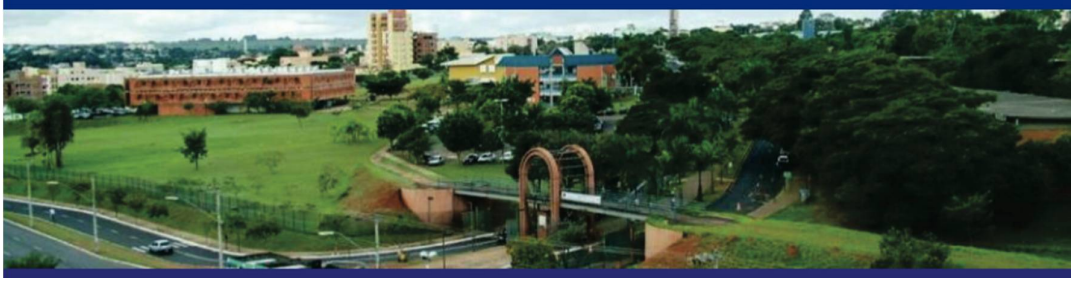
I Workshop em Corpos Finitos e Aplicações



Resumos das conferências

ANALYTIC AND PROBABILISTIC COMBINATORICS FOR POLYNOMIALS OVER FINITE FIELDS

DANIEL PANARIO
SCHOOL OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY

The central objects of this talk are univariate polynomials over finite fields. We first comment on a methodology from analytic combinatorics that allows the study of the decomposition of polynomials into its irreducible factors and the derivation of algorithmic properties as well as the estimation of average-case analysis of algorithms. This methodology can be naturally used to provide precise information on the factorization of polynomials into its irreducible factors similar to the classical problem of the decomposition of integers into primes. Examples of these results are provided. The shape of a random univariate polynomial over a finite field is also given. Periodicity properties of the iterations of random polynomials over finite fields are also commented.

Then, we briefly show several results for random polynomials over finite fields that were obtained using other methodologies based for example on probability and probabilistic combinatorics. We conclude providing several open problems for polynomials over finite fields related to number theory.

FACTORAÇÃO DE COMPOSIÇÃO DE POLINÔMIOS E DE POLINÔMIOS DE DICKSON E APLICAÇÕES

FABIO BROCHERO
UFMG

Seja $\mathbb{F}_q$ um corpo finito com q elementos e n um inteiro tal que todo divisor primo de n divide $q-1$. Neste trabalho tem dois objetivos

1. A caraterização completa dos fatores irredutíveis de polinômios da forma $f(x^n)$, onde $f(x)$ é um polinômio irreductível em $\mathbb{F}_q$ de grau k e ordem e, onde $mdc(ke, q-1) = 1$.]

2. A caraterização dos fatores irredutíveis de $D_n(x;a)$, o n-ésimo polinômio de Dickson.

A primeira parte foi feita em colaboração com Lucas Reis e Lays Silva Jesus, e a segunda parte em colaboração com Nelcy E. Arévalo.

$\mathbb{F}_p$-MAXIMAL CURVES WITH MANY AUTOMORPHISMS ARE GALOIS-COVERED BY THE HERMITIAN CURVE

FERNANDO TORRES

Let $\mathbf{F}$ be the finite field with q^2 elements where $q = p^t$, p is a prime and $t \geq 1$ is an integer. A projective, non-singular, geometrically irreducible algebraic curve $\mathcal{X}$ defined over $\mathbf{F}$ of genus $g = g(\mathcal{X})$ is $\mathbf{F}$-*maximal* if its number $\#\mathcal{X}(\mathbf{F})$ of $\mathbf{F}$-rational points attains the Hasse-Weil bound $q+1+2g\cdot\sqrt{q}$. Apart from being interesting mathematical objects by their own, these curves are used as a building blocks to construct relevant structures in Coding Theory or Cryptography; see the book [3].

For an $\mathbf{F}$ maximal curve $\mathcal{X}$, $g(\mathcal{X}) \leq q(q-1)/2$ (Ihara's bound) [5, Prop. 5.3.3]; we have equality if and only if $\mathcal{X}$ is $\mathbf{F}$-isomorphic to the Hermitian curve $\mathcal{H}_{q+1} : y^{q+1} = x^q + x$ [4]. It is commonly attributed to J.P. Serre the fact that any curve $\mathbf{F}$-dominated by $\mathcal{H}$ is also $\mathbf{F}$-maximal. However the converse is not true as was pointed out by Giulietti and Korchmáros [2]. Their example is not $\mathbf{F}$-covered by $\mathcal{H}_{q+1}$ provided that $q = p^{2t} > 8$ and $t \equiv 0 \pmod 3$.

In this talk we show that an $\mathbf{F}$-maximal curve, where $q = p$, of genus $g \geq 2$ whose automorphism group is large, in the sense that $\#\mathrm{Aut}(\mathcal{X}) > 84(g-1)$, is Galois-covered by $\mathcal{H}_{p+1}$. We do observe that the hypothesis on the automorphisms cannot be dismissed since there exists an example $\mathcal{X}_0$ with $p = 71$, $g = 7$ and $\#\mathcal{X}(\mathcal{X}_0) = 81(7-1)$ which is not Galois-covered by $\mathcal{H}_{72}$. The curve $\mathcal{X}_0$ is in fact a reduction to positive characteristic of a well-known example in characteristic zero, namely the so called Fricke-Macbeath curve. Concerning $\mathcal{X}_0$ we have the following question:

- Is the curve $\mathcal{X}_0$ dominated by $\mathcal{H}_{72}$?

A positive answer to this question will give the first example of a maximal curve which is covered but not Galois-covered by the corresponding Hermitian curve; while, otherwise $\mathcal{X}_0$ would be the first known example of a $\mathbf{F}$-maximal curve which is not dominated by $\mathcal{H}_{q+1}$ with $q = p^{2t}$, $t \not\equiv 0 \pmod 3$. This would highlight the relevance of the construction of Giulietti and Korchmáros curve.

This talk is based on the preprint [1] with D. Bartoli and M. Montanucci.

References

[1] Bartoli, D., Montanucci, M., and Torres, F., $\mathbb{F}_{p^2}$-maximal curves with many automorphisms are Galois-covered by the Hermitian curve, (2018), preprint.

[2] Giulietti, M. and Korchmáros, G., *A new family of maximal curves over a finite field*, Math. Ann. **343** (2009), 229–245.
[3] Hurt, N.E., "Many Rational Points, coding theory and algebraic geometry", Kluwer Academic Publishers, 2003.
[4] Rück, H.G. and Stichtenoth, H., *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.
[5] Stichtenoth, H., "Algebraic Function Fields and Codes", second ed., Grad. Texts in Math., vol. 254, Springer-Verlag, 2009.

Institute of Mathematics, Statistics and Scientific Computing (IMECC), R. Sérgio Buarque de Holanda, 651, Cidade Universitária "Zeferino Vaz", 13083-859, University of Campinas (UNICAMP), Campinas, SP, Brazil

Email address: ftorres@ime.unicamp.br