Gênero de Curvas Maximais sobre Corpos Finitos

Stéfani Concolato Vieira

Unicamp - IMECC

s163561@dac.unicamp.com.br

Conselho Nacional de Desenvolvimento Científico e Tecnológico

Resumo

Em Teoria de Códigos, Criptografia ou Geometria Finita é muito interessante o estudo de curvas com "muitos pontos". Fixado um corpo finito, o problema de determinar a possível existência de uma curva com essa propriedade sobre tal corpo está intrinsecamente relacionado com o invariante gênero. Neste caso, existem cotas para o gênero de uma curva com muitos pontos e consequentemente, em certos corpos finitos com cardinalidade pequena podemos explicitar todos os gêneros possíveis apesar que em outros, a resposta ainda está em aberto.

Introdução

Seja $\mathcal{X}$ uma curva (algébrica, não singular, algebricamente irredutível) sobre um corpo finito k de q^2 elementos de gênero g e $\mathcal{X}(k)$ o conjunto de pontos $k-$racionais de $\mathcal{X}$. Devido aos trabalhos dos matemáticos Hasse e Weil, existe uma cota para a quantidade de pontos $k-$racionais:

$$\mathcal{X}(k) \leq 1 + q^2 + 2gq.$$

Aquelas curvas que atingem a Cota de Hasse-Weil são ditas **maximais**. Dado q potência de um primo, um problema interessante no estudo de curvas é calcular o conjunto

$$M(q^2) := \{g_0 \in \mathbb{N}_0 : \text{existe uma curva } k-\text{maximal de gênero } g_0\},$$

chamado *Espectro dos Gêneros* sobre k.

Objetivos

Com o intuito de explicitar o Espectro dos gêneros, seria muito interessante apresentar cotas para o gênero de uma curva $k-$maximal.

1 *Cotas para o gênero de curvas maximais*

Teorema 1 (Ihara-1981):

$$M(q^2) \subseteq [0, \frac{q(q-1)}{2}] \tag{1}$$

Teorema 2 (Ruck-Stichtenoth-1994) Se $\mathcal{X}$ é uma curva $k-$maximal de gênero $g = \frac{q(q-1)}{2}$ então $\mathcal{X}$ é isomorfa a curva Hermitiana $\mathcal{H} : y^{q+1} = x^q + x$.

Teorema 3 (Furhmann-Torres-1995):

$$M(q^2) \subseteq [0, \frac{(q-1)^2}{4}] \cup \left\{\frac{q(q-1)}{2}\right\}. \tag{2}$$

Usando a Cota de Furhmann-Torres:

$$M(2^2) = \{0, 1\} \quad \text{e} \quad M(3^2) = \{0, 1, 3\},$$

Em 2000, Garcia, Xing e Stichtenoth mostraram

$$M(4^2) = \{0, 1, 2, 6\} \text{ e } M(5^2) = \{0, 1, 2, 3, 4, 10\}.$$

Teorema 4 (Castelnuovo): Seja $\mathcal{X}$ uma curva $k-$maximal de gênero g. Considere um sistema linear $\mathcal{D} = |(q+1)P_0| = g^r_{q+1}$, com $P_0 \in \mathcal{X}(\mathbb{F}_{q^2})$ de grau d e dimensão projetiva r. Assim

$$g \leq c_0(r) := \begin{cases} \dfrac{(2q-(r-1))^2}{8(r-1)}, & \text{se } r \text{ ímpar} \\ \dfrac{(2q-(r-1))^2-1}{8(r-1)}, & \text{se } r \text{ par} \end{cases} \tag{3}$$

2 *Aplicando a cota de Castelnuovo para determinar r*

Para $\mathcal{X}$ curva $k-$maximal de gênero g, usando $\mathcal{D} = |(q+1)P_0|$, com $P_0 \in \mathcal{X}(k)$ e $\phi : \mathcal{X} \longrightarrow \mathcal{X}$ o morfismo Frobenius relativo a k. Portanto

$$(q+1)P_0 \sim qP + \phi(P), \quad P \in \mathcal{X}.$$

Assim $r \geq 2$. Se $r = 2$ se, e somente se, $\mathcal{X}$ é isomorfa a curva hermitiana.

Teorema 5, [3]:

$$M(q^2) \subseteq [0, \frac{q^2-q+4}{6}] \cup \{\lfloor c_0(3) \rfloor\} \cup \{c_0(2)\} \tag{4}$$

Teorema 6, [3]: Se $\mathcal{X}$ é uma curva $k-$maximal de gênero g tal que $q \not\equiv 0 \ mod \ 3$ e $g > \frac{(q-1)(q-2)}{6}$ então $g \geq \frac{(q^2-2q+3)}{6}$.

Com tais resultados para a determinação de $M(7^2)$, faltava apenas o caso $g = 4$ o qual foi mostrado a não existência, por Kudo e Harashita em 2016.

$$M(7^2) = \{0, 1, 2, 3, 5, 7, 9, 21\}.$$

Conclusão

O problema de determinar $M(q^2)$ para $2 \leq q \leq 16$ já está resolvido para $q \leq 7$ e a tabela abaixo mostra alguns valores de g para os quais não se sabe ainda existência para certos q.

q	g
8	5
9	5, 7, 10, 11
11	8, 12, 14, 17
13	4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 21, 22
16	5, 7, 9, 10, 11, 13,..., 22, 23, 25, 26, 27, 29, 30, 31, 32, 33, 34, 35, 38, 39

Referências

[1] R. Fuhrmann and F. Torres. The genus of curves over finite fields with many rational points. *Manuscripta Math.*, (89):103–106, 1996.

[2] M. Kudo and S. Harashita. Superspecial curves of genus 4 in small characteristic. *arXiv: 1607.01114v1.*

[3] Saeed Tafazolian Nazar Arakelian and Fernando Torres. On the spectrum for the genera of maximal curves over small fields. *Adv. Math. Commun.*, (12):143 – 49, 2018.

[4] K.O. Stohr and J.F. Voloch. Weierstrass point and curves over finite fields. *Proc. London Math. Soc.*, (52):1–19, 1986.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001 e com o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ).