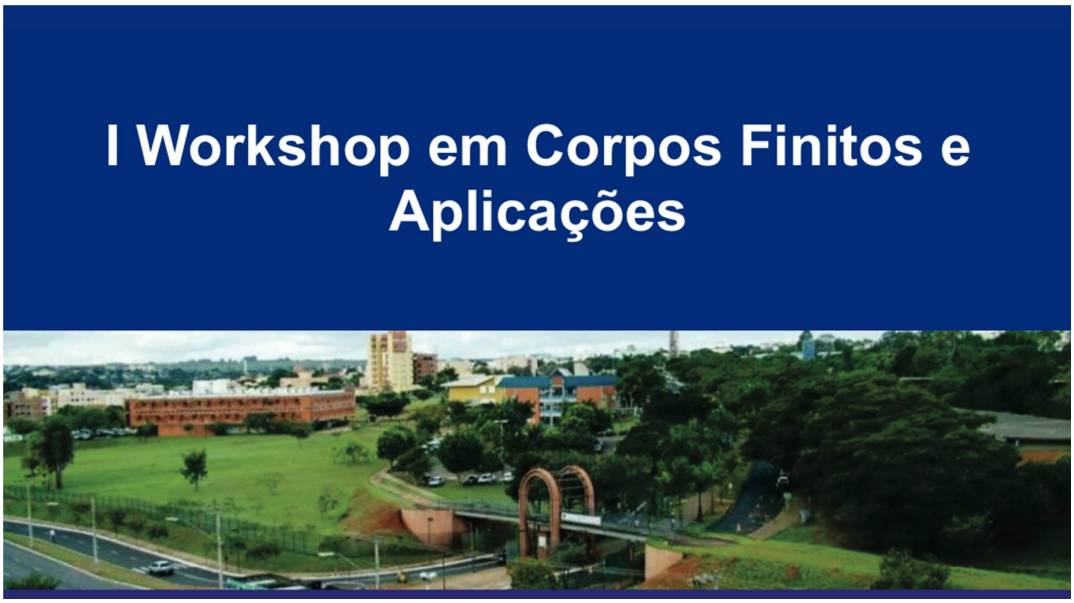

Resumos das palestras

MÉTODOS DE BASES DE GROBNER EM CÓDIGOS DE AVALIAÇÃO

CÍCERO CARVALHO
UFU

Nesta palestra pretendo discutir alguns resultados da teoria de bases de Gröbner que têm sido utilizados para determinar parâmetros de códigos de avaliação, especialmente os do tipo Reed-Muller.

Submissão de trabalhos - Apresentação oral

Título: Ações de grupos sobre polinômios irredutíveis
Autores: Daniela Alves de Oliveira
Fabio Enrique Brochero Martínez
Lucas da Silva Reis

Resumo: Dado um corpo finito $\mathbb{F}_q$, para inteiro positivo $k \geq 1$ definimos $\mathcal{I}(q,k)$ como sendo o conjunto de polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ de grau k. Para $[A] = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}(2,q)$ e $f(x) \in \mathcal{I}(q,k)$, se define $[A] \circ f$ como sendo o único polinômio mônico tal que é múltiplo escalar do polinômio

$$[A] \circ f := (bx+d)^n f\left(\frac{ax+c}{bx+d}\right).$$

Esta aplicação define uma ação do grupo $\mathrm{PGL}(2,q)$ sobre o conjunto $\mathcal{I}(q,k)$, que foi estudada por Stichtenoth e Topuzoğlu em [2].
Para $k \geq 2$ e $[A] \in \mathrm{PGL}(2,q)$, dizemos que $f \in \mathcal{I}(q,k)$ é $[A]$-invariante se $[A] \circ f = f$. Se $D := \mathrm{ord}[A]$, foi provado em [2] que o número de $[A]$-invariantes de grau Dn, denotado por $\varphi_A(Dn)$, converge para

$$\varphi(D)\frac{q^n}{Dn}, \text{ quando } n \to \infty,$$

onde φ é a função de Euler.
Podemos estender naturalmente essa ação. Seja q um potência de um primo e n um inteiro positivo. Denotamos por $\mathrm{Gal}(\mathbb{F}_{q^n} : \mathbb{F}_q)$ o grupo de Galois da extensão $\mathbb{F}_{q^n}/\mathbb{F}_q$. Este grupo é cíclico de ordem n e é gerado por σ_1, o automorfismo de Frobenius dado por: $\mathbb{F}_{q^n} \to \mathbb{F}q^n$ com $\alpha \mapsto \alpha^q$. Denotamos para cada $i \geq 1$, σ_i como sendo a i-ésima composição de σ_1. Observemos que σ_i é extendido naturalmente para o anel de polinômios $\mathbb{F}_{q^n}[x]$ e, por simplicidade, σ_1 também denota esta extensão.
Em particular, seja $\mathrm{P\Gamma L}(2,q^n) = \mathrm{PGL}(2,q^n) \rtimes \mathrm{Gal}(\mathbb{F}_{q^n} : \mathbb{F}_q)$, que é chamado de grupo projetivo semi-linear. Este grupo induz uma aplicação do tipo de Frobenius no conjunto de polinômios mônicos irredutíveis sobre $\mathbb{F}_{q^n}$. Para $\mathcal{I}_k := \mathcal{I}(q^n,k)$ com $k \geq 2$ e $[A,\sigma_i] \in \mathrm{P\Gamma L}(2,q^n)$, definimos a aplicação

$$[A,\sigma_i] * f(x) = [A] \circ (\sigma_i(f)).$$

Esta composição define uma ação do grupo $\mathrm{P\Gamma L}(2,q^n)$ sobre os conjuntos $\mathcal{I}_k$ com $k \geq 2$. Generalizando as ideias de Stichtenoth e Topuzoğlu, em [1] estudamos o números de pontos fixos desta ação, i.e, dado $k \geq 2$ e $[A,\sigma_i] \in \mathrm{P\Gamma L}(2,q^n)$, determinamos propriedades sobre os $f \in \mathcal{I}_k$ tais que $[A,\sigma_i] * f = f$.

Referências

[1] Möbius-Frobenius maps on irreducible polynomials. Disponível em `https://arxiv.org/abs/1812.08900`

[2] Stichtenoth, H.; Topuzoğlu, A. Factorization of a class of polynomials over finite fields. *Finite Fields Appl.* 18 (2012) 108–122.

INTEGRABILIDADE DE DARBOUX-JOUANOLOU PARA FORMAS DIFFERENCIAIS POLINOMIAIS SOBRE CORPOS ARBITRÁRIOS

EDILENO DE ALMEIDA SANTOS

O trabalho seminal de G. Darboux (1878) mostrou a fascinate relação entre integrabilidade e existência de soluções algébricas para um sistema diferencial polinomial planar. A abordadem clássica de Darboux mostra que, para um campo vetorial polinomial planar de grau d, em $\mathbb{R}^2$ ou $\mathbb{C}^2$, a partir de $\binom{d+1}{2}+1$ curvas algébricas irredutíveis invariantes podemos computar uma integral primeira analítica (possivelmente multivaluada). Este método foi estudado com entusiasmo por H. Poincaré (1891), que observou a dificuldade em se obter algoritmicamente tais curvas invariantes.

Baseado no método de Darboux, J.-P. Jouanolou (1979) demonstrou que se K é um corpo de característica 0 e ω é uma 1-forma polinomial de grau d em K^n admitindo pelo menos $\binom{d-1+n}{n}\cdot\binom{n}{2}+2$ hipersuperfícies algébricas irredutíveis invariantes, então ω possui uma integral primeira racional, obtida a partir das hipersuperfícies invariantes.

De um outro ponto de vista, sobre um corpo algebricamente fechado K de característica positiva $p>0$, M. Brunella e M. Nicollau (1999) provaram que se ω é uma 1-forma racional (em uma variedade projetiva suave sobre K) admitindo infinitas hipersuperfícies algébricas invariantes, então ω admite uma integral primeira racional.

Em forte contraste com o caso de característica 0, onde um teorema também de Jouanolou revela que um campo vetorial genérico no plano complexo não adimite nenhuma curva algébrica invariante, J. V. Pereira (2001) mostrou que um campo de vetores genérico em um espaço afim de característica positiva admite pelo menos uma curva algébrica invariante (a condição genérica é que o divergente do campo seja nulo).

Nosso objetivo é apresentar a seguinte versão geral do *Critério de Darboux-Jouanolou*: dado um corpo arbitrário (finito ou infinito) K de característica $p\geq 0$, definimos um número natural $N_K(n,d,r)$, que depende apenas de n, r, d e p, de modo que $N_K(n,d,r)\leq\binom{d+n}{n}\cdot\binom{n}{r}$ e vale o

Teorema A. *Seja $\omega\in\Omega^1(K^n)$ uma r-forma polinomial de grau d sobre um corpo arbitrário K. Se ω possui $N_K(n,d-1,r+1)+r+1$ hipersuperfícies algébricas irredutíveis invariantes, então ω admite uma integral primeira racional.*

Faculdade de Ciências Exatas e Tecnologia (FACET) - Universidade Federal da Grande Dourados (UFGD), Rodovia Dourados - Itahum, Km 12 - Cidade Universitátia, Dourados - MS, Brazil

E-mail address: edilenosantos@ufgd.edu.br

I Workshop em Corpos Finitos e Aplicações

Uberlândia, September 4-6, 2019

The a-number of Artin-Schreier curves

Speaker: Gregory Duran Cunha (IMECC-UNICAMP)
Joint work with: Pietro Speziali (ICMC-USP)

Let $\mathcal{X}$ be an algebraic curve defined over an algebraically closed field of positive characteristic p. The a-number $a(\mathcal{X})$ of $\mathcal{X}$ is the dimension of the space of exact holomorphic differentials on $\mathcal{X}$, that is, the dimension of the kernel of the Cartier operator on $\mathcal{X}$. In this talk we give a technique to determine exact holomorphic differentials when $\mathcal{X}$ is some Artin-Schreier curve, thus obtaining a lower bound for $a(\mathcal{X})$.

The Hurwitz curve over $\overline{\mathbb{F}_q}$ and its Weierstrass points for the morphism of lines

Herivelto Borges

(Joint work with N. Arakelian and P. Speziali)

Let $\mathcal{X}$ be an irreducible algebraic curve defined over an algebraically closed field $\mathbb{K}$ of characteristc $p \geq 0$. The genus of $\mathcal{X}$ is certainly the most famous birational invariant of $\mathcal{X}$. If $\mathbb{K}(\mathcal{X})$ denotes the function field of $\mathcal{X}$, the group all $\mathbb{K}$-automorphisms of $\mathbb{K}(\mathcal{X})$ is called *automorphism group* of $\mathcal{X}$, and it is denoted by $\mathrm{Aut}(\mathcal{X})$. Such group is another birational invariant of $\mathcal{X}$, and the study of $\mathrm{Aut}(\mathcal{X})$ has become a central problem within the theory of algebraic curves. In this talk, we will consider smooth Hurwitz curve

$$\mathcal{H}_n : XY^n + YZ^n + X^nZ = 0$$

over $\overline{\mathbb{F}_q}$, and provide an explicit description of its Weierstrass points for the morphism of lines. That is, we will completely characterize the special set of points $P \in \mathcal{H}_n$ for which the intersection multiplicity $I(P, \mathcal{H}_n \cap T_P\mathcal{H}_n)$ is somewhat large. As a consequence, the full automorphism group $\mathrm{Aut}(\mathcal{H}_n)$ as well as bounds for the number of $\mathbb{F}_q$-rational points on $\mathcal{H}_n$ will be presented. In addition, we will discuss how this information can be used to answer a question raised by Prof. F. Torres in 2015.

Título: Decomposição de Funções Racionais sobre Corpos Finitos

Autores: Jonas Szutkoski (Universidade Federal de Ciências da Saúde de Porto Alegre), Mark van Hoeij (Florida State University), Luiz Emílio Allem (Universidade Federal do Rio Grande do Sul) e Juliane Capaverde (Universidade Federal do Rio Grande do Sul).

Resumo: Seja $\mathbb{F}_q$ um corpo finito com q elementos e seja $f(t) = f_n(t)/f_d(t)$ uma função racional, com $f_n(t), f_d(t) \in \mathbb{F}_q[t]$. O grau da função $f(t)$ é definido como $\max\{\deg(f_n), \deg(f_d)\}$. Uma decomposição de $f(t)$ é uma expressão da forma $f(t) = g \circ h(t) = g(h(t))$, onde $g(t), h(t) \in \mathbb{F}_q(t)$. A função racional $f(t)$ é dita indecomponível se $f(t) = g \circ h(t)$ implicar em $\deg(g(t)) = 1$ ou $\deg(h(t)) = 1$. Uma decomposição minimal de $f(t)$ é uma decomposição da forma $f = g \circ h(t)$, onde $g(t), h(t) \in \mathbb{F}_q(t)$ e $h(t)$ é indecomponível. Nesta apresentação falaremos sobre o problema de encontrar todas as decomposições minimais de $f(t) \in \mathbb{F}_q(t)$.

Seja $f(t) = f_n(t)/f_d(t) \in \mathbb{F}_q(t)$ uma função racional e consideremos os corpos $k = \mathbb{F}_q(f(t))$ e $K = \mathbb{F}_q(t)$. Sem perda de generalidade, podemos assumir que $f_n(t)$ é mônico e que $\deg(f_n(t)) > \deg(f_d(t))$. Dessa forma, $\Phi_f(x) := f_n(x) - f(t)f_d(x) \in k[x]$ é o polinômio minimal de t sobre k. O principal resultado no qual nos basearemos para encontrar um algoritmo que calcule todas as decomposições minimais de $f(t)$ resume-se nas seguintes equivalências (ver [1]):

1) $f(t) = g \circ h(t)$, para certos $g(t), h(t) \in \mathbb{F}_q(t)$;

2) $L := \mathbb{F}_q(h(t))$ é um subcorpo da extensão K/k.

3) Φ_f divide Φ_h, onde $\Phi_h := h_n(x) - h(t)h_d(x) \in K[x]$.

Algoritmos anteriores, tais como [1, 2 e 4], baseavam-se nas equivalências 1) e 3). Isto é, as decomposições minimais de f podem ser obtidas fatorando-se completamente o polinômio Φ_f e então combinando-se tais fatores de modo a obter fatores de Φ_f que poderiam ser escritos na forma $\Phi_h = h_n(x) - h(t)h_d(x)$ e que resultariam em um subcorpo maximal no reticulado de subcorpos de K/k. Claramente, esta abordagem se torna problemática quando o número de fatores de Φ_f aumenta devido à natureza combinatorial do algoritmo.

Apresentaremos uma nova abordagem para este problema. Analisando as equivalências 1) e 2), vemos que, para encontrar todas as decomposições minimais de $f(t)$, precisamos encontrar todos os subcorpos maximais do reticulado de subcorpos de K/k. Para tanto, utilizaremos a definição de subcorpos principais, dada em [3]: seja $t \in K$ um gerador de K sobre k (isto é, $K = k(t)$) e seja $\Phi_f(x) \in k[x]$ o polinômio minimal de t sobre k com fatores irredutíveis $F_1, \ldots, F_r$ sobre K. Para cada fator F_i definimos

$$L_i = \{g(t) \in K : F_i \mid \Phi_g\} \subseteq K, \quad 1 \leq i \leq r.$$

Cada L_i é um subcorpo de K/k, denominado de subcorpo principal de K/k (relativo ao fator F_i). A importância dos subcorpos principais se resume na seguinte afirmação: se L é um subcorpo de K/k, então

$$L = \bigcap_{i \in I} L_i, \quad \text{para algum subconjunto } I \subseteq \{1, 2, \ldots, r\},$$

isto é, L é a interseção de alguns subcorpos principais (ver [3]). Utilizando essa abordagem, conseguimos evitar a parte combinatorial das estratégias anteriores, tornando o algoritmo mais eficiente. Por exemplo, quando $f(t) \in \mathbb{F}_q[t]$, a complexidade de calcular as decomposições minimais de $f(t)$ foi reduzida de $\tilde{\mathcal{O}}(n^6)$ (ver [4]) para $\tilde{\mathcal{O}}(n^3)$ operações de bit, onde n é o grau de $f(t)$. Estes resultados podem ser conferidos em [5].

[1] C. Alonso, J. Gutierrez, and T. Recio. A rational function decomposition algorithm by near-separated polynomials. JSC, 19(6):527-544, 1995.
[2] M. Ayad and P. Fleischmann. On the decomposition of rational functions. JSC, 43(4):259 - 274, 2008.
[3] M. van Hoeij, J. Klüners, and A. Novocin. Generating Subfields. JSC, 52:17-34, 2013.
[4] R. Blankertz. A polynomial time algorithm for computing all minimal decompositions of a polynomial. ACM Commun. Comput. Algebra, 48(1/2):13-23, 2014.
[5] L. E. Allem, J. G. Capaverde, M. van Hoeij, and J. Szutkoski. Functional decomposition using principal subfields. ISSAC' 17, 421-428, New York, NY, USA, 2017.

CONTADEM DE BINÔMIOS DE PERMUTAÇÃO

JOSÉ ALVES OLIVEIRA AND F. E. BROCHERO MARTÍNEZ

Seja $\mathbb{F}_q$ um corpo com q elementos. Dizemos que um polinômio $f(x) \in \mathbb{F}_q[x]$ é um polinômio de permutação sobre $\mathbb{F}_q$ se a função $x \mapsto f(x)$ permuta os elementos de $\mathbb{F}_q$. Precisar o número de polinômios com determinada característica tem se mostrado bastante interessante. Um problema em aberto é encontrar o número exato de elementos $a \in \mathbb{F}_q$ para os quais o binômio $x^n(x^{\frac{q-1}{r}} + a)$ é um polinômio de permutação. O resultado apresentado por Ariane M. Masuda e Michael E. Zieve (2009) afirma que o número T de elementos $a \in \mathbb{F}_q$ para os quais o binômio $x^n(x^{\frac{q-1}{r}} + a)$ é uma permutação satisfaz

$$\frac{r!}{r^r}\left(q + 1 - \sqrt{q}M_r - (r+1)r^{r-1}\right) \leq T \leq \frac{r!}{r^r}\left(q + 1 + \sqrt{q}M_r\right),$$

onde $M_r := r^{r+1} - 2r^r - r^{r-1} + 2$.

Nessa exposição, apresentaremos o número exato de binômios de permutação da forma $x^n(x^{\frac{q-1}{2}} + a)$ e a relação existente entre o número de binômios de permutação da forma $x^n(x^{\frac{q-1}{3}} + a)$ e o número de pontos racionais sobre curvas elípticas. Por fim, apresentaremos o número exato de binômios de permutação da forma $x^n(x^{\frac{q-1}{3}} + a)$, seguido de alguns exemplos.

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 31270-901, Brazil,

E-mail address: jose-alvesoliveira@hotmail.com

E-mail address: fbrocher@mat.ufmg.br

On κ-sparse numerical semigroups

Juan Villanueva[1], Guilherme Tizziotti[2]

[1] Universidade Federal de Mato Grosso, Câmpus Universitário do Araguaia, Instituto de Ciências Exatas e da Terra

[2] Universidade Federal de Uberlândia, Câmpus Santa Mônica, Faculdade de Matemática

In this talk, we investigate the class of numerical semigroups verifying the property that every two subsequent non-gaps are spaced by at least κ (positive integer). These semigroups will be called ê-sparse and generalize the concept of sparse numerical semigroups.

References

[1] Guilherme Tizziotti and Juan Villanueva, *On κ-sparse numerical semigroups*, Journal of Algebra and Its Applications, Volume 17 (2018). Number 11, pp. 1850209-1 – 1850209–13

On linear equations over finite fields

Lucas Reis
University of São Paulo

Abstract

Let q be a prime power, $\mathbb{F}_q$ be the finite field with q elements and $d_1, \ldots, d_k$ be positive integers. In this note we explore the number of solutions $(z_1, \ldots, z_k) \in \overline{\mathbb{F}}_q^k$ of the equation

$$L_1(x_1) + \cdots + L_k(x_k) = b, \tag{1}$$

with the restrictions $z_i \in \mathbb{F}_{q^{d_i}}$, where each $L_i(x)$ is a nonzero polynomial of the form $\sum_{j=0}^{m} a_j x^{q^j} \in \mathbb{F}_q[x]$. We characterize the elements $b \in \overline{\mathbb{F}}_q$ for which the equation above has a solution and, in affirmative case, we determine the exact number of solutions. We provide two applications of our main result: we obtain the cardinality of the sumset

$$\sum_{i=1}^{k} \mathbb{F}_{q^{d_i}} := \{\alpha_1 + \cdots + \alpha_k \,|\, \alpha_i \in \mathbb{F}_{q^{d_i}}\},$$

and solve systems of equations involving trace functions.

Keywords: q-linearized polynomials, factorization, irreducible polynomails

Construction of sequences with high Nonlinear Complexity from Hermitian Function Fields

Luciane Quoos

joint work with Alonso S. Castellanos and Guilherme Tizziotti

August 13, 2019

Abstract

The theory of algebraic functions of one variable over the finite field $\mathbb{F}_q$ of cardinality q has several applications in distinct areas of mathematics such as coding theory, permutation polynomials and sequences. Sequences over finite fields from the complexity-theoretic standpoint can also be applied on cryptography and pseudorandom generation, one of the requirements of such sequences is that it should be very hard to replicate the entire sequence from the knowledge of a part of it, that is, its complexity should be large. Many different complexity measures are available in the literature, the most usual being the *linear complexity*. In recent years paper researchers have constructed sequences with large *nonlinear complexity* measure.

We provide a sequence with high nonlinear complexity from the Hermitian function field $\mathcal{H}$. This sequence was obtained using a function with pole divisor in ℓ collinear rational places $P_1, \ldots, P_\ell$ on $\mathcal{H}$.

ON THE CLASSICALITY AND THE FROBENIUS CLASSICALITY OF SOME GENERALIZED FERMAT CURVES WITH RESPECT TO LINEAR SYSTEMS OF CURVES OF DEGREE s

MARIANA COUTINHO

Let $\mathcal{X}$ be the nonsingular model defined over $\mathbb{F}_q$ of

$$\mathcal{F} : F(X,Y) = aX^nY^n - X^n - Y^n + b = 0$$

and let $\overline{\mathbb{F}_q}(\mathcal{X}) = \overline{\mathbb{F}_q}(x,y)$ be the function field of $\mathcal{X}$, where x and y satisfy $F(x,y) = 0$. In this talk, for a particular choice of n and s, we will discuss the classicality and the $\mathbb{F}_q$-Frobenius classicality of $\mathcal{X}$ with respect to the morphism

$$(\cdots : x^iy^j : \cdots),$$

where $0 \leqslant i,j \leqslant s-1$ and $0 \leqslant i+j \leqslant s$.

(Mariana Coutinho) IMECC-UNICAMP
Email address: mariananery@alumni.usp.br

Semigrupos numéricos: aspectos aritméticos

Matheus Bernardini - Universidade de Brasília

Esta é uma proposta para a sessão de Discussão de Problemas.

Um semigrupo numérico S é um submonoide de $(\mathbb{N}_0, +)$ tal que o *conjunto de lacunas* $G(S) = S \setminus \mathbb{N}_0$ é finito. O gênero de S é denotado por $g(S)$.

Dado um inteiro não negativo g, denotamos o conjunto de semigrupos numéricos por $\mathcal{S}_g$ e sua cardinalidade por n_g. Zhai provou que $\frac{n_{g+1}}{n_g}$ se aproxima do número áureo $\frac{1+\sqrt{5}}{2}$. Em particular, $n_g < n_{g+1}$ para g suficientemente grande. Um problema em aberto é decidir se $n_g < n_{g+1}$, para todo $g > 0$. Esse problema surge como versão fraca de uma conjectura proposta por Bras-Amorós em 2008: é verdade que $n_g + n_{g+1} \leq n_{g+2}$ para todo g?

A proposta de programação é:

- Dia 1: apresentar conceitos básicos, resultados elementares e o problema citado acima; propor a discussão.
- Dia 2: apresentar abordagens utilizando outro invariante do semigrupo numérico apresentadas por alguns autores; propor a discussão.
- Dia 3: apresentar uma abordagem recente para o problema; propor a discussão.

Grau separável do mapa de Gauss e curvas duais estritas sobre corpos finitos

Nazar Arakelian

CMCC- Universidade Federal do ABC
E–mail: n.arakelian@ufabc.edu.br

Seja $\mathcal{X}$ uma curva algébrica projetiva e denote por $\mathcal{X}'$ sua curva dual estrita, ou seja, a curva definida pelo fecho (no espaço projetivo dual) dos hiperplanos osculadores à $\mathcal{X}$ nos pontos não singulares. O morfismo que leva $\mathcal{X}$ em $\mathcal{X}'$ é chamado de mapa de Gauss (estrito). Nesse trabalho, apresentamos alguns resultados referentes ao grau separável do mapa da Gauss de curvas sobre corpos finitos. Em particular, apresentamos uma generalização de um resultado conhecido sobre o mapa de Gauss de curvas planas Frobenius não clássicas. Também apresentamos uma caracterização de certas curvas estranhas, ou seja, curvas tais que suas tangentes em pontos não singulares são concorrentes.

Sobre a Curva GK e algumas Subcoberturas

Paulo César Oliveira

DEMPA - Urca
I Workshop em Corpos Finitos e Aplicações

Abstract

A partir do trabalho de [1], mostraremos que a curva GK, para $q = 8$ é coberta pela curva hermitiana. Apresentaremos subcoberturas da curva GK, daremos equações explícitas dessas subcoberturas e calculamos seus gêneros. Em [1,Thm 3.2] são definidas curvas maximais $\mathcal{C}_i, i = 1, 2, 3$ com paramêtros d_1, d_2 e d_3 os quais são divisores de $n+1$ e M ó máximo divisor comum entre d_1, d_2 e $d_3(n^2-n+1)$. Para certos valores dos paramêtros d_1, d_2 e d_3, mostraremos que estas curvas têm o mesmo modelo plano das que apresentamos.

Referências

1 Giulietti, M., Quoos, L., Zini, G., *Maximal curves from subcovers of the GK-curve*, J. of Pure and Applied Algebra, vol. 220, Issue 10, p. 3372 − 3383(2016).

I Workshop em Corpos Finitos e Aplicações

Uberlândia, September 4-6, 2019

Curves with automorphism groups of large prime order

Speaker: Pietro Speziali (ICMC-USP)
Joint work with: Nazar Arakelian (CMCC-UFABC)

Let $\mathcal{X}$ be a (algebraic, projective, absolutely irreducible) curve defined over an algebraically closed field K of characteristic $p \geq 0$. The automorphism group $\mathrm{Aut}_K(\mathcal{X})$ is defined as the automorphism group of the transcendency degree one function field $K(\mathcal{X})$.

Let q be a prime dividing $|\mathrm{Aut}_K(\mathcal{X})|$. A result by Homma states that either $q \leq g+1$ or $q = 2g+1$, where g is the genus of $\mathcal{X}$.

We say that $\mathcal{X}$ is a *q-curve* if $\mathrm{Aut}_K(\mathcal{X})$ contains a (necessarily cyclic) subgroup G of order equal to q. Homma completely characterized $(2g+1)$-curves up to birational equivalence.

In this work, we study q-curves for $g-1 \leq q \leq g+1$. Our main result is the complete characterization of $(g+1)$-curves up to birational equivalence. We also give a necessary and sufficient condition for a $(g+1)$-curve to be hyperelliptic.

Finally, we discuss some further developments, generalizations and applications of our results to the broader study of automorphism groups of algebraic curves.

Title: On permutation polynomials over finite fields.

Author: Rohit Gupta, Universidade Federal do Rio de Janeiro (UFRJ), Brazil

Abstract: Permutation polynomials have applications in various areas such as coding theory, cryptography and combinatorial designs. Construction of permutation polynomials is not difficult but finding a class of permutation polynomials with some addition requirements is a difficult task. In this talk, we discuss basic properties of permutation polynomials and prove the permutation property of a class of trinomials.

CÓDIGOS METACÍCLICOS À ESQUERDA

SAMIR ASSUENA

Nesta palestra, vamos considerar álgebras $\mathbb{F}_q G$ de grupos metacíclicos que cindem não abelianos sobre corpos finitos e construir bons códigos à esquerda em $\mathbb{F}_q G$ no caso em que a ordem do grupo G é $p^m \ell^n$, onde p e ℓ são números primos distintos.

References

[1] S. Assuena, C. Polcino Milies *Good codes from metacyclic groups*, Contemporary Mathematics, 727 (2019), 39-47.

[2] S. Assuena, C. Polcino Milies *Group Algebras of Metacyclic Groups over Finite Fields*, So Paulo J. Math. Sci. DOI 10.1007/s40863-016-0043-7.

[3] G. K. Bakshi, M. Raka, *Minimal cyclic codes of lenght $p^n q$*, Finite Fields and Their Applications, 9 (2003), 432-448.

[4] F. S. Dutra, R. A. Ferraz, C. Polcino Milies, *Semisimple group codes and dihedral codes*, Algebra and Disc. Math., 3 (2009), 28-48.

[5] R. A. Ferraz, C. Polcino Milies, *Idempotents in group algebras and minimal abelian codes*, Finite Fields and Their Applications, 13 (2007), 382-393.

[6] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes.* Online available at http://www.codetables.de .

[7] G. Olteanu, I. Van Gelder, *Construction on minimal non-abelian left group codes*, Des. Codes Cryptogr. (2015), 75:359-373.

Centro Universitário da Fei

E-mail address: samir.assuena@fei.edu.br

A NEW PERMUTATION CLASS AND ITS INDUCED PERMUTATION POLYNOMIAL

SÁVIO RIBAS

ABSTRACT. Let m, n be positive integers such that $m|n$, $m > 1$ and $\gcd(m, n/m) = 1$. During the talk, we will introduce a special class of *piecewise-affine permutations* of the finite set $[1, n] := \{1, 2, \ldots, n\}$ with the property that the reduction $\pmod m$ of m consecutive elements in any of its cycles is, up to a cyclic shift, a fixed permutation of $[1, m]$. Our main result provides the cycle decomposition of such permutations. We further apply the case $n = q - 1$ to show that such permutations give rise to permutations of finite fields $\mathbb{F}_q$ of order q, where q is a prime power. In particular, we explicitly obtain new classes of permutation polynomials of finite fields whose cycle decomposition is explicitly given.

This is a joint work with Lucas Reis (Departamento de Matemática, ICMC, Universidade de São Paulo, e-mail: `lucasreismat@gmail.com`).

Keywords: permutations; cycle decomposition; permutation polynomials; finite fields.

DEPARTAMENTO DE MATEMÁTICA, ICEB, UNIVERSIDADE FEDERAL DE OURO PRETO,

E-mail address: `savio.ribas@ufop.edu.br`

Prova da Hipótese de Riemann para Funções Zeta de Curvas sobre Corpos Finitos

Marcos Antônio Sobral Filho*
Fábio Enrique Brochero Martinez (orientador)†

Em Novembro de 1859, Bernhard Riemann publicou o artigo *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*, onde ele conjecturou que todos os zeros "não-óbvios" da sua função zeta tinham parte real $\frac{1}{2}$. Não sabemos ainda se a conjectura é verdadeira, mas sabemos que ela vale quando se trata de uma função zeta de uma curva algébrica definida sobre um corpo finito. Apesar de ser definida como uma série formal a partir dos divisores positivos da curva, a função zeta é uma função racional do tipo

$$Z(t) = \frac{L(t)}{(1-qt)(1-t)}$$

onde $L(t) \in \mathbb{Z}[t]$ com grau $2g$ (onde g é o genus da curva), satisfazendo $L(0) = 1$ e $L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right)$. Essa simetria em $L(t)$ garante que se $\alpha_1, \ldots, \alpha_{2g}$ são os recíprocos das raízes desse polinômio, então $\alpha_i \alpha_{g+1} = q$, para todo $i = 1, \ldots, g$. O que a **Hipótese de Riemann** afirma é que as raízes de $\zeta(s, C) \doteq Z(q^{-s}, C)$ estão todas sobre a linha crítica $Re\,(s) = \frac{1}{2}$. O que claramente é equivalente ao

Teorema 1. *Os recíprocos das raízes de $L(t)$ satisfazem $|\alpha_j| = q^{\frac{1}{2}}$, para todo $j = 1, \ldots, 2g$.*

A primeira prova para esse resultado instigante foi dada por André Weil na década de 1940. Em 1969, Stepanof forneceu um novo método de prova, o qual foi generalizado por Bombieri em 1973. Neste trabalho, vamos prová-lo a partir do Lema de Bombieri, cuja demonstração será omitida para fins didáticos.

Referências

[1] MORENO, C. J. - *Algebraic Curves over Finite Fields*, Cambrigde Tracts in Mathematics, 1991;

[2] MACK-CRANE, S. - *The Riemann Hypothesis for Varieties over Finite Fields*, Berkeley, 2015.

*Discente, UFMG, MG, Brasil $e-mail$: *sobralmarquinhos@gmail.com*
†Professor,UFMG, MG, Brasil $e-mail$: *fbrochero@ufmg.br*

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

Fernando Torres (UNICAMP) and Steve 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.

SÉRIES DE POINCARÉ ASSOCIADAS A SEMIGRUPOS DE WEIERSTRASS GENERALIZADOS

WANDERSON TENÓRIO (UFMT)

Os semigrupos de Weierstrass generalizados, associados a um ou mais pontos racionais de uma curva algébrica sobre um corpo finito, são estruturas que carregam informações sobre o comportamento dos espaços de Riemann-Roch de divisores com suporte específico. Associadas a essas estruturas aritméticas, podemos definir as séries de Poincaré, que são objetos combinatórios.

Neste apresentação discutiremos como essas ferramentas combinatórias codificam informações essenciais sobre seus semigrupos correspondentes. Em especial, veremos como interpretá-las como um invariante de seus respectivos semigrupos e suas possíveis interações que surgem a partir de recobrimentos especiais de curvas.

*Trabalho em conjunto com F. Torres e J. Moyano.