Theory and Application of Finite Fields
Théorie et applications de corps finis
(Org: **Daniel Panario**, **David Thomson** and/et **Qiang Wang** (Carleton University))

FARZANE AMIRZADE, Carleton University
QC-LDPC construction free of small size elementary trapping sets based on multiplicative subgroups of a finite field

An algebraic-based quasi-cyclic low-density parity-check (QC-LDPC) code is developed from an exponent matrix whose entries belong to a finite field $\mathbb{F}_q$, where q is a power of a prime. A QC-LDPC code with variable node degree m and check node degree n is an (m, n)-regular QC-LDPC code. The length of the shortest cycle in the Tanner graph is the girth. It is experimentally known that short cycles and other graphical structures of the Tanner graph named as (a, b) elementary trapping set ((a, b)-ETSs) with small size a cause high decoding failure rate.

We propose a new method to construct algebraic-based QC-LDPC codes with girth 6, using multiplicative subgroups of a finite field. Some algebraic-based QC-LDPC code constructions in the literature are special cases of our construction. Then, we provide sufficient conditions to construct $(3, n)$-regular algebraic-based QC-LDPC codes with girth 6 and free of (a, b) ETSs with $a \leq 5$ and $b \leq 2$.

ALEXANDER BORS, Carleton University
Wreath products and cascaded feedback shift registers

In cryptography, cascade connections are a means of combining multiple feedback shift registers (FSRs) into hopefully more secure stream ciphers. In this talk, we present recent results, obtained in joint work with Maghsoudi and Wang, on the periods of bit sequences produced by cascade connections of two FSRs. We observe that those periods may be viewed as cycle lengths of a certain permutation on vectors that is an element of a so-called imprimitive permutational wreath product (a certain kind of permutation group). This allows us to study periods of cascade connections with algebraic methods, obtaining both an upper bound on the maximum period of a cascade connection and a complete understanding of the periods in the important case of the cascade connection of an n-dimensional De Bruijn sequence into an m-dimensional linear FSR.

DELARAM KAHROBAEI, The City University of New York, QC, GC, University of York (UK)
Post-quantum hash functions using $SL_n(F_p)$

We define new families of Tillich-Zémor hash functions, using higher dimensional special linear groups over finite fields as platforms. The Cayley graphs of these groups combine fast mixing properties and high girth, which together give rise to good preimage and collision resistance of the corresponding hash functions. We justify the claim that the resulting hash functions are post-quantum secure. Joint work with Corentin Le Coz, Christopher Battarbee, Ramón Flores, Thomas Koberda.

SIMON KUTTNER, Carleton University
Applications of the subset sum problem over finite abelian groups

Given a finite abelian group G, a finite set D, and a mapping $f : D \to G$, we find the number of r-subsets $S \subseteq D$ where for $b \in G$,

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

We obtain simple exact expressions when f is an abelian group homomorphism. When $G = \mathbb{F}_q$, we extend known results when $D \in \{\mathbb{F}_q, \mathbb{F}_q^*\}$ and $f(x) = x^N$, which include quadratic and semiprimitive cases. We count degree n monic polynomials over

$\mathbb{F}_q$ with r distinct roots in a set $D \subseteq \mathbb{F}_q$ when the leading terms of degree at least $n-\ell$ are fixed. We obtain new formulas for $\ell = 1$ when D is a multiplicative subgroup of $\mathbb{F}_q^*$, and for $\ell = 2$ when D is an arbitrary subfield of $\mathbb{F}_q$ with q odd.

ARIANE MASUDA, New York City College of Technology, CUNY

On permutation binomials of the form $x^r(x^{q-1}+a)$ over $\mathbb{F}_{q^e}$

Let $\mathbb{F}_q$ be the finite field of order q. A polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial over $\mathbb{F}_q$ if $f(\mathbb{F}_q) = \mathbb{F}_q$. We will present results on permutation binomials of the form $x^r(x^{q-1}+a)$ over $\mathbb{F}_{q^e}$, where $e \geq 2$ and $a \in \mathbb{F}_{q^e}^*$. This is joint work with Ivelisse Rubio and Javier Santiago.

FERNANDO NERANGA, College of the Holy Cross

Reversed Dickson polynomials of the (k+1)-th kind over finite fields

Let p be a prime and q a power of p. Let $\mathbb{F}_q$ be the finite field with q elements. The concept of the reversed Dickson polynomial $D_n(a,x)$ was first introduced by Xiang-dong Hou, Gary Mullen, James Sellers and Joseph Yucas in 2009 by reversing the roles of the variable and the parameter in the Dickson polynomial $D_n(x,a)$. In 2012, Steven Wang and Joseph Yucas introduced the reversed Dickson polynomials of the $(k+1)$-th kind $D_{n,k}(a,x)$. For $a \in \mathbb{F}_q$, the n-th reversed Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(a,x)$ is defined by

$$D_{n,k}(a,x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-x)^i a^{n-2i},$$

and $D_{0,k}(a,x) = 2-k$.

I am primarily interested in the question: When is $D_{n,k}(a,x)$ a permutation polynomial of $\mathbb{F}_q$? In this talk, I will explain my recent results on the permutation behavior of reversed Dickson polynomials over finite fields. I will also talk about some general properties of the reversed Dickson polynomials of the $(k+1)$-th kind. These results unify and generalize many previously discovered results on reversed Dickson polynomials over finite fields. Moreover, I will talk about my current research on reversed Dickson polynomials.

MARK SAALTINK, unaffiliated

An extremal problem in vector spaces over finite fields.

What is the largest number of bases contained in n points in the r-dimensional vector space over $\mathbb{F}_q$?

In this talk I provide asymptotic results, exact results for some values of n, and upper and lower bounds. Along the way I will introduce an interesting question on uniform hypergraphs, with connections to a theorem of Turán.

This is joint work with Brett Stevens.

HUGO TEIXEIRA, Carleton University

On the functional graph of $f(X) = c(X^{q+1} + aX^2)$ over quadratic extensions of finite fields

Let $X = \mathbb{F}_q$ be the finite field with q elements and $char(\mathbb{F}_q)$ odd. In this work we discuss the characteristics of the functional graph of the map $X \mapsto c(X^{q+1} + aX^2)$ over the field $\mathbb{F}_{q^2}$, where $c, a \in \mathbb{F}_q$. We observe that this function defines a quadratic form over $\mathbb{F}_q$, therefore it is a natural generalization of the function $x \mapsto cx^2$ over $\mathbb{F}_q$. We give the number of cycles of each length and the precise behavior of the pre-cycles for $a \in \{\pm 1\}$ and some partial results for the other cases. In particular, we describe the connected components that contains the fixed points of f.

XI XIE, Hubei University & Carleton Univeresity

On the Niho type locally-APN power functions and their boomerang spectrum

In this talk, we focus on the so-called locally-APN power functions introduced by Blondeau, Canteaut and Charpin, which generalize the well-known notion of APN functions and possibly more suitable candidates against differential attacks. Specifically, given two coprime positive integers m and k such that $\gcd(2^m+1, 2^k+1) = 1$, we investigate the locally-APN-ness property of the Niho type power function $F(x) = x^{s(2^m-1)+1}$ over the finite field $\mathbb{F}_{2^{2m}}$ for $s = (2^k+1)^{-1}$, where $(2^k+1)^{-1}$ denotes the multiplicative inverse modulo 2^m+1. By employing finer studies of the number of solutions of certain equations over finite fields, we prove that $F(x)$ is locally-APN and determine its differential spectrum. We emphasize that computer experiments show that this class of locally-APN power functions covers all Niho type locally-APN power functions for $2 \leq m \leq 10$. In addition, we also determine the boomerang spectrum of $F(x)$ by using its differential spectrum, which particularly generalizes a recent result by Yan, Zhang and Li.