Theory and Applications of Finite Fields
Corps finis: théorie et applications

(Org: **Daniel Panario** (Carleton University), **Luciane Quoos** (Federal University of Rio de Janeiro), **Ivelisse Rubio** (University of Puerto Rico) and/et **David Thomson** (Carleton University))

TONI BLUHER, Department of Defense
Dickson polynomials

Dickson polynomials, which are close relatives of the Chebyshev polynomials, are defined by the recursion $D_0(x) = 2$, $D_1(x) = x$, and $D_{k+1}(x) = xD_k(x) - D_{k-1}(x)$. The American mathematician Leonard Eugene Dickson proved in his PhD thesis (1896) that $D_k(x)$ is a permutation polynomial on the field with p^n elements if and only if GCD$(k, p^{2n} - 1) = 1$. Since then, there have been many theorems about the values taken by Dickson polynomials over finite fields. We obtain new results following this theme, including some surprising connections with elementary number theory. This talk assumes only a background in finite fields.

LISA BROMBERG, United States Military Academy
Navigating in the Cayley graph of $\mathrm{SL}(2, \mathbb{F}_p)$ *and applications to hashing*

Hashing with matrices refers to a simple idea of using a pair of matrices, A and B (over a finite ring), to hash the "0" and "1" bit, respectively, and then to hash an arbitrary bit string in the natural way, by using multiplication of matrices. Since there are many known pairs of 2×2 matrices over $\mathbb{Z}$ that generate a free monoid, this yields numerous pairs of matrices over $\mathbb{F}_p$, for sufficiently large primes p, that are candidates for collision-resistant hashing. However, this trick can "backfire", and lifting matrix entries to $\mathbb{Z}$ may facilitate finding a collision. This "lifting attack" was successfully used by Tillich and Zemor in the special case where two matrices A and B generate (as a monoid) the whole group $\mathrm{SL}_2(\mathbb{Z})$. However, in this paper we show that the situation with other, "similar", pairs of matrices from $\mathrm{SL}_2(\mathbb{Z})$ is different, and the "lifting attack" can (in some cases) produce collisions in the group generated by A and B, but not in the positive monoid. Therefore, we argue that for these pairs of matrices, there are no known attacks at this time that would affect security of the corresponding hash functions. We also give explicit lower bounds on the length of collisions for hash functions corresponding to some particular pairs of matrices.

ANTONIO CAFURE, UNGS, UBA, CONICET
Cyclotomic polinomials over finite fields

Let n be an odd natural number and let p be an odd prime such that $p \nmid n$. Following the techniques of [1] and well known results about cyclotomic polynomials, we are able to show that the coefficients of the cyclotomic polynomial $\Phi_{np} \in \mathbb{Q}[t]$ can be computed as the unique solution of a linear system of equations $Tx = b$, where T is a semicirculant matrix involving coefficientes of Φ_n, and b is a vector whose entries are certain coefficients of Φ_n determined according to some congruences modulo p.

In this talk we will study to what extent this characterization of cyclotomic polynomials over the rationals may be considered over a finite field and the potential implications of such a characterization.

[1] A. Cafure y E. Cesaratto. Irreducibility criteria for reciprocal polynomials and applications. Am. Math. Month. 124, No 1, 37–53.

MARIA CHARA, Instituto de Matemática Aplicada del Litoral
An Artin-Schreier tower of function fields in even characteristic

Let $\mathbb{F}_2$ be a finite field with two elements. In 2006 Beleen, Garcia and Stichtenoth proved that any recursive tower of function fields over $\mathbb{F}_2$, defined by $g(Y) = f(X)$ with $g(T), f(T) \in F_2(T)$ and $\deg f = \deg g = 2$ is given by the Artin-Schreier equation

$$Y^2 + Y = \frac{1}{(1/X)^2 + (1/X) + b} + c$$

with $b, c \in \mathbb{F}_2$. They checked that all the posible cases were already considered in previous works, except when $b = c = 1$. In fact, they left as an open problem to determine whether this tower is asymptotically good or not over $\mathbb{F}_{2^s}$, for any positive integer s. In this talk we will discuss the asymptotic behavior of this tower.

RICARDO CONCEIÇÃO, Gettysburg College

Definition and first properties of Markov polynomials

The sequence of Markov numbers (A002559 in the OEIS)

$$1, 2, 5, 13, 29, 34, 89, 169, \ldots$$

is generated from the integral solutions of Markov's equation $x^2 + y^2 + z^2 = 3xyz$. In this talk, we define a sequence of polynomials over a finite field $\mathbb{F}_q$, with $q \equiv 1 \mod 4$, which is analogous to the sequence of Markov numbers. We discuss some recently discovered and conjectured properties of these so-called Markov polynomials.

CLAUDE GRAVEL, Tutte Institute for Mathematics and Computing

Permutations with one cycle of maximal length, and output bits of maximal algebraic degree

Let $n \geq 3$ be an odd positive integer. We study a subset $A \subset S_{2^n}$ for which every element has four properties. Properties are: (I) no more than $2n$ bits are needed to describe a permutation in A, (II) the algebraic degree of all the n output boolean functions is $n-1$; an element of A takes $(a_0, \ldots, a_{n-1}) = a \in \{0,1\}^n$ as an input and produces an output $(\varphi_0(a), \ldots, \varphi_{n-1}(a)) \in \{0,1\}^n$ where φ_j is a boolean function for $j \in \{0, \ldots, n-1\}$, (III) every permutation in A has one cycle of length 2^n, and (IV) the expected number of terms (products of the a_i's) of the boolean functions φ_j for $j \in \{0, \ldots, n-1\}$ is $O(2^{n-1})$. Every element in A is associated to some irreducible polynomial $Q \in \mathbb{Z}_2[X]$ such that $\deg(Q) = n$, and to an exponent $d \in \{n, \ldots, 2^n - 2\}$; the output of an element $a \in \{0,1\}^n$ is computed by (1) the input a be encoded as $P_a(X) = a_0 + \ldots + a_{n-1}X^{n-1}$, (2) let $R_{a,0}(X) = P_a(X)$ and for $\ell \in \{1, \ldots, n\}$, let $R_{a,\ell}(X) = (R_{a,\ell-1}(X) + X^d)^{-2^{\ell-1}} \mod Q(X)$, and (3) output the coefficients of $R_{a,n-1}(X)$. The cardinality of A is smaller than $\frac{1}{n}\sum_{d|n} 2^d \mu(\frac{n}{d})$ which is the number of irreducible polynomials of degree n. For a given n, characterizing polynomials that yields the four properties is my main goal together with proving the fourth property. Properties one and two are proven mathematically. Properties three and four are supported by symbolic computation with some yet unfigured steps for the proof of property three. I wish eventually to show that the ratio of the cardinality of A and $\frac{1}{n}\sum_{d|n} 2^d \mu(\frac{n}{d}) \in O\big(\frac{2^n}{n}\big)$ is *not* zero asymptotically with respect to n.

JONATHAN JEDWAB, Simon Fraser University

A strong external difference family with more than two subsets

Strong external difference families (SEDFs) were introduced by Paterson and Stinson as a more restrictive version of external difference families. SEDFs can be used to produce optimal strong algebraic manipulation detection codes. We characterize the parameters (v, m, k, λ) of a nontrivial SEDF that is near-complete (satisfying $v = km + 1$). We construct the first known nontrivial example of a (v, m, k, λ) SEDF having $m > 2$ subsets. The parameters of this example are $(243, 11, 22, 20)$, giving a near-complete SEDF, and its group is $\mathbb{Z}_3^5$. The construction uses the point-orbits of the Mathieu group M_{11} acting on the projective geometry PG$(4, 3)$.

This is joint work with Shuxing Li, Simon Fraser University.

DANIEL KATZ, California State University, Northridge

Valuations of Weil Sums of Binomials

Weil sums of binomials are finite field character sums that arise naturally in number theory and its technological applications. In cryptography, such sums determine the Walsh spectrum of a power permutation of a finite field, which measures its nonlinearity. Weil sums of binomials also determine 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

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

where

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

Let v_p be the p-adic valuation, and for fixed q and d let

$$V_{q,d} = \min_{a \in \mathbf{F}_q} v_p(W_{q,d}(a)),$$

so that $V_{q,d}$ indicates the p-divisibility of the entire Walsh spectrum $\{W_{q,d}(a) : a \in \mathbf{F}_q\}$. We present a proof that $V_{q,d}$ is never more than $2n/3$, where $q = p^n$. We also present stronger upper bounds in special cases and discuss some conjectures. This is joint work with Philippe Langevin of Université de Toulon and Sangman Lee and Yakov Sapozhnikov of California State University, Northridge.

CHRISTINE KELLEY, University of Nebraska-Lincoln
Multilevel coding and multistage decoding on partial erasure channels

Partial erasure channels have recently been introduced to model erasure events in applications such as flash memories. We show how multilevel coding and multistage decoding may be applied on different q-ary partial erasure channels for $q = p^k$, and classify when the subchannels are simple p-ary erasure channels. We show how to choose component codes to achieve channel capacity using multistage decoding in some cases. This is joint work with Carolyn Mayer and Kathryn Haymaker.

ARIANE MASUDA, New York City College of Technology, CUNY
Goppa Codes over Kummer extensions

We compute the Weierstrass semigroup at one totally ramified place for Kummer extensions defined by $y^m = f(x)^\lambda$ where $f(x)$ is a separable polynomial over $\mathbb{F}_q$. In addition, we compute the Weierstrass semigroup at two certain totally ramified places. Then we apply our results to construct one- and two-point Goppa codes with good parameters.

GRETCHEN MATHEWS, Clemson University
AG codes as products of Reed-Solomon codes

In this talk, we consider families of algebraic geometry (AG) codes which can be expressed as products of Reed-Solomon codes and discuss applications.

LUCIA MOURA, University of Ottawa
Ordered Orthogonal Array Construction Using LFSR Sequences

In this talk, we discuss a new construction of ordered orthogonal arrays (OOA) of strength t with $(q+1)t$ columns over a finite field $\mathbb{F}_q$ using linear feedback shift register sequences (LFSRs). OOAs are naturally related to (t, m, s)-nets, linear codes, and MDS codes. Our construction selects suitable columns from the array formed by all subintervals of length $\frac{q^t-1}{q-1}$ of an LFSR sequence generated by a primitive polynomial of degree t over $\mathbb{F}_q$. The set of parameters of our OOAs are the same as the ones given by Rosenbloom and Tsfasman (1997) and Skriganov (2002), but the constructed arrays are different. We experimentally verify that our OOAs are stronger than the Rosenbloom-Tsfasman-Skriganov OOAs in the sense that ours are "closer" to being a "full" orthogonal array. We also discuss how our OOA construction relates to previous techniques to build OOAs from a set of linearly independent vectors over $\mathbb{F}_q$, as well as to hypergraph homomorphisms. This is joint work with André Castoldi (Brazil), Daniel Panario (Canada) and Brett Stevens (Canada), which recently appeared in *IEEE Transactions on Information Theory* vol. 68 (2017).

LUCAS REIS, Universidade Federal de Minas Gerais
On the explicit factorization of $f(x^n)$ over finite fields.

Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree k and exponent e and n be a positive integer such that rad(n) divides $q-1$ and gcd$(ek, n) = 1$. In this talk we discuss the explicit factorization of the polynomial $f(x^n)$ over $\mathbb{F}_q$. In particular, we apply our main result to certain classes of cyclotomic polynomials.

This is a joint work with F.E. Brochero Martínez (Universidade Federal de Minas Gerais).

IVELISSE RUBIO, University of Puerto Rico, Río Piedras
A refinement of a theorem of Carlitz

We refine some results of Carlitz about the existence of non-trivial solutions of polynomial equations in several variables $Y_1, \ldots, Y_n$ and coefficients in $F_q[X]$ by considering the p-weight degrees of the polynomials. We also present an extension of a theorem of Moreno and Moreno that gives a bound on the p-divisibility of the number of solutions of this type of systems.

DAVID THOMSON, Carleton University
Doubly-periodic Costas arrays

A *Costas array* of order n is a $n \times n$ permutation array (of 0s and 1s) where the vectors connecting any two 1s are distinct. Costas arrays have optimal *autocorrelation*; hence they have applications in, e.g., RADAR and SONAR systems and for digital communications.

Costas arrays can equivalently be viewed as permutations f on $[n] = \{0, 1, \ldots, n-1\}$ such that for $d \in (0, n-1]$, $f(x+d) - f(x)$ are distinct for all $x \in [0, n-d-1]$. If the domain (respectively, codomain) of f is instead considered to be $\mathbb{Z}/n\mathbb{Z}$, the Costas array is *domain-periodic* (respectively, *range-periodic*) modulo n; geometrically, consider the array wrapped around a vertical (respectively, horizontal) cylinder. It is known that no Costas array may be simultaneously domain- and range-periodic modulo n, though the classical Welch construction of Costas arrays provides a map that is domain-periodic modulo $p-1$ and range-periodic modulo p.

We prove a 1993 conjecture of Golomb and Moreno that any array exhibiting the Welch style of dual-periodicity must be indeed be Welch. Doing so, we show the equivalent result that any polynomial $f \in \mathbb{F}_p[x]$ that satisfies: (1) $f(0) = 0$ and (2) $f(xd) - f(x)$ is a permutation for all $d \neq 1$, is a monomial permutation polynomial.

We will also present some generalizations and related open-problems.

ANDREAS WEINGARTNER, Southern Utah University
The degree distribution of polynomial divisors over finite fields

We will describe a number of asymptotic estimates related to the degree distribution of polynomial divisors over finite fields, as well as analogous estimates concerning the distribution of integer divisors. Due to a very recent discovery of an explicit formula for the constant factor in these asymptotic estimates, we are now able to give numerical approximations of this factor. For example, the proportion of monic polynomials of degree n over the field with two elements, which have a divisor of every degree up to n, is asymptotic to $3.400335...n^{-1}$ as n grows.