Finite Fields and Applications

(Org: **Ariane Masuda** (New York City College of Technology (CUNY)) and/et **Daniel Panario** (Carleton University))

NERANGA FERNANDO, College of the Holy Cross, Worcester, Massachusetts, United States of America

Idempotents and Tripotents in Quandle Rings

A *quandle* is a set Q with a binary operation $* : Q \times Q \to Q$ satisfying:

- For all $x \in Q$, $x * x = x$
- For all $y \in Q$, the map $\beta_y : Q \to Q$ defined by $\beta_y(x) = x * y$ is invertible.
- For all $x, y, z \in Q$, $(x * y) * z = (x * z) * (y * z)$.

The three axioms of a quandle algebraically encode the three Reidemeister moves in knot theory. Let R be an associative ring with unity, and $R[Q]$ be the set of all formal finite R-linear combinations of elements of Q:

$$R[Q] := \Big\{ \sum_i \alpha_i x_i \,|\, \alpha_i \in R,\, x_i \in Q \Big\}$$

The set $R[Q]$ is a non-associative ring with coefficients in R. We study idempotents and tripotents in quandle rings $\mathbb{F}_p[Q]$. The Gröbner basis technique plays a pivotal role in our study.

This is a joint work with Zhaoqi Wu (College of the Holy Cross).

KENZA GUENDA, UVIC/ USTHB

Code-based cryptography

In the realm of post-quantum cryptography, code-based cryptography has garnered significant attention. The ongoing NIST standardization process for post-quantum cryptographic primitives has further heightened interest and accelerated research in this field. Code-based cryptographic primitives, which rely on the difficulty of decoding seemingly random error-correcting codes, have proven particularly robust against quantum computer-based attacks. Unlike traditional cryptographic methods that rely on the hardness of number-theoretic problems (such as the factorization problem or the discrete logarithm problem), code-based cryptography exploits the complexity of general decoding issues, like the syndrome decoding problem. The purpose of this talk is to discuss the codes based cryptography. We will discuss some systemes preset their weakess, discuss some attacks. We also present our new variants .

JONATHAN JEDWAB, Simon Fraser University

Quaternary Legendre pairs of even length

One of the most famous open problems in discrete mathematics is Paley's 1933 conjecture that there is a Hadamard matrix of order $n > 2$ if and only if n is a multiple of 4. It has long been known that this conjecture would follow from the existence of a pair of binary Legendre sequences for every odd length. It has recently been shown that this conjecture would also follow from the existence of a pair of quaternary Legendre sequences for every even length.

We use finite fields to give the first general constructions of quaternary Legendre sequences of even length. In particular, we modify a classical construction due to Szekeres to show that there is a quaternary Legendre sequence of even length $(q-1)/2$ for every prime power q congruent to 1 modulo 4.

This is joint work with Thomas Pender.

DANIEL KATZ, California State University, Northridge
Almost perfect nonlinear power functions with exponents expressed as fractions

Let F be a finite field, let f be a function from F to F, and let a be a nonzero element of F. The discrete derivative of f in direction a is $\Delta_a f\colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$. The differential spectrum of f is the multiset of cardinalities of all the fibers of all the derivatives $\Delta_a f$ as a runs through F^*. The function f is almost perfect nonlinear (APN) if the largest cardinality in the differential spectrum is 2. Almost perfect nonlinear functions are of interest as cryptographic primitives. If d is a positive integer, the power function over F with exponent d is the function $f\colon F \to F$ with $f(x) = x^d$ for every $x \in F$. There is a small number of known infinite families of APN power functions. In this talk, we re-express the exponents for one such family in a more convenient form. This enables us to give the differential spectrum and, even more, to give a very precise determination of individual fibers of the derivatives.

HASSAN KHODAIEMEHR, The University of British Columbia (UBC)
Quantum Bosonic Codes and Finite Fields

In this talk, we explore the intersection of quantum error correction and finite field theory through the lens of quantum bosonic codes. As quantum systems, particularly those involving continuous variables, become increasingly relevant in quantum computing and communication, the development of robust error-correcting codes is essential for enhancing the reliability of quantum information processes. We begin by discussing bosonic codes, specifically designed to protect quantum information encoded in bosonic systems, such as photons and phonons. These codes leverage the mathematical properties of harmonic oscillators and are described using coherent state representations and lattice structures. We will explore the underlying mathematical framework of these codes, highlighting their connection to finite fields and the algebraic structures that aid in encoding and decoding processes. In particular, we will examine the construction of Gottesman-Kitaev-Preskill (GKP) codes, illustrating how finite fields enhance the design and optimization of these codes to improve their error correction capabilities.

SHUXING LI, University of Delaware
On the Nonexistence of Generalized Bent Functions

An (m, n)-generalized bent function is a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$ so that its associated Fourier transformations have constant absolute value. It is known that an (m, n)-generalized bent function exists whenever one of the following holds:

(1) both m and n are even.

(2) $4 \mid m$.

On the other hand, all known results suggest that for (m, n) pair that fails to satisfy both of the above conditions, (m, n)-generalized bent function does not exist. In this talk, we will discuss the recent nonexistence result of $(m, 4)$-generalized bent functions with m being odd. This result crucially relies on analyzing vanishing sums of complex roots of unity.

This is joint work with Ka Hin Leung (National University of Singapore) and Songtao Mao (Johns Hopkins University).

PETR LISONEK, Simon Fraser University
On a new class of Hadamard matrices

A complex Hadamard matrix is a square matrix whose each entry is a complex number with absolute value 1, and whose any two distinct rows are orthogonal. In this talk we focus on the class of complex Hadamard matrices called S-Hadamard, which satisfy the additional condition that the elementwise product of the matrix with itself (Schur product) is also a complex Hadamard matrix. We will discuss algebraic constructions of such matrices using finite fields, as well as various methods that can be employed for computational constructions. Our recently discovered parametric construction provides further insight into possible structure of these matrices. Existence results will be presented; for some matrix orders the existence question remains open. The study of these matrices is motived by an application in quantum information theory.

ARIANE MASUDA, New York City College of Technology, CUNY
Involutions over finite fields

In the context of memory-limited environments, involutions are desirable because they allow for efficient use of limited memory resources. Specifically, in many applications, both the permutation and its inverse must be stored in memory, which can be a challenge in resource-constrained environments. By using an involution as the interleaver, the same structure and technology used for encoding can be used for decoding as well. Fixed points are points that remain unchanged under the permutation. In cryptographic applications, such as the design of S-boxes, it is desirable to have permutations with a small number of fixed points to increase the security of the system. Therefore, understanding the number of fixed points and how to construct involutions with few fixed points is an important area of research. In this talk we will present some families of involutions over finite fields, including some explicit constructions based on a prescribed number of fixed points.

LUCIA MOURA, University of Ottawa
New families of strength-3 covering arrays using LFSR sequences

A *covering array* of strength t, denoted by CA$(N; t, k, v)$, is an $N \times k$ array C over an alphabet with v symbols with the property that for any subarray consisting of t columns of C, every t-tuple of the alphabet appears at least once as a row of the subarray. An additional parameter λ is used when we require that every t-tuple of the alphabet appears at least λ times as a row of the subarray. An *orthogonal array* is a special case of a covering array, where each t-tuple appears exactly λ times, so in this case $N = \lambda v^t$. Given t, k, v, we aim to determine CAN(t, k, v) which is the minimum N for which a CA$(N; t, k, v)$ exists. This is a hard problem in general, so we seek good upper bounds for CAN.

Raaphorst, Moura and Stevens (DCC 2014) gave a construction for a CA$(2q^3 - 1; 3, q^2 + q + 1, q)$, for every prime power q, using linear feedback shift register (LFSR) sequences over finite fields. In the present work (to appear in the Journal of Combinatorial Designs), we explore the use of this "good" ingredient to build covering arrays of strength 3 with a larger number of columns via recursive constructions and elimination of redundant rows. Several of these covering arrays improve the best upper bounds currently found in Colbourn's covering array tables. This is joint work with Kianoosh Shokri.

DANIEL PANARIO, Carleton University
Stable binomials over finite fields

We study stable binomials over finite fields, that is, irreducible binomials $x^t - b \in \mathbb{F}_q[x]$ such that all their iterates are also irreducible over $\mathbb{F}_q$. We obtain a simple criterion on the stability of binomials based on the forward orbit of 0 under the map $z \mapsto z^t - b$. In particular, our criterion extends the one obtained by Jones and Boston (2011) for the quadratic case. As applications of our main result, we obtain an explicit 1-parameter family of stable quartics over prime fields $\mathbb{F}_p$ with $p \equiv 5 \pmod{24}$, and also develop an algorithm to test the stability of binomials over finite fields. Finally, building upon a result of Ostafe and Shparlinski (2010), we employ character sums to bound the complexity of such algorithm.

Joint work with Arthur Fernandes and Lucas Reis (Universidade Federal de Minas Gerais, Brazil).

WELINGTON SANTOS, University of Wisconsin Stout
Codes for Secure Distributed Matrix Multiplication

In this talk, we will explore how elements of coding theory can be applied to the problem of Secure Distributed Matrix Multiplication (SDMM). In this scenario, a user seeks to compute the product of two matrices, A and B, with the assistance of N honest-but-curious servers, ensuring that no server gains any information about either A or B. Specifically, we will introduce the HerA scheme, an SDMM model based on Hermitian codes. Additionally, we will demonstrate how matrix Reed-Solomon codes and their duality theory can be employed to detect malicious servers in the context of the SDMM problem.

JOZSEF SOLYMOSI, University of British Columbia
On the Thue-Vinogradov Lemma

Thue's Lemma is a helpful tool in elementary number theory. The most famous application of the lemma is to prove Fermat's theorem on sums of two squares. Vinogradov extended this Lemma to an asymmetric form. He used it in the paper *"On a general theorem concerning the distribution of the residues and non-residues of powers"*, where he gave an elementary proof of the Pólya-Vinogradov inequality. Vinogradov's formulation is the following: Let p be a prime. For any $a \in \mathbb{N}$, $p \nmid a$, and $\alpha \in \mathbb{F}_p^*$, there are x, y where $x \in \{1, 2, \ldots, \alpha\}$, $\quad y \in \left\{1, 2, \ldots, \left\lfloor \frac{p}{\alpha} \right\rfloor\right\}$ such that $ax \equiv \pm y \pmod{p}$.

The proof is based on a clever application of the pigeon-hole principle. We will extend this result to smaller sets and show some applications of the improved result. We will use Rédei polynomials and a simple variant of Stepanov's method for the proof.

BIANCA SOSNOVSKI, Queensborough Community College/The City University of New York
Applications of Finite Fields in Cayley Hash Functions

Cayley hash functions are a class of cryptographic hashing algorithms that employ group-theoretic constructions based on Cayley graphs to achieve security and efficiency. This presentation explores the role of finite fields within Cayley hash functions, illustrating how finite field structures enable efficient encoding and provide a robust defense against conventional cryptographic attacks. We will examine specific examples of Cayley hash functions, analyze their constructions using various groups and finite fields, and discuss the key properties and trade-offs associated with different types of Cayley hash functions.

HUGO TEIXEIRA, Carleton University
The functional graph of $f(X) = (cX^q + aX)(X^q - X)^{n-1}$ over quadratic extensions of finite fields

Let $\mathbb{F}_q$ be the finite field with q, where q is an odd prime power. In this presentation we describe completely the dynamics of the family of functions $f(X) = (cX^q + aX)(X^q - X)^{n-1}$, for $a, c \in \mathbb{F}_q$ and $n \geq 2$, over the finite field $\mathbb{F}_{q^2}$. We provide the number and size of its cycles as well as the behavior of the trees hanging from each periodic element.

DAVID THOMSON, Tutte Institute for Mathematics and Computing
Derivatives in Finite Fields

Derivative-like transformations over finite fields arise in numerous applications: they measure autocorrelations of permutation arrays and they are used in cryptanalysis of both symmetric and asymmetric cryptography. Interestingly, these finite derivatives are expressed in the same way as bilinear forms associated with a quadratic form. Quadratic maps are also of significant interest in applications.

In this talk, we make explicit a correspondence between uni- and multi-variate polynomials that translates q-degrees in univariate representations to algebraic degrees in the familiar sense. We view so-called Dembowski-Ostrom polynomials (with q-degree 2) as quadratic forms and continue to pull on this thread to find out where this correspondence leads.

CHI HOI (KYLE) YIP, Georgia Institute of Technology
Extensions of Carlitz-McConnel theorem on permutations over finite fields

Let p be a prime, $q = p^n$, and $D \subset \mathbb{F}_q^*$. A celebrated result of Carlitz-McConnel states that if D is a proper subgroup of $\mathbb{F}_q^*$, and $f : \mathbb{F}_q \to \mathbb{F}_q$ is a function such that $(f(x) - f(y))/(x - y) \in D$ whenever $x \neq y$, then $f(x)$ necessarily has the form $ax^{p^j} + b$. In this talk, I will discuss some extensions of this result and their applications.