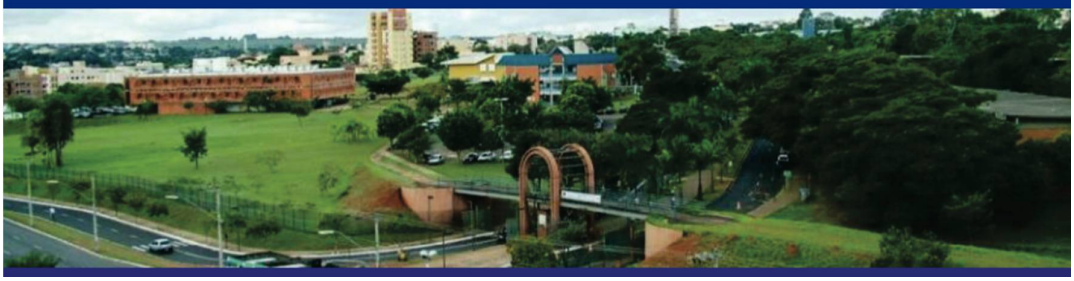
I Workshop em Corpos Finitos e Aplicações



Resumos dos pôsteres

Elliptic Function Fields

Abraham Rojas Vega [1]

[1] Instituto de Ciências Matemáticas e Computação. Universidade de São Paulo.

Elliptic function fields have many conections with different branch of mathematics, such as Complex Analysis and Number Theory. Also, their applications in Code Theory and Criptography are widespread. In this talk I would like to show some well-known properties of elliptic function fields and how they are derived from their algebraic structure.
First, I will present some basic facts about algebraic function fields and talk about their importance, which goes beyond the present topic. This facts are

- The Riemann-Roch Theorem
- Ramification of Places
- The Hurwitz Genus-Formula

Then I will explain how these theorems are applied in the elliptic case (most of the poster regards this part, so I won't take much time in that). Finally, I will say some words about the group law, and how it relates with the theory in [2].
Most of this talk is based on section 6.1 of [1]. In that book can also be found most of the theory regarding algebraic function fields that I will asume.

References

[1] H. Stichtenoth , *Algebraic Function Fields and Codes* , Springer. 2009

[2] Joseph H. Silverman , *The Arithmetic of Elliptic Curves* , Springer . 2009

Introdução aos Códigos Localmente Recuperáveis

B. Souza V. Neumann A. Paschoarelli

Universidade Federal de Uberlândia

Resumo

A Teoria dos Códigos Corretores de Erros é utilizada sempre que se deseja transmitir ou armazenar informações garantindo a sua confiabilidade.

Definição 1. *Seja $\mathbb{F}_q$ um corpo finito com q elementos tomado como alfabeto. Um Código $\mathcal{C} \subset \mathbb{F}_q^n$, com $n \in \mathbb{N}$, é dito Código Linear se for um subespaço vetorial de $\mathbb{F}_q^n$*

Em particular, estamos interessados em Códigos Localmente Recuperáveis (códigos *LRC*) cuja definição é a seguinte:

Definição 2. *Dizemos que um código $\mathcal{C} \subset \mathbb{F}_q^n$ é localmente recuperável com localidade r se, cada símbolo da palavra do código $x \in \mathcal{C}$ puder ser recuperado de um subconjunto de r outros símbolos de x, isto é, se cada símbolo na codificação for uma função de um pequeno número (no máximo r) outros símbolos.*

Em [1], Itzhak Tamo e Alexander Barg apresentam uma família de códigos *LRC* que atingem o valor máximo possível da distância para um dado parâmetro de localidade e cardinalidade do código. As palavras do código são obtidas como avaliações de polinômios construídos sobre um corpo finito. O procedimento de recuperação é feito via interpolação polinomial sobre r pontos.

Eles também construiram códigos com vários conjuntos de recuperação separados para cada símbolo, o que permite que um sistema realize vários processos de recuperação independentes e simultâneos de um símbolo, acessando diferentes partes da palavra do código.

O objetivo do nosso trabalho é construir tais códigos a partir de variedades algébricas específicas.

Referências

[1] I. Tamo. e A. Barg, "A family of optimal locally recoverable codes", *IEEE Trans. Inf. Theory,* vol. 60, no. 8, pp. 4661-4676,2014.

[2] I. Tamo, A. Barg, e S. Vladut, "Locally Recoverable Codes on Algebraic Curves", *IEEE Trans. Inf. Theory,* Vol. 63, no.8, pp. 4928-4939, 2017.

[3] A. Barg, K. Haymaker, E. Howe, G. Matthews, e A. Várilly-Alvarado, "Locally Recoverable Codes from Algebraic Curves and Surfaces", *Algebraic Geometry for Coding Theory and Cryptography. Association for Women in Mathematics Series, vol 9. Springer, Cham.* 2017.

[4] A. Hefez e M. Villela, "Códigos Corretores de Erros",*Série Computação e Matemática, IMPA*, Rio de Janeiro, 2008.

.

Cotas inferiores para a distância mínima de Códigos Algébricos Geométricos

Erik Antonio Rojas Mendoza

Universidade Federal do Rio de Janeiro

Os códigos corretores de erros são usados para controlar erros no processo de transmissão de dados. O número de erros que podem ser corrigidos está fortemente relacionado com o valor da distância mínima do código, pois quanto maior é o valor deste parâmetro, mais erros podem ser detectados e corrigidos. V. D. Goppa construiu, fazendo o uso de curvas algébricas sobre corpos finitos, uma família de códigos que são objeto de estudo até hoje, pois eles apresentam bons parâmetros. Estes códigos são chamados Códigos Algébricos Geométricos.

Em geral é complicado determinar o valor da distância mínima, mesmo usando ferramentas computacionais, é por isso que esses valores são estimados mediante cotas inferiores. Nosso objetivo é apresentar algumas das cotas inferiores para a distância mínima de Códigos de Algébricos Geométricos desenvolvidas nos últimos anos, entre elas as cotas d_{BPT} (Garcia e Lax, 1992), d_{LM} (Lundell e McCullough, 2006), d_{ABZ} (Duursma e Park, 2010), d_{ABZ^+} (Duursma, Kirov e Park, 2011), $d_{ABZ'}$ (Duursma e Park, 2010), d_{DK} (Duursma e Kirov, 2009) e d_{DP} (Duursma e Park, 2010). Mostraremos a relação existente entre estas cotas, determinando assim, sob certas condições, qual cota apresenta uma melhor estimativa para a distância mínima. Além disso nós veremos como o semigrupo de Weierstrass e o conjunto de *gaps* associado aos pontos racionais da curva correspondente, curva sobre a qual o código é construído, fornece informação para otimizar as cotas inferiores apresentadas.

Referências

[1] Iwan Duursma, Radoslav Kirov and Seungkook Park, *Distance bounds for algebraic geometric codes*. Journal of Pure and Applied Algebra 215.8 (2011): 1863-1878.

PARES PRIMITIVOS SOBRE CORPOS FINITOS

C. CARVALHO, J.P. GUARDIEIRO SOUSA, V. NEUMANN AND G. TIZZIOTTI
UNIVERSIDADE FEDERAL DE UBERLÂNDIA

No estudo de corpos finitos, alguns elementos desempenham um papel fundamental na determinação dessas estruturas. Entre eles, estão os elementos primitivos: os geradores do grupo multiplicativo associado ao corpo.[4] nos traz um estudo aprofundado sobre a obtenção de um elemento primitivo a partir de um quociente polinomial, e é nesse artigo que baseamos o trabalho.

Conseguimos generalizar o resultado, não apenas para quocientes de polinômios de um dado grau, mas para o conjunto de funções racionais dado por

$$\Upsilon_{p^k}(m_1, m_2) := \left\{ f = \frac{f_1}{f_2} \in \mathbb{F}_{p^k}^*(x) \mid \deg(f_1) \leq m_1,\ \deg(f_2) \leq m_2,\ \gcd(f_1, f_2) = 1 \text{ e } \Lambda_{p^k}(f_1, f_2) \neq \emptyset \right\}$$

onde $\Lambda_{p^k}(f_1, f_2) := \{(n, g) \in \mathbb{N} \times \mathbb{F}_q[x] \setminus \{x\}$; g é irredutível, $g^n \mid f_1 f_2,\ g^{n+1} \nmid f_1 f_2$ e $\gcd(n, q-1) = 1\}$.

Além de termos mais "liberdade" na escolha dos graus dos polinômios, também não nos restringimos à característica 2. Nós pudemos repetir os resultados (fazendo alterações adequadas em uma determinada cota) para corpos finitos de característica ímpar.

References

[1] www.sagemath.org, version 8.1, 2017.

[2] S. D. Cohen, *Pair of primitive elements in fields of even order*, Finite Fields Appl. v. 28, pp. 22–42, 2014.

[3] A.Gupta and R. K. Sharma,. *Existence of some special primitive normal elements over finite fields*. Finite Fields and Their Applications, v. 46, pp. 280–303, 2017.

[4] K. Sharma, A. Awasthi and A. Gupta, *Existence of pair of primitive elements over finite fields of characteristic 2*. Journal of Number Theory, v. 193, p. 386-394, 2018.

Funções de Distância Mínima e sua Aplicação sobre Códigos de tipo Reed-Muller

Matheus Manoel Dantas, Cícero Carvalho

Universidade Federal de Uberlândia

Inicialmente vamos definir e estudar as chamadas funções de distância mínima de um ideal graduado em $\mathbb{K}[x_1, \ldots, x_n]$ onde $\mathbb{K}$ é um corpo. Depois vamos mostrar que estas funções generalizam a ideia de distância mínima para códigos projetivos de tipo Reed-Muller sobre corpos finitos. Dessa maneira conseguimos uma formulação algébrica da distância mínima para um tipo especial de código em termos de invariantes algébricos e da estrutura do ideal dos polinômios que se anulam sobre o código. E por fim explicamos um método, utilizando bases de Gröbner e funções de Hilbert, para calcular limites inferiores para a distância mínima de alguns códigos do tipo Reed-Muller.

References

[1] José Martínez-Bernal, Yuriko Pitones, Rafael H. Villarreal, *Minimum distance functions of graded ideals and Reed-Muller-type codes*, Journal of Pure and Applied Algebra.

[2] D. Cox, J. Little, D. O'shea, *Ideals, Varieties and Algorithms*, Springer-Verlag, 1992.

[3] Brendan Hassett, *Introduction to Algebraic Geometry*, Cambridge University Press, 2007.