XXXI Congresso de Iniciação Científica Unicamp 2023

INVARIANTES SEPARADORES SOBRE CORPOS FINITOS

Palavras-Chave: Invariantes Separadores, Corpos Finitos, Grupo Simétrico.

Aluno: Pedro Antonio Muniz Martins - Universidade Estadual de Campinas
Professor orientador: Artem Lopatin - Universidade Estadual de Campinas

1. Síntese e Objetivos

O projeto teve como objetivo o estudo de invariantes separadores sobre corpos finitos, primeiramente foi estudado o grupo simétrico, nosso objetivo era encontrar um conjunto separador mínimo $S \subset \mathbb{F}_q[V^m]^{S_n}$, para $m = 1$. Entretanto, conseguimos recuperar um conjunto separador mínimo publicado por Oliver Aberth [2], em 1964. Com esse conjunto podemos conseguir alguns resultados sobre um separador mínimo com a menor quantidade de elementos possível.

2. Resumo das Atividades

2.1. **Algumas Definições.** Para contextualizar o que foi estudado é nescessário algumas definições. Consideramos um espaço vetorial V , $\dim(V) = n$, com ação linear de um subgrupo $G < GL(V)$.

Definition 2.1. O anel de coordenadas é o anel de polinômios seguinte:

$$\mathbb{F}[V] = \mathbb{F}[\, x_i \,|\, 1 \leq i \leq n],$$

Onde pode interpretar x_i como uma função $V \to \mathbb{F}$, que envia um vetor v para i-ésima coordenada v_i de v

Seja o anel de coordenadas $\mathbb{F}[V] = \mathbb{F}[x_1, \dots, x_n]$ de V isomorfo a álgebra simetrica $S(V^*)$ sobre o espaço dual V^*, com $x_1, \dots, x_n$ uma base de V^*. Em que G age sobre $\mathbb{F}[V]$ da forma: $(g \cdot f)(v) = f(g^{-1} \cdot v)$ para todo $f \in V^*$ e $v \in V$.

Definition 2.2. A álgebra de invariantes

$$\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \,|\, g \cdot f = f \text{ para todos } v \in V, g \in G\}$$

Trata-se de um objeto clássico da matemática, ela remonta a segunda metade do século XIX, estando associada a nomes como Buhl, Cayley, Sylvester, Hermite, Jacobi, Clebsch, Gordan.

Inicialmente, o desafio foi encontrar um conjunto gerador para esta álgebra. Atualmente, já conhecemos estes conjuntos e dentre os problemas modernos na teoria de invariantes, temos alguns associados a separadores.

Invariantes separadores foram introduzidos por Derksen e Kemper em 2002 como uma simplificação da noção de geradores de invariantes.

Definition 2.3. Seja $u, v \in V$, dizemos que $f \in \mathbb{F}[V]$ separa u e v se $f(u) \neq f(v)$, ou seja, u e v são separáveis.

Definition 2.4. Um conjunto $S \subset \mathbb{F}[V]^G$ é separador se ele separa todos elementos separáveis de V.

Nosso interesse esta em quando $G = S_n$, agindo nos polinomios como permutação, e o corpo $\mathbb{F} = \mathbb{F}_q$, ou seja um corpo finito com p elementos. Nesse caso temos diversas aplicações para nossos conjuntos separadores, como no problema de isomorfismo entre grafos.

2.2. **Aplicação em Isomorfismo de Grafos.** Seja g e g' dois grafos com n vértices, não orientados, com pesos em $\mathbb{F}$ não nulos nas arestas . Considere $m_{\{i,j\}}$ uma função que associa a aresta entre os vértices i e j com seu respectivo peso (Onde $i \neq j$). Por conveniência se não existe nenhuma aresta entre i e j, denotemos $m_{i,j} = 0$.

Definition 2.5. Dois grafos g e g' são isomorfos se, e somente se, existe $\sigma \in S_n$ tal que $m_{\{i,j\}} = m'_{\{\sigma(i),\sigma(j)\}}$ para todo $1 \leq i < j \leq n$.

Logo, considerando grafos como elementos do espaço vetorial V, de forma que as coordenadas são os pesos das arestas entre vertices $\{i, j\}$, dizer que dois grafos são isomorfos é equivalente a dizer que $g \in G_{g'}$.

Portanto, basta determinar se dois grafos estão na mesma orbita. Seja o conjunto separador $S \subset \mathbb{F}[V]^{S_n}$ de V. Se $f(g) = f(g')$ para todo $f \in S$, então temos que g e g' não são separáveis, ou seja, os grafos correspondentes são isomorfos.

2.3. **Um Conjunto Separador Mínimo.** O resultado abaixo foi provado por Oliver Aberth, em 1964, [2].

Theorem 2.6. *Seja $\mathbb{F}$ um corpo finito com p elementos e V um espaço vetorial, com $dimV = n$, temos que um conjunto separador $S_I(n)$ da álgebra $\mathbb{F}[V]^{S_n}$ é:*

$$S(n) = \{s_i(x_1, \dots, x_n) \,|\, i \in [n]_p\}$$
$$[n]_p = \{jp^k \,|\, j \in \{1, \dots, p-1\},\, k \in \mathbb{N},\, jp^k \leq n\}$$

Assim, utilizando um resultado obtido por Artem Lopatin, Gregor Kemper e Fabian Reimers [1]:

- O número mínimo possível de elementos do conjunto separador para $\mathbb{F}[V]^G$ é $\gamma = \gamma(p,k) = \lceil \log_p(k) \rceil$, onde k é o número de G-órbitas sobre V, e p característica do corpo $\mathbb{F}$;

Foi possível demonstrar que quando $p = 3$ o conjunto de Aberth é na verdade o separador com a menor quantidade de elementos, para alguns espaços com dimensões especificas. Além disso, foi possível demonstrar que quando $\dim V < p$ temos que, para algumas dimensões específicas, o gerador da álgebra de invariantes é de fato o separador com a menor quantidade de elementos.

2.4. **Resultados sobre minimalidade.** Como tratamos do grupo S_n o número de órbitas é $k = \binom{n+p-1}{p-1}$, ou seja $\gamma = \left\lceil \log_p \binom{n+(p-1)}{(p-1)} \right\rceil$. Tendo isso em mente, obtivemos o seguinte lema que foi usado na demonstração do Teorema 2.8, quando $p = 3$.

Lemma 2.7. *Seja $n \in \mathbb{N}$ e $r \geq 3$. Assim, com $f_1(x) = \log_3 x^2$, $f_2(x) = \log_3 \frac{(x+2)(x+1)}{2}$, e $f_3(x) = \log_3 \frac{2}{1+\frac{3}{x}+\frac{2}{x^2}}$ temos*

$$\lfloor f_1(n) \rfloor + \lfloor -f_2(n) \rfloor = \begin{cases} \lfloor f_3(n) \rfloor & , \quad n \in \left[3^{\frac{r}{2}}, \frac{-3+\sqrt{8\cdot 3^r+1}}{2}\right) \\ \lfloor f_3(n) \rfloor - 1 & , \quad n \in \left[\frac{-3+\sqrt{8\cdot 3^r+1}}{2}, 3^{\frac{r+1}{2}}\right) \end{cases}$$

Theorem 2.8. *Seja $n \in \mathbb{N}$, $p = 3$ e:*

$$S(n) = \{s_i(x_1, \ldots, x_n) \mid i \in [n]_3\}$$
$$[n]_3 = \{j \cdot 3^k \mid j \in \{1,2\},\, k \in \mathbb{N},\, j \cdot 3^k \leq n\}$$

Temos:

- $\#S_I(n) - \gamma = 1$ *se* $n \in \left[3^r, \frac{-3+\sqrt{8\cdot 3^r+1}}{2}\right)$
- $\#S_I(n) - \gamma = 0$ *se* $n \in \left[\frac{-3+\sqrt{8\cdot 3^r+1}}{2}, 3^{r+\frac{1}{2}}\right)$
- $\#S_I(n) - \gamma = 0$ *se* $n \in [3^{r+\frac{1}{2}}, 2\cdot 3^r)$
- $\#S_I(n) - \gamma = 1$ *se* $n \in \left[2\cdot 3^r, \frac{-3+\sqrt{8\cdot 3^{2r+1}+1}}{2}\right)$
- $\#S_I(n) - \gamma = 0$ *se* $n \in \left[\frac{-3+\sqrt{8\cdot 3^{2r+1}+1}}{2}, 3^{r+1}\right)$

Com $r \geq 2$ e $r \in \mathbb{N}$.

Proof. Sabemos que :

$$\#S(n) = \begin{cases} 2\cdot\lfloor \log_3 n \rfloor + 1 & , \quad n \in [3^r, 2\cdot 3^r) \\ 2\cdot\lfloor \log_3 n \rfloor + 2 & , \quad n \in [2\cdot 3^r, 3^{r+1}) \end{cases}$$

Com $r \in \mathbb{N}$, e $\gamma = \left\lceil \log_3 \frac{(n+2)(n+1)}{2} \right\rceil$. Portanto, seja $\alpha \in \{1,2\}$:

$$\#S(n) - \gamma = 2\cdot\lfloor \log_3 n \rfloor + \alpha - \left\lceil \log_3 \frac{(n+2)(n+1)}{2} \right\rceil$$

Usando as propriedades das funções piso e teto, temos:

$$\#S(n) - \gamma = 2 \cdot \lfloor \log_3 n \rfloor + \left\lfloor -\log_3 \frac{(n+2)(n+1)}{2} \right\rfloor + \alpha$$

Assim usando o Lemma 2.7 conseguimos separar em 3 casos: $n \in [3^r, 3^{r+\frac{1}{2}})$, $n \in [3^{r+\frac{1}{2}}, 2 \cdot 3^r)$ e $n \in [2 \cdot 3^r, 3^{r+1})$. Quando $n \in [3^r, 3^{r+\frac{1}{2}}) \cap [3^{\frac{k}{2}}, \frac{-3+\sqrt{8 \cdot 3^k+1}}{2})$, temos:

$$\#S(n) - \gamma = \left\lfloor \log_3 \frac{2}{1 + \frac{3}{n} + \frac{2}{n^2}} \right\rfloor + 1$$

Se $n > 4$, $\left\lfloor \log_3 \frac{2}{1+\frac{3}{n}+\frac{2}{n^2}} \right\rfloor = 0$, portanto:

$$\#S(n) - \gamma = 1$$

Seguindo o mesmo processo, fazendo a intersecção com todos os intervalos possíveis temos que:

Para $n \in [3^r, 3^{r+\frac{1}{2}}) \cap \left[\frac{-3+\sqrt{8 \cdot 3^k+1}}{2}, 3^{\frac{k+1}{2}}\right)$, temos:

$$\#S(n) - \gamma = 0$$

Para $n \in [3^{r+\frac{1}{2}}, 2 \cdot 3^r) \cap \left[3^{\frac{k}{2}}, \frac{-3+\sqrt{8 \cdot 3^k+1}}{2}\right)$:

$$\#S(n) - \gamma = 0$$

Para $n \in [2 \cdot 3^r, 3^{r+1}) \cap \left[3^{\frac{k}{2}}, \frac{-3+\sqrt{8 \cdot 3^k+1}}{2}\right)$:

$$\#S(n) - \gamma = 1$$

Para $n \in [2 \cdot 3^r, 3^{r+1}) \cap \left[\frac{-3+\sqrt{8 \cdot 3^k+1}}{2}, 3^{\frac{k+1}{2}}\right)$

$$\#S(n) - \gamma = 0$$

Logo para $n > 4$, encontramos uma forma de separar o intervalo $[3^r, 3^{r+1})$, seja:

$$\begin{array}{rlrl} A_{1r} = & \left[3^r, \frac{-3+\sqrt{8 \cdot 3^{2r}+1}}{2}\right) & A_{2r} = & \left[\frac{-3+\sqrt{8 \cdot 3^{2r}+1}}{2}, 3^{r+\frac{1}{2}}\right) \\ A_{3r} = & [3^{r+\frac{1}{2}}, 2 \cdot 3^r) & A_{4r} = & \left[2 \cdot 3^r, \frac{-3+\sqrt{8 \cdot 3^{2r+1}+1}}{2}\right) \\ A_{5r} = & \left[\frac{-3+\sqrt{8 \cdot 3^{2r+1}+1}}{2}, 3^{r+1}\right) & & \end{array}$$

Portanto, se $r \geq 2$ temos $[3^r, 3^{r+1}) = A_{1r} \cup A_{2r} \cup A_{3r} \cup A_{4r} \cup A_{5r}$. Assim, usando as relações acima:

$$\begin{array}{ll} A_{1r} : \#S(n) - \gamma = 1 & A_{2r} : \#S(n) - \gamma = 0 \\ A_{3r} : \#S(n) - \gamma = 0 & A_{4r} : \#S(n) - \gamma = 1 \\ A_{5r} : \#S(n) - \gamma = 0 & \end{array}$$

$\square$

Pensando em quando $\dim V < p$, onde p é a característica do corpo, demonstramos em quais casos o conjunto gerador da álgebra de invariantes é o conjunto separador com a menor quantidade de elementos .

Lemma 2.9. *Seja* $\dim V = n \leq p$ *e* S *o conjunto dos geradores da álgebra de invariantes.* S *é o conjunto separador com a menor quantidade de elementos se, e somente se,* $n < n_0$ *em que :*

$$p^{n_0-1} = (n_0+1)\cdot \ldots \cdot \left(\frac{n_0}{p-1}+1\right)$$

Proof. Sabemos que $\#S = n$ e $\gamma = \left\lceil \log_p \frac{(n+p-1)\cdot\,\ldots\,\cdot(n+1)}{(p-1)!}\right\rceil$, assim:

$$\#S - \gamma = n - \left\lceil \log_p \frac{(n+p-1)\cdot\,\ldots\,\cdot(n+1)}{(p-1)!}\right\rceil$$

Portanto, utilizando as propriedades das funções teto e piso:

$$\#S - \gamma = \left\lfloor \log_p \frac{(p-1)!\cdot p^n}{(n+p-1)\cdot\,\ldots\,\cdot(n+1)}\right\rfloor$$

Logo

$$\#S - \gamma = 0 \quad \text{se, e somente se} \quad \log_p \frac{(p-1)!\cdot p^n}{(n+p-1)\cdot\,\ldots\,\cdot(n+1)} < 1$$

Ou seja $\frac{(p-1)!\cdot p^n}{(n+p-1)\cdot\,\ldots\,\cdot(n+1)} < p$, assim:

$$\#S - \gamma = 0 \quad \text{se, e somente se} \quad p^{n-1} < (n+1)\cdot \ldots \cdot \left(\frac{n}{p-1}+1\right)$$

Tirando o logarítmo da inequação, temos:

$$(n-1)\cdot \ln p < \sum_{i=1}^{p-1} \ln\left(\frac{n}{i}+1\right)$$

Seja $f_1(x) := (x-1)\cdot \ln p$ e $f_2(x) := \sum_{i=1}^{p-1} \ln\left(\frac{x}{i}+1\right)$, assim $f_1'(x) = \ln p$ e $f_2'(x) = \sum_{i=1}^{p-1} \frac{1}{x+i}$ portanto:

$$f_1'(x) > f_2'(x) \quad \text{para} \quad x \in \mathbb{N}$$

Dessa forma, so precisamos encontrar $n_0 \in \mathbb{N}$ tal que:

$$p^{n_0-1} = (n_0+1)\cdot \ldots \cdot \left(\frac{n_0}{p-1}+1\right)$$

Assim a condição $p^{n-1} < (n+1)\cdot \ldots \cdot \left(\frac{n}{p-1}+1\right)$ segue válida para $n < n_0$, uma vez que para $n = 1$ a inequação vale.

□

References

[1] G. Kemper, A. Lopatin, F. Reimers, *Separating invariants over finite fields*, Journal of Pure and Applied Algebra.

[2] O. Aberth *The elementary symmetric functions in a finite field of prime order*, Illinois J. Math.