG}(1, q^3)$. In the proof we use some properties of a degree t hypersurface of $\mathrm{PG}(2t-1, q)$ studied by Lavrauw, Sheekey and Zanella. Our proof also involves the study of point sets $\ell^d := \{\langle z^d\rangle_q\colon\ z \in \mathbb{F}_{q^t},\ \langle z\rangle_q \in \ell\}$, where ℓ is a line of $\mathrm{PG}_q(\mathbb{F}_{q^t})$ and d is an integer of a special form. It is well-known that ℓ^{-1} is a rational normal curve. We generalize this result
One of the most natural questions about linear sets is their equivalence. Let L be a linear set of pseudoregulus type in $\Lambda = \mathrm{PG}(1, q^t)$, $t = 5$ or $t > 6$. We show that there exist projective configurations (Γ, Σ) and (Γ', Σ') such that $L = p_{\Gamma,\Lambda}(\Sigma) = p_{\Gamma',\Lambda}(\Sigma')$ and there is no collineation mapping Γ to Γ' and Σ to Σ'. We give a characterization of linear sets L for which $L = p_{\Gamma,\Lambda}(\Sigma) = p_{\Gamma',\Lambda}(\Sigma')$ implies PΓL-equivalence of the projective configurations (Γ, Σ) and (Γ', Σ').

Joint work with Corrado Zanella.

Near complete external difference sets

JAMES A. DAVIS (University of Richmond, USA)

We introduce near-complete external difference families, a partitioning of the nonidentity elements of a group so that each nonidentity element of the group can be written as a difference of elements from distinct subsets a fixed number of times. We provide examples and general constructions at least some of which lead to new parameter families of near-resolvable designs. Construction techniques include cyclotomy, partial difference sets, and Galois Rings.

This is joint work with Gary Mullen and Sophie Huczynska.

A Polynomial Type Oil-Vinegar Signature

ADAMA DIENE (United Arab Emirates University)

An oil-vinegar scheme (OV) is a signature scheme based on multivariate quadratic polynomials over finite fields. The system contains m equations and n variables divided into two groups; v variables called "vinegar variables" and o variables called "oil variables". The scheme is called balanced oil-vinegar scheme or unbalanced oil-vinegar scheme (UOV) depending whether or not $v = o$. These schemes are very fast and require modest computational resources, which make them ideal for low cost devices like smartcards. The balanced one has been already broken and it is proven that the unbalance one is very vulnerable for many choices of the parameters. In this paper, we propose a polynomial type of these schemes. The main idea of our construction, is to use matrices whose entries are product of randomly chosen polynomials and through matrix multiplication, we obtain the central map. We call this new signature scheme PTOV scheme. It can be as efficient as the UOV but with higher security claims. Some parameters for practical and secure implementation are also proposed.

Expander graphs and linear codes

MICHAEL DOWLING (Clemson University, USA)

Expander graphs are highly connected sparse finite graphs. They play an important role in several areas of mathematics, including number theory (e.g. sieves for primes in group orbits), representation theory and geometric embeddings. They are also featured in theoretical computer science and in digital signal processing in applications such as communication network designs, pseudorandom number generators, compressive sensing, and algorithm designs, among others. In this talk, we present a survey of expander graphs (including Ramanujan graphs) and their connections to constructions of expander codes (or LDPC codes) that can be decoded by fast algorithms. In particular, we show that expander codes from bipartite graphs with an arbitrary vertex expansion can be decoded in linear time (assuming the inner code has certain minimum distance depending on the expansion factor), which improves previous work of Sipser and Spielman (1996), Feldman et. al. (2007), and Viderman (2013).

This is joint work with Shuhong Gao.

Complete and Nearly-Complete Sets of Class-r Hypercubes

DANIEL DROZ (The Pennsylvania State University, USA)

Latin squares are combinatorial objects, but many of the most elegant and useful results about them come from finite-field constructions. A latin square of order q is a square array on q symbols such that each symbol occurs

once in each row and column. Two latin squares are called orthogonal when superimposing them gives each of the q^2 ordered pairs of symbols exactly once. It is well known that if q is a prime power, the squares formed from the polynomials $ax + y$, $a \in \mathbb{F}_q$ form $q - 1$ latin squares which are mutually orthogonal (each pair of squares is orthogonal).
Extending the definition of orthogonality of latin squares to latin hypercubes always features a slight inelegance: when the dimension is d, superimposing two hypercubes of order q produces q^d pairs; since only q symbols are used, we define orthogonality to occur when each of the q^2 possible pairs occurs q^{d-2} times. The uniqueness of all pairs is so appealing in the case of $d = 2$ that it seems worthwhile to search for a higher-dimensional situation that replicates it. We can achieve this by introducing a larger alphabet: a class-r latin hypercube of dimension d, type j, and order q is a d-dimensional array, q units in each direction, on an alphabet of q^r symbols such that by fixing any j coordinates, the q^{d-j} symbols remaining have each symbols repeated exactly q^{d-j-r} times. Usually $j = d - r$ so that we have each symbol occurring once. When $r = j$ and $d = 2r$, we can define a "unique-pairs" orthogonality, since superimposing two hypercubes gives q^{2r} pairs, and the longer alphabet produces $(q^r)^2$ pairs.
Ethier et al. (citation below) established an upper bound on sets of mutually orthogonal class-r hypercubes ($q^r - 1$) and showed that such sets can be constructed from a set of matrices over $\mathbb{F}_q$ satisfying certain conditions. The authors constructed complete sets for most cases where $r = 2$. Addressing two open problems left from this work, we have successfully constructed suitable sets of matrices for all larger values of r; we also give some attention to the cases where the original method failed to produce complete sets, giving large though not quite complete sets of hypercubes in these cases.

Ethier/Mullen/Panario/Stevens/Thomson, "Sets of orthogonal hypercubes of class r," J. Combin. Thy., A 2011.

From r-Linearized Polynomial Equations to r^m-Linearized Polynomial Equations

NERANGA FERNANDO (Northeastern University Boston, USA)

Let r be a prime power and $q = r^m$. For $0 \leq i \leq m-1$, let $f_i \in \mathbb{F}_r[\mathtt{X}]$ be q-linearized and $a_i \in \mathbb{F}_q$. Assume that $z \in \overline{\mathbb{F}}_r$ satisfies the equation $\sum_{i=0}^{m-1} a_i f_i(z)^{r^i} = 0$, where $\sum_{i=0}^{m-1} a_i f_i^{r_i} \in \mathbb{F}_q[\mathtt{X}]$ is an r-linearized polynomial. We show that z satisfies a q-linearized polynomial equation with coefficients in $\mathbb{F}_r$. This result provides an explanation for numerous permutation polynomials previously obtained through computer search.

This is a joint work with Xiang-dong Hou.

Rational points and Galois points for a plane curve over a finite field

SATORU FUKASAWA (Yamagata University, Japan)

We study the relationship between rational points and Galois points for a plane curve over a finite field.
We recall the definition of Galois point, which was given by H. Yoshihara in 1996. Let $C \subset \mathbf{P}^2(k)$ be an irreducible plane curve of degree $d \geq 4$ over an algebraically closed field k of characteristic $p \geq 0$ and let $K(C)$ be its function field.
A point $P \in \mathbf{P}^2(k)$ is said to be Galois for C, if the function field extension $K(C)/\pi_P^* K(\mathbf{P}^1)$ induced by the projection $\pi_P : C \to \mathbf{P}^1(k)$ from P is Galois. We denote by $\Delta(C)$ the set of all Galois points on the projective plane.
Let C be a plane curve over a finite field $\mathbf{F}_q$ which is irreducible over the algebraic closure $\overline{\mathbf{F}}_q$.
We consider Galois points over $\overline{\mathbf{F}}_q$. Summarizing the results of Homma (2006) and Fukasawa (2010, 2013), we have the following very interesting theorem.

Fact (Homma, Fukasawa)**.**

(1) For the Hermitian curve $H_{\sqrt{q}+1}$: $X\sqrt{q}Z + XZ\sqrt{q} - Y\sqrt{q}+1 = 0$, $\Delta(H_{\sqrt{q}+1}) = \mathbf{P}^2(\mathbf{F}_q)$.
(2) For the Klein quartic curve K_4: $(X^2+XZ)^2+(X^2+XZ)(Y^2+YZ)+(Y^2+YZ)^2+Z^4 = 0$ in $p = 2$, $\Delta(K_4) = \mathbf{P}^2(\mathbf{F}_2)$.
(3) For the Ballico-Hefez curve B_{q+1}, which is the image of the morphism $\mathbf{P}^1 \to \mathbf{P}^2$; $(s : t) \mapsto (s^{q+1} : (s+t)^{q+1} : t^{q+1})$, $\Delta(B_{q+1}) = \mathbf{P}^2(\mathbf{F}_q)$.

We propose the following problem:

Problem. Let C be a plane curve over $\mathbf{F}_q$. Assume that $\Delta(C) = \mathbf{P}^2(\mathbf{F}_q)$. Then, is it true that C is projectively equivalent to the Hermitian, Klein quartic or Ballico-Hefez curve?

When C is smooth, it is already known that the answer is affirmative (Fukasawa 2013). Therefore, we consider singular curves. Let C_{sm} be the smooth locus of C. When $C_{\mathrm{sm}}(\mathbf{F}_q) \neq \emptyset$ and the geometric genus of C is zero or one, we give an affirmative answer. The following is the main theorem.

Theorem. Assume that the geometric genus of C is zero or one. Then, $C_{\mathrm{sm}}(\mathbf{F}_q) \neq \emptyset$ and $\Delta(C) = \mathbf{P}^2(\mathbf{F}_q)$ if and only if C is projectively equivalent to the Ballico-Hefez curve B_{q+1} (over $\mathbf{F}_q$).

Almost perfect nonlinear functions which are not equivalent to permutations

FARUK GÖLOĞLU (KU Leuven, Belgium, and CU Prague, Czech Republic)

Almost perfect nonlinear (APN) functions are cryptographically important functions. Gold functions $x \mapsto x^{2^k+1}$ with $(n,k) = 1$ provide an infinite family of examples for all n. For cryptographical purposes, existence of APN funtions which are permutations is an important problem. Gold functions are permutations of $GF(2^n)$ when n is odd, and three-to-one on $GF(2^n)^*$ when n is even. There are no APN permutations for $n = 2$ and $n = 4$. Dillon gave the first example of an APN permutation on an even extension ($n = 6$) during F_q9 in Dublin [1]. The APN permutation is CCZ-equivalent to the quadratic function $\kappa(x)$ on $GF(2^6)$ [1].
The question of existence of APN permutations on even $n > 6$ is an open problem. All the known functions on even dimensions $n < 12$ were shown to be inequivalent to permutations by computer search. We will present (to our knowledge, first) theoretical inequivalence results for infinite families of APN functions, including the Gold functions.

This is joint work with Philippe Langevin.

[1] BROWNING, K., DILLON, J., MCQUISTAN, M., AND WOLFE, A. An APN permutation in dimension six. In *Finite fields. Theory and applications. Proceedings of the 9th international conference on finite fields and applications, Dublin, Ireland, July 13–17, 2009*. Providence, RI: American Mathematical Society (AMS), 2010, pp. 33–42.

Cyclotomic polynomials of the second kind part 2

JAVIER GOMEZ-CALDERON (The Pennsylvania State University, USA)

We define a set of polynomials that can be seen as cyclotomic polynomials of the second kind. We relate these polynomials with the well-known Dickson Polynomials and provide a recursive method for their evaluation. We also show an integral basis for the number fields generated by these polynomials.

On Repeated-Root Constacyclic Codes of Length $2^a mp^r$ over Finite Fields

K. GUENDA (University of Algiers)

The class of constacyclic codes over finite fields is an important class of linear codes, as these codes include the family of cyclic codes. These codes also have many practical applications as they can be efficiently encoded using simple shift register circuits. They have a rich algebraic structure which can be used for efficient error detection and correction. As a consequence, they are preferred in numerous applications.
Recently, H.Q. Dinh in a series of papers determined the generator polynomials of constacyclic codes over F_q of lengths $2p^r$, $3p^r$ and $6p^r$. These results have subsequently been extended to more general code lengths. In this paper, we extend the results of Batoul, Guenda and Gulliver concerning the constacyclic codes to the repeated root constacyclic codes of length $2^a mp^r$ over F_{p^s}, where $a \geq 1$ and m is an odd integer with $(m, p) = 1$. We give the structure of the generator polynomial of constacyclic codes of length mp^r and more generally the generators of constacyclic codes of length $2^a mp^r$. Further, cases where the constacyclic codes are equivalent to cyclic codes are given. It is well known that the only self-dual constacyclic codes over finite fields are either cyclic codes with even characteristic or negacyclic codes. Thus, we give conditions on the existence of self-dual negacyclic codes of length $2^a mp^r$ over F_{p^s} where p is odd.

Flat polynomials, difference sets and cyclotomy

CHRISTIAN GÜNTHER (Otto-von-Guericke-University Magdeburg, Germany)

We consider the problem, independently raised by Littlewood and Golay, of constructing polynomials with all coefficients in $\{-1, 1\}$ and large merit factor. Equivalent formulations involve the minimisation of the L^4 norm on the unit circle of such polynomials or the minimisation of the mean-squared aperiodic autocorrelations of binary sequences. This problem arises naturally in complex analysis, condensed matter physics, and digital communications engineering.
Most known constructions arise from classical difference sets in cyclic groups, namely Paley and Singer difference sets. After a review of known constructions, I will present more recent results involving cyclotomy and other difference sets. These constructions provide the first essentially new examples since 1991, answer questions posed by Jensen, Jensen, and Høholdt; and prove conjectures due to Jedwab, Katz, and Schmidt.

This talk is based on joint work with Kai-Uwe Schmidt.

The operational degree of Gröbner basis algorithms for systems of equations over finite fields

TIMOTHY J HODGES (University of Cincinnati, USA)

Multivariate public key cryptosystems have public keys that are multivariate polynomial functions over a finite field. Thus the problem of solving systems of such equations is fundamental to understanding the security of such systems. Analysis of the operational degree of Gröbner basis algorithms raises numerous difficult algebraic questions, many of which have remained open for 10 years. We review some of these problems, their importance and recent successes and failures in answering them.

Permutation Polynomials of $\mathbb{F}_{q^2}$ of the Form $a\mathtt{X} + \mathtt{X}^{r(q-1)+1}$

XIANG-DONG HOU (University of South Florida, USA)

Let q be a prime power, $2 \leq r \leq q$, and $f = a\mathtt{X} + \mathtt{X}^{r(q-1)+1} \in \mathbb{F}_{q^2}[\mathtt{X}]$, where $a \neq 0$. The conditions on r, q, a that are necessary and sufficient for f to be a permutation polynomial (PP) of $\mathbb{F}_{q^2}$ are not known. The question concerning the permutation property of this type of polynomials becomes increasingly interesting because of some recent results. When $a^{q+1} = 1$, it is known that f is a PP of $\mathbb{F}_{q^2}$ if and only if $(-a)^{(q+1)/\gcd(r,q+1)} \neq 1$ and $\gcd(r-1, q+1) = 1$ [4]. In the general situation, that is, without the assumption that $a^{q+1} = 1$, all PPs of the above type have been determined for $r = 2, 3, 5, 7$ [1, 2, 3]. It turns out that for $r = 3, 5, 7$ and $a \in \mathbb{F}_{q^2}^*$ with $a^{q+1} \neq 1$, there are numerous but *finitely many* (q, a) for which f is a PP of $\mathbb{F}_{q^2}$. A conjecture has been formulated based on this observation:

Conjecture. Let $r > 2$ be a fixed prime. Under the assumption that $a^{q+1} \neq 1$ ($a \in \mathbb{F}_{q^2}^*$), there are only finitely many (q, a) for which f is a PP of $\mathbb{F}_{q^2}$.

In this talk we will outline a proof of this conjecture.

[1] X. Hou, *Determination of a type of permutation trinomials over finite fields, II*, Finite Fields Appl. 35 (2015) 16 – 35.

[2] X. Hou and S. D. Lappano, *Determination of a type of permutation binomials over finite fields*, J. Number Theory 147 (2015), 14 – 23.

[3] S. D. Lappano, *A note regarding permutation binomials over* $\mathbb{F}_{q^2}$, Finite Fields Appl. 34 (2015), 153 – 160.

[4] M. E. Zieve, *Permutation polynomials on* $\mathbb{F}_q$ *induced from bijective Rédei functions on subgroups of the multiplicative group of* $\mathbb{F}_q$, `arXiv:1310.0776`, 2013.

Lower Bounds for Maximal Sets such that Basis Size Subsets are Bases over Finite Fields

MICHAEL HUA (University of Michigan, USA)

In this talk we will discuss lower bounds for the maximal size of sets over Finite Fields $\mathbb{F}_q$ where q is a power of a prime. Our sets have the property that subsets of basis size are bases. We will discuss a Pascal approach to this problem.

This is joint work with Daniel Capodilupo (University of Michigan), Steven Damelin (Mathematical Reviews and the University of Michigan), Samuel Freedman (University of Michigan, Jeffrey Sun (University of Michigan) and Ming Yu (Australian National University).

On Complete Mappings of Finite Fields

LEYLA IŞIK (Sabancı University, Turkey)

In this work, we present a new method for constructing complete mappings of finite fields. We also discuss value sets of particular classes of polynomials over finite fields.

Proof of a Conjecture of Dobbertin, Helleseth, Kumar, and Martinsen on Three-Level Cross-correlation

DANIEL J. KATZ (California State University Northridge, USA)

Weil sums of binomials arise naturally in arithmetic calculations, and in several applications: they give the nonlinearity of finite field power permutations in cryptography, the cross-correlation between two maximal linear sequences in digital sequence design, and the weight distribution of certain cyclic error-correcting codes. Consider the Weil sum

$$W_{q,d}(a) = \sum_{x \in \mathbb{F}_q} \psi_q(x^d - ax),$$

where

- ψ_q is the canonical additive character of finite field $\mathbb{F}_q$,
- $\gcd(d, q-1) = 1$, so that $x \mapsto x^d$ is a permutation of $\mathbb{F}_q$,
- d not a power of p modulo $q-1$, to prevent $\psi_q(x^d - ax)$ degenerating to $\psi_q((1-a)x)$, and
- $a \in \mathbb{F}_q^*$.

Fix q and d and consider the spectrum of values $W_{q,d}(a)$ obtained as a runs through $\mathbb{F}_q^*$. In 1976, Helleseth showed that at least three distinct values must appear. From 1966 to the present, only nine infinite families of (q, d) pairs that furnish three-valued spectra have been found. These furnish power permutations with three-valued Walsh spectra, pairs of m-sequences with three-level cross-correlation, and cyclic codes with two zeroes whose duals have three nonzero weights.
In 2001 Dobbertin, Helleseth, Kumar, and Martinsen conjectured another infinite family of m-sequence pairs with three-valued cross-correlation, or equivalently, an infinite family of three-valued Weil sums of binomials. Their family uses fields of order $q = 3^n$ with n odd, and exponent $d = 3^r + 2$ with $4r \equiv 1 \pmod{n}$. We prove their conjecture, thus adding a tenth infinite family of three-valued Weil sums of binomials. The proof employs diverse methods involving trilinear forms, counting points on curves via multiplicative character sums, and divisibility properties of Gauss sums. Computational graph theory techniques inspired by Hollmann and Xiang are used, and a computer-free proof is also given.

This is joint work with Philippe Langevin of Université de Toulon.

Pseudo-Randomness of Elliptic Curve Encoding Functions

TAECHAN KIM (NTT Secure Platform Laboratories, Japan)

Let E be an elliptic curve defined over the finite field $\mathbb{F}_p$ (a prime field, say) and $f\colon \mathbb{F}_p \to E(\mathbb{F}_p)$ a point encoding function in the sense of [2]. To fix ideas, we can take f to be Icart's function [1]. Since $f(\mathbb{F}_p)$ consists of about $5/8$ of all $\mathbb{F}_p$-points on the elliptic curve, and since membership testing is easy, one can efficiently distinguish between the x-coordinate of a random image of f and that of a random point in $E(\mathbb{F}_p)$.
On the other hand, Farashahi et al. [2] have shown that the bit string formed by (slightly fewer than) the lower *half* bits of the x-coordinate of $f(u)$ for a random $u \in \mathbb{F}_p$ is indistinguishable from a random bit string of the same length (and in particular, it is also indistinguishable from the corresponding lower order bits of the x-coordinate of a random point in $E(\mathbb{F}_p)$).
In this talk, we improve this result by showing that we can in fact take *almost all* bits of $f(u)$ and still get a bit string that is indistinguishable from random. Precisely, we prove the following theorem:

Theorem. *Let U_k and $U_{\mathbb{F}_p}$ denote the uniform distributions over $\{0,1\}^k$ and $\mathbb{F}_p$, respectively. For $u \in \mathbb{F}_p$, denote the k least significant bits of the x-coordinate of $f(u) \in E(\mathbb{F}_p)$ by $\mathrm{LSB}_{x,k}(f(u))$. Then, the statistical distance between the distribution $\mathrm{LSB}_{x,k}(f(U_{\mathbb{F}_p}))$ and the uniform distribution satisfies:*

$$\mathrm{SD}\left(\mathrm{LSB}_{x,k}\left(f(U_{\mathbb{F}_p})\right), U_k\right) = O\left(\frac{2^k \log_2(p)}{p}\right),$$

where the implied constant in the big O is absolute. In particular, the two distribution are indistinguishable as soon as $k \leq (1-\epsilon)\log_2(p)$ for some $\epsilon > 0$.

Moreover, this result generalizes easily to other rational maps than the x-coordinate, and to arbitrary elliptic curve encoding functions.

Joint work with Mehdi Tibouchi.

[1] T. Icart, "How to hash into elliptic curves," in S. Halevi (Ed.), *CRYPTO*, LNCS vol. 5677, Springer, 2009, pp. 303–316.

[2] R.R. Farashahi, P.-A. Fouque, I.E. Shparlinski, M. Tibouchi and J.F. Voloch, *Indifferentiable deterministic hashing to elliptic and hyperelliptic curves*, Math. Comp. **82**(281), AMS, 2013, pp. 491–512.

The second largest number of points of plane curves over finite fields

SEON JEONG KIM (Gyeongsang National University, Korea)

In [1], we proved the Sziklai bound:

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

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

except for the curve over $\mathbb{F}_4$ which is projectively equivalent to the curve defined by the equation

$$X^4 + Y^4 + Z^4 + X^2Y^2 + Y^2Z^2 + Z^2X^2 + X^2YZ + XY^2Z + XYZ^2 = 0$$

Since the number of points in $\mathbb{P}^2(\mathbb{F}_q)$ is $q^2 + q + 1$, the Sziklai bound makes sense in the range $2 \leq d \leq q + 2$. We know that for $d = 2$, $\sqrt{q} + 1$ (if q is square), $q - 1$, q, $q + 1$ and $q + 2$, this bound is sharp. Thus, for those degrees, it is natural to consider the second largest number for $N_q(C)$.
In this talk, we give the second largest number of points on plane curves of degree d for $d = q + 2$ and $q + 1$.

Collaboration with Masaaki Homma, Kanagawa University, Japan.

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

Full Degree Two Del Pezzo Surfaces

AMANDA KNECHT (Villanova University, USA)

A smooth two dimensional variety X defined over a field k is called a *del Pezzo* surface if its anticanonical divisor $-\omega_X$ is ample. The *degree* d of a del Pezzo surface is the self intersection number of its canonical class and $1 \leq d \leq 9$. The most popular examples of del Pezzo surfaces are cubic surfaces because they are the zero sets of degree three homogeneous polynomials in four variables. Over algebraically closed fields, the geometry of del Pezzo surfaces is well understood. For example, we know exactly how many lines each surface contains based on the degree. Over finite fields, these lines may not be defined. In the rare case that they are all defined over the finite field, we call the surface split. Hirschfeld classified split del Pezzo surfaces of degree at least three whose points are all contained on the lines in the surface. We continue his work and begin the classification of split degree two del Pezzo surfaces over finite fields whose points are all on the fifty-six lines of the surfaces.

Value sets of Lattès maps over finite fields

ÖMER KÜÇÜKSAKALLI (Middle East Technical University Ankara, Turkey)

We give an alternative computation of the value sets of Dickson polynomials over finite fields by using a singular cubic curve. Our method is not only simpler but also it can be generalized to the non-singular elliptic case. We determine the value sets of Lattès maps over finite fields which are rational functions induced by isogenies of elliptic curves with complex multiplication.

A family of permutation trinomials over $\mathbb{F}_{q^2}$

STEPHEN LAPPANO (University of South Florida, USA)

Let p be an odd prime, and q a power of p. Define $g_r = x^r(a + bx^{q-1} + x^{2(q-1)}) \in \mathbb{F}_q[x]$. When $r = 1$, Hou proved that the map $x \mapsto g_1(x)$ induces a permutation on $\mathbb{F}_{q^2}$ if and only if one of the following occurs:

(I) $a(a-1)$ is a square in $\mathbb{F}_q^\times$, and $b^2 = a^2 + 3a$.

(II) $a = 1$, and $b^2 - 4$ is a square in $\mathbb{F}_q^\times$.

(III) $a = 3, b = 0, q \equiv -1 \pmod 6$.

(IV) $a = b = 0, q \equiv 1, 3 \pmod 6$.

When $r = 3$, we employ a similar method to show the map $x \mapsto g_3(x)$ induces a permutation on $\mathbb{F}_{q^2}$ if and only if one of the following occurs:

(A) $a = b = 0$, and $(2q + 1, q^2 - 1) = 1$.

(B) $a = 1$, and $b^2 - 4$ is a square in $\mathbb{F}_q^\times$.

(C) $b = 0$, and one of the following occurs:

  (a) $a = 1$, and $q \equiv 1 \pmod 4$.

  (b) $a = \dfrac{1}{3}$, and $q \equiv -1 \pmod 6$.

  (c) $a = -\dfrac{1}{3}$, and $q \equiv -1 \pmod{12}$.

(D) $a = 0$ and $b \neq \pm 1$.

(E) $a(a-1)b \neq 0, b^2 = 3a + 1$, and $1 - a$ is a square in $\mathbb{F}_q^\times$.

We also comment on the situation when r is an odd integer greater than 3.

Connectivity of some algebraically defined digraphs

FELIX LAZEBNIK (University of Delaware, USA)

Let p be a prime, e a positive integer, $q = p^e$, and let $\mathbb{F}_q$ denote the finite field of q elements. Let $f_i \colon \mathbb{F}_q^2 \to \mathbb{F}_q$ be arbitrary functions, where $1 \leq i \leq l$, i and l are integers. The digraph $D = D(q; \mathbf{f})$, where $\mathbf{f} = (f_1, \ldots, f_l) \colon \mathbb{F}_q^2 \to \mathbb{F}_q^l$, is defined as follows. The vertex set of D is $\mathbb{F}_q^{l+1}$. There is an arc from a vertex $\mathbf{x} = (x_1, \ldots, x_{l+1})$ to a vertex $\mathbf{y} = (y_1, \ldots, y_{l+1})$ if $x_i + y_i = f_{i-1}(x_1, y_1)$ for all i, $2 \leq i \leq l + 1$. In this paper we study the strong connectivity of D and completely describe its strong components. The digraphs D are directed analogues of some algebraically defined graph, which have been studied extensively and have many applications.

This is joint work with Alexandr Kodess, Department of Mathematics, University of Rhode Island, kodess@uri.edu.

Secret sharing schemes based on additive codes

NARI LEE (Sogang University, Korea)

A secret sharing scheme was first introduced by Shamir [4] in 1979 using polynomial interpolation. This was later turned out to be equivalent to a secret sharing scheme based on a Reed-Solomon code. Since then secret sharing schemes based on linear codes were extensively studied by many researchers [2][3]. Even though the class of additive codes is a generalization of linear codes, there is no work on secret sharing schemes based on additive codes up to now. It will be be an interesting question how secret sharing schemes based on linear codes are generalized to secret sharing schemes based on additive codes.
In this paper, we redefine the construction method for secret sharing schemes based on additive codes over a finite field $GF(4)$. This construction naturally provides higher security level than that of a secret sharing scheme based on a linear code since it requires at least two steps of calculations to recover the secret, while secret sharing scheme based on a linear code requires only one step. Next, we show how to define the access structures for secret sharing schemes based on additive codes over $GF(4)$ by employing the notion of generalized t-designs [1]. We also find a generating functions for the access structure distribution of secret sharing scheme based on an additive code over $GF(4)$. Finally we give two examples using extremal additive even self-dual codes over $GF(4)$ which hold generalized 2-designs.

This is a joint work with Jon-Lark Kim at Sogang University.

[1] P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Inform. and Control, Vol. 23 (1973), 407-438.

[2] C. Ding, D. R. Kohel, S. Ling, *Secret-sharing with a class of ternary codes*, Theoretical Computer Science, 246(1) (2000), 285-298.

[3] J. L. Massey, *Minimal codewords and secret sharing*, Proceedings 6th Joint Swedish-Russian International Workshop on Information Theory, (1993), 276-279.

[4] A. Shamir, *How to share a secret*, Communications of the ACM, 22 (1979), 612-613.

Why Is Finite Mathematics The Most Fundamental?

FELIX M. LEV (Artwork Conversion Software Inc., USA)

The present quantum theory is based on standard mathematics involving the notions of infinitely small/large and continuity. Historically those notions have arisen from a belief based on everyday experience that any macroscopic object can be divided into arbitrarily large number of arbitrarily small parts. However, the very existence of elementary particles indicates that those notions have only a limited meaning. A common belief is that standard mathematics is fundamental while finite mathematics is something inferior which is used only in special applications. However, we argue that the situation is the opposite: standard mathematics is only a degenerate case of finite one in the formal limit when the characteristic of the ring or field used in finite mathematics goes to infinity, and finite mathematics is more pertinent for describing nature than standard one. We also argue that from the philosophy of quantum theory it is clear why, in spite of efforts of many great mathematicians, foundational problems of standard mathematics have not been resolved while the foundation of finite mathematics is natural.
We consider two examples indicating that ultimate quantum theory will be based on finite mathematics:

- Existence of antiparticles and the fact that a particle and its antiparticle have equal masses automatically follow from a theory based on a finite field rather than the field of complex numbers.
- In a theory based on a finite field gravity is simply a kinematical consequence of the fact that particles are described by representations of the de Sitter algebra over a finite field.

On the subset counting problems for polynomials

JIYOU LI (MIT, USA)

Let D be a subset of a finite commutative ring R with identity. Let $f(x) \in R[x]$ be a polynomial of degree d. For integer $0 \leq k \leq |D|$, we study the number $N_f(D, k, b)$ of k-subsets $S \subseteq D$ such that

$$\sum_{x \in S} f(x) = b.$$

In this talk, recent progress on this very general counting problem will be introduced.

This is a joint work with Daqing Wan.

Codes from algebraic surfaces with small Picard number

JOHN B. LITTLE (College of the Holy Cross, Worcester, USA)

We study error-control codes obtained from projective surfaces over a finite field $\mathbb{F}_q$. In earlier work on toric surface codes, we obtained bounds on the minimum distance by finding global sections of the line bundle on the toric surface corresponding to the polygon with reducible zero locus. The Hasse-Weil bound shows that for sufficiently large q the zero loci of such sections will have more $\mathbb{F}_q$-rational points than irreducible sections. In 2007, M. Zarzar suggested that surfaces $X \subset \mathbb{P}^3$ over $\mathbb{F}_q$ with small Picard number (the rank of the Néron-Severi group over the finite field) might be used to produce good evaluation codes. His key idea was that limiting the Picard number of X puts restrictions on the irreducible curves on the surface that can appear as irreducible components of divisors in small multiples of the hyperplane divisor class. We study this idea and evaluate its potential by considering a number of cases including codes from various types of cubic surfaces in the Swinnerton-Dyer classification over $\mathbb{F}_q$, various rational surfaces, $K3$ surfaces, and so forth.
As might be expected, surfaces with small Picard number do not automatically produce good codes; the sectional genus of the surface also has a major influence, especially over small fields. However, we find bounds on the minimum distance in situations where we can control the number and genus of irreducible components of the curves in a given class. We will present several new examples of such codes with minimum distance as good as the best known bounds in Grassl's tables.

This is joint work with Hal Schenck of the University of Illinois.

Character Sums and Generating Sets

LIAN LIU (University of Southern California, USA)

We derive sufficient conditions for a subset of elements of a finite abelian group to generate the entire group by analyzing character sums over the given subset. In particular, we consider groups of the form $(\mathbb{F}_{p^n}[x]/f^e)^\times$ where p is a prime number, $n, e \geq 1$, are integers and $f \in \mathbb{F}_{p^n}[x]$ is an irreducible polynomial. For $e = 1$, a well known theorem of F.R.K. Chung states that if $\sqrt{p} > n - 1$, the set of linear polynomials $\{x + t : t \in \mathbb{F}_p\}$ form a generating set for $(\mathbb{F}_p[x]/f)^\times$. Chung's proof relies on a bound on character sums proven by Katz. Our work relies on a proven conjecture of Katz stating that the character sum estimate should remain valid even if the underlying algebra over the finite field is not étale. We present two basic types of generating sets for the group $(\mathbb{F}_{p^n}[x]/f^e)^\times$: when both p and n are large, we can simply use $\{x + t : t \in \mathbb{F}_{p^n}\}$ as a generating set for this group; otherwise, if p is large but n is relatively small, we show that $\{x + \pi(t) : t \in \mathbb{F}_{p^n}[x]/f\}$ forms a generating set where π is an embedding of $\mathbb{F}_{p^n}[x]/f$ into $\mathbb{F}_{p^n}[x]/f^e$, which can be computed efficiently. We

then describe algorithms for constructing minimal generating sets based on the above results.

AFSRs Synthesis with the Euclidean Algorithm

WEIHUA LIU (University of Kentucky, USA)

Pseudo-random sequence generators are widely used in many areas, such as stream ciphers, radar systems, Monte-Carlo simulation and multiple access systems. Algebraic feedback shift registers (AFSRs) are pseudo-random sequence generators that can generate sequences over an arbitrary finite field. They are generalizations of linear feedback shift registers (LFSRs) and feedback with carry shift registers (FCSRs). The register synthesis problem is: given an eventually periodic sequence $\mathbf{a}$, how can we construct a device that will generate the sequence? In the case of LFSRs, the most widely used algorithm is the Berlekamp-Massey algorithm [4]. FCSRs are good alternatives to LFSRs as building blocks to proffer resistance to algebraic attacks. The algorithms that can be used for finding smallest FCSRs are the lattice approximation algorithm [2], the extended Euclidean rational approximation algorithm [1] and Xu's algorithm [3].
Let R be an integral domain and π be an element in R. Let S be a complete set of representatives for the quotient ring $R/(\pi)$. An AFSR over (R, π, S) outputs an eventually periodic sequence $a_0, a_1, \ldots$ of elements in S satisfing a *linear recurrence with carry*. That is, $-q_0 a_n + \pi z_n = q_1 a_{n-1} + \cdots + q_m a_{n-m} + z_{n-1}$, for all $n \geq m$, where m is the length of the AFSR, $q_i \in R$ and z_i's are carry values in R.
In this talk, we will develop two algorithms that can efficiently find an AFSR of the smallest size for a given sequence. One algorithm is based on the extended Euclidean algorithm. It is an analog of the extended Euclidean rational approximation algorithm. We remark that with this algorithm for a given sequence $\mathbf{a}$, $2\Lambda(\mathbf{a}) + 1$ consecutive terms of $\mathbf{a}$ are enough to find the smallest AFSR, where $\Lambda(\mathbf{a})$ is a complexity measure. The other algorithm is based on the generalized Euclidean algorithm over lattices. It can solve the synthesis problem for AFSR over any quadratic extensions of $\mathbb{Z}$.

This is joint work with Andrew Klapper (University of Kentucky) and Zhixiong Chen (Putian University, China)

[1] F. Arnault, T. P. Berger, and A. Necer. Feedback with carry shift registers synthesis with the Euclidean algorithm. *IEEE Transactions on Information Theory*, 50(5):910-917, 2004.

[2] A. Klapper and M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. *Journal of Cryptology*, 10(2):111-147,1997.

[3] A. Klapper and J. Xu. Register synthesis for algebraic feedback shift registers based on non-primes. *Designs, Codes and Cryptography*, 31(3):227-250, 2004.

[4] J. Massey. Shift register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 15(1):122-127,1969.

Boolean ideals and their varieties

SAMUEL LUNDQVIST (Stockholm University, Sweden)

We say that an ideal I in $\mathbb{F}_2[x_1, \ldots, x_n]$ is *boolean* if $x_i^2 - x_i \in I$ for $i = 1, \ldots, n$. A *boolean monomial* is a square free monomial in $\mathbb{F}_2[x_1, \ldots, x_n]$ and a *boolean polynomial* is a sum of different boolean monomials. It is well known that there is a one-to-one correspondence between boolean ideals and boolean polynomials; each boolean ideal can be written uniquely as $(x_1^2 - x_1, \ldots, x_n^2 - x_n, f)$, where f is boolean. We call such an f the *defining polynomial* of the ideal $(x_1^2 - x_1, \ldots, x_n^2 - x_n, f)$. Along with the one-to-one correspondence between boolean ideals and subsets of $\mathbb{F}_2^n$, we will investigate properties of boolean ideals, especially their varieties, but also their lexicographic standard monomials, in terms of their defining polynomial.
One rather suprising result of this investigation is the following: Consider a boolean polynomial f in $\mathbb{F}_2[x_1, \ldots, x_n]$ and regard each element in the rational zero set of f as an exponent vector of a boolean monomial and add these

boolean monomials together to construct a new boolean polynomial $\phi(f)$. It turns out that the fourth power of ϕ is the identity. For instance, applying ϕ on the boolean polynomial $x_1x_2 + x_2 \in \mathbb{F}_2[x_1, x_2]$ gives rise to the chain

$$x_1x_2 + x_2 \mapsto x_1^1x_2^1 + x_1^1x_2^0 + x_1^0x_2^0 = x_1x_2 + x_1 + 1 \mapsto x_1 \mapsto x_2 + 1 \mapsto x_1x_2 + x_2.$$

The talk is based upon the paper S. Lundqvist, Boolean ideals and their varieties, J. Pure Appl. Alg. 219 (2015), no. 5, 4521–4540.

On communication over networks via skew polynomials

FELICE MANGANIELLO (Clemson University, USA)

In this talk we explore the network communication techniques based on particular mathematical structures. It has been proven that linear network coding is a capacity achieving communication technique for multicast networks. A generalization of this result states that it is possible to achieve capacity by using representable matroids.
Skew polynomial rings are non-commutative generalization of ordinary polynomial rings which recently have been investigated in connection with coding theory and cryptography. Although not commutative, these rings are still right (left) Euclidean rings without zero divisors. As a consequence, it is possible to define a right evaluation via quotient rings. The notion of evaluation comes with that of the right root of a polynomial.
In this talk, we explore the matroid structure defined by the right zero loci of skew polynomials and see the benefit of applying this matroid to multicast networks.

This is a joint work with Siyu Liu and Frank R. Kschischang from the Electrical & Computer Engineering Department of the University of Toronto.

Estimates for the average cardinality of the value set in linear families of univariate polynomials

GUILLERMO MATERA (Universidad Nacional de General Sarmiento, Buenos Aires, Argentina)

We estimate the average cardinality of the value set of linear families of univariate polynomials with coefficients in a finite field. Let $M(n)$ be the set of monic univariate polynomials of degree n with coefficients in the finite field $\mathbb{F}_q$ of $q := p^k$ elements and let $\mathcal{L} \subset M(n)$ be a linear family, namely the set of elements of $M(n)$ whose coefficients satisfy certain linear relations. For $f \in M(n)$, we denote by $\mathcal{V}(f) := |\{f(c) : c \in \mathbb{F}_q\}|$ the cardinality of the value set of f. A well–known result by S. D. Cohen asserts that, for $p > n$ and provided that $\mathcal{L}$ satisfies certain technical conditions, the average cardinality $\mathcal{V}_\mathcal{L}$ of the value set in $\mathcal{L}$ satisfies

$$\mathcal{V}_\mathcal{L} = \mu_n\, q + \mathcal{O}(q^{1/2}),$$

where $\mu_n := \sum_{j=1}^{n}(-1)^{j-1}/j!$. Our main result is an explicit version of this estimate which holds for fields of characteristic $p > 2$ and simplifies significantly the conditions that the linear variety $\mathcal{L}$ must satisfy. An expression for the $\mathcal{O}$–constant in terms of n and $\dim \mathcal{L}$ is provided.
In order to establish this result, we express $\mathcal{V}_\mathcal{L}$ in terms of certain "interpolating sets" $\mathcal{S}_r$ $(\dim \mathcal{L} \leq r \leq n)$. To each $\mathcal{S}_r$ we associate an algebraic variety V_r defined over $\mathbb{F}_q$. We prove that V_r satisfies certain geometric conditions, which allows us to estimate the number of $\mathbb{F}_q$–rational points of V_r, and thus $\mathcal{V}_\mathcal{L}$. The general methodology can also be applied to estimate the number of elements in the linear family $\mathcal{L}$ with a given factorization pattern.

This is joint work with Mariana Pérez and Melina Privitelli.

Polynomial method and a zero-sum problem

ESHITA MAZUMDAR (Harish-Chandra Research Institute, India)

For a finite abelian group G with $\exp(G) = n$, the arithmetical invariant $\mathsf{s}_{mn}(G)$ is defined to be the least integer k such that any sequence S with length k of elements in G has a zero-sum subsequence of length mn. When $m = 1$, it is *the Erdős-Ginzburg-Ziv constant* and is denoted by $\mathsf{s}(G)$. There are weighted versions of these constants. A multidimenssional problem in this line of research is to find out the value of $s_n(\mathbb{Z}_n^d)$, for some $d > 1$. Kemnitz conjectured that $s_n(\mathbb{Z}_n^2) = 4n - 3$. It is Rónyai who proved by using polynomial method that $s_n(\mathbb{Z}_n^2) \leq 4n - 2$.
In my talk I would like to present some modification of Rónyai method [[1],[2]]for making some progress towards finding out the value of these arithmetic constants in the higher dimenssion with different weights.

[1] S. D. Adhikari, E. Mazumdar, Modification of some methods in the study of zero-sum constant, Integers **14** (2014), paper A 25.

[2] S. D. Adhikari, E. Mazumdar, The polynomial method in the study of zero-sum problem, (To appear).

Bent functions from maximal partial spreads

SIHEM MESNAGER (University of Paris 8 and Paris 13, France)

A partial spread of $\mathbb{F}_{p^n}$, $n = 2m$, is a set of pairwise When $p = 2$, Dillon [3] has introduced two classes of bent functions constructed from partial spreads : $\mathcal{PS}^+$ and $\mathcal{PS}^-$. Those functions have the property that any restriction to an element of the partial spread is constant, except at 0. The number of elements of a partial spread is at most $p^m + 1$. A partial spread of maximal cardinality covers the whole space and is simply called a spread. In the line of Dillon's work, other classes of bent functions have been constructed but from the Desarguesian spread. Notably, new classes of hyperbent functions have been found by the author [5]. An overview of those classes can be found in [6]. Recently, other spreads constructed from pre-quasifields have led to other classes of bent functions [8, 1, 2]. In this talk, we shall consider partial spreads and not only spreads. But above, we shall present a framework that unifies all the recent results on this topic found recently, especially, the bent functions constructed from pre-quasifields. More precisely, we shall consider functions of the shape $f = \sum_{r \in R} m_r 1_{E_r}$ for some partial spreads $\{E_r, r \in R\}$ of $\mathbb{F}_{p^m}$ and some sequence $(m_r)_{r \in R}$ of elements of $\mathbb{F}_p$. We shall present a characterization of the bentness of a function of this shape that only involves the elements of the sequence $(m_r)_{r \in R}$ and not the elements of the spread.

Theorem. *f is bent if and only if $\chi_p(\sum_{r \in R} m_r) - \sum_{r \in R} \chi_p(m_r) = p^m + 1 - |R|$ (where $\chi_p(a) = \xi_p^a$ and ξ_p is a primitive pth-root of unity).*

Another important feature is that those bent functions are regular bent and that we are able to compute their dual functions. Recently, Lisonek and Lu have established another characterization in [4]. We investigate the link between their characterization and ours. But above, the most important point is that our characterization does allow to consider other families of spreads than those considered in [8, 1, 2]. Indeed, there is another family of partial spreads that are important objects in finite geometry : maximal partial spreads. A partial spread is said to be maximal if it is not contained in another partial spread except itself. This opens new leads in the search for bent functions constructed from partial spreads. We shall notably show how to translate results of Galois geometry in $PG(3, q)$ (q odd) presented by Storme in [7] to obtain classes of bent functions that does not enter in the scope of [8, 2, 1].

[1] C. Carlet. More $\mathcal{PS}$ and $\mathcal{H}$-like bent functions. *Cryptology ePrint Archive, Report 2015/168*, 2015.

[2] A. Cesmelioglu, W. Meidl, and A. Pott. Bent functions, spreads, and o-polynomials. *SIAM Journal on Discrete Mathematics*, 29(2):854–867, 2015.

[3] J. Dillon. Elementary Hadamard difference sets. *PhD dissertation, University of Maryland*, 1974.

[4] P. Lisonek and Y. Lu. Bent functions on partial spreads. *Des. Codes Cryptography*, 73(1):209–216, 2014.

[5] S. Mesnager. Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. *IEEE Transactions on Information Theory*, 57(9):5996–6009, 2011.

[6] S. Mesnager. Bent from spreads. *Journal of the American Mathematical Society (AMS), Contemporary Mathematics*, 632:295–316, 2015.

[7] L. Storme, Spectrum results in Galois geometries. *Advances in Mathematics Research*, 12:147–172, 2012.

[8] B. Wu. $\mathcal{PS}$ bent functions constructed from finite pre-quasifield spreads. *ArXiv e-prints*, 2013.

Dickson polynomials that are involutions

SIHEM MESNAGER (University of Paris 8 and Paris 13, France)

Very recently, following novel requirements in symmetric cryptography, the interest of involutions have been highlighted. The involutions have been deployed in cryptographic designs, however, the literature lacked a detailed study on involutions over the finite field of order 2^n, denoted by F_{2^n}) and their cryptographic properties. In ISIT 2015 [1], the authors have provided a rigorous study of involutions over F_{2^n} which are relevant primitives for cryptographic designs. In this talk the authors focus on particular class of involutions polynomials, more precisely on Dickson polynomials that are involutions.
Dickson polynomials form an important class of permutation polynomials. They have been extensively investigated in recent years under different contexts. An excellent reference on Dickson polynomials and its developments is the book of Lidl, Mullen and Turnwald [2]. Attention has been drawn (but not explicitly) to Dickson polynomials that are involutions in the book mentioned above and Dickson permutation polynomials that decompose in cycles of the same length have been discussed in [3].
The aim of this talk is to present our study on Dickson polynomials of the first kind which induce an involution of any fixed finite field. Using modular arithmetic's tools, we provide a characterization of those Dickson involutions and a study of the corpus of involutions. Further we present infinite classes of Dickson involutions. This helps us study their fixed points more precisely. Consequently that allows us to understand the applicability of Dickson involutions in cryptography. Our study reveals that Dickson involutions have very high number of fixed points.

[1] P. Charpin, S. Mesnager and S. Sumanta, *On involutions of finite fields*, Proceedings of 2015 IEEE International Symposium on Information Theory, ISIT 2015, Hong-Kong, 2015.

[2] R. Lidl, G.L. Mullen and G. Turnwald, *Dickson Polynomials*, Pitman Monographs in Pure and Applied Mathematics, Vol. 65, Addison-Wesley, Reading, MA 1993.

[3] I.M. Rubio, G.L. Mullen, C. Corrada and F. N. Castro, *Dickson permutation polynomials that decompose in cycles of the same length*, Finite Fields and applications, pages 229-239, Contemp. Math., 461, Amer. Math. Soc., Providence, RI, 2008.

On unimodular matrices over integrally closed subrings of function fields

GIACOMO MICHELI (University of Zurich, Switzerland)

Let q be a prime power, and let $F/\mathbb{F}_q$ be an algebraic function field in one variable over $\mathbb{F}_q$. Let g be the genus of F, and let $\mathcal{P}$ be the set of its places.

Let $\emptyset \neq \mathcal{S} \subsetneq \mathcal{P}$ be a nonempty proper subset of places. We recall that the holomorphy ring of $\mathcal{S}$ (using the terminology of [5]) is defined as

$$R := \bigcap_{P \in \mathcal{S}} \mathcal{O}_P$$

As it is well known, these rings are integrally closed and any integrally closed subring of F has this particular form. Define furthermore $\mathcal{D} := \{D \in \mathrm{Div}(F) \mid D \geq 0, \, \mathrm{supp}(D) \subseteq \mathcal{P} \setminus \mathcal{S}\}$. It follows that

$$R = \bigcup_{D \in \mathcal{D}} \mathcal{L}(D),$$

where $\mathcal{L}(D)$ denotes the Riemann-Roch space associated to a divisor D. We define the zeta function of R as

$$\zeta_R(s) = \prod_{P \in \mathcal{S}} \left(1 - \frac{1}{q^{\deg(P)}}\right)^{-1}$$

Let T be a set, we will denote by $T^{k \times m}$ the set of $k \times m$ matrices having entries in T. For a subset $M \subseteq R^{k \times m}$, we define its density by setting

$$\overline{\mathbb{D}}(M) := \limsup_{D \in \mathcal{D}} \frac{|M \cap \mathcal{L}(D)^{k \times m}|}{|\mathcal{L}(D)^{k \times m}|}, \, \underline{\mathbb{D}}(M) := \liminf_{D \in \mathcal{D}} \frac{|M \cap \mathcal{L}(D)^{k \times m}|}{|\mathcal{L}(D)^{k \times m}|}, \, \mathbb{D}(M) := \lim_{D \in \mathcal{D}} \frac{|M \cap \mathcal{L}(D)^{k \times m}|}{|\mathcal{L}(D)^{k \times m}|}.$$

the last being defined only when $\overline{\mathbb{D}}(M) = \underline{\mathbb{D}}(M)$. This definition is well-posed thanks to Moore-Smith convergence for nets [3, Chapter 2]. For fixed positive integers $k \leq m$, we wish to study the set E of $k \times m$ matrices over the ring R which can be extended to $m \times m$ unimodular matrices. Since R is a Dedekind domain we have

$$E = \{A \in R^{k \times m} \mid I_A = R\},$$

where I_A denotes the ideal of R generated by the $k \times k$ minors of A (see for example [2, 4]). The main result is:

Theorem. *Let $m \geq 2k + 1$, then*

$$\mathbb{D}(E) = \prod_{j=m-k+1}^{m} \frac{1}{\zeta_R(j)}.$$

This theorem extends the results of [1] by setting $F = \mathbb{F}_q(x)$ and$R = \bigcap_{P \in \mathcal{P} \setminus \{P_\infty\}} \mathcal{O}_P = \mathbb{F}_q[x]$. The ingredients for the proof are basically Riemann Roch Theorem, Hasse-Weil bound and a combinatorial argument to estimate the number of matrices having entries in $\mathcal{L}(D)$, whose reduction modulo P is not full rank.

[1] Xiangqian Guo and Guangyu Yang. The probability of rectangular unimodular matrices over $\mathbb{F}_q[x]$. *Linear Algebra and its Applications*, 438(6):2675–2682, 2013.

[2] William H Gustafson, Marion E Moore, and Irving Reiner. Matrix completions over dedekind rings. *Linear and Multilinear Algebra*, 10(2):141–144, 1981.

[3] John L. Kelley. *General topology*. New York: Van Nostrand, 1955.

[4] Daniel Quillen. Projective modules over polynomial rings. *Inventiones mathematicae*, 36(1):167–171, 1976.

[5] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer, 2009.

Character Values of the Sidelnikov-Lempel-Cohn-Eastman Sequences

GOLDWYN MILLAR (Carleton University, USA)

Binary sequences with good autocorrelation properties and large linear complexity are useful in stream cipher cryptography. The Sidelnikov-Lempel-Cohn-Eastman (SLCE) sequences have nearly optimal autocorrelation, and so it is natural to try to determine their linear complexity. However, the problem of finding the linear complexity of these sequences seems to be quite difficult.
Authors who have worked on this problem have drawn on tools such as cyclotomic numbers and Jacobsthal sums. By contrast, our approach is to exploit the fact that character values associated with the SLCE sequences can be expressed in terms of a certain type of Jacobi sum. By making use of known evaluations of Gauss and Jacobi sums in the "pure" and "small index" cases, we are able to obtain new insight into the linear complexity of the SLCE sequences.

This is joint work with Saban Alaca.

On the Existence of Semi-regular Sequences

SERGIO MOLINA (University of Cincinnati, USA)

Semi-regular sequences over $\mathbb{F}_2$ are sequences of homogeneous elements of the algebra

$$B^{(n)} = \mathbb{F}_2[X_1, ..., X_n]/(X_1^2, ..., X_n^2),$$

which have as few relations between them as possible. They were introduced in order to assess the complexity of Gröbner basis algorithms such as $\mathbf{F}_4, \mathbf{F}_5$ for the solution of polynomial equations. Despite the experimental evidence that semi-regular sequences are common, it was unknown whether there existed semi-regular sequences for all n, except in extremely trivial situations.
We prove some results on the existence and non-existence of semi-regular sequences. In particular, we show that if an element of degree d in $B^{(n)}$ is semi-regular, then we must have $n \leq 3d$. Also, we show that if $d = 2^t$ and $n = 3d$ there exists a semi-regular element of degree d establishing that the bound is sharp for infinitely many n. Finally, we generalize the result of non-existence of semi-regular elements to the case of sequences of a fixed length m.

Critical sets in generalizations of latin squares and Sudoku puzzles

ILENE H. MORGAN (Missouri University of Science and Technology, USA)

One way to generalize the concept of orthogonal latin squares is to equiorthogonal frequency squares. Various authors have studied critical sets in latin squares, frequency squares, and pairs of orthogonal latin squares, but little work has been done studying critical sets for sets of orthogonal frequency squares. While the usual definition of orthogonality for frequency squares provides little, if any, reduction of the size of a critical set, it turns out that the size of a critical set for a pair of equiorthogonal frequency squares may be significantly smaller than the union of the critical sets of the individual squares. Critical sets in Sudoku puzzles have been investigated by several authors. Newspapers that publish traditional 9 by 9 Sudoku puzzles also publish 6 by 6 puzzles in which the boxes are 2 by 3. We have investigated critical sets of 6 by 6 Sudoku puzzles with a specific structure and generalized this idea to 2n by 2n puzzles with boxes of size 2 by n. We have also begun to investigate orthogonal Sudoku squares which, if the parameters are suitable, can be constructed using polynomials over a finite field.

Everything in this talk is joint work with Prof. Rita SahaRay.

Character sums and congruences equations

MARC MUNSCH (University of Montreal, Canada)

I will discuss some recent work with Igor Shparlinski on character sums and its applications to some congruence equations. These have a lot of applications, for instance the distribution of quadratic residues. We will focus on the solvability of $au = x$ modulo a prime p, where x lies in an interval I and u in some approximate subgroup U of F_p. It has been recently shown by Cilleruelo and Garaev that this equation is solvable for almost all a, provided that $|I| > p^{5/8+\epsilon}$ and $|U| > p^{3/8}$ (where U is a subgroup or a set of consecutive powers of a primitive root). Combinatorics arguments together with some bounds on character sums for almost all primes allow us to obtain similar results for a wider range of sizes for U and I.

Polynomial Factorization and Euler-Poincare Characteristics of Drinfeld Modules

ANAND KUMAR NARAYANAN (California Institute of Technology, USA)

We propose and rigorously analyze two randomized algorithms to factor univariate polynomials over finite fields using rank 2 Drinfeld modules. The first algorithm estimates the degree of an irreducible factor of a polynomial from Euler-Poincare characteristics of random Drinfeld modules. Knowledge of a factor degree allows one to rapidly extract all factors of that degree. As a consequence, the problem of factoring polynomials over finite fields in time nearly linear in the degree is reduced to finding Euler-Poincare characteristics of random Drinfeld modules with high probability. Notably, the worst case complexity of polynomial factorization over finite fields is reduced to the average case complexity of a problem concerning Drinfeld modules. The second algorithm is a random Drinfeld module analogue of Berlekamp's algorithm. During the course of its analysis, we prove a new bound on degree distributions in factorization patterns of polynomials over finite fields in certain short intervals.

A preprint is available at http://arxiv.org/abs/1504.07697

On the structure of certain reduced linear modular systems

EDUSMILDO OROZCO (University of Puerto Rico)

Given a nonsingular linear modular system (LMS) $L_S = (\mathbf{F}_q, S)$ over a finite field $\mathbf{F}_q$ and a nonsingular matrix M that commutes with S, a *reduced linear modular system* (RLMS) R_{MS}, associated with L_S, is the finite dynamical system that results from the action of M on the cycles of L_S. The structure of such a system resembles the cyclic structure of an LMS. The study of RLMSs involves two problems. The first problem is to determine the cyclic structure of an RLMS R_{MS} when S and M are nonsingular. The second problem is, given a nonsingular LMS L_S, find an associated nonsingular RLMS R_{MS} with the least possible number of cycles. The solution to the last problem has implications in the efficient computation of multidimensional fast Fourier transforms of prime–edge length with linear symmetries in its inputs [1].
When the characteristic polynomial of an LMS is irreducible over the integers mod a prime p, it is shown in [2] that the structure of any associated RLMS is composed of cycles of equal length, besides the trivial zero–cycle of length one. In this case, an *optimal* RLMS is one where the characteristic polynomial of M is primitive and the cyclic structure of the RLMS is composed of one nontrivial cycle with length depending on the periods of S and M. In this work we discuss some results about the case when the minimal polynomials of S and M are nontrivial powers of irreducible polynomials and S and M are non–derogatory matrices over a finite field. We also discuss a connection with Lucas' theorem and the chinese remainder theorem.

[1] J. Seguel, D. Bollman, E. Orozco. *A new prime edge–length crystallographic FFT.*, in: Lecture Notes on Computer Science, Part II (2002) 548–557, Springer–Verlang.

[2] E. Orozco, *Reduced Linear Modular Systems.* Contemporary Mathematics, Vol. 461, 2008, pp. 205–212.

Code Automorphisms and Permutation Decoding of Linear Codes

NICOLA PACE (Universidade de São Paulo, Brazil)

Linear codes with large automorphism groups are of interest from many points of view. There are several techniques that use the code's automorphism group to reduce the number of computations needed for encoding and decoding. In 1964, MacWilliams developed a method, called permutation decoding, that is feasible when a sufficiently large automorphism group ensures the existence of a set of automorphisms—called a PD-set—with specific properties.
In this talk, we consider linear codes with a prescribed minimal automorphism group. In particular, we are interested in codes arising from Galois Geometries and the problem of constructing PD–sets.

On the Heuristic of Approximating Polynomials over Finite Fields by Random Mappings

DANIEL PANARIO (Carleton University, Canada)

The study of iterations of functions over a finite field and the corresponding functional graphs is a growing area of research with connections to cryptography. The behaviour of such iterations is frequently approximated by what is know as the Brent-Pollard heuristic, where one treats functions as random mappings. We aim at understanding this heuristic and focus on the expected rho length of a node of the functional graph of a polynomial over a finite field.
Since the distribution of indegrees (preimage sizes) of a class of functions appears to play a central role in its average rho length, we survey the known results for polynomials over finite fields giving new proofs and improving one of the cases for quartic polynomials.
We discuss the effectiveness of the heuristic for many classes of polynomials by comparing our experimental results with the known estimates for random mapping models defined by different restrictions on their distribution of indegrees.
We prove that the distribution of indegrees of general polynomials and mappings have similar asymptotic properties, including the same asymptotic average coalescence. The combination of these results and our experiments suggests that these polynomials behave like random mappings, extending a heuristic that was known only for degree 2. We show numerically that the behaviour of Chebyshev polynomials of degree $d \geq 2$ over finite fields present a sharp contrast when compared to other polynomials in their respective classes.

Joint work with Rodrigo S. V. Martins (Federal University of Rio de Janeiro).

Difference Sets and Partial Difference Sets with a Linking Property

JOHN POLHILL (Bloomsburg University of Pennsylvania, USA)

Recently Davis, Martin, and Polhill exhibited constructions of linked systems of symmetric designs using difference sets. Previously known constructions had relied on finite fields with even order, while our new constructions made use of Galois rings also having even order. In this talk we also investigate how similar ideas might be applied to partial difference sets. The natural place to begin is in the elementary abelian case where we can make use of the rich structure of finite fields. Any success along these lines would result in strongly regular graphs with a linking property.

Cayley graphs with diameter 2 from difference sets

ALEXANDER POTT (Otto-von-Guericke-University Magdeburg, Germany)

Let $C(d,D)$, $AC(d,D)$ and $CC(d,D)$ be the largest order of a Cayley graph, a Cayley graph based on an abelian group and based on a cyclic group, respectively, of degree d and diameter D. When $D=2$, it is well-known that $C(d,2) \leq d^2+1$ with equality if and only if the graph is a Moore graph. In the cyclic and abelian case, we have $CC(d,2) \leq AC(d,2) \leq \frac{d^2}{2}+d+1$. In this talk, we consider constructions of large graphs of diameter $D=2$ using difference sets. We obtain better lower bounds on $AC(d,2)$ for infinitely many d's. The constructions of the difference sets use the interplay between additive and mutliplicative structure of finite fields.

Weierstrass semigroups and Kummer extensions

LUCIANE QUOOS (Universidade Federal do Rio de Janeiro, Brazil)

For Kummer extensions $y^m = f(x)$, $f(x)$ a polynomial, we discuss conditions for an integer be a Weierstrass gap at a point P. For the totally ramified points, the condition will be necessary and sufficient. As a consequence, we extend independent results of Hasse, Valentini-Madan, Leopoldt and Towse. We also present a general class of polynomials $f(x)$ in $\mathbb{F}_{q^2}[x]$ for which the $\mathbb{F}_{q^2}$ -maximality of the algebraic curve $y^m = f(x)$, implies that m is a divisor of $q+1$.

This is a joint work with Miriam Abdon (UFF) and Herivelto Borges (USP-São Carlos).

New examples of maximal partial line spreads in $PG(3,q)$, q even

SANDRO RAJOLA (Istituto Tecnico Per Il Turismo "C. COLOMBO", Italy)

A *partial line spread* in $PG(3,q)$, the projective space of dimension three over the field $\mathbb{F}_q$, is a set of pairwise disjoint lines. A *maximal partial line spread* in $PG(3,q)$ is a partial line spread in this space which cannot be extended to a larger partial line spread. Many authors have investigated maximal partial line spreads in $PG(3,q)$, but the complete knowledge of them is still far away, especially in the case q even. In this talk we give many new examples of maximal partial line spreads in $PG(3,q)$, with q even, $q \geq 8$. To this end, we call *regulus* of the non-singular quadric $Q(4,q)$ of $PG(4,q)$ (the projective space of dimension four over the field $\mathbb{F}_q$) a regulus of a hyperbolic quadric hyperplane section of $Q(4,q)$. Also, for every point V of $Q(4,q)$, we call *lined tangent cone of vertex V* of $Q(4,q)$ the set of all the lines of $Q(4,q)$ through V. As well known, the union of these lines is the tangent cone of vertex V of $Q(4,q)$.
In order to construct our maximal partial line spreads, first we transfer the whole geometry of $PG(3,q)$ over the non-singular quadric $Q(4,q)$. More precisely we get the following mapping. The points of $PG(3,q)$ are the lines of $Q(4,q)$, and the lines of $PG(3,q)$ are the lined tangent cones and the reguli of $Q(4,q)$. Also, each plane of $PG(3,q)$ is the set of all the lines of $Q(4,q)$ meeting a fixed line of this quadric, and viceversa. Secondly, we consider the non-singular quadric $Q(4,q)$ of $PG(4,q)$, with q even and $q \geq 8$, an elliptic quadric $\mathcal{E}$, hyperplane section of $Q(4,q)$, and a suitable collection of non-singular conics over the quadric $\mathcal{E}$. Through the quadric $\mathcal{E}$ and through the mentioned collection of non-singular conics, we construct a set $\mathcal{F}$ of lined tangent cones and reguli of $Q(4,q)$ such that any two distinct elements of $\mathcal{F}$ have no common line, and such that every lined tangent cone and every regulus of $Q(4,q)$ has a line in common with an element of $\mathcal{F}$. So $\mathcal{F}$ is a maximal partial line spread in $PG(3,q)$, q even and $q \geq 8$, by means of the above mapping of $PG(3,q)$ over $Q(4,q)$. By this we get many new values for the sizes of maximal partial line spreads in $PG(3,q)$, q even and $q \geq 8$.

An Infinite Family of Tight Sets in $\mathcal{Q}^+(5,q)$

MORGAN RODGERS (Università di Padova, Italy)

Cameron-Liebler line classes are sets of lines in $\mathrm{PG}(3,q)$ having a constant intersection size will all line spreads of the projective space. Under the Klein correspondence, these sets of lines correspond to tight point sets in the

hyperbolic polar space $\mathcal{Q}^+(5,q)$. A set $\mathcal{T}$ of points in $\mathcal{Q}^+(5,q)$ is *x-tight* if

$$|P^\perp \cap \mathcal{T}| = \begin{cases} x(q+1)+q^2 & \text{for every point } P \in \mathcal{T}, \text{ and} \\ x(q+1) & \text{for every point } P \notin \mathcal{T}. \end{cases}$$

Tight sets can also be characterized in terms of the eigenspaces of the collinearity matrix of the polar space, and can be used to construct strongly regular graphs.
In [2] a family of new examples of $\frac{q^2-1}{2}$-tight sets in $\mathcal{Q}^+(5,q)$ for all $q \equiv 5$ or $9 \bmod 12$ were described. We will look at how these examples were originally found using a computer search in [1], and how the use of techniques such as field reduction and Gauss sums were used to generalize these examples and to prove the necessary intersection properties.

[1] M. Rodgers. *On some new examples of Cameron–Liebler line classes*. PhD thesis, University of Colorado Denver, 2012.

[2] J. De Beule, J. Demeyer, K. Metsch, M. Rodgers. A new family of tight sets in $\mathcal{Q}^+(5,q)$, *Designs, Codes and Cryptography*, 2014.

Unitals with many Baer secants through a fixed point

SARA ROTTEY (Vrije Universiteit Brussel, Belgium)

In this talk, we investigate unitals in the Desarguesian projective plane of square order q^2, $q = p^h$, p prime, denoted by $\mathrm{PG}(2,q^2)$. A *unital* U in $\mathrm{PG}(2,q^2)$ is a set of q^3+1 points of $\mathrm{PG}(2,q^2)$ such that each line contains exactly 1 or $q+1$ points of U. A line is a *tangent* or *secant* of U if it contains 1 or $q+1$ points of U, respectively. An example of a unital in $\mathrm{PG}(2,q^2)$ is given by the set of absolute points of a unitary polarity, called a *classical unital*. In [1], Buekenhout constructed a class of unitals, called *ovoidal Buekenhout-Metz unitals*. Every known unital can be obtained by this construction.
Combining the results of [3] (for q odd and $q > 3$), and [2] (for $q > 2$ even and $q = 3$) the following characterisation of ovoidal Buekenhout-Metz unitals is obtained.

Result. [3, 2]
Let U be a unital in $\mathrm{PG}(2,q^2)$, $q > 2$, containing a point P such that all secants through P intersect U in a Baer subline, then U is an ovoidal Buekenhout-Metz unital.

We will improve this result by finding a new upper bound for the minimum required number of Baer sublines through a fixed point of the unital. It is worth noticing that our Main Theorem implies the result of [3] and [2] for $q \geq 16$.

Main Theorem.
Suppose $q \geq 16$ and $\epsilon = 2q$ for q even, $\epsilon = \frac{q^{3/2}}{2}$ for q odd. Let U be a unital in $\mathrm{PG}(2,q^2)$ containing a point P such that at least $q^2 - \epsilon$ of the secants through P intersect U in a Baer subline, then U is an ovoidal Buekenhout-Metz unital.

This is joint work with Geertrui Van de Voorde.

[1] F. Buekenhout. Existence of unitals in finite translation planes of order q^2 with a kernel of order q. *Geom. Dedicata* **5** (1976), 189–194.

[2] L.R. Casse, C.M. O'Keefe and T. Penttila. Characterizations of Buekenhout-Metz unitals. *Geom. Dedicata* **59 (1)** (1996), 29–42.

[3] C.T. Quinn and R. Casse. Concerning a characterisation of Buekenhout-Metz unitals. *J. Geom.* **52 (1–2)** (1995), 159–167.

On the Differential Probability of Substitution-Permutation Networks

JOËLLE ROUÉ (Inria, project-team SECRET, France)

Block ciphers are central primitives in symmetric encryption. One of the most widely-used constructions for iterated block ciphers is Substitution-Permutation Network (SPN). Its round function is composed of a linear mixing permutation and of a nonlinear substitution function which consists of several copies of a permutation S called Sbox operating on fewer bits. Differential cryptanalysis consists in exploiting a statistical bias in the distribution of the difference b in $\mathbf{F}_2^n$ between the images under the cipher E_k of two inputs which differ from a fixed value a: $\Pr_X[E_k(X+a)+E_k(X)=b]$. A precise evaluation of the complexity of differential cryptanalysis has led to some design criteria. In particular, the linear layer must have a high branch number. This quantity corresponds to the smallest number of active Sboxes (Sboxes with nonzero input differences) within a two-round differential characteristic. Indeed, for a given choice of the Sbox, the maximal probability for an r-round differential characteristic decreases when the number of active Sboxes within r rounds increases. Thus, many security analyses focus on the minimal number of active Sboxes within r consecutive rounds when r varies.

However, the complexity of a differential attack depends on the probability of *a differential*, *i.e.*, on the sum of the probabilities of all characteristics starting by a given input difference and ending by a given output difference. And, within two consecutive rounds of an SPN, the number of constituent characteristics increases with the Hamming weight of the differential. Then, the maximum expected probability (MEDP) for a two-round differential may result from a differential which contains a huge number of characteristics each with a low but nonzero probability, rather than from a differential which contains a few characteristics having a high probability.

Though it appears to be the case for most known examples (including the AES, the block cipher standard [1]), there is *a priori* no reason to believe that the best differential corresponds to a differential with the lowest number of active Sboxes.

We prove that there are situations for which the two-round MEDP is achieved by a differential with the smallest number of active Sboxes, for instance when the Sbox is carefully chosen. However, we show that this phenomenon is not general by exhibiting the first examples of SPNs where the two-round MEDP is achieved by a differential in which the number of active Sboxes exceeds the branch number.

[1] Liam Keliher and Jiayuan Sui, *Exact maximum expected differential and linear probability for two-round Advanced Encryption Standard*, IET Information Security **1** (2007), no. 2, 53–57.

[2] Anne Canteaut and Joëlle Roué, *On the behaviors of affine equivalent Sboxes regarding differential and linear attacks*, Advances in Cryptology - EUROCRYPT 2015, LNCS, vol. 9056, Springer, 2015, pp. 45–74.

Primitivity of Four-Dimensional Finite Semifields

IGNACIO FERNÁNDEZ RÚA (Universidad de Oviedo, Spain)

A *finite semifield* (or finite division ring) D is a finite nonassociative ring with identity such that the set of nonzero elements D^* is closed under the product (and so it is a loop). The multiplicative structure of associative finite semifields (i.e., of finite fields) is well-known: D^* is a cyclic group. However, for a *proper* finite semifield D, the structure of its multiplicative loop D^* is not known. In particular, it is unknown which finite semifields are *primitive*, in the sense that all left (or right) principal powers of a single element exhaust D^*. In this talk we will present recent results on the primitivity of four-dimensional finite semifields.

Finding a Groebner basis for the ideal of recurrence relations on m-dimensional periodic arrays

IVELISSE RUBIO (University of Puerto Rico)

Recent developments in applications of multidimensional periodic arrays have drawn new attention to the computation of Groebner bases for the set of linear recurrence relations on the arrays. An m-dimensional infinite array can be represented by a multivariate power series sitting within the ring of multivariate Laurent series. In this joint work with Moss Sweedler, Mathematics Department, Cornell University, we reinterpret the problem of finding linear recurrence relations on m-dimensional periodic arrays as finding the kernel of a module map involving quotients of Laurent series and present a Groebner bases algorithm to compute a generating set for this kernel.

Hermitian and symmetric rank distance codes

KAI-UWE SCHMIDT (Otto-von-Guericke-University Magdeburg, Germany)

Let X be a set of matrices of fixed shape over a finite field. This talk is about subsets Y of X with the property that, for all distinct $A, B \in Y$, the rank of $A - B$ is at least a given integer d. Call such a set a *d-code* in X. For fixed d, one is usually interested in d-codes containing as many elements as possible. In the case that X is the set of all matrices of a given shape over a finite field, such objects have been studied since the 1970s and have since found numerous applications. I will consider the cases that X is the set of all Hermitian or all symmetric matrices of a given shape over a finite field. In both cases, I present sharp bounds for the size of a d-code that is closed under addition and provide constructions of such sets for which equality holds. Moreover, in case of equality, it is possible to obtain the distribution of the ranks in the set. These results have applications in classical coding theory. For example, they give the weight enumerators of certain cyclic codes, for which numerous special cases have been previously obtained using long ad hoc calculations. The principal new insights come from a better understanding of the association schemes of Hermitian and symmetric bilinear forms.

Warning's Second Theorem with Restricted Variables

JOHN R. SCHMITT (Middlebury College, USA)

We present a restricted variable generalization of Warning's Second Theorem (a result giving a lower bound on the number of solutions of a low degree polynomial system over a finite field, assuming one solution exists). This is analogous to Schauz's (and later Brink's) restricted variable generalization of Chevalley's Theorem (a result giving conditions for a low degree polynomial system *not* to have exactly one solution). Just as Warning's Second Theorem implies Chevalley's Theorem, our result implies Schauz's Theorem. We include several combinatorial applications, enough to show that we have a general tool for obtaining quantitative refinements of combinatorial existence theorems.

Upper bounds on pairs of dot products in vector spaces over finite fields

STEVEN SENGER (Missouri State University, USA)

Given a subset, E, of F_q^d, the d-dimensional vector space over a finite field of q elements, we give bounds on how many triples of points determine a fixed pair of dot products. Specifically, given $\alpha, \beta \in F_q$, and assumptions on $E \subset F_q^d$, we estimate the size of the set

$$\{(x, y, z) \in E \times E \times E : x \cdot y = \alpha, x \cdot z = \beta\}.$$

On Identification of irreducible polynomials over $\mathbb{F}_p$

P.L. SHARMA (Himachal Pradesh University, India)

Irreducible polynomials over finite fields receive much importance in mathematical sciences and computer sciences. The properties of the irreducible polynomials over finite fields have been widely studied.
We give structures of $\mathbb{F}_{p^n}^*$, where p is prime and n is positive integer by two different ways. The first one is starting with the primitive element α and the second one beginning with the element α^{p^n-1}. Further, we characterize the elements of both the structures of $\mathbb{F}_{p^n}^*$ to identify the irreducible polynomials of degree n over finite field $\mathbb{F}_p$. Also, we show the correspondence between the elements of rows and columns of the structure $\mathbb{F}_{p^n}^*$.

Maximum rank distance codes and finite semifields

JOHN SHEEKEY (Universiteit Gent, Belgium)

A *rank metric code* is a code consisting of $n \times n$ matrices with the distance function $d(X, Y) := \mathrm{rank}(X - Y)$. Rank metric codes have close ties to *subspace codes*, which have important applications in network coding.
Maximum rank distance (MRD) codes are rank metric codes $\mathcal{C}$ meeting the Singleton-like bound $|\mathcal{C}| = q^{n(n-d+1)}$, where d is the minimum distance. Linear MRD-codes for each parameter were constructed by Delsarte, and later by Gabidulin. The first non-trivial example of a non-linear MRD-code was recently given by Cossidente, Marino and Pavese for the case $n = 3$, $d = 2$.
In the case $n = d$, linear MRD-codes correspond to *finite (pre)semifields*, that is, nonassociative division algebras. Semifields have received much attention in recent years, though their applications to coding theory have not been exploited to date. We will give an overview on the theory of semifields, and their links to codes. Until recently, no other linear MRD-codes were known. In this talk we will introduce a new family of linear MRD-codes for each parameter, which include the Delsarte/Gabidulin codes, as well as many new examples inequivalent to any previously known codes. The construction is inspired by a family of semifields constructed by Albert in the 1960's (Generalized twisted fields). We will also present the automorphism groups of this new family.

On generating functions for special numbers and polynomials and their applications

YILMAZ SIMSEK (University of Akdeniz, Antalya, Turkey)

In this talk, by using generating functions, we study various special numbers and polynomials, including the Bernoulli numbers and polynomials, the Euler numbers and polynomials, the Central factorial numbers , the array polynomials and the Stirling numbers. We give some functional equations and differential equations for these generating functions. By applying these equations, we give fundamental properties, including recurrence relation, Raabe's formula, consecutive sums formula related to these numbers and polynomials. We also give many identities and relations associated with these numbers and polynomials. Integrating these identities and relations, we derive various combinatorial sums involving binomial coefficients, some old and some new, for these numbers and polynomials. Our results have many applications in a wide variety of areas of mathematics, including finite fields, algebra and analytic number theory, as well as in statistics and computer science.

Authenticated Key Exchange from Ring Learning with Errors

MICHAEL SNOOK (University of Cincinnati, USA)

We describe a new protocol for authenticated key exchange based on the Ring Learning with Errors problem. The protocol starts with a Ring Learning with Errors based key exchange protocol similar to the classic Diffie–Hellman key exchange protocol, then applies techniques similar to the HMQV protocol to attain authentication. As the Ring Learning with Errors problem is largely considered to be difficult to solve even on quantum computers, this construction presents an important step for information security in a world where quantum computers exist.

Joint work with Jiang Zhang, Zhenfeng Zhang, Jintai Ding, Özgür Dagdelen.

Hermitian Codes with Automorphism Group Isomorphic to $P\Gamma L(2,q)$

PIETRO SPEZIALI (Università degli Studi della Basilicata, Italy)

Functional and differential algebraic-geometry codes arising from algebraic curves defined over a finite field $\mathbf{F}_q$ often have good parameters. For this reason, such codes have intensively been investigated. Their general construction technique is due to Goppa, and it requires an algebraic curve $\mathcal{F}$ defined over $\mathbf{F}_q$ with a $\mathbf{F}_q$-rational divisor G and a set D of $\mathbf{F}_q$-rational points of $\mathcal{F}$ disjoint from the support of G. Goppa's construction works particularly well when applied to the Hermitian curve $\mathcal{H}$ of $PG(2,q^2)$.
Typically, one takes $G = mP$ with $P \in \mathcal{H}(\mathbf{F}_{q^2})$ and m a positive integer, together with $D = \mathcal{H}(\mathbf{F}_{q^2}) \setminus \{P\}$. The arising functional and differential codes are the so-called *one-point Hermitian codes* and have thoroughly been studied; see for instance [3, 4]. Another choice is $G = m_1P_1 + m_2P_2$ and $D = \mathcal{H}(\mathbf{F}_{q^2}) \setminus \{P_1, P_2\}$. The corresponding codes are the *two-point Hermitian codes* and they are investigated in [2]. Hermitian codes have also been constructed from degree 3 closed points, that is, $G = m(P + \Phi(P) + \Phi^2(P))$ and $D = \mathcal{H}(\mathbf{F}_{q^2})$ where P is an $\mathbf{F}_{q^6}$-rational point of $\mathcal{H}$ and Φ is the Frobenius map of $\mathbf{F}_{q^2}$; see [1].
In this talk, $\mathcal{H}$ is given by the equation $Y^q+Y = X^{q+1}$. We investigate the functional Hermitian code $C_L(D,G)$ where $G = m\mathcal{P}$ with $\mathcal{P} = \sum_{\mathcal{H}(\mathbf{F}_q)} P$ and $D = \mathcal{H} \setminus \mathcal{P}$. All the $(q+1)$ points in $\mathcal{P}$ lie in a conic and $\mathcal{P}$ is left invariant by a subgroup $PGL(2,q)$ of the linear automorphism group $PGU(3,q)$ of $\mathcal{H}$. Using classical tools both from Algebraic and Finite Geometry, such as linear series on curves and the action of $PGL(2,q)$ on points and lines in the projective plane $PG(2,q)$, we completely determine the parameters of those codes for $m \leq q(q-1)/2$. Remarkably, in some cases the Goppa designed minimum distance is beaten. Also, $\mathrm{Aut}(C_L(D,G))$ contains a subgroup $G \cong P\Gamma L(2,q)$; we investigate the question whether G is the full automorphism group.

[1] G. Korchmáros and G.P. Nagy, Hermitian codes from higher degree places, *Journal of Pure and Applied Algebra*, **217** (2013), 2371-2381.

[2] G. L. Matthews, Weierstrass pairs and minimum distance of Goppa codes, *Des. Codes Cryptogr.*, **22** 107-121, 2001.

[3] H. Stichtenoth, A note on Hermitian codes over $GF(q^2)$, *IEEE Trans. Inform. Theory* **34** (1988), 1345-1348.

[4] C. Xing, H. Chen, Improvements on parameters of one-point AG codes from Hermitian curves, *IEEE Trans. Inform. Theory* **48** (2002), 535-537.

Orthogonal graphs over finite commutative rings of odd characteristic

SONGPON SRIWONGSA (Chulalongkorn University, Bangkok, Thailand)

Graphs arising from linear algebra over finite fields and finite commutative rings have been widely studied. In 2006, Tang and Wan worked on the general symplectic graph over the finite field $\mathbb{F}_q$. Meemark and Prinyasart

introduced the symplectic graphs over the ring of integers modulo p^n. Meemark and Puirod extended this work to the symplectic graphs over finite local rings and finite commutative rings. Gu and Wan defined and studied the orthogonal graphs over finite fields $\mathbb{F}_q$ of odd characteristic. The orthogonal graphs of characteristic 2 were introduced by Wan and Zhou. Recently, Li, Guo and Wang studied the orthogonal graphs over Galois rings of odd characteristic using matrix theory over finite Galois rings. In this work, we defined orthogonal space (V, β) and the orthogonal graphs over finite commutative rings of odd characteristic as $\mathcal{G}_{\mathrm{O}_R(V)}$ whose vertex set $\mathcal{V}(\mathcal{G}_{\mathrm{O}_R(V)})$ is the set of lines

$$\{R\vec{x} : \vec{x} \text{ is a unimodular vector in } V \text{ and } \beta(\vec{x}, \vec{x}) = 0\}$$

its adjacency condition is given by

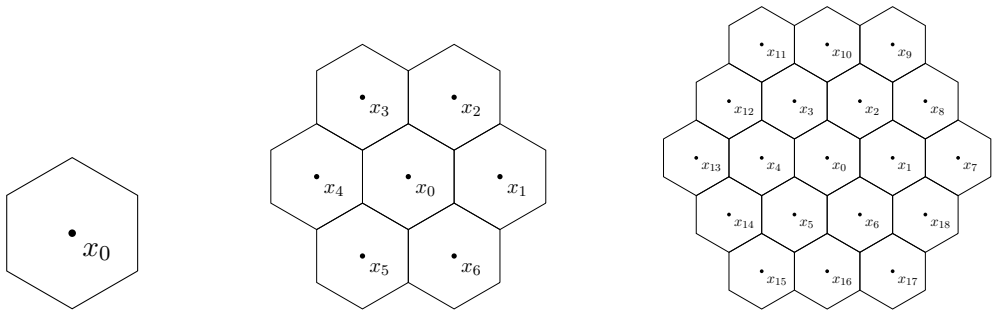
$$R\vec{x} \text{ is adjacent to } R\vec{y} \iff \beta(\vec{x}, \vec{y}) \in R^{\times} (\text{or equivalently, } \beta(\vec{x}, \vec{y}) = 1).$$

We show that our graph is vertex and arc transitive and determine the chromatic number. Moreover, if R is a finite local ring, we can classify if it is a strongly regular of quasi-strongly regular graph and we obtain its automorphism group by using the results of the orthogonal graphs over finite fields.

On the Existence of Aperiodic Complementary Hexagonal Lattice Arrays

YIN TAN (University of Waterloo, Canada)

Binary aperiodic and periodic complementary sequences have been studied extensively due to their wide range of applications in engineering, for example in optics, radar and communications. They are linked to topics in coding theory, combinatorics and Boolean functions as well. Starting from the binary aperiodic complementary sequences pair, i.e. the so-called Golay pair, complementary sequences have been generalized either by being defined over larger alphabets or by being defined from one dimension to multi-dimensions. Recently, Ding and Tarokh introduced and constructed the aperiodic complementary two-dimensional arrays over the alphabet $\mathfrak{A}_p^* = \{\zeta_p^i : 0 \le i \le p-1, p \text{ is a prime number}\}$, whose support set is a subset of the hexagonal lattice. In most cases, the support set is chosen as a set of ℓ-layer consecutive hexagons, and we call an array with such a support set and over alphabet $\mathfrak{A}_p^*$ an *ℓ-layer hexagonal lattice array* (ℓ-HLA for short), see below for examples when $\ell = 1, 2, 3$. It was demonstrated by Ding and Tarokh that aperiodic complementary ℓ-HLA can be used on coded aperture imagining with ideal efficiency.



(a) 1-HLA (b) 2-HLA (c) 3-HLA

In this work, we study the conditions for which aperiodic complementary set of ℓ-HLAs exist (may have more than two ℓ-HLAs). We first show that aperiodic complementary hexagonal lattice arrays over the alphabet $\mathfrak{A}_p^*$ leads to aperiodic (hence periodic) complementary sequences over the alphabet $\mathfrak{A}_p = \mathfrak{A}_p^* \cup \{0\}$. Then we make use of group ring equations to characterize periodic complementary sequences over alphabet $\mathfrak{A}_p$. As of independent interest, we show that, if the alphabet of the periodic complementary sequences is $\mathfrak{A}_p^*$, the

notion of periodic complementary sequences is equivalent to the notion of certain relative difference family. The conditions for the existence of periodic complementary sequences over alphabet $\mathfrak{A}_p$ are derived from this characterization. As a result, we determine the existence of a pair (triple) aperiodic complementary binary hexagonal lattice arrays whose support set is an ℓ-layer consecutive hexagons. A table listing the existence status for a pair of complementary hexagonal lattice arrays with $1 \leq \ell \leq 20$ is presented.

On some dual hyperovals

HIROAKI TANIGUCHI (National Institute of Technology, Kagawa College, Japan)

The concept of dimensional dual hyperoval was introduced by Huybrechts and Pasini in [1]. We show that the dual hyperovals $S_c(l, GF(2^r))$ in [2], where l, r positive integers, and $c \in GF(2^r)$ with the absolute trace $Tr(c) = 1$, have interesting properties. For example, we show that a $S_c(l, GF(2^r))$ is simply connected iff $GF(2^r) = GF(2)(c)$, which gives us many non-isomorphic examples of simply connected dual hyperovals. We show that $S_c(l, GF(2^r))$ is covered by $S_c(l', GF(2^{r'}))$ if $lr = l'r'$ and r' is a divisor of r. We also determine the automorphism group of $S_c(l, GF(2^r))$, and show that $Aut(S_c(l, GF(2^r)))$ is a subgroup of $Aut(S_c(l', GF(2^{r'})))$ if $lr = l'r'$ and $r'|r$.

[1] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, Contribution to Algebra and Geometry, **40** (1999), 503–532.

[2] H. Taniguchi, New dimensional dual hyperovals, which are not quotients of the classical dual hyperovals, Discrete Mathematics, **337** (2014), 65–75.

Constacyclic codes over a class of finite local non-chain Frobenius ring

HORACIO TAPIA-RECILLAS (Universidad Autónoma Metropolitana-I, México)

Following the work of R. Hammons et al., the study of linear codes over finite rings was considered a worthwhile research topic. Progress has been made in several directions including the description of structural properties of codes over several families of rings, particularly finite chain rings. A generalization of cyclic codes are the γ-constacyclic codes, i.e., those codes invariant under the mapping
$\sigma_\gamma : \mathrm{A}^n \longrightarrow \mathrm{A}^n$ given by $\sigma_\gamma(a_0, a_1, ..., a_{n-1}) = (\gamma a_{n-1}, a_0, ..., a_{n-2})$, where γ is a unit of the finite ring A taken as the alphabet.
An interesting family of rings in Coding theory is the finite local Frobenius rings, due to the fact that MacWilliams identities on the weight enumerator polynomial of a linear code are satisfied.
Finite chain rings are a subfamily of finite local Frobenius rings and γ-constacyclic codes over finite chain rings have been studied by several researchers, thus it would be attractive to study this type of
codes over finite local non-chain Frobenius rings.
In this talk results are given on the number and structure of γ-constacylic codes in which the alphabet is a finite local non-chain Frobenius ring, the maximal ideal of which has nilpotency index 3, and the length of the code is relatively prime to the characteristic of the residue field of the ring. It is worth mentioning that this family of rings contains the finite local non-chain Frobenius rings with p^4 elements, where p is a prime.

Research done with the collaboration of C. A. Castillo-Guillén (UAM-I and ESIME-IPN) and C. Rentería-Márquez (ESFM-IPN)

k-normal elements are cyclic vectors of Frobenius

DAVID THOMSON (Carleton University, Canada)

The notion of a k-normal element over a finite field was introduced by Huczynska, et al (2013), as generalizations of normal elements. In this talk, we consider k-normal elements as cyclic vectors of Frobenius-stable subspaces of finite fields. The full splitting of the finite field into Frobenius-stable subspaces admitting cyclic vectors then gives a succinct description of all k-normal elements. Explicit descriptions of the k-normal elements for all k depends on the explicit factorization of $x^n - 1$, so we give as examples some explicit characterizations of k-normal elements in fields where this factorization is known.

This is joint work with Colin Weir (Simon Fraser University).

The digraphs of the kth power mapping over some finite commutative rings

ITTIWAT TOCHAROENIRATTISAI (Chulalongkorn University, Bangkok, Thailand)

Let n, r be any positive integers and p a prime. Consider the quotient ring $R = \mathbb{Z}_{p^n}[x]/(f(x)^a)$, where $f(x)$ is a monic polynomial in $\mathbb{Z}_{p^n}[x]$ of degree r such that the reduction $\overline{f}(x)$ in $\mathbb{Z}_p[x]$ is irreducible, and $a \geq 1$. If $a = 1$, this ring is called a Galois ring. For $k \geq 2$, let $G^{(k)}(R)$ be the kth power mapping digraph over R whose vertex set is R and there is a directed edge from a to b if and only if $a^k = b$.
This functional digraph is defined by using the idea of Somer and Křížek who studied the structure of digraphs $G^{(k)}(\mathbb{Z}_n)$. Later, Y. Meemark and N. Wiroonsri worked on digraphs $G^{(k)}(\mathbb{F}_{p^n}[x]/(f(x)))$, where $f(x)$ is a monic polynomial of degree ≥ 1 in $\mathbb{F}_{p^n}[x]$, where $\mathbb{F}_{p^n}$ is the field with p^n elements and gave some conditions for symmetric digraphs. In this work, we determine the exponent of R and study the kth power mapping digraph (t-cycle, indegree of each vertex, etc.). In addition, we present some conditions when our digraphs are symmetric.

On the inverses of some classes of permutations of finite fields

ALEKSANDR TUXANIDY (Carleton University, Canada)

Recently much progress has taken place in the area of construction of permutation polynomials (PPs) over finite fields. However, how to go about inverting such permutations has remained unclear to the present. There is, in literature, a marked absence of explicit formulas describing compositional inverses, but also a general lack of methods to attain these formulas. Nevertheless there is some recent progress in this area.
In this talk we discuss new methods for the inversion of PPs over finite fields, as well as present several new results in the area.

This is a joint work with Qiang Wang

Algebraic Problems Equivalent to Beating Exponent 3/2 for Polynomial Factorization over Finite Fields

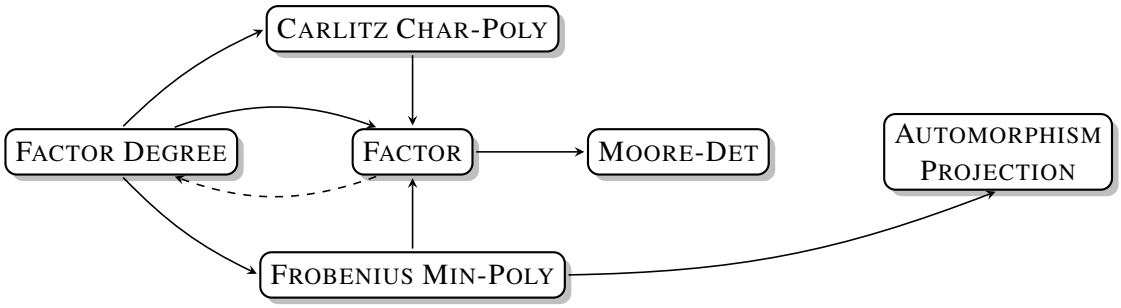
CHRIS UMANS (California Institute of Technology, USA)

The fastest known algorithm for factoring univariate polynomials over finite fields is the Kedlaya-Umans [KU08] implementation of the Kaltofen-Shoup algorithm [KS98, § 2] using fast modular composition. It is randomized and takes $\mathcal{O}\left((n^{3/2}\log q + n\log^2 q)^{1+o(1)}\right)$ time to factor polynomials of degree n over $\mathbb{F}_q$ into their irreducible factors. A significant open problem is to improve the $3/2$ exponent.

In this work, we study a collection of algebraic problems and establish a web of reductions between them. A consequence is that an algorithm for any one of the problems with exponent better than $3/2$ would yield an

algorithm for polynomial factorization with exponent better than $3/2$. A listing of the problems follows with a diagram illustrating the reductions.

- FACTOR: *Given a monic $f \in \mathbb{F}_q[x]$, write f as a product of its irreducible factors.*
- FACTOR DEGREE: *Given a reducible $f \in \mathbb{F}_q[x]$, find the degree of a non trivial factor of f.*
- FROBENIUS MIN-POLY: *Given a monic square free $f \in \mathbb{F}_q[x]$, compute the minimal polynomial of the Frobenius endomorphism on $\mathbb{F}_q[x]/(f)$ which takes $x \mod f$ to $x^q \mod f$.*
- CARLITZ CHAR-POLY: *Given a monic square free $f \in \mathbb{F}_q[x]$, compute the characteristic polynomial of the Carlitz endomorphism on $\mathbb{F}_q[x]/(f)$ which takes $a(x) \mod f$ to $xa(x) + a(x)^q \mod f$.*
- MOORE-DET: *Given a monic square free $f \in \mathbb{F}_q[x]$ and a positive integer $m \leq \deg(f)$, compute the determinant modulo f of the m by m square matrix M with entries $m_{ij} := x^{jq^i}$.*
- AUTOMORPHISM PROJECTION: *Given a monic square free $f \in \mathbb{F}_q[x]$, $\alpha \in \mathbb{F}_q[x]/(f)$ and an $\mathbb{F}_q$-linear transformation $u : \mathbb{F}_q[x]/(f) \longrightarrow \mathbb{F}_q$, compute $u(\alpha^{q^i}), \forall i \in \{1, 2, \ldots, \deg(f)\}$.*



Solid lines indicate nearly linear time reductions. The dotted line indicates that an algorithm with exponent less that $3/2$ for FACTOR DEGREE would yield one with exponent less than $3/2$ for FACTOR. An interesting open question is if the dotted line can be made solid. Except for AUTOMORPHISM PROJECTION, every listed problem has a known randomized algorithm with exponent $3/2$. If the matrix multiplication exponent is 2, then a randomized algorithm for AUTOMORPHISM PROJECTION with exponent $3/2$ is known. An open problem is if this dependence on the matrix multiplication exponent can be removed. Kaltofen and Shoup [KU08] established that FACTOR is nearly linear time reducible to AUTOMORPHISM PROJECTION assuming an $\mathbb{F}_q$-linear straight line program algorithm for AUTOMORPHISM PROJECTION. Our reductions to AUTOMORPHISM PROJECTION hold without any assumptions.
Most of our reductions entail substantial new ideas.

(Based on joint work with Zeyu Guo and Anand Kumar Narayanan.)

[KS98] E. Kaltofen and V. Shoup, Subquadratic-time factoring of polynomials over finite fields, Math. Comput., 67(223):1179-1197, July 1998.

[KU08] K. Kedlaya and C. Umans, Fast modular composition in any characteristic, Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS). pages 146-155. 2008.

Constructing covering arrays from m-sequences

GEORGIOS TZANAKIS (Herzberg Laboratories Ottawa, Canada)

A *covering array* $CA(N; t, k, v)$ is a $N \times k$ array with entries from an alphabet of size v, with the property that any $N \times t$ sub-array has at least one row equal to every possible t-tuple. The minimum number of rows N such that a $CA(N; t, k, v)$ exists is the *covering array number* for the parameters t, k, and v. Few constructions of covering arrays are known that attain the minimum number of rows. New constructions aim instead to improve upon current upper bounds for covering array numbers.

A *q-ary m-sequence* is a linear recurrence sequence of elements from $\mathbb{F}_q$ with maximum period. Moura, Raaphorst and Stevens (2014) give a construction for covering arrays of strength 3 over $\mathbb{F}_q$ using q-ary m-sequences. In this talk we present a method that extends this construction to strengths higher than 3. Our computer implementation of this method yielded 22 new covering arrays that improve upon previously best known upper bounds for covering array numbers.
Furthermore, our findings show connections of our construction with finite geometry.

This is joint and ongoing work with Lucia Moura (University of Ottawa), Daniel Panario, and Brett Stevens (Carleton University).

On coefficients of powers of polynomials and their compositions

QIANG WANG (Carleton University, Canada)

For any given polynomial f over the finite field $\mathbb{F}_q$ with degree at most $q-1$, we associate it with a $q \times q$ matrix $A(f) = (a_{ik})$ consisting of coefficients of its powers $(f(x))^k = \sum_{i=0}^{q-1} a_{ik}x^i$ modulo $x^q - x$ for $k = 0, 1, \ldots, q-1$. This matrix has some interesting properties such as $A(g \circ f) = A(f)A(g)$ where $(g \circ f)(x) = g(f(x))$ is the composition of the polynomial g with the polynomial f. In particular, $A(f^{(k)}) = (A(f))^k$ for any k-th composition $f^{(k)}$ of f modulo $x^q - x$ with $k \geq 0$. As a consequence, we prove that the rank of $A(f)$ gives the cardinality of the value set of f. Moreover, if f is a permutation polynomial then the matrix associated with its inverse $A(f^{(-1)}) = A(f)^{-1} = PA(f)P$ where P is an antidiagonal permutation matrix. As an application, we study the period of a nonlinear congruential pseduorandom sequence $\bar{a} = \{a_0, a_1, a_2, ...\}$ generated by $a_n = f^{(n)}(a_0)$ with initial value a_0, in terms of the order of the associated matrix. Finally we show that $A(f)$ is diagonalizable in some extension field of $\mathbb{F}_q$ when f is a permutation polynomial over $\mathbb{F}_q$.

This is a joint work with Gary L. Mullen and Amela Muratović-Ribić.

The Structure of Holomorphic Differentials

KENNETH A. WARD (NYU-ECNU, Shanghai)

We discuss recent developments in the theory of Galois module structure for holomorphic differentials, focusing on wild ramification where less is known. We determine explicitly the representation of the Galois group for cyclotomic function fields and rank one Drinfel'd modules in characteristic $p > 0$. We will also discuss various other approaches to this problem which employ group structure, ramification, and Witt vectors.

A function-field analogue of Conway's topograph

MICHAEL WIJAYA (Dartmouth College, USA)

In [1], Conway introduces a new visual method to display values of an integral binary quadratic form $Q(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$. This topograph method, as he calls it, leads to a simple and elegant method of classifying all integral binary quadratic forms and answering some basic questions about them. In particular, Conway shows that the topograph of any definite binary quadratic form has a unique "well", while the topograph of any indefinite binary quadratic form has a unique "river". In our work, we develop an analogue of Conway's topograph method for binary quadratic forms with coefficients in $\mathbb{F}_q[T]$, where q is an odd prime power.

Let $A = \mathbb{F}_q[T]$ be the ring of polynomials over a finite field of odd order q and $K = \mathbb{F}_q(T)$ its field of fractions. The completion of K with respect to the usual valuation arising from the degree function is $\widehat{K} = \mathbb{F}_q((T^{-1}))$.

Our starting point is the connection between Conway's topograph method and hyperbolic geometry. Conway himself notes that it is most natural to consider the 3-regular tree central to his approach as embedded on the hyperbolic plane. In [2], Paulin provides an interpretation of continued fraction expansions of elements of $\widehat{K}$

in terms of the action of $\mathrm{SL}_2(A)$ on the Bruhat–Tits tree $\mathcal{T}_{q+1}$ of $\mathrm{SL}_2(\widehat{K})$. Since the classical reduction theory for indefinite integral binary quadratic forms relies on the theory of continued fractions, Paulin's work led us to consider $\mathcal{T}_{q+1}$ as a suitable function-field analogue of the hyperbolic plane for our purposes.

After we recast the underlying infrastructure of Conway's topograph in terms of constructions on $\mathcal{T}_{q+1}$, we formulate and prove an analogue of Conway's climbing lemma. We then show that just as in the classical setting, there is a unique "well" on the topograph of any definite binary quadratic form over A and a unique "riverön the topograph of any indefinite binary quadratic form over A.

[1] John H. Conway, *The sensual (quadratic) form*, Carus Mathematical Monographs, vol. 26, Mathematical Association of America, Washington, DC, 1997.

[2] Frédéric Paulin, *Groupe modulaire, fractions continues et approximation diophantienne en caractéristique* p, Geom. Dedicata, **95** (2002), 65–85.

On cyclic codes of general type and the construction of Quantum MDS codes

MAOSHENG XIONG (Hong Kong University of Science and Technology)

Quantum error-correcting codes are useful in quantum computing and in quantum communications. Quantum maximum-distance-separable (MDS) codes form an important class of quantum codes. It has been a great challenge to construct new quantum MDS codes. A lot of recent interest has been on constacyclic codes which slightly generalize cyclic codes and their remarkable applications on constructing new quantum MDS codes. In the talk, we show that by extending the concept of constacyclic codes even further, we can construct many new quantum MDS codes with more flexible parameters.

Maximal curves from subcovers of the GK-curve

GIOVANNI ZINI (Universitá degli studi di Firenze, Italy)

For every $q = n^3$ with n a prime power greater than 2, the GK-curve $\mathcal{X}$ is an $\mathbf{F}_{q^2}$-maximal curve that is not $\mathbf{F}_{q^2}$-covered by the Hermitian curve. The problem of giving explicit equations for maximal curves is relevant for applications to Coding Theory. In this work we compute explicit equations for some families of maximal curves that are Galois-covered by the GK-curve.
We also determine the genera of the curves; some of them are new values in the spectrum of genera of $\mathbf{F}_{q^2}$-maximal curves. We provide some further examples of maximal curves that cannot be covered by the Hermitian curve, as well as infinite families of maximal curves not Galois-covered by the Hermitian curve.

This is a joint work witk Massimo Giulietti and Luciane Quoos.