Permutando corpos finitos

Luciane Quoos

Universidade Federal do Rio de Janeiro

II Workshop de Mulheres na Matemática - UFRPE 2023

Conjunto de valores

Se p é um número primo $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ é um corpo finito com p elementos.

Dado $f(x) \in \mathbb{Z}_p[x]$ considero o conjunto de valores

$$V_f = \{f(\alpha) \mid a \in \mathbb{Z}_p\}.$$

Conjunto de valores

Se p é um número primo $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ é um corpo finito com p elementos.

Dado $f(x) \in \mathbb{Z}_p[x]$ considero o conjunto de valores

$$V_f = \{f(\alpha) \mid a \in \mathbb{Z}_p\}.$$

Exemplo

$f(x) = x^2 + x + 1 \in \mathbb{Z}_5[x] \Rightarrow$

Conjunto de valores

Se p é um número primo $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ é um corpo finito com p elementos.

Dado $f(x) \in \mathbb{Z}_p[x]$ considero o conjunto de valores

$$V_f = \{f(\alpha) \mid a \in \mathbb{Z}_p\}.$$

Exemplo

$f(x) = x^2 + x + 1 \in \mathbb{Z}_5[x] \Rightarrow$

$$f(0) = 1, f(1) = 3, f(2) = 7 = 2, f(3) = 13 = 3, f(4) = f(-1) = 1$$

Logo $V_{x^2+x+1} = \{1, 2, 3\}$.

Corpos finitos

Corpos finitos

Exemplo

Seja p primo e $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$

$$V_{x^{p-1}-1} = \{0, p-1\}$$

pelo Teorema de Fermat.

Se $\deg f = d \leq p - 1$, como um polinômio de grau d tem no máximo d raízes num corpo

$$\frac{p}{d} \leq \# V_f \leq p$$

Corpos finitos

Exemplo

Seja p primo e $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$

$$V_{x^{p-1}-1} = \{0, p-1\}$$

pelo Teorema de Fermat.

Se $\deg f = d \leq p-1$, como um polinômio de grau d tem no máximo d raízes num corpo

$$\frac{p}{d} \leq \#V_f \leq p$$

Em geral isso é feito sobre um corpo finito qualquer!

Corpos Finitos

- Seja K um corpo finito, então $\mathbb{Z}_P \subseteq K$ para algum primo p.

Corpos Finitos

- Seja K um corpo finito, então $\mathbb{Z}_P \subseteq K$ para algum primo p.
- Temos $K|\mathbb{Z}_p$ é uma extensão de corpos e podemos ver K como um Espaço Vetorial sobre $\mathbb{Z}_p$.

Corpos Finitos

- Seja K um corpo finito, então $\mathbb{Z}_P \subseteq K$ para algum primo p.
- Temos $K|\mathbb{Z}_p$ é uma extensão de corpos e podemos ver K como um Espaço Vetorial sobre $\mathbb{Z}_p$.
- Se $\alpha_1, \ldots \alpha_n$ é uma base de K como EV sobre $\mathbb{Z}_p$ temos

$$K = \mathbb{Z}_p\alpha_1 + \cdots + \mathbb{Z}_p\alpha_n$$

Corpos Finitos

- Seja K um corpo finito, então $\mathbb{Z}_P \subseteq K$ para algum primo p.
- Temos $K|\mathbb{Z}_p$ é uma extensão de corpos e podemos ver K como um Espaço Vetorial sobre $\mathbb{Z}_p$.
- Se $\alpha_1, \dots \alpha_n$ é uma base de K como EV sobre $\mathbb{Z}_p$ temos

$$K = \mathbb{Z}_p\alpha_1 + \cdots + \mathbb{Z}_p\alpha_n$$

- Logo $\#K = p^n$ e denotamos por $\mathbb{F}_q$ o corpo finito com q elementos.

Corpos Finitos

- Seja K um corpo finito, então $\mathbb{Z}_P \subseteq K$ para algum primo p.
- Temos $K|\mathbb{Z}_p$ é uma extensão de corpos e podemos ver K como um Espaço Vetorial sobre $\mathbb{Z}_p$.
- Se $\alpha_1, \ldots \alpha_n$ é uma base de K como EV sobre $\mathbb{Z}_p$ temos

$$K = \mathbb{Z}_p\alpha_1 + \cdots + \mathbb{Z}_p\alpha_n$$

- Logo $\#K = p^n$ e denotamos por $\mathbb{F}_q$ o corpo finito com q elementos.
- $\mathbb{F}_q = \{\alpha \in \overline{\mathbb{F}_q} \mid \alpha$ é uma raiz de $x^q - x = 0\}$ e $\mathbb{F}_q^*$ é um grupo cícilo com $q - 1$ elementos.

Polinômios de permutação

Se $f \in \mathbb{F}_q[x], \deg f = d \leq q-1$, então

$$\lceil \frac{q}{d} \rceil \leq \# V_f \leq q$$

Polinômios de permutação

Se $f \in \mathbb{F}_q[x], \deg f = d \leq q-1$, então

$$\lceil \frac{q}{d} \rceil \leq \#V_f \leq q$$

Fixado um corpo finito $\mathbb{F}_q$ quais os possíveis valores de $\#V_f, f \in \mathbb{F}_q[x]$?

Polinômios de permutação

Se $f \in \mathbb{F}_q[x], \deg f = d \leq q-1$, então

$$\lceil \frac{q}{d} \rceil \leq \# V_f \leq q$$

Fixado um corpo finito $\mathbb{F}_q$ quais os possíveis valores de $\# V_f, f \in \mathbb{F}_q[x]$?

$\bullet \mathbb{F}_q = \{a \in \overline{\mathbb{F}_q} \mid a^q - a = 0\} \Rightarrow \# V_{x^{q-1}-1} = 2$

Polinômios de permutação

Se $f \in \mathbb{F}_q[x], \deg f = d \leq q - 1$, então

$$\lceil \frac{q}{d} \rceil \leq \# V_f \leq q$$

Fixado um corpo finito $\mathbb{F}_q$ quais os possíveis valores de $\# V_f, f \in \mathbb{F}_q[x]$?

•$\mathbb{F}_q = \{a \in \overline{\mathbb{F}_q} \mid a^q - a = 0\} \Rightarrow \# V_{x^{q-1}-1} = 2$

•$\mathbb{F}_q^*$ é um grupo cíclico de ordem $q - 1 \Rightarrow \# V_{x^{q-2}} = q$

Polinômios de permutação

Se $f \in \mathbb{F}_q[x], \deg f = d \leq q-1$, então

$$\lceil \frac{q}{d} \rceil \leq \# V_f \leq q$$

Fixado um corpo finito $\mathbb{F}_q$ quais os possíveis valores de $\# V_f, f \in \mathbb{F}_q[x]$?

$\bullet \mathbb{F}_q = \{a \in \overline{\mathbb{F}_q} \mid a^q - a = 0\} \Rightarrow \# V_{x^{q-1}-1} = 2$

$\bullet \mathbb{F}_q^*$ é um grupo cíclico de ordem $q-1 \Rightarrow \# V_{x^{q-2}} = q$

Se $\# V_f = q$ dizemos que f é um polinômio de permutação - PP.

Polinômio de Permutação

É fácil de ver que x^d é um PP sobre $\mathbb{F}_q$ se e somente se $mdc(q-1, d) = 1$.

Polinômio de Permutação

É fácil de ver que x^d é um PP sobre $\mathbb{F}_q$ se e somente se $mdc(q-1, d) = 1$.

Sabemos caracterizar binômios, trinômios... polinômios com poucos termos?

Polinômio de Permutação

É fácil de ver que x^d é um PP sobre $\mathbb{F}_q$ se e somente se $mdc(q-1, d) = 1$.

Sabemos caracterizar binômios, trinômios... polinômios com poucos termos?

Critério de Hermite

Theorem

Um polinômio $f \in \mathbb{F}_q[x]$ é um PP se, e somente se,

i) $f(x)^{q-1} \pmod{x^q - x}$ *tem grau* $q-1$.

ii) *Para todo* $1 \leq t \leq q-2$ *tal que* $p \nmid t$, *tem-se* $f(x)^t \pmod{x^q - x}$ *tem grau* $\leq q-2$.

Critério de Polinômios de Permutação

Em 1896 - 1897, Dickson classificou todos os PP de grau ≤ 5 sobre $\mathbb{F}_q$ e grau 6 em característica ímpar. (Tese de doutorado)

Critério de Polinômios de Permutação

Em 1896 - 1897, Dickson classificou todos os PP de grau ≤ 5 sobre $\mathbb{F}_q$ e grau 6 em característica ímpar. (Tese de doutorado)

Em 2010, Li-Chandler-Xiang classificaram PP de grau 6 e 7 sobre $\mathbb{F}_{2^n}$.

Critério de Polinômios de Permutação

Em 1896 - 1897, Dickson classificou todos os PP de grau ≤ 5 sobre $\mathbb{F}_q$ e grau 6 em característica ímpar. (Tese de doutorado)

Em 2010, Li-Chandler-Xiang classificaram PP de grau 6 e 7 sobre $\mathbb{F}_{2^n}$.

Em 2019 Fan classificou PP de grau 7 sobre $\mathbb{F}_q, q$ ímpar.

Critérios Polinômio de Permutação

Seja $f(x) \in \mathbb{F}_q[x], \deg f = d \geq 1$. Considere $\Phi(x, y) \in \mathbb{F}_q[x, y]$ por

$$\Phi(x, y) = \frac{f(x) - f(y)}{x - y},$$

que possui grau $d - 1$.

Critérios Polinômio de Permutação

Seja $f(x) \in \mathbb{F}_q[x], \mathrm{deg} f = d \geq 1$. Considere $\Phi(x, y) \in \mathbb{F}_q[x, y]$ por

$$\Phi(x, y) = \frac{f(x) - f(y)}{x - y},$$

que possui grau $d - 1$.

Pela definição de Φ, temos que

$$f \text{ é um PP } \Leftrightarrow \Phi(x, y) \neq 0 \text{ para } x \neq y$$

ou, equivalentemente,

$$\Phi(x, y) = 0 \text{ não possui solução } (x, y) \in \mathbb{F}_q^2 \text{ fora da reta x=y}$$

Critérios Polinômio de Permutação

Seja $f(x) \in \mathbb{F}_q[x], \mathrm{deg} f = d \geq 1$. Considere $\Phi(x, y) \in \mathbb{F}_q[x, y]$ por

$$\Phi(x, y) = \frac{f(x) - f(y)}{x - y},$$

que possui grau $d - 1$.

Pela definição de Φ, temos que

$$f \text{ é um PP } \Leftrightarrow \Phi(x, y) \neq 0 \text{ para } x \neq y$$

ou, equivalentemente,

$$\Phi(x, y) = 0 \text{ não possui solução } (x, y) \in \mathbb{F}_q^2 \text{ fora da reta x=y}$$

Se $\Phi(x, y)$ tem "muitos pontos racionais" então f não é um PP.

Aplicações

Teorema devido a Hou

Theorem

Sejam q ímpar, $a, e \in \mathbb{Z}$ *tais que* $2 < a \leq e/4 + 1$. *Então*

$$F_{a,q}(x) = x^{q-2} + x^{q^2-2} + \ldots + x^{q^{a-1}-2}$$

não é um polinômio de permutação de $\mathbb{F}_{q^e}$.

Aplicações

Teorema devido a Hou

Theorem

Sejam q ímpar, $a, e \in \mathbb{Z}$ tais que $2 < a \leq e/4 + 1$. Então

$$F_{a,q}(x) = x^{q-2} + x^{q^2-2} + \dots + x^{q^{a-1}-2}$$

não é um polinômio de permutação de $\mathbb{F}_{q^e}$.

Teorema devido a Nurdagul Meidl - 2019

Theorem

Seja $n \geq 2$ e $\gamma \in \mathbb{F}_{q^n}$. Se $gcd(k, q^n - 1) > 1$, então $x^k - \gamma Tr(x)$ não é um polinômio de permutação de $\mathbb{F}_{q^n}$.

Conjectura proposta por Gary Mullen e provada em 1993 por D. Q. Wan que fornece outro critério para decidir se um polinômio é de permutação.

Theorem

Sejam $f(x) \in \mathbb{F}_q[x]$ um polinômio de grau d e $V_f = \{f(a) \mid a \in \mathbb{F}_q\}$. Se

$$\#V_f > q - \frac{q-1}{d},$$

então f é um polinômio de permutação.

Polinômios de permutação

Note que $f \in \mathbb{F}_q[x]$ é um PP se e somente se $f + a$ é um PP para todo $a \in \mathbb{F}_q$. Posso supor $f(0) = 0$

$$f = a_r x^r + a_{r+1} x^{r+1} + \cdots + a_{r+s} x^{r+s} = x^r g(x^s)$$

onde $g \in \mathbb{F}_q[x]$.

Critério AGW

Critério de Akbary, Ghioca and Wang

Lema (AGW-criterion)

Escreva $q-1=ds$ *para inteiros positivos* d *e* s, *e* $r \geq 1$. *Então*

$$f(X)=X^r g(X^s), g(X) \in \mathbb{F}_q[X]$$

é um PP de $\mathbb{F}_q$ *se e somente se*

1. $mdc(r,s)=1$, *e*
2. $X^r g(X)^s$ *permuta o conjunto* $\mu_d=\{\xi \in \mathbb{F}_q \mid \xi^d=1\}$ *das* d*-ésimas raízes da unidade em* $\mathbb{F}_q$

In 2018, a class of permutation quadrinomials of the form

$$f(X) = X^3(X^{3(q-1)} + aX^{2(q-1)} + bX^{q-1} + c)$$

over $\mathbb{F}_{q^2}$ was investigated by Tu, Zeng and Helleseth, where $q = 2^m$ for an odd integer m.

In 2018, a class of permutation quadrinomials of the form

$$f(X) = X^3(X^{3(q-1)} + aX^{2(q-1)} + bX^{q-1} + c)$$

over $\mathbb{F}_{q^2}$ was investigated by Tu, Zeng and Helleseth, where $q = 2^m$ for an odd integer m.

An incomplete characterization of the coefficients $a, b, c \in \mathbb{F}_{2^{2m}}$ was obtained to ensure that the polynomial was a PP over $\mathbb{F}_{2^{2m}}$.

Zheng, Liu, Kan, Peng and Tang investigated the permutation property of the quadrinomial

$$f(X) = X + ax^{s_1(q-1)+1} + bX^{s_2(q-1)+1} + cX^{s_3(q-1)+1} \in \mathbb{F}_{q^2}[x],$$

where $q = 2^m$. The authors found sufficient conditions for the triplets (s_1, s_2, s_3) in the set

$$\{(\frac{-1}{2^k-1}, 1, \frac{2^k}{2^k-1}), (\frac{1}{2^k+1}, 1, \frac{2^k}{2^k+1}), (\frac{1}{4}, 1, \frac{3}{4})\}$$

such that $f(X)$ is a permutation polynomial over $\mathbb{F}_{q^2}$.

In 2016, Gupta and Sharma provided four new classes of permutation trinomials over $\mathbb{F}_{2^{2m}}$ from small degree polynomials with all coefficients equal to one and without any roots in μ_{q+1}.

In 2016, Gupta and Sharma provided four new classes of permutation trinomials over $\mathbb{F}_{2^{2m}}$ from small degree polynomials with all coefficients equal to one and without any roots in μ_{q+1}.

This results inspired the next work...

Trabalho em conjunto com Rohit Gupta e Fábio Brochero

Um polinômio $f(x) = \sum_{i=0}^{d} a_i X^i$ in $\mathbb{F}_q[X]$ de grau d é dito um *self reciprocal* polinômio se $f(X) = X^d f(1/X)$, isto é $a_{d-i} = a_i$.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_2 x^{d-2} + a_1 x^{d-1} + a_0 x^d$$

Trabalho em conjunto com Rohit Gupta e Fábio Brochero

Um polinômio $f(x) = \sum_{i=0}^{d} a_i X^i$ in $\mathbb{F}_q[X]$ de grau d é dito um *self reciprocal* polinômio se $f(X) = X^d f(1/X)$, isto é $a_{d-i} = a_i$.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_2 x^{d-2} + a_1 x^{d-1} + a_0 x^d$$

Lemma

Let q be even and let $h(X) \in \mathbb{F}_q[X]$ be a self reciprocal polynomial of degree d and u be an integer satisfying $(d - 2u, q + 1) = 1$.

Trabalho em conjunto com Rohit Gupta e Fábio Brochero

Um polinômio $f(x) = \sum_{i=0}^{d} a_i X^i$ in $\mathbb{F}_q[X]$ de grau d é dito um *self reciprocal* polinômio se $f(X) = X^d f(1/X)$, isto é $a_{d-i} = a_i$.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_2 x^{d-2} + a_1 x^{d-1} + a_0 x^d$$

Lemma

Let q be even and let $h(X) \in \mathbb{F}_q[X]$ be a self reciprocal polynomial of degree d and u be an integer satisfying $(d-2u, q+1) = 1$. For $\alpha \in \mathbb{F}_q^*$ with $\alpha \neq h(1)$, the polynomial $g(X) = h(X) + \alpha X^u$ has no roots in μ_{q+1}.

Let q be even and $h(X) = bX^2 + aX + b$ a self reciprocal polynomial. For $\alpha = 1$ and $u = 3$, we conclude that the polynomial

$$g(X) = X^3 + bX^2 + aX + b$$

has no roots in μ_{q+1}

We classify the family of permutation quadrinomials over $\mathbb{F}_{q^2}$

$$f(X) = X^2 g(X^{q-1}) = X^{3q-1} + bX^{2q} + aX^{q+1} + bX^2$$

Let q be even and $h(X) = bX^2 + aX + b$ a self reciprocal polynomial. For $\alpha = 1$ and $u = 3$, we conclude that the polynomial

$$g(X) = X^3 + bX^2 + aX + b$$

has no roots in μ_{q+1}

We classify the family of permutation quadrinomials over $\mathbb{F}_{q^2}$

$$f(X) = X^2 g(X^{q-1}) = X^{3q-1} + bX^{2q} + aX^{q+1} + bX^2$$

In a similar way we obtain and classify the family

$$f(X) = X^{4q-1} + aX^{2q+1} + bX^{q+2} + X^3$$

over $\mathbb{F}_{2^{2m}}$ with $a, b \in \mathbb{F}_{2^m}^*$

Theorem

Let q be even. Then for $a, b \in \mathbb{F}_q^*$, the polynomial

$$f(X) = X^2 g(X^{q-1}) = X^{3q-1} + bX^{2q} + aX^{q+1} + bX^2$$

is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $a \neq 1$ and the cubic $c(X) = bX^3 + aX^2 + bX + 1$ has no roots in $\mathbb{F}_{q^2}$.

Theorem

Let q be even. Then for $a, b \in \mathbb{F}_q^*$, the polynomial

$$f(X) = X^2 g(X^{q-1}) = X^{3q-1} + bX^{2q} + aX^{q+1} + bX^2$$

is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $a \neq 1$ and the cubic $c(X) = bX^3 + aX^2 + bX + 1$ has no roots in $\mathbb{F}_{q^2}$.

We investigate the curve $\frac{f(X)-f(Y)}{X-Y}$ that is, for $z := xy + 1$

$$\frac{bx^2y^2z + (x+y)^3 + az^2(x+y) + bz(x+y)^2 + bz}{xy} = 0$$

And show that if the curve has a solution $x \neq y$, then the cubic $C(X)$ has no roots in $\mathbb{F}_{q^2}$

Theorem

Let q be even. Then for $a, b \in \mathbb{F}_q^*$, the polynomial

$$f(X) = X^2 g(X^{q-1}) = X^{3q-1} + bX^{2q} + aX^{q+1} + bX^2$$

is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $a \neq 1$ and the cubic $c(X) = bX^3 + aX^2 + bX + 1$ has no roots in $\mathbb{F}_{q^2}$.

We investigate the curve $\frac{f(X)-f(Y)}{X-Y}$ that is, for $z := xy + 1$

$$\frac{bx^2y^2z + (x+y)^3 + az^2(x+y) + bz(x+y)^2 + bz}{xy} = 0$$

And show that if the curve has a solution $x \neq y$, then the cubic $C(X)$ has no roots in $\mathbb{F}_{q^2}$

Conversely, if the cubic $C(X)$ has a root in $\mathbb{F}_{q^2}$ we prove that $g(X) = X^3 + bX^2 + aX + b$ has a roots in μ_{q+1}

Theorem

Let $q = 2^m$. *Then for* $a, b \in \mathbb{F}_q^*$, *the polynomial*

$$f(X) = X^{4q-1} + aX^{2q+1} + bX^{q+2} + X^3$$

is a permutation polynomial over $\mathbb{F}_{q^2}$ *if and only if*

a) $a \neq b$,

b) m *is odd,*

c) $Tr_1^m\left(\frac{1}{a+b}\right) = 0$, *and*

d) *the polynomial*

$$C_u(X): \ (a+b+(a^2+b^2)u^2)(X^4+X^2)+b(X^3+X)+(a+b)^2u^4+1 \quad (1)$$

has no roots in $\mathbb{F}_q$ *for any* $u \in \mathbb{F}_q$ *with* $Tr_1^m(u) = 1$.

Theorem

Let $q = 2^m$ and $a, b \in \mathbb{F}_q^*$ be such that $a^2 + b^2 + b = 0$. Then

$$f(X) = X^{4q-1} + aX^{2q+1} + bX^{q+2} + X^3$$

is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if m is odd and $Tr_1^m(\frac{1}{b}) = 0$.

Obrigada a todes e bom fim de semana!