MOHAMMED BARDESTANI

The degree of the splitting field of a polynomial over finite fields

Motivated by the work of Dixon and Panario on the degree of the splitting field of a random polynomial over a finite field, we will consider the dual of this distribution by studying the splitting field of a given polynomial over finite fields $\mathbb{F}_p$ when $p$ varies.

DANIELE BARTOLI

Large Algebraic curves and Random Network Codes

(joint work with Matteo Bonini and Massimo Giulietti) 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.


ROBERT COULTER

_Coordinatising projective planes revisited_

Coordinatisation is a well-known method for studying projective planes by introducing a coordinate system onto the plane and then deriving algebraic properties on the coordinates. Through the medium of a three-variabled function known as a planar ternary ring (PTR), an algebraic representation of the plane is obtained that is equivalent to the plane.

In this talk we will revisit this coordinatising method for planes of prime power order. We will discuss how, by restricting to such orders, this allows us to represent the PTR by a three-variabled polynomial, naturally called a PTR polynomial.

The motivation for doing this is to try to exploit the theory of polynomials over finite fields to get meaningful/useful restrictions on PTR polynomials from the properties of the plane/PTR. These properties are closely connected to central collineations and the Lenz-Barlotti classification system.

Ultimately, the question is whether or not we can utilise the classification system and the theory of polynomials together to derive results on projective planes. The talk’s central objective is to show how this can be done. We’ll end up discussing not just the coordinatisation method, PTR polynomials, and the Lenz-Barlotti classification, but also a form of representation theory for single and bivariate polynomials.

BENCE CSAJBOK

_Minimal number of lines meeting an n-set of PG(2,q), q odd, in an odd number of points._

This question was studied lately by Balister, Bollobás, Fredi and Thompson, and also by Vandendriessche because of applications to coding theory. We use polynomial techniques to deduce new results about Rdei type blocking sets of PG(2,q) and apply them to improve a lower bound of Balister et al., and to answer an open question of Vandendriessche.

SEYED HOSSEINI LAVASANI

_Algorithmic approach to identify weak trace zero varieties._

I would like to go over function field related algorithms that I used to generate curves with weak trace zero varieties. This talk is intended to foster collaboration about the choice and efficiency of these algorithms and determine if I can use better method for each stage.
DAVID JAO

Common Subexpression Algorithms for Space-Complexity Reduction of Gaussian Normal Basis Multiplication

The use of normal bases for representing elements in a binary field is attractive in some applications because it is easy to perform squaring operations in hardware. In such cases, the costs of implementing the multiplication operation become a primary concern. We present new algorithms for reducing the space complexity of Gaussian normal basis (GNB) multipliers over binary fields of odd dimension. Compared to previous results, our approach incurs no additional costs in time complexity, and achieves improvements in space complexity over a wide range of finite fields and digit sizes. For the binary fields specified in the NIST FIPS 186-3 elliptic curve digital signature algorithm (ECDSA) standards document, our algorithms reduce by 16

MICHEL LAVRAUW

Finite semifields: recent developments and applications

The theory of finite semifields has received a lot of attention in recent years. The concept was of a semifield was first studied by L. E. Dickson in 1905 [1]. His motivation was purely algebraic: what happens if one omits the axiom of associativity for multiplication in the definition of a finite (skew)field? This question arose naturally after it had been shown that the axiom of commutativity for multiplication is redundant in the axiomatic definition of a finite field (the Wedderburn Theorem or Dickson-Wedderburn Theorem).

Nowadays these (non-associative) algebraic structures are called semifields, a notion introduced by Knuth [2] They turn up in various areas of mathematics related to finite fields, and play a key role in finite geometry (Galois geometry).

We will introduce the main concepts and explain recent developments in the theory of finite semifields, and will conclude with applications to cryptography and coding theory. We will follow the notation and terminology from [3].

References


Maiorana-McFarland bent functions with respect to the subfield

Gohar M. Kyureghyan
Otto-von-Guericke University Magdeburg, Germany

A bent function is a Boolean function with an even number of variables which has the maximal possible Hamming distance from the set of affine Boolean functions. More precisely, a function $f : \mathbb{F}_{2^t} \rightarrow \mathbb{F}_2$ is called bent if

$$\sum_{x \in \mathbb{F}_{2^t}} (-1)^{f(x) + \text{Tr}_{2t}(\alpha x)} = \pm 2^\frac{2^t}{2},$$

for any $\alpha \in \mathbb{F}_{2^t}$, where $\text{Tr}_{2t}$ is the absolute trace on $\mathbb{F}_{2^t}$.

The Maiorana-McFarland bent functions on $\mathbb{F}_{2^t}$, are the concatenation of $2^t$ different affine functions, defined on some fixed subspace of dimension $t$ of $\mathbb{F}_{2^t}$. If the fixed subspace is the subfield $\mathbb{F}_{2^t}$, then the corresponding bent functions are called Maiorana-McFarland with respect to the subfield and they are defined as:

Let $W \subset \mathbb{F}_{2^t}$ be such that $\mathbb{F}_{2^t} = \mathbb{F}_{2^t} \oplus W$. Assume that a Boolean function $f : \mathbb{F}_{2^t} \rightarrow \mathbb{F}_2$ can be expressed in the form

$$f(x) = f(y + a) = \text{Tr}_{t} (y \pi(a) + h(a)),$$

where $x = y + a$, with $y \in \mathbb{F}_{2^t}$, $a \in W$, $\pi, h : W \rightarrow \mathbb{F}_{2^t}$ and $\pi$ is bijective. Then $f$ is bent and it belongs to the subclass $\mathcal{M}(\mathbb{F}_{2^t})$ of Maiorana-McFarland bent functions with respect to the subfield.

In this talk we describe briefly the cryptographic properties of bent functions. Further we discuss how it can be seen whether a Boolean function $f$ is in $\mathcal{M}(\mathbb{F}_{2^t})$. As an application we introduce two families of maps $F : \mathbb{F}_{2^t} \rightarrow \mathbb{F}_{2^t}$ with the maximum possible number of bent components $\text{Tr}_{2t}(\alpha \cdot F(x))$, $\alpha \in \mathbb{F}_{2^t}$.
**PETR LISONEK**

*Large Highly nonlinear functions on finite fields*

We will consider two classes of highly nonlinear mappings from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$: bent functions and almost perfect nonlinear (APN) functions. The properties that make these functions relevant for applications in cryptography are their high nonlinearity and low differential uniformity.

We will consider Boolean bent functions ($m = 1$) as well as vectorial bent functions ($m > 1$). In particular we will focus on Dillon type bent functions in the trace form, where we will deal with the monomial case and the multinomial case. We will see efficient characterizations, constructions and nonexistence results for these families of functions. The characterizations are often given in terms of certain types of exponential sums, for which we will observe natural and fruitful connections with algebraic curves.

We will consider the open problem of the existence of APN permutations in even dimensions greater than 6. There is a known connection with binary linear codes of minimum distance 5 whose dual code decomposes as a direct sum of two simplex codes. We will consider some related combinatorial problems for binary linear codes.

**FELICE MANGANIELLO**

*Theory and Applications of Skew Polynomial Rings*

Skew polynomial rings are a non commutative generalization of polynomial rings. Their applications to coding theory and cryptography have been investigated in the last decade. In this talk, we explore the algebraic structure of these rings when defined over a finite field, as well as the evaluation of their polynomials. From the evaluation, we construct a notion of independency which induces a matroid structure on the finite field. Two are the applications we then focus on: a duality theory for codes defined by skew evaluation and the use of the underlined matroid in multicast network communication.

**GUILLERMO MATERA**

*On the computation of rational points of a hypersurface over a finite field.*

I will analyze a family of algorithms for computing rational points of hypersurfaces defined over a finite field based on searches on ”vertical strips”, namely searches on parallel lines in a given direction. I will discuss the asymptotic probability distribution of the number of searches, showing that it decays with an exponential ratio. I will also consider the probability distribution of outputs, using the notion of Shannon entropy, and prove that the algorithm somewhat close to any ”ideal” equidistributed algorithm.

This is joint work with Eda Cesaratto and Mariana Prez.
LUCIANE QUOOS

*New Maximal Curves over finite fields not covered by the Hermitian Curve.*

For every $q = n^3$ with $n$ a prime power greater than 2, the GK-curve is an $\mathbb{F}_{q^2}$-maximal curve that is not $\mathbb{F}_{q^2}$-covered by the Hermitian curve curve. In this paper we compute explicit equations for some families of curves that are Galois-covered by the GK curve. New values in the spectrum of genera of $\mathbb{F}_{q^2}$-maximal curves are obtained, as well as some further examples of maximal curves that cannot be covered by the Hermitian curve. (This is a joint work with M. Giulietti and G. Zini).

CLAUDIO QURESHI

*Estimates for the cycle structure of iterating Redei functions.*

Shallit and Vasiga (2004) obtain several results about tails and cycles in orbits of iterations of quadratic polynomials over prime fields. These results were extended to repeated exponentiation by Chou and Shparlinski (2004). In this talk, using a different strategy based on isomorphisms of Redei iteration graphs, we show analogous results to Chou and Shparlinski but for Redei functions. This approach also extends our previous work on Redei actions on finite fields (Qureshi and Panario, to appear in SIAM Journal on Discrete Mathematics).

MORGAN RODGERS

*Tutorial of field reduction techniques*

Field reduction is a technique whereby we consider a vector space over a field $\mathbb{E}$ over one of it’s subfields $\mathbb{F}$, in order to obtain a vector space of higher dimension. If $V$ is $r$-dimensional over $\mathbb{E}$, and $\mathbb{F}$ is a subfield with index $t$, then $V$ is $rt$-dimensional over $\mathbb{F}$; in terms of the associated finite geometries over finite fields, from a projective space $PG(r-1, q^t)$, we obtain a projective space $PG(rt-1, q)$. When applied to a quadratic space, we can use the trace map to get a quadratic space over the smaller field.

The field reduction map has many important uses. For example, the point set of $PG(r-1, q^t)$ maps to a Desarguesian spread of $PG(rt-1, q)$; also field reduction techniques have been used to study two-intersection sets, and other interesting geometric objects. One application we will focus on in this talk relates to cyclic collineation groups; we will look at how to exploit the multiplicative group of $\mathbb{F}_{q^t}$; multiplication by a scalar induces the identity map on $PG(r-1, q^t)$, but not necessarily on $PG(rt-1, q)$. Certain number-theoretic conditions can allow us to determine the order of the collineation group induced on this space; in many cases we can obtain a nice representation for a large cyclic
RENATE SCHEIDLER

Construction of all cubic function fields of a given square-free discriminant

For any square-free polynomial $D$ over a finite field of characteristic at least $5$, we present an algorithm for generating all cubic function fields of discriminant $D$. We also provide a count of all these fields according to their splitting at infinity. The method uses a construction due to Berwick as well as ideas from an unpublished manuscript by D. Shanks from the late 1980s, and makes extensive use of ideal arithmetic in the corresponding quadratic resolvent field of discriminant $-3D$. While the mathematical ingredients of our construction are largely classical, our algorithm has the major computational advantage of producing very small minimal polynomials for the fields in question.

This is joint work with Mike Jacobson, Yoonjin Lee and Hugh Williams.

YIN TAN

Graphs, Schemes and Codes from Quadratic Zero-difference Balanced Functions

The topics of this work include: (1) new constructions of strongly (distance) regular graphs, association schemes and linear codes from a special type of quadratic zero-difference balanced functions over fields $GF(p^n)$. (2) The geometry behind such special quadratic zero-difference balanced functions. (3) The distribution of the Walsh spectrum of such zero-difference balanced functions; and their application on determining the weight distribution of their relevant codes. (4) The work presented here unifies and generalizes previous work on (almost) perfect nonlinear functions.

COLIN WEIR

The proportion on non-ordinary hyperelliptic curves

It is well known that an elliptic curve (a hyperelliptic curve of genus 1) in characteristic $p$ is either ordinary or supersingular depending on whether or not it has a point of order $p$ defined over the algebraic closure. Moreover, it is well understood how many supersingular elliptic curves there are for a given characteristic. We will discuss generalizations of this to higher genus hyperelliptic curves, and present recent joint work with Derek Garton on the size of the non-ordinary locus of a fixed genus.
MAOSHENG XIONG

Cyclic codes of general type and construction of quantum MDS codes.

Recently constacyclic codes have proved useful in the construction of quantum MDS codes. In this talk we show that by extending the concept much further, we can construct many new quantum MDS codes.