Talks Proposal

V Encuentro Argentino de Cuerpos Finitos y Temas Afines

Characterizing graphs with second largest distance eigenvalue less than $-1/2$

Speaker: Miriam Abdón

Institution: IME, Universidade Federal Fluminense (UFF), Brasil

Email: miriam_abdon@id.uff.br

Coauthors: Lilian Markenzon, NCE-PPGI, Universidade Federal do Rio de Janeiro, Brasil. Cybele T. M. Vinagre, IME, Universidade Federal Fluminense (UFF), Brasil

Abstract: Let G be a connected graph with vertex set $V(G)$. The *distance* between two vertices u and v in G, denoted $d_G(u,v)$, is defined as the length of a shortest path connecting them in G. The *distance matrix* of G is the matrix $\mathbf{D}(G) = [d_G(u,v)]_{u,v\in V(G)}$. The *second largest distance eigenvalue* of G, that is, the second largest eigenvalue of $\mathbf{D}(G)$, has recently attracted interest among spectral graph theorists. In this work, we provide a complete characterization of connected graphs whose second largest distance eigenvalue is less than $-\frac{1}{2}$, using both spectral and structural properties.

Superelliptic curves defined by linearized polynomials

Speaker: Daniela Alves de Oliveira

Institution: Universidade de São Paulo

Email: danielaalvesoliveira@gmail.com

Coauthors: José Alves de Oliveira, Universidade Federal de Lavras Fabio, Enrique Brochero Martínez, Universidade Federal de Minas Gerais.

Abstract: Let $\mathbb{F}_{q^n}$ be a finite field with q^n elements. In this presentation, we employ results on character sums, combined with an approach involving linearized polynomials, to derive an explicit formula for the number of $\mathbb{F}_{q^n}$-rational points on the affine superelliptic curve

$$y^d = F(x),$$

where $F(x)$ is a q-polynomial over $\mathbb{F}_{q^n}$ satisfying certain algebraic conditions. In particular, we provide an explicit formula for the number of $\mathbb{F}_{q^n}$-rational points on the generalized Artin–Schreier curve

$$y^d = b(x^{q^m} - ax),$$

when d satisfies specific conditions. We also establish conditions under which these curves are maximal or minimal.

El conjunto de valores de polinomios ciclótomicos de orden primo en $\mathbb{F}_q$

Speaker: Gastón Bidart Gauna

Institution: Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento

email: gbidart@campus.ungs.edu.ar

Coauthors: Antonio Cafure, Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, CONICET.

Abstract. Sea $\mathbb{F}_q$ el cuerpo finito de q elementos de característica p. Si f es un polinomio con coeficientes en $\mathbb{F}_q$, decimos que $V(f) = \{f(c) : c \in \mathbb{F}_q\}$ es el conjunto de valores de f. El cardinal de este conjunto se denota como $|V(f)|$. La sección 8.3 del *Handbook of Finite Fields* [2] presenta un amplio panorama sobre el estudio del conjunto de valores de polinomios sobre $\mathbb{F}_q$.

En este trabajo vamos a estudiar el conjunto de valores de la clase Φ_q de polinomios ciclótomicos $\Phi_r \in \mathbb{F}_q[x]$ de orden primo r, con $p \geq 3$. En particular, estudiamos el espectro $v(\Phi_q) = \{|V(\Phi_r)| : \Phi_r \in \Phi_q\}$. La noción de espectro de una familia de polinomios fue introducida en [3]. Para llevar adelante esta tarea, estudiamos las curvas

$$\frac{\Phi_r(x) - \Phi_r(y)}{x - y} = 0$$

asociadas a cada polinomio Φ_r (ver [1, 4, 5]).

References

[1] J. Gomez-Calderon, *On the cardinality of value set of polynomials with coefficients in a finite field*, 1992. Disponible en: `https://api.semanticscholar.org/CorpusID:122103777`.

[2] G. Mullen y D. Panario (eds.), *Handbook of Finite Fields*, CRC Press, 2013.

[3] A. Topuzoğlu y L. Isik, *A note on value sets of polynomials over finite fields*, arXiv:1701.06158 [math.CO] (2017).

[4] S. Uchiyama, *Sur le nombre des valeurs distinctes d'un polynôme à coefficients dans un corps fini*, 1954. Disponible en: `https://api.semanticscholar.org/CorpusID:120799357`.

[5] J. F. Voloch, *On the number of values taken by a polynomial over a finite field*, *Acta Arith.* **52** (1989), 197–201.

Clasificación de códigos AG cíclicos racionales

Speaker: Gustavo Cabaña

Institution: Universidad Nacional del Litoral y Universidad Nacional de Rafaela

Email: cabanagusti@gmail.com

Abstract:
La teoría de códigos autocorrectores se encarga de estudiar y construir herramientas que sirvan para detectar y corregir errores en la transmisión de información. En esta charla presentaremos una construcción de códigos algebraicos geométricos cíclicos racionales y veremos cómo clasificarlos según la equivalencia monomial.

Rédei permutations with the same cycle structure

Speaker: Juliane Capaverde

Institution: Universidade Federal do Rio Grande do Sul

Email: juliane.capaverde@ufrgs.br

Coauthors: Ariane Masuda, The City University of New York and Virgínia Rodrigues, Universidade Federal do Rio Grande do Sul.

Abstract: Permutation polynomials over finite fields have been extensively studied over the past decades. Among the major challenges in this area are the questions concerning their cycle structures as they capture relevant properties, both theoretically and practically.

In this talk we focus on a family of permutation polynomials, the so-called Rédei permutations. Although their cycle structures are known, there are other related questions that can be investigated. For example, when do two Rédei permutations have the same cycle structure? We give a characterization of such pairs, and present explicit families of Rédei permutations with the same cycle structure.

Properties of p-ary Binomial Sequences

Speaker: Sara D. Cardell

Institution: São Paulo State University (Unesp), Institute of Geosciences and Exact Sciences, Rio Claro, Brazil

Email: sd.cardell@unesp.br

Coauthors: Miguel Beltrá, Verónica Requena (University of Alicante, Spain).

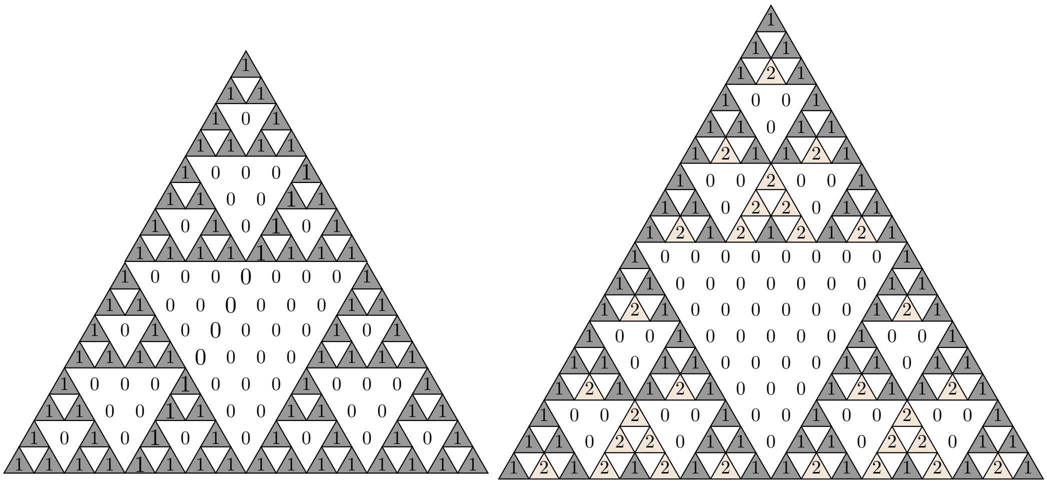

Figure 1: Pascal's triangle modulo 2 and 3, respectively.

Abstract:

The binary binomial sequences correspond to the diagonals of the binary Pascal's triangle (see Figure 1). They have interesting properties, such as all binary sequences with a period power of 2 can be computed as the XOR of a finite set of binomial sequences [1]. Other properties of these sequences (period, linear complexity, construction rules, or relations among them) have been deeply analyzed for the binary case [1].

Let p be a prime number, $\mathbb{F}_p$ be the Galois field of p elements, and $k \geq 0$ a fixed integer. The **($p-$ary) $k-$th binomial sequence** $\left\{\binom{n}{k}\right\}_{n\geq 0}$ is the sequence whose terms are given by the binomial coefficients modulo p, that is, $\binom{n}{k} \mod p$, if $n \geq k$ and 0 if $n < k$. These sequences correspond to the diagonals of Pascal's triangle modulo p. For instance, in Figure 1, Pascal's triangle modulo 3 is displayed, revealing the fractal structure of the sequences and their underlying patterns.

In this work, we study the construction rules of these sequences and other properties of this family of sequences over $\mathbb{F}_p$. For example, it is possible to prove that the linear complexity of the sequence $\left\{\binom{n}{k}\right\}_{n\geq 0}$ is $LC = k+1$ and the characteristic polynomial of the sequence is $p(x) = (x-1)^{k+1}$. Furthermore, we show that any p-ary sequence $\{a_n\} = \{a_0, a_1, a_2, \ldots, a_{p^L-1}, \ldots\}$ of period $T = p^L$, with $L > 0$ an integer, can be written as a linear combination of p-ary binomial sequences. That is, there exist $\alpha_i \in \mathbb{F}_p$, with $i \in \{0, 1, \ldots, p^L - 1\}$, such that

$$\{a_n\} = \sum_{i=0}^{p^L-1} \alpha_i \left\{\binom{n}{i}\right\}_{n\geq 0}. \tag{1}$$

The expression (1) is called the **binomial representation** of $\{a_n\}_{n\geq 0}$. It is possible to deduce properties of the sequence $\{a_n\}_{n\geq 0}$ simply by observing its binomial representation.

Acknowledgments: The first author was supported by CNPq with process 405842/2023-6 and by FAPESP with process 2024/05051- 7. The work of the second and third author was supported by I+D+i projects VIGROB23- 287 and UADIF23-132 of the Universitat d'Alacant.

References

[1] Sara D. Cardell, Amparo Fúster-Sabater, Binomial Representation of Cryptographic Binary Sequences and Its Relation to Cellular Automata, *Complexity* **2108014**(2019), 1–13 doi: https://doi.org/10.1155/2019/2108014.

On the Construction of Iso-Dual AG Codes via Towers of Function Fields

Speaker: María Chara

Institution: Researcher of CONICET at UNL, Argentina and Professor at UdelaR, Uruguay

Email: maria.chara@pedeciba.edu.uy

Coauthors: Ricardo Podestá, Universidad Nacional de Córdoba; Luciane Quoos, Universidade Federal do Rio de Janeiro; and Ricardo Toledano, Universidad Nacional del Litoral.

Abstract:

In this talk, we present a general and relatively simple method for constructing asymptotically good sequences of iso-dual AG-codes, which form a slightly more general family of linear codes than the self-dual AG-codes. For a linear $[n,k,d]$ code $\mathcal{C}$ over a finite field $\mathbb{F}_q$, the dual code is defined as

$$\mathcal{C}^{\perp} := \{z \in \mathbb{F}_q^n : z \cdot c = 0 \text{ for all } c \in \mathcal{C}\};$$

where the product is the usual (Euclidean) dot product. A linear code is called *iso-dual* if it is equivalent to its dual.

Given a function field $\mathcal{F}/\mathbb{F}_q$, we consider the divisor $D = P_1 + \cdots + P_n$, which is the sum of pairwise distinct rational places of $\mathcal{F}$, and another divisor G such that P_i is not in the support of G for $i = 1, \ldots, n$. A code is said to be algebraic geometry (AG) over $\mathcal{F}$ if it is of the form

$$\mathcal{C} = C_{\mathcal{L}}(D,G) = \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n,$$

where $\mathcal{L}(G) = \{z \in \mathcal{F} : (z) \geq -G\} \cup \{0\}$ denotes the Riemann-Roch space associated with the divisor G.

We begin by presenting a method to produce iso-dual AG-codes over a finite field $\mathbb{F}$ with q elements. Given a finite separable extension $\mathcal{M}/\mathcal{F}$ of function fields and an iso-dual AG-code $\mathcal{C}$ defined over $\mathcal{F}$, we provide a general method to lift the code $\mathcal{C}$ to another iso-dual AG-code $\tilde{\mathcal{C}}$ over $\mathcal{M}$, under certain assumptions on the parity of the involved different exponents. Then, we use this method to build sequences of iso-dual codes using a tower of function fields. As a result, we prove the existence of a sequence of iso-dual AG-codes over non-prime fields of quadratic cardinality that achieves the Tsfasman–Vlăduţ–Zink lower bound in a relatively simple way. We also exhibit good sequences of iso-dual AG-codes over finite fields of cubic cardinality and even characteristic.

References

[1] M. Chara, R. Podestá, L. Quoos, and R. Toledano, *Lifting iso-dual algebraic geometry codes*, Designs, Codes and Cryptography, vol. 92, pp. 2743–2767, 2024.

[2] M. Chara, R. Podestá, L. Quoos, and R. Toledano, *Good iso-dual AG-codes from towers of function fields*, preprint (available at `https://arxiv.org/abs/2503.08899`), 2025.

Di-Cayley graphs over finite fields

Speaker: Paula Mercedes Chiapparoli

Institution: CIEM (CONICET) - Universidad Nacional de Córdoba

Email: pauchiapp@gmail.com

Coauthors: Ricardo A. Podestá, CIEM (CONICET) - Universidad Nacional de Córdoba.

Abstract: Let G be a group and S_ℓ, S_r, S_m subsets of G. The di-Cayley graph $DX(G; S_\ell, S_r, S_m)$ has vertex set $G \times \{0,1\}$ such that the vertices (h,i) and (g,i) form a directed edge if $i = 0$ and $gh^{-1} \in S_\ell$ or $i = 1$ and $gh^{-1} \in S_r$; the vertices $(h,0)$ and $(g,1)$ form a directed edge if $gh^{-1} \in S_m$ and the vertices $(h,1)$ and $(g,0)$ form a directed edge if $hg^{-1} \in S_m$.

We give the adjacency matrices of the di-Cayley graphs and from them we obtain the spectrum in the case where the connection sets S_ℓ, S_r and S_m are closed under conjugation. In particular, in the case of $G = \mathbb{F}_q$, $S_\ell = S_r = \{x^k : x \in \mathbb{F}_q\}$, and $S_m = \{x^\ell : x \in \mathbb{F}_q\}$, the eigenvalues of the mirror di-Cayley graph $\Gamma = DX(\mathbb{F}_q; S_\ell, S_r, S_m)$ can be expressed in terms of Gaussian periods.

This allows us to give criteria of isospectrality and equienergy.

References

[1] On mirror di-Cayley (sum) graphs and their spectrum (work in progress).

[2] On di-Cayley graphs and their spectrum (work in progress).

Códigos LRC con tasa de transmisión $R > \frac{1}{2}$ sobre torres de cuerpos de funciones

Speaker: Francisco Galluccio

Institution: Universidad Nacional del Litoral, CONICET.

Email: frangallu996@gmail.com

Abstract: En esta charla completaremos la construcción de códigos LRC dada en un trabajo en conjunto con María Chara y Edgar Martinez-Moro, utilizando torres de cuerpos de funciones. Se presentará la construcción general que nos permite obtener códigos LRC lineales de gran longitud $n \approx q^4$, dimensión k y distancia mínima d del orden de q^4, con localidad $r = q - 1$. En particular, comentaremos un ejemplo donde la tasa $R = k/n$ es estrictamente mayor a 1/2.

Frobenius nonclassical quadrinomial curves

Speaker: João Paulo Guardieiro

Institution: Universidade Estadual de Campinas (UNICAMP)

Email: joaopgs@ime.unicamp.br

Coauthors: Tiago Aprigio, Universidade de São Paulo (USP).

Abstract: In [1], we characterized all minimal value set binomials over $\mathbb{F}_q$, that is, binomials whose size of the set of images is the smallest possible. With this information, we also classified all quadrinomial curves with separated variables that are $\mathbb{F}_q$-Frobenius nonclassical for the morphism of lines. In this talk, I will present the second part of this project. This study was financed, in part, by the São Paulo Research Foundation (FAPESP), Brazil. Process Number #2024/19443-4.

References

[1] APRIGIO, T.; GUARDIEIRO, J. P. Minimal value set binomials and Frobenius nonclassical curves. arXiv preprint arXiv:2508.16541, 2025.

Construction B lattices from linear q-ary codes

Speaker: Grasiele C. Jorge

Institution: Federal University of São Paulo

Email: grasiele.jorge@unifesp.br

Coauthors: Franciele do Carmo Silva and Sueli I. R. Costa, University of Campinas

Abstract: Lattices in $\mathbb{R}^n$ are discrete additive subgroups [1]. For $q \in \mathbb{N}$, a linear q-ary code is a subgroup of $\mathbb{Z}_q^n$. A classical connection between linear q-ary codes and lattices is given by Construction A [2]. In this work, we extend Construction B, originally formulated for binary codes, to the setting of linear q-ary codes. We prove that the lattice obtained from a linear q-ary code via Construction B contains qD_n as a sublattice and can alternatively be realized as the Construction A lattice of a linear $2q$-ary code. We also provide a multilevel description of Construction B lattices under certain restrictions, extending previous results for the binary case. Under suitable hypotheses, we determine generator matrices and minimum distance. This is a work in progress aimed at studying the structural properties of these lattices, considering their potential applications in coding theory and in cryptography [3].

References

[1] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Springer-Verlag, New York, 1999.

[2] S. I. R. Costa, F. Oggier, A. Campello, J.-C. Belfiore, and E. Viterbo, *Lattices Applied to Coding for Reliable and Secure Communications*, Springer, 2017.

[3] F. C. Silva, *On Lattice Constructions and Some Applications in Cryptography*, Ph.D. Thesis, University of Campinas (UNICAMP), 2025.

The permutation group of some evaluation codes

Speaker: Hiram H. López

Institution: Virginia Tech

Email: hhlopez@vt.edu

Coauthors: Jun Bo, Lau, KU LEuven. Eduardo, Camps-Moreno, Virginia Tech. Welington, Santos, Universities of Wisconsin-Stout.

Abstract: In this talk, we will see how the permutation group of a Reed-Solomon code is given by the polynomials of degree one that leave the set of evaluation points invariant. Then, we will see how to extend the result to the permutation group of other families of evaluation codes.

Un algoritmo à la Kronecker para la resolución de sistemas de ecuaciones e inecuaciones polinomiales

Speaker: Guillermo Matera

Institution: Universidad Nacional de General Sarmiento, CONICET

Email: gmatera@campus.ungs.edu

Coauthors: Joos Heintz (UBA-CONICET), Nardo Giménez (UNAHUR-CONICET), Luis Miguel Pardo, Mariana Pérez (UNAHUR-CONICET) y Melina Privitelli (UNAHUR-CONICET).

Abstract: En este trabajo presentamos un algoritmo probabilístico para la resolución ”à la Kronecker” de un sistema de ecuaciones e inecuaciones polinomiales definido sobre un cuerpo perfecto. El método avanza de manera incremental, ecuación por ecuación, calculando a cada paso una representación -que denominamos ”solución geométrica”- de una sección lineal de dimensión cero de las variedades intermedias asociadas a las sucesivas ecuaciones e inecuaciones de entrada, a las que llamamos ”fibras de levantamiento”. La elección de las ecuaciones lineales que definen estas fibras de levantamiento se realiza mediante elecciones genéricas de coordenadas, cuya probabilidad de éxito controlamos por medio de cotas explícitas. El algoritmo incorpora técnicas de levantamiento de tipo de Newton-Hensel, evaluación dinámica y cálculo incremental de soluciones geométricas, y extiende enfoques previos desarrollados tanto para cuerpos finitos como para el caso de los racionales. Proveemos demostraciones de correctitud y obtenemos estimaciones explícitas de la complejidad -medida en términos de operaciones aritméticas y chequeos de nulidad sobre el cuerpo de base-, así como de la probabilidad de éxito del algoritmo. El resultado es un marco unificado que permite tratar variedad localmente cerradas sobre un cuerpo perfecto arbitrario de manera eficaz y con garantías probabilísticas explícitas.

Permutation decoding of algebraic geometry codes from Hermitian and norm-trace curves

Speaker: Gretchen L. Matthews

Institution: Virginia Tech

Email: gmatthews@vt.edu

Coauthors: Monica Lichtenwalner, Virginia Tech; Hiram H. López; Virginia Tech; Padmapani Seneviratne, East Texas A&M University.

Abstract: Permutation decoding is a process that utilizes the permutation automorphism group of a linear code to correct errors in received words. Given a received word, a set of automorphisms, called a PD set, moves errors out of the information positions so that the original message can be determined. In this talk, we investigate permutation decoding for certain families of algebraic geometry codes. Automorphisms of the underlying curve are used to specify permutation automorphisms of the code. Specifically, we describe permutation decoding sets that correct specific burst errors for one-point codes on Hermitian and norm-trace curves.

A tiny Rank Metric McEliece Cryptosystem

Speaker: Diego Napp

Institution: Universidad de Alicante

Email: diegonapp@gmail.com

Abstract:

In this talk I will present a novel rank metric code-based public key cryptosystem (PKC). In contrast to classical McEliece cryptosystems, where block codes are used, we propose a convolutional encoder to be part of the public key. The masking constant matrices typically used in the McEliece PKC are substituted by two polynomial matrices in such a way that allows Gabidulin codes to be securely included as secret codes. Equivalently, these polynomial matrices can be represented as block circulant matrices. Hence, the security of our system relies on the hardness of the problem of decoding random families of quasi-cyclic codes for the rank metric with non-homogeneous errors and on the problem of the indistinguishability of Gabidulin codes multiplied by a homogeneous matrix of given rank. The scheme benefits from a deterministic decryption algorithm together with interesting key and ciphertext sizes. For example, the total size of the public key and ciphertext is 1.16 KB and 3 KB, respectively, for 128-bit and 192-bit security

Iterating Generalized Cyclotomic Mappings of Finite Fields

Speaker: Daniel Panario

Institution: Carleton University

Email: daniel@math.carleton.ca

Abstract:

When we iterate functions over finite structures, there is an underlying natural functional graph. For a function f over a finite field $\mathbb{F}_q$, this graph has q nodes and a directed edge from vertex a to vertex b if and only if $f(a) = b$. It is well known, combinatorially, that functional graphs are sets of connected components, components are directed cycles of nodes, and each of these nodes is the root of a directed tree.

Some functions over finite fields when iterated present strong symmetry properties. These symmetries allow mathematical proofs of some dynamical properties such as the period and preperiod of a generic element, (average) “rho length” (number of iterations until a cycle is formed), number of connected components, cycle lengths, and permutational properties (including the cycle decomposition).

We briefly survey the main problems and results in this area. Then, we concentrate on the functional graph of generalized cyclotomic mappings of finite fields. These are a natural and manageable generalization of monomial functions. We study periodic points, cycle structure, and rooted trees attached to periodic points. We provide both theoretical and algorithmic results on the structure of their functional graphs.

Based on the following:

1. “A survey on iterations of mappings over finite fields”, R. Martins, D. Panario and C. Qureshi; Radon Series on Computational and Applied Mathematics de Gruyter, 23, 135-172, 2019.

2. “Functional graphs of generalized cyclotomic mappings of finite fields”, A. Bors, D Panario and Q. Wang; Memoirs of the European Mathematical Society, vol. 23, 2026, 262 pages.

R-sequences of non-abelian groups

Speaker: Adrián Pastine

Institution: Universidad Nacional de San Luis, CONICET.

Email: agpastine@gmail.com

Coauthors: María Valentina, Soldera Ruiz, Universidad Nacional de San Luis

Abstract: A group of order n is said to be R-sequenceable if there exist an ordering of its non-identity elements

$$g_1, g_2, \cdots, g_{n-1}$$

such that the products $g_i^{-1}g_{i+1}$ for $1 \leq i \leq n-2$ and the product $g_{n-1}^{-1}g_1$ are all different. The problem of R-sequenceability was first introduced by Ringel in [7] while studying embeddings of the complete graphs on orientable surfaces of a some genus. Over the years several articles were published on this and related topics (see [1, 6]). About the families of groups that were studied, R-sequenceable abelian groups were characterized in a series of articles culminating in [2], while for non-abelian groups only dihedral groups ([4]), dicyclic groups ([5]), groups of order pq where p and q are prime ([4, 5]), and groups of order 27 ([3]) were studied.

Given a normal subgroup N of a group G, in this talk we present a technique to find an R-sequence of G from an R-sequence of G/N and a particular permutation of N. We then use this technique to prove that groups of order coprime with 30 are R-sequenceable.

References

[1] Alspach, B. Variations on the sequenceable theme. In *50 Years of Combinatorics, Graph Theory, and Computing*. Chapman and Hall/CRC, 2019, pp. 37–53.

[2] Alspach, B., Kreher, D. L., and Pastine, A. The friedlander-gordon-miller conjecture is true. *Australas. J Comb. 67* (2017), 11–24.

[3] Bedford, D. On groups of order p, p^2, pq and p^3, p, q prime: their classification and a discussion as to whether they are super p-groups, 1987. Undergraduate Special Studies, University of Surrey.

[4] Cheng-De Wang Philip, A. L. More on sequences in groups. *Australasian Journal of Combinatorics 21* (2000), 187–196.

[5] Keedwell, A. On r-sequenceability and rh-sequenceability of groups. In *North-Holland Mathematics Studies*, vol. 78. Elsevier, 1983, pp. 535–548.

[6] Ollis, M. Sequenceable groups and related topics. *the electronic journal of combinatorics* (2012), DS10–Feb.

[7] Ringel, G. Cyclic arrangements of elements of a group. In *Notices of the American Mathematical Society* (1974), vol. 21, AMER MATHEMATICAL SOC 201 CHARLES ST, PROVIDENCE, RI 02940-2213, pp. A95–A96.

Connected Components and non-bipartiteness of generalized Paley Graphs

Speaker: Ricardo A. Podestá

Institution: CIEM (CONICET) - Universidad Nacional de Córdoba

Email: richarpodesta@gmail.com

Coauthors: Denis Videla, CIEM (CONICET) - Universidad Nacional de Córdoba.

Abstract:

In this work we consider the class of Cayley graphs known as *generalized Paley graphs* (GP-graphs for short), given by

$$\Gamma(k,q) = \mathrm{Cay}(\mathbb{F}_q, \{x^k : x \in \mathbb{F}_q^*\}),$$

where $\mathbb{F}_q$ is a finite field with q elements, both in the directed and undirected case. Hence $q = p^m$ with p prime, $m \in \mathbb{N}$, and one can assume that $k \mid (q-1)$.

We first give the connected components of an arbitrary GP-graph. We show that these components are smaller GP-graphs all isomorphic to each other (generalizing Lim and Praeger's result from 2009 to the directed case). We then characterize those GP-graphs which are disjoint unions of odd cycles. Finally, we show that $\Gamma(k,q)$ is non-bipartite except for the graphs

$$\Gamma(2^{m-1}, 2^m), \quad m \in \mathbb{N},$$

which are isomorphic to $K_2 \sqcup \cdots \sqcup K_2$, the disjoint union of 2^{m-1} copies of K_2.

Algebraic Geometry Codes with special features

Speaker: Luciane Quoos

Institution: Universidade Federal do Rio de Janeiro

Email: luciane@im.ufrj.br

Abstract: Algebraic Geometry (AG) codes are an important class of error-correcting codes, renowned for exceeding classical performance limits. In this talk we introduce the family of Algebraic Geometry Codes (AG codes) and explore their role in modern information theory presenting two constructions: lifting of iso-dual AG codes, and linear complementary pairs (LCP) of AG codes.

References

[1] Castellanos, Alonso S.; Marques, A. V.; and Quoos, L.. *Linear Complementary Dual codes and Linear Complementary Pairs of AG codes in function fields.* IEEE Transactions on Information Theory, vol. 71, no. 3, pp. 1676-1688, 2025.

[2] Chara, M.; Podestá, R.; Quoos, L.; and Toledano, R.. *Lifting iso-dual algebraic geometry codes.* Designs, Codes and Cryptography, 1-25, 2024.

On the Dynamics of Circulant Finite Dynamical Systems Over Galois Rings

Speaker: Claudio Qureshi

Institution: Universidad de la República

Email: cqureshi@gmail.com

Coauthors: Jonas Kantic (Technical University of Munich), Fabian Legl (Technical University of Munich) and Daniel Panario (Carleton University)

Abstract: A Linear Finite Dynamical System is called circulant if its system function can be represented by a circulant matrix. This class of systems plays an important role, for instance, in coding theory and in simulations. However, methods for analyzing such systems are often limited to cases where the system is defined over a finite field, or where the specific structure of the state space is not fully exploited. In this work, we propose an extension of Hensel's Lemma for the ring of polynomials with coefficients in Galois rings, which allows certain factorizations to be lifted even when the factors are not necessarily coprime, provided they satisfy suitable restrictions, and we use this result to extend the analysis of the dynamics of circulant systems to the setting of Galois rings. Furthermore, we propose algorithms to compute the set of cycle lengths and the height of the trees that appear in their functional

graphs.

On Weierstrass semigroups and fiber product of Kummer covers

Speaker: Guilherme Tizziotti

Institution: Universidade Federal de Uberlândia

Email: guilhermect@ufu.br

Coauthors: Alonso Castellanos, Universidade Federal de Uberlândia, and Erik Mendoza, Universidade Federal do Rio de Janeiro.

Abstract: In this talk, we explore the properties of Weierstrass semigroups and pure gaps in the context of fiber products of Kummer extensions, with applications to algebraic geometry codes (AG codes). We establish an arithmetic criterion to determine gaps and pure gaps at totally ramified places in fiber products of Kummer extensions, and determine a system of generators for the Weierstrass semigroup at any totally ramified place, generalizing previous results for single Kummer extensions. Finally, we apply our results to specific maximal curves to construct AG codes with good relative parameters compared to existing codes derived from the GK curve.

References

[1] A. Castellanos, E. Mendoza, and G. Tizziotti, *On Weierstrass semigroups and fiber product of Kummer covers*, Bulletin of the Brazilian Mathematical Society, to appear.

Cyclotomic function fields over finite fields

Speaker: Ricardo Toledano

Institution: Universidad Nacional del Litoral (Santa Fe, Argentina)

Email: ridatole@gmail.com

Coauthors: María Chara (UNL–CONICET, Santa Fe, Argentina; UdelaR, Uruguay), Ricardo Podestá (UNC–CONICET, Córdoba, Argentina), and Luciane Quoos (UFRJ, Río de Janeiro, Brasil).

Abstract:

We will explain the construction of cyclotomic function fields over a finite field $\mathbb{F}_q$, as developed by D. Hayes in his famous work [3] of 1974, where he was able to obtain the function field version of many remarkable properties that cyclotomic number fields have. We will

also explain how the arithmetic of these function fields was used by H. Quebemann [5] and V. Guruswami [2] to construct algebraic-geometry codes (AG-codes) over non-prime fields $\mathbb{F}_q$ with good properties. Following an alternative method given by Niederreiter and Xing [4] to obtain some optimal function fields over $\mathbb{F}_2$, we will explain how we used the theory of cyclotomic function fields in [1] to construct isodual AG-codes over $\mathbb{F}_2$ and $\mathbb{F}_3$.

References

[1] M. Chara, R. Podestá, R. Toledano, and L. Quoos, *Isodual algebraic-geometry codes*, *Designs, Codes and Cryptography*, 2024.

[2] V. Guruswami, *Cyclotomic function fields, Artin–Frobenius automorphisms and list error correction with optimal rate*, *Algebra and Number Theory*, 2010.

[3] D. Hayes, *Explicit class field theory for rational function fields*, *Trans. Amer. Math. Soc.*, 1974.

[4] H. Niederreiter and C. Xing, *Explicit global function fields over the binary field with many rational places*, *Acta Arithmetica*, 1996.

[5] H. Quebemann, *Cyclotomic Goppa codes*, *IEEE Trans. on Information Theory*, 1988.