Curvas planas e arcos

Beatriz Casulari da Motta Ribeiro

UNIVERSIDADE
FEDERAL DE JUIZ DE FORA

O plano projetivo

Se $q = p^n$, sabemos que o plano $PG(2, q)$ possui:

1. $q^2 + q + 1$ pontos;
2. $q^2 + q + 1$ retas;
3. $q + 1$ pontos em cada reta;
4. $q + 1$ retas passando por cada ponto.

Arcos planos

Definição

Um conjunto $\mathcal{K}$ de n pontos em $PG(2,q)$ é um $(n,d)-$arco plano se

- Qualquer reta de PG(2,q) passa por, no máximo, d pontos de K.
- Existe pelo menos uma reta passando por exatamente d pontos de K.

Arcos planos

Há uma série de perguntas interessantes que surgem dessa definição, como, por exemplo:

1. Fixados q e d para quais n_i existe algum $(n_i, d)-$arco sobre $\mathbb{F}_q$?
2. De tais n_i qual é o maior?
3. Existem dois (n_i, r)-arcos não *isomorfos* com $n_i = n_j$?

Cota

Proposição

O número de pontos n de um $(n, d)-$arco satisfaz:

$$n \leq (d-1)q + d \ .$$

- De fato, seja $P \in \mathcal{K}$.
- Cada linha que contém P contém, no máximo, outros $d-1$ pontos de $\mathcal{K} \setminus \{P\}$.
- Como passam $q+1$ linhas por P, obtemos a cota.

Arcos planos completos

Seja $\mathcal{K}$ um $(n, d)-$arco plano em $PG(2, q)$.

Definição

Dizemos que $\mathcal{K}$ é um $(n, d)-$arco *completo* se não está contido em um $(n+1, d)-$arco plano.

Isto é, adicionando um ponto a $\mathcal{K}$, passamos a ter $d+1$ pontos colineares.

Arcos $\times$ Códigos

Teorema

Um $(n, d)-$arco $\mathcal{K}$ é equivalente a um $[k, 3, k - d']_q$-código $\mathcal{C}$, onde $d' \leq d$.

Mais ainda:

Se o $(n, d)-$arco for completo, então a distância mínima de $\mathcal{C}$ é exatamente $k - d$ e o código não pode ser estendido a outro com distância mínima maior.

Ainda sobre arcos e códigos

Cota de Griesmer para $[n, k, r]_q-$códigos

$$n \geq \sum_{i=0}^{k=1} \lceil \frac{r}{q^i} \rceil$$

Teorema

Se $\mathcal{K}$ é um (n, d)-arco em $PG(2, q)$ tal que $n > (d-2)q + d$, então o $[n, 3, n-d]_q-$código correspondente atinge a cota de Griesmer.

Uma fonte de exemplos

Teorema de Bezout

Sejam F, G curvas planas projetivas sem componentes em comum, então o número de pontos na interseção de F e G é, no máximo, igual ao produto dos graus de F e G.

Um exemplo natural de $(n, d')-$arco é o conjunto de n pontos racionais de uma curva plana de grau d, onde $d' \leq d$.

Nem sempre o arco é completo! No caso em que é e $d' = d$, então dizemos que $\mathcal{X}$ tem a propriedade do arco.

Os primeiros a questionarem se uma curva tem ou não a propriedade do arco foram Hirschfeld e Voloch, no fim da década de 1980.

Exemplo 1

- Cônicas irredutíveis em característica ímpar.
- Hermitiana: $y^{q+1} = x^q + x$ sobre $\mathbb{F}_{q^2}$.
- Quártica de Klein: $x^3y + y^3 + x = 0$ sobre $\mathbb{F}_8$.

Exemplo 2

No artigo *On complete arcs arising from plane curves*, Giulietti, Torres, Pambianco e Ughi:

$$\mathcal{F}: \ y^{p^2+p+1} = -(ax^{p^2+p+1} + 1)/b$$

$$\mathcal{G}: \ y^{p^2+p+1} = x^{p^2+p+1} + x^{p^2} + x^p + x$$

Note que tanto $\mathcal{F}$ quanto $\mathcal{G}$ tem

- grau $d = p^2 + p + 1$.
- d pontos na reta $z = 0$.

Obs

- Casos especiais da família $\mathcal{Z}$: $N(y) = aN(x) + bTr(x) + c$ sobre $\mathbb{F}_{q^\ell}$ com $a, b, c \in \mathbb{F}_q$.
- Se $b = 0$, então não há pontos singulares.
- Se $b \neq 0$, os pontos singulares são $(1 : 0 : z)$ tais que $N(z) = -a/b$ e $Tr(z) = ca/b^2$.
- Se $a = 0$, ok.
- Se $a \neq 0$, a quantidade $N_\ell(-a/b, ca/b^2)$ de elementos de $\mathbb{F}_{q^\ell}$ com tal propriedade é limitada por Moisio-Wan como

$$\left| N_\ell(-a/b, ca/b^2) - \frac{q^{\ell-1} - 1}{q - 1} \right| \leq (\ell - 1)q^{\frac{\ell-2}{2}} .$$

- Com o crescimento do número de pontos singulares, torna-se cada vez mais difícil estudar a propriedade do arco de $\mathcal{Z}$.

não-Exemplo 3

- Por exemplo: $a = 0$ e $b \neq 0$, consideremos

$$y^{q^{\ell-1}+\cdots+q+1} = b(x^{q^{\ell-1}} + \cdots + x^q + x) + c$$

- Único ponto singular $(1 : 0 : 0)$.
- Dado $P = (\alpha : 1 : 0)$, tomemos as retas $x = \alpha y + \gamma$ com $\gamma \in \mathbb{F}_{q^\ell}$.
- Temos que o polinômio $N(y) = bTr(\alpha y) + bTr(\gamma) + c$ tem menos de $q^{\ell-1} + \cdots + q + 1$ raízes se $\alpha \in \mathbb{F}_q$ (Moisio-Wan).
- Ainda a reta $z = 0$ intercepta $\mathcal{Z}$ em apenas um ponto, segue que a curva não pode ter a propriedade do arco.

Exemplo 4

No mesmo artigo, são apresentadas as seguintes curvas sobre $\mathbb{F}_q$, cujas componentes irredutíveis são Hermitianas.

$$\mathcal{X}_B : \prod_{\lambda \in B} (\lambda x^{\sqrt{q}+1} + xy^{\sqrt{q}} + x^{\sqrt{q}} y + z^{\sqrt{q}+1} = 0$$

$$\mathcal{Y}_B : \prod_{\lambda \in B} (\lambda x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1}) = 0$$

onde q é um quadrado e $B \subset \mathbb{F}^*_{\sqrt{q}}$.

- $\mathcal{X}_B$ tem a propriedade do arco se $1 \leq \#B \leq \sqrt{q} - 1$
- $\mathcal{Y}_B$ tem a propriedade do arco se $1 \leq \#B \leq \sqrt{q} - 2$.

Exemplo 5

Em *On complete $(N, d)-$arcs derived from plane curves*, Borges apresenta mais alguns exemplos de curvas com a propriedade do arco.

Teorema

Sejam $p > 2$ e $k < (q-1)/2$ um divisor de $q-1$ tal que $p \nmid (k+1)$. Seja $m = \dfrac{q-1-2k}{k}$, então a curva $\sum_{r+s+t=m} (x^r y^s z^t)^k = 0$ tem a propriedade do arco se e somente se $k = 1, 2, 4, 6, (p^r - 1/2)$ ou $2(p^r - 1)$.

Teorema

Sejam $p > 3$ e q potência de p tal que $3|(q+1)$. Então, a curva de Fermat

$$x^{q-1} + y^{q-1} + z^{q-1} = 0$$

sobre $\mathbb{F}_{q^2}$ tem a propriedade do arco.

(não) Exemplo 6

Sejam $3 \leq n \in \mathbb{N}$ e $\alpha \in \mathbb{F}_2$.
Consideremos a seguinte família sobre $\mathbb{F}_{2^n}$:

$$\mathcal{X}_0 : \ y^{2^n-1} = \frac{x^{2^n} + x}{x^2 + x}$$

- Temos que $\mathcal{X}_0$ tem grau $d = 2^n - 1$, é não-singular e tem $3d$ pontos racionais.
- Suponhamos que tal curva tenha a propriedade do arco.

(não) Exemplo 6

- Seja $P_1 \notin \mathcal{X}_0(\mathbb{F}_{2^n})$. Existe uma reta L_1, tal que $\#(\mathcal{X}_0 \cap L_1) = d$.
- Seja $P_2 \notin (\mathcal{X}_0(\mathbb{F}_{2^n}) \cup \{P_1\})$. Existe uma reta L_2 tal que $\#(L_2 \cap \mathcal{X}_0) = d$.
- Temos que $L_1 \cap L_2 = \emptyset$ ou $L_1 \cap L_2 = \{\text{um único ponto racional de } \mathcal{X}_0\}$.
- Isto significa que até aqui já contamos $2d$ ou $2d - 1$ pontos racionais de $\mathcal{X}_0$ distintos.

(não) Exemplo 6

- Escolhemos agora $P_3 \notin (\mathcal{X}_0(\mathbb{F}_{2^n}) \cup \{P_1, P_2\})$.
- Existe uma reta L_3 tal que $\#(L_3 \cap \mathcal{X}_0) = d$ e tal reta pode interceptar nenhuma, uma ou duas das retas anteriores.
- Se há interseção, deve ser em um único ponto racional de $\mathcal{X}_0$ em cada reta.
- Depois desse passo, contamos pelo menos $3d - 3$ pontos racionais distintos em $\mathcal{X}_0$.
- Repetindo isso para um quarto ponto P_4, teríamos pelo menos $4d - 6$ pontos, que já é mais dos que os $3d$ pontos racionais de $\mathcal{X}_0$. Portanto, $\mathcal{X}_0$ não pode ter a propriedade do arco.

Exemplo 7

Sejam $p \geq 3$ e $\ell \geq 3$ ímpar e $r = (\ell + 1)/2$. Seja $Tr : \mathbb{F}_{q^\ell} \to \mathbb{F}_q$ a aplicação traço. Considere em $PG(2, q^\ell)$ a curva

$$\mathcal{H} : \ Tr(y) = Tr(x^{q^r+1}) \pmod{x^{q^\ell} - x}$$

Tal curva tem as seguintes propriedades:

- grau $q^{\ell-1} + q^{r-1}$.
- gênero $q^r(q^{\ell-1} - 1)/2$.
- $q^{2\ell-1} + 1$ pontos racionais.
- apenas um ponto no infinito $(0 : 1 : 0)$.
- apenas um ponto singular $(0 : 1 : 0)$.

A curva $\mathcal{H} : \ Tr(y) = Tr(x^{q^r+1}) \pmod{x^{q^\ell} - x}$ tem a propriedade do arco.

Uma ideia da demonstração

Para uma reta $L: \ y = bx + c$ definimos

$$M_{r,n}(b,c) := \#L \cap \mathcal{H}(\mathbb{F}_{q^\ell})$$

Então, $M_{r,n}(b,c)$ é o número de $\mathbb{F}_{q^\ell}$-raízes da equação

$$tr(bx + c) = tr(x^{q^r+1}) \pmod{x^{q^\ell} - x}$$

isto é, o número de $\mathbb{F}_{q^\ell}$-raízes de

$$tr(x^{q^r+1} - bx - c) \pmod{x^{q^\ell} - x} = 0\,,$$

e, portanto, o mesmo número de $\mathbb{F}_{q^\ell}$-raízes de

$$tr(x^{q^r+1} - bx - c) = 0\,,$$

Uma ideia da demonstração

Portanto o número de pontos $M_{r,n}(b,c)$ na interseção de L e $\mathcal{H}$ pode ser calculado usando a relação

$$N_{r,n}(1,-b,-c) = qM_{r,n}(b,c)\,, \tag{1}$$

onde $N_{r,n}(1,-b,-c)$ é o número de $\mathbb{F}_{q^\ell}$-pontos afins da curva de Artin-Schreier

$$y^q - y = x^{q^r+1} - (bx+c)\,. \tag{2}$$

Portanto, o problema de estudar o arco associado a $\mathcal{H}$ é reduzido ao problema de contar os $\mathbb{F}_{q^\ell}$-pontos afins da curva (2).

Ideia

Vamos provar, por fim, que por cada ponto $P \in PG(2, q^\ell) \setminus \mathcal{H}(\mathbb{F}_{q^\ell})$ passa uma reta racional que intercepta $\mathcal{H}$ em $d = q^{\ell-1} + q^{r-1}$ (grau de $\mathcal{H}$) pontos racionais.

- Suponha $p \equiv 1 \pmod 4$ (outro caso é análogo).
- Seja $(a : b : 1) \in PG(2, q^\ell) \setminus \mathcal{H}(\mathbb{F}_{q^\ell})$.
- Prova-se que $y = m(x - a) + b$ intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em d pontos se e somente se existe pelo menos um ponto afim na curva de Artin-Schreier

$$y^q - y = x_0^{q^r+1} - a(x_0^{q^r} + x_0^{q^{r-1}}) + b - \lambda'$$

  para certos x_0, λ' fixos, que dependem de m, a, b.
- Mas tal curva tem pelo menos $q^\ell - q^{\ell/2}$ pontos afins (Borges, Motta e Torres)
- Logo, existe reta $y = m(x - a) + b$ que intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ in $q^{\ell-1} + q^{r-1}$ $\mathbb{F}_{q^\ell}$-pontos racionais.

Ideia

- Seja agora $P = (1 : b : 0)$ com $b \in \mathbb{F}_{q^\ell}$.
- As retas por P são do tipo $L: \ y = bx + \gamma$ com $\gamma \in \mathbb{F}_{q^\ell}$.
- L intercepta $\mathcal{H}(\mathbb{F}_{q^\ell})$ em $N = q^{\ell-1} + q^{r-1}$ pontos se e somente se $tr(x_0^{q^r+1} + \gamma)$ é um quadrado não-nulo em $\mathbb{F}_q$ (para certo x_0 fixo).
- Sejam $\lambda \in \mathbb{F}_q$ um quadrado não-nulo e $\lambda' \in \mathbb{F}_{q^\ell}$ tais que $tr(\lambda') = \lambda$.
- Escolhemos $\gamma := \lambda' - x_0^{q^r+1}$.
- Então:

$$tr(x_0^{q^r+1} + \gamma) = tr(x_0^{q^r+1} + \lambda' - x_0^{q^r+1}) = tr(\lambda') = \lambda$$

- Isso conclui a prova de que $\mathcal{H}(\mathbb{F}_{q^\ell})$ tem a propriedade do arco.

Obrigada!