Book of Abstracts
XXV Brazilian Algebra Meeting

State University Campinas, December 3 - 7, 2018

Session: Finite fields and applications

	December 3rd	**December 4th**	**December 5th**
14h10 - 14h30:	Tizzioti	Polcino	Bernardini
14h40 - 15h00:	Borges	Carvalho	Duran
15h10 - 15h30:	Motta	Neumann	Tenorio
15h40 - 16h00:	Arakelian	Quoos	Vicentim
16h00 - 16h30:	Coffee Break	Coffee Break	Coffee Break
16h40 - 17h00:	Speziali	Reis	Alves
17h10 - 17h30:	Coutinho	Castoldi	Jorge
17h40 - 18h00:	Gonçalves		Benedito

Subcovers and Codes on the $X_{n,r}$ curves

Guilherme Tizziotti
Universidade Federal de Uberlandia
Av. Joao Naves de Avila, 2121, Uberlandia-MG

Abstract:

In this work, we construct some class of explicit subcovers of the curve $\mathcal{X}_{n,r}$ defined over $\mathbf{F}_{q^n}$ by affine equation $y^{q^{n-1}} + \cdots + y^q + y = x^{q^{n-r}+1} - x^{q^n+q^{n-r}}$. These subcovers are defined over $\mathbf{F}_{q^n}$ by affine equation $g_s(y) =$

$x^{q^n+q^{n-r}} - x^{q^{n-r}+1}$, where $g_s(y)$ is a q-polynomial of degree q^s. The Weierstrass semigroup $H(P_\infty)$, where P_∞ is the only point at infinity on such subcovers, is determined for $1 \leq s \leq 2r - n + 1$ and the corresponding one-point AG codes are investigated. Codes establishing new records on the parameters with respect to the previously known ones are discovered, and 108 improvements on MinT tables are obtained.

Galois Points on double Frobenius nonclassical curves

Herivelto Borges
(Joint work with S. Fukasawa)
Instituto de Ciências Matemáticas e Computação
Universidade de São Paulo

Abstract:
An open problem in the theory of Galois points for curves over finite fields $\mathbb{F}_q$ is the characterization of curves for which the set of Galois points is the whole of the projective plane $\mathbb{P}^2(\mathbb{F}_q)$. In this talk, we discuss the distribution of Galois points for plane curves over $\mathbb{F}_q$ which are Frobenius nonclassical for different powers of q. In particular, within this setting, we give an answer for the problem and present new curves that have $\mathbb{P}^2(\mathbb{F}_q)$ as its set of Galois points.

On arcs from covering of curves

Beatriz Motta
(Joint work with Fernando Torres)
Departamento de Matemáticas
Universidade Federal de Juiz de Fora, MG

Abstract:
Let $n \geq 2$ be an integer, p a prime such that $p \nmid d := n^2 - n + 1$. Let K be the algebraic closure of the finite field $\mathbb{F}_p$ of order p. Our main goal is to discuss results and conjectures about arcs in the projective plane $\mathbb{P}^2(K)$ arising from certain morphisms on the Hurwitz or on the degree d Fermat curve which are defined respectively by $H_n : x^n y + y^n z + z^n x = 0$ and $F_d : x^d + y^d + w^d = 0$. We notice that both plane curves are non-singular. First we consider the morphism $\pi : H_n \to \mathbb{P}^2(K)$ given by $(u : v : 1) \mapsto (a : b : 1) := (u^{n-1}v : u^{-1}v^n : 1)$, and then we study the covering $\psi : F_d \to H_n$ defined by $\phi : (x : y : 1) \mapsto (u : v : w) := (x^n y^{-1} : xy^{n-1} : 1)$. The matters we are dealing with are concerning the complete arc property of the sets $\pi^{-1}(a : b : 1)$ and $\phi^{-1}(u : v : 1)$.

The Hurwitz curve over a finite field and its Weierstrass points for the morphism of lines

Nazar Arakelian
CMCC-Universidade Federal do ABC, SP

Abstract:
For any smooth Hurwitz curve $\mathcal{H}_n : XY^n + YZ^n + X^nZ = 0$ over the finite field $\mathbb{F}_p$, an explict description of its Weierstrass points for the morphism of lines is presented. As a consequence, the full automorphism group $\mathrm{Aut}(\mathcal{H}_n)$, as well as the genera of all Galois subcovers of $\mathcal{H}_n$, with $n \neq 3, p^r$, are computed. Moreover, thanks to such description, we show that a certain smooth maximal curve is not isomorphic neither to a curve of Fermat type nor to a curve of Hurwitz type. This talk is based on a joint work with Herivelto Borges and Pietro Speziali.

Ideals in Matrix Rings and error correcting codes

Polcino Milies (Instituto de Matemática e Estatística da Universidade de São Paulo - Brazil)

Rational Points on some Fermat Curves and Gröbner bases

Pietro Speziali
(Joint work with Cícero Carvalho)
Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo

Abstract:
Let $d \geq 3$ a divisor of a prime $p > 3$. Consider the polynomial ring $\mathbb{F}_p[x, y]$. We deal with the computation of the reduced Gröbner basis $G(I_d)$ for the ideal

$$I_d = \langle x^d + y^d + 1, x^p - x, y^p - y \rangle.$$

As an application, results on the size of the variety $V(I_d)$ are presented.

On the number of $\mathbb{F}_{q^n}$-rational points of $Y^q - Y = X^{q_0}(X^q - X)$

Mariana Coutinho
(Joint work with Herivelto Borges)
Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo

Abstract:
Let p be a prime number and, for any $t > 1$, consider $\mathcal{X}$ the nonsingular model defined over

$\mathbb{F}_q$ of the projective absolutely irreducible plane algebraic curve given in affine coordinates by

$$Y^q - Y = X^{q_0}(X^q - X),$$

where $q_0 = p^t$ and $q = p^{2t-1}$. For p even, $\mathcal{X}$ is the so-called Deligne?Lusztig curve associated with the Suzuki group, which has remarkable properties, for instance its large automorphism group and its property of being $\mathbb{F}_{q^4}$-maximal. In the present work, we address the study of the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{X}$ for p an odd prime number.

The Hasse-Witt invariant of a class of hyperelliptic curves

Cirilo Gonçalves Júnior
(Joint work with Herivelto Borges)
Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo

Abstract:
In this talk, we discuss the problem of computing the Hasse-Witt inavariant of the hyperelliptic curve

$$y^2 = x^n + 1.$$

This problem can be related to the problem of computing the number of solutions to

$$a_1x_1 + a_2x_2 + \ldots + a_hx_h \equiv 0 \pmod{m},$$

where $0 \leq x_i \leq tm + r$ and $a_1, \ldots, a_h \in \{1, \ldots, m-1\}$ are units in $\mathbb{Z}/m\mathbb{Z}$, for some integers m, h, t and r.

On Reed-Muller type codes defined on higher dimensional scrolls

Cícero Carvalho
Universidade Federal de Uberlândia

Abstract:
In 1988 Lachaud introduced the class of projective Reed-Muller codes, which are obtained by evaluating the space of homogeneous polynomials of a fixed degree d on the points of $\mathbb{P}^n(\mathbb{F}_q)$. In this talk we will introduce another class of codes, defined by evaluating the same space of polynomials on the points of a higher dimensional scroll, a variety obtained from a set of rational normal curves contained in complementary linear subspaces of a projective space. We determine a formula for the dimension of the codes, and the exact value of the minimum distance in some special cases. This is a joint work with Victor G.L. Neumann, Xavier Mondragón and Horacio Tapia-Recillas.

An extension of Delsarte, Goethals and Mac Williams theorem on minimal weight codewords to a class of Reed-Muller type codes

Victor Gonzalo Lopez Neumann
Universidade Federal de Uberlândia

Abstract:
In 1970 Delsarte, Goethals and Mac Williams published a seminal paper on generalized Reed-Muller codes where, among many important results, they proved that the minimal weight codewords of these codes are obtained through the evaluation of certain polynomials which are a specific product of linear factors, which they describe. In the present paper we extend this result to a class of Reed-Muller type codes defined on a product of (possibly distinct) finite fields of the same characteristic. The paper also brings an expository section on the study of the structure of low weight codewords, not only for affine Reed-Muller type codes, but also for the projective ones. Joint work with Cícero Carvalho.

A bound on the Carlitz rank of permutation polynomials

Luciane Quoos
(Joint work with Nurdagül Anbar, Almasa Odžak, Vandita Patel, Anna Somoza, Alev Topuzoğlu)
Universidade Federal de Rio de Janeiro

Abstract:
Let $\mathbb{F}_q$ be the finite field with $q \geq 3$ elements. A polynomial $f \in \mathbb{F}_q[x]$ is a *permutation polynomial*(PP) of $\mathbb{F}_q$ if it induces a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$. By a Carlitz's Theorem any permutation f of $\mathbb{F}_q$ can be represented by a polynomial of the form

$$P_n(x) = P_n(a_0, ..., a_{n+1}; x) = (\dots((a_0x + a_1)^{q-2} + a_2)^{q-2} \dots + a_n)^{q-2} + a_{n+1}, \qquad (1)$$

where $a_i \neq 0$, for $i = 0, 2, \dots, n$. The *Carlitz rank* of f over $\mathbb{F}_q$ is the smallest integer $n \geq 0$ satisfying $f = P_n$ for a permutation P_n of the form (1). For a certain family of PPs a bound involving the Carlitz Rank, the degree of a certain polynomial and the cardinality of the finite field will be given.
Let f and $f + g$ be permutation polynomials of $\mathbb{F}_q$, where $\mathrm{Crk}(f) = n \geq 1$, *$f \in \mathcal{L}_1$, and the degree k of $g \in \mathbb{F}_q[x]$ satisfies $1 \leq k < q - 1$. Then*

$$k(1 + (k-1)\sqrt{q}) \geq q - 2n - m + 1,$$

where $m = \gcd(k, q-1)$.

Factorization of iterates of polynomials

Lucas Reis
USP, Campus de São Carlos

Abstract:
Let $\mathbb{F}_q$ be the finite field with q elements and $f, g \in \mathbb{F}_q[x]$ be polynomials of degree at least one. In this talk, we discuss the asymptotic growth of certain arithmetic functions associated

to the factorization of the iterated polynomials $f(g^{(n)}(x))$ over $\mathbb{F}_q$, such as the largest degree of an irreducible factor and the number of irreducible factors. In particular, we provide significant improvements on the results of D. Gómez-Pérez, A. Ostafe and I. Shparlinski (2014).

Ordered Orthogonal Array Construction using LFSR sequences

André Castoldi
UTFPR

Abstract:
In this talk, I will present a joint work with Lucia Moura, Daniel Panario and Brett Stevens. We present 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). 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 $\mathbb{F}_q$. We prove properties about the relative positions of runs in an LFSR which guarantee that the constructed OOA has strength t. 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.

A polytope approach for counting numerical semigroups by genus

Matheus Bernardini
Universidade de Brasilia

Abstract:
For a nonnegative integer g, we denote the set of numerical semigroups of genus g by $\mathcal{S}_g$ and its cardinality by n_g. Zhai proved that $\frac{n_{g+1}}{n_g}$ approaches the golden ratio, hence $n_g < n_{g+1}$, for large enough g. It remains as an open problem to decide if $n_g < n_{g+1}$ holds true for all g.

For nonnegative integers g and γ, we denote the set of numerical semigroups of genus g and γ even gaps by $\mathcal{S}_\gamma(g)$ and its cardinality by $N_\gamma(g)$. Torres proved that if $S \in \mathcal{S}_\gamma(g)$, then $2g \geq 3\gamma$; hence $n_g = \sum_{\gamma=0}^{\lfloor 2g/3 \rfloor} N_\gamma(g)$. Bernardini and Torres studied $N_\gamma(g)$; it was proved that $N_\gamma(g) = N_\gamma(3\gamma)$, if $g \geq 3\gamma$ and, otherwise, $N_\gamma(g) < N_\gamma(3\gamma)$. From the surjective map $\mathbf{x} : \mathcal{S}_\gamma(g) \to \mathcal{S}_\gamma, S \mapsto S/2$, $N_\gamma(g)$ can be computed as $\sum_{T \in \mathcal{S}_\gamma} \#\mathbf{x}^{-1}(T)$.

In this talk, we study the problem of computing the numbers $N_\gamma(g)$ by using the multiplicity of $T \in \mathcal{S}_\gamma$ and its Apéry set. This leads to a polytope problem and has a close relation with the problem of deciding if the sequence (n_g) is increasing.

On Weirstrass pure gaps of curves with a special triangle

Gregory Duran Cunha
IMECC/UNICAMP

Abstract:
For smooth plane curves $\mathcal{X}$ of degree $n+1 > 3$, defined over a perfect field, for which there are three distinct lines that cut out on $\mathcal{X}$ the divisors $nP_1 + P_2$, $nP_2 + P_3$, and $nP_3 + P_1$, we explicitly determine the set of pure gaps at any subset of $\{P_1, P_2, P_3\}$.

Maximal elements in Weierstrass semigroups at several points

Wanderson Tenorio
UFMT

Abstract:
The knowledge of Weierstrass semigroups at several points on an algebraic curve over a finite field allows understanding the behavior of certain Riemann-Roch spaces. Motivated by successful applications in the analysis of AG codes, the elements in these structures (non-gaps), as well as in their complements (gaps), have been quite explored recently. In this talk we discuss how the notion of maximality, introduced by F. Delgado, can be used to describe gaps and non-gaps at several points.

On (N, r)-Galois-Weierstrass numerical semigroups

Steve da Silva Vicentim
UFCA

Abstract:
We study a generalization of the concept of cyclic semigroup introduced by Kim and Komeda (Arch. Math., 2001). We say that a numerical semigroup $H = \{0 < h_1 < h_2 < ...\}$ is (N, r)-Galois-Weierstrass if there exists a Galois covering $\mathcal{X} \to \mathbb{P}^1$ of degree N and a point $P \in \mathcal{X}$ totally ramified by this morphism such that $H = H(P)$, the Weierstrass semigroup of P. We characterize (N, r)-Galois-Weierstrass numerical semigroups by means of certain linear system. We also show a criterion to verify that H is not a (N, r)-Galois-Weierstrass for some N, and finally we give some examples and applications.

Connection between algebraic lattices and well-rounded lattices in the plane

Carina Alves
UNESP

Abstract:
Let Λ be a lattice of full rank in the n-dimensional Euclidean space $\mathbb{R}^n$ for $n \geq 2$. The lattice Λ is called well-rounded (abbreviated WR) if the set $S(\Lambda) := \{x \in \Lambda : ||x||^2 = |\Lambda|\}$ spans $\mathbb{R}^n$. WR lattices are important in discrete optimization, in particular in the investigation of sphere packing, sphere covering, kissing number problems and coding theory. Another class of lattices

that comes up frequently in connection with optimization problems and in coding theory are the algebraic lattices, i.e, lattices constructed through canonical homomorphism via ideals of a ring of algebraic integers. The importance and applicability of these two special classes of lattices motivates the following natural question: when are algebraic lattices well-rounded? In this work we study well-rounded lattices coming from ideals in quadratic rings of integers, showing that there exist infinitely many real and imaginary quadratic number fields containing ideals which give rise to well-rounded lattices in the plane.

Rotated A_2, E_6 and E_7-lattices via Galois extensions

Grasiele C. Jorge
São Jose dos Campos

Abstract:
Let $\mathbb{K}$ be a number field and $\mathcal{O}_{\mathbb{K}}$ its ring of integers. An algebraic lattice is a lattice in $\mathbb{R}^n$ associated with a number field through a twisted embedding. In this talk we will present a necessary condition for constructing an algebraic lattice with determinant D via a fractional ideal of $\mathcal{O}_{\mathbb{K}}$ when $\mathbb{K}$ is a Galois extension. In particular, we will discuss on some Galois extensions that is not possible to construct rotated A_2, E_6 and E_7-lattices. Lastly, we will exhibit some algebraic constructions for A_2, E_6 and E_7. For A_2 and E_6 these constructions were obtained via ideals of $\mathcal{O}_{\mathbb{K}}$ and for E_7 via free $\mathbb{Z}$-modules contained in $\mathcal{O}_{\mathbb{K}}$.

Algebraic Constructions of Lattices via Division Algebras

Cintya Wink de Oliveira Benedito
São João da Boa Vista-SP

Abstract:
It has been shown that algebraic lattices, i.e., lattices constructed via the canonical embedding of an algebraic number field, provide an efficient tool for designing lattice codes [**?**]. More recently, lattices and quaternion algebras have been connected. In [**?**] was presented a construction of ideal lattice from quaternion algebras, in [**?**] the E_8-lattice was constructed using quaternion algebras over an imaginary quadratic field and in [**?**], hyperbolic lattices via maximal quaternion orders was obtained. In this work we propose algebraic constructions of lattices in dimension 2^n via division algebras, more specifically, via orders of quaternion and octonion algebras over a totally real number field. These lattices are identified through their Gram and generator matrix. With these constructions it is possible to obtain lattices with densest packings known for dimensions 4, 8, 12, 16 and 24 via quaternion algebras, and for dimensions 8, 16 and 32 via octonion algebras.

Posters Finite fields and applications

Hyperplane arrangements over finite field

Cesar A. Ipanaque Zapata (USP)

Abstract:
A hyperplane arrangement $\mathcal{A}$ in an $l-$dimensional vector space V is a finite set of linear subspaces of codimension one. Let $\mathcal{A}$ be an arrangement in $V = \mathbb{F}_q^l$. In this work we will study the complement

$$M(\mathcal{A}) := \mathbb{F}_q^l - \bigcup_{A \in \mathcal{A}} A.$$

This work is supported by FAPESP 2016/18714-8.