4
Códigos de avaliação definidos sobre $\mathbb{F}_q$-álgebras

Neste capítulo iniciaremos uma nova formulação dos códigos já vistos anteriormente seguindo os resultados obtidos nos trabalhos de Pellikaan, Høholdt e van Lint (veja (Pel3), (Pel5), (Pel1) e (Pel2)).

Consideremos V_l um espaço vetorial de polinômios de grau menor ou igual a l em duas variáveis X, Y e coeficientes em $\mathbb{F}_q$. Consideremos um polinômio $G \in \mathbb{F}_q[X,Y]$ de grau m em que a forma homogênea G^* define uma curva não-singular. Sejam $P_1, P_2, ..., P_n$ pontos racionais da curva plana definida pela equação $G = 0$, isto é, $P_i = (a_i, b_i) \in \mathbb{F}_q^2$ e $G(P_i) = 0$ para $1 \leq i \leq n$. Definimos então o código C por

$$C = \{(F(P_1), F(P_2), ..., F(P_n)) \mid F \in V_l\}.$$

Teorema 4.0.11 *Seja $n > lm$. A distância mínima d e a dimensão k de C são dadas por*

$$d \geq n - lm,$$

$$k = \begin{cases} \binom{l+2}{2}, & se \quad l < m \\ lm + 1 - \binom{m-1}{2}, & se \quad l \geq m \end{cases}$$

Prova:

Os monômios da forma $X^\alpha Y^\beta$ com $\alpha + \beta \leq l$ formam uma base de V_l. Logo V_l possui dimensão $\binom{l+2}{2}$.

Seja $F \in V_l$. Se G é um fator de F, então a palavra do código associada a F será a palavra identicamente nula. Por outro lado, se esta palavra do código for nula, então as curvas dadas pelas equações $F = 0$ e $G = 0$ (onde $deg\, F = l' \leq l$ e $\deg G = m$) se intersectam em pelo menos n pontos distintos, a saber $P_1, ..., P_n$. Como $n > lm > l'm$ pelo teorema de Bezout devemos ter que F e G têm um fator em comum e já que G é irredutível, F deve ser divisível por G. Logo os polinômios $F \in V_l$ associados à palavra nula pertencem ao subspaço vetorial dado por $GV_{l-m} = \{GF | F \in V_{l-m}\}$. Isto implica que se $l < m$ então $k = \binom{l+2}{2}$, e se $l \geq m$ então

$$k = \binom{l+2}{2} - \binom{l-m+2}{2} = lm + 1 - \binom{m-1}{2}$$

Também segue-se do teorema de Bezout que uma palavra do código não-nula tem no máximo lm coordenadas iguais a zero, isto é, seu peso é no mínimo $n - lm$. Logo $d \geq n - lm$.

$\square$

Note que se $F_1, ..., F_k$ é uma base para V_l modulo GV_{l-m}, então

$$(F_i(P_j) \mid 1 \leq i \leq k, 1 \leq j \leq n)$$

é a matriz geradora de C. Então esta é a matriz de paridade para o dual de C. A distância mínima $d^{\perp}$ de $C^{\perp}$ é igual ao número mínimo de colunas dependentes desta matriz. Logo para todo $t < d^{\perp}$ e todo subconjunto Q de $\mathcal{P} = \{P_1, ..., P_n\}$ consistindo de t pontos distintos, a submatriz correspondente $k \times t$ tem como posto máximo t.

Seja $L_l = V_l / GV_{l-m}$. Então a função avaliação polinomial em Q induz uma aplicação sobrejetiva de L_l em $\mathbb{F}_q^t$. O núcleo, que denotaremos por $L_l(Q)$, é o espaço de todos os polinômios $F \in V_l$ tais que todo ponto de Q é zero de $\bar{F}$, onde $\bar{F}$ denota a classe de F módulo GV_{l-m}. Temos então que $dim\,(L_l(Q)) = k - t$ se $t < d^{\perp}$. Mais ainda, a dimensão de $L_l(Q)$ é no mínimo $k - t$ para todos t-subconjuntos Q de $\mathcal{P}$ (um t-subconjunto Q de $\mathcal{P}$ é simplesmente um subconjunto com t elementos).

Mas para obter a limitação para $d^{\perp}$, temos que mostrar que $dim(L_l(Q)) = k - t$ para todo $t < d^{\perp}$.

O que faremos agora é generalizar os códigos descritos acima. Para isso introduziremos as noções de funções de ordem, grau e peso e um método para obter tais funções.

4.1
Funções Ordem, Grau e Peso

$\mathbb{N}$ denotará o conjunto dos inteiros positivos e $\mathbb{N}_0$ denotará o conjunto dos inteiro não-negativos.

Definição 4.1 *Uma $\mathbb{F}$-álgebra R é um anel comutativo com unidade tal que os elementos de $\mathbb{F}^*$ são inversíveis em R.*

O exemplo mais simples de uma $\mathbb{F}$-álgebra é $R = \mathbb{F}[X_1, ..., X_m]$.

Para generalizar os códigos estudados anteriormente, vamos precisar definir uma relação de ordem " especial" para os polinômios em R. Esta relação estará dada como segue:

Definição 4.2 *Seja $R = \mathbb{F}[X_1, ..., X_m]$. Suponha que $\prec$ seja uma relação total de ordem no conjunto dos monômios nas variáveis $X_1, ..., X_m$ tal que para todos os monômios M_1, M_2 e M vale que:*

(R.1) *se $M \neq 1$ então $1 \prec M$;*

(R.2) *se $M_1 \prec M_2$ então $MM_1 \prec MM_2$.*

Então $\prec$ será chamada de uma ordem de redução sobre os monômios.

Denotaremos um monômio nas variáveis $X_1, ..., X_m$ da seguinte forma:

$$X^\alpha = \prod_{i=1}^{m} X_i^\alpha \quad \text{se } \alpha = (\alpha_1, ..., \alpha_m).$$

O grau de um monômio é dado por

$$deg\,(X^\alpha) = deg\,(\alpha) = \sum_{i=1}^{m} \alpha_i.$$

Definir uma ordem de redução sobre os monômios em m variáveis é equivalente a definir uma ordem total no conjunto $\mathbb{N}_0^m$ tal que para todo $\alpha_1, \alpha_2, \alpha \in \mathbb{N}_0^m$ temos

(E.1) se $\alpha \neq 0$ então $0 \prec \alpha$;

(E.2) se $\alpha_1 \prec \alpha_2$ então $\alpha + \alpha_1 \prec \alpha + \alpha_2$.

Usaremos $\prec$ para denotar a ordem definida tanto para os monômios quanto para os expoentes.

Exemplo 4.1.1 *A ordem lexicográfica $\prec_L$ definida por*

$$X^\alpha \prec_L X^\beta \quad \textit{se, e somente se,}$$

$$\alpha_1 = \beta_1, ..., \alpha_{l-1} = \beta_{l-1} \;\; e \;\; \alpha_l < \beta_l \quad \textit{para algum } l \textit{ tal que } 1 \leq l \leq m.$$

A ordem lexicográfica é uma relação de ordem de redução no sentido da definição 4.2.

Por exemplo, para $m = 2$, sejam $X = X_1$ e $Y = X_2$ e $\prec = \prec_L$. A ordem lexicográfica é da seguinte forma:

$$1 \prec Y \prec Y^2 \prec Y^3 \prec ... \prec Y^j \prec Y^{j+1} \prec ...$$
$$X \prec XY \prec XY^2 \prec XY^3 \prec ... \prec XY^j \prec XY^{j+1} \prec ...$$
$$X^2 \prec X^2Y \prec X^2Y^2 \prec X^2Y^3 \prec ... \prec X^2Y^j \prec X^2Y^{j+1} \prec ...$$

Então X^{i+1} é o supremo do conjunto $\{X^iY^j \mid j \in \mathbb{N}\}$.

Note que se $m \geq 2$, então a ordem lexicográfica não é isomorfa aos inteiros positivos com a ordem usual.

Exemplo 4.1.2 *A ordem lexicográfica graduada $\prec_D$ é definida por*

$$X^\alpha \prec_D X^\beta \quad \textit{se, e somente se,}$$
$$\textit{ou } deg\,(X^\alpha) = deg\,(X^\beta) \textit{ ou } deg\,(X^\alpha) \neq deg\,(X^\beta) \textit{ e } X^\alpha \prec_L X^\beta.$$

A ordem lexicográfica graduada é uma relação de ordem de redução que é isomorfa aos inteiros positivos com a ordem usual.

Uma relação de ordem nos monômios pode ser estendida a uma função definida sobre todos os polinômios da seguinte forma: seja $\prec$ uma relação de ordem de redução que é isomorfa aos inteiros positivos com a ordem usual. Digamos que o conjunto dos monômios $\{f_1, f_2, ...\}$ seja uma base de $\mathbb{F}[X_1, ..., X_m]$ e esteja ordenado de tal forma que $f_i \prec f_{i+1}$ para todo i. Como todo polinômio f pode ser escrito como

$$f = \sum_{i=1}^{j} \lambda_i f_i,$$

onde $\lambda_i \in \mathbb{F}$ para todo i, e $\lambda_j \neq 0$ para algum j, definimos uma função

$$\rho : \mathbb{F}[X_1, ..., X_m] \longrightarrow \mathbb{N}_0 \cup \{-\infty\}$$

como segue:

$$\rho(f) = \begin{cases} -\infty & \text{se } f = 0 \\ j-1 & \text{onde } j \text{ é o menor inteiro positivo tal que } f \text{ pode} \\ & \text{ser escrito como combinação linear dos } j \text{ primeiros monômios} \end{cases}$$

Claramente temos as seguintes propriedades desta função:

(O.0) $\rho(f) = -\infty \Longleftrightarrow f = 0$;

(O.1) $\rho(\lambda f) = \rho(f)$ para todo $\lambda \in \mathbb{F}$;

(O.2) $\rho(f+g) \leq max\{\rho(f), \rho(g)\}$ e a igualdade vale se $\rho(f) < \rho(g)$;

(O.3) se $\rho(f) < \rho(g)$ e $h \neq 0$, então $\rho(fh) < \rho(gh)$;

(O.4) se $\rho(f) = \rho(g)$, então existe $\lambda \in F$ tal que $\rho(f - \lambda g) < \rho(g)$;

para todo $f, g, h \in R$, para todo $n \in \mathbb{N}$, assumindo que $-\infty < n$, $\forall n \in \mathbb{N}$.

Definição 4.3 *Seja R uma $\mathbb{F}$-álgebra. Uma função de ordem em R é uma aplicação*

$$\rho : R \longrightarrow \mathbb{N}_0 \cup \{-\infty\},$$

que satisfaz as condições $(O.0), ..., (O.4)$.

Definição 4.4 *Seja R uma $\mathbb{F}$-álgebra. Uma função peso em R é uma função de ordem em R que satisfaz também a seguinte propriedade*

$$(O.5)\ \ \rho(fg) = \rho(f) + \rho(g) \quad \textit{para todo } f, g \in R.$$

(Aqui estamos assumindo que para todo $n \in \mathbb{N}_0$ temos que $-\infty + n = -\infty$.)

Se ρ é uma função peso e $\rho(f)$ é divisível por um inteiro $d > 1$ para todo $f \in R$, então $\rho(f)/d$ é outra função peso. Daí, podemos assumir que o maior divisor comum entre os inteiros $\rho(f)$ onde $f \in R$ é 1.

Definição 4.5 *Uma função grau em R será uma aplicação que satisfaz as condições $(O.0), (O.1), (O.2)$ e $(O.5)$.*

É claro que $(O.3)$ é consequência de $(O.5)$.

Exemplo 4.1.3 *O exemplo clássico de uma $\mathbb{F}_q$-álgebra R com uma função grau ρ é o seguinte: $R = \mathbb{F}_q[X_1, \cdots, X_m]$ e $\rho(f) = deg(f)$.*
ρ será uma função de ordem se, e somente se, $m = 1$ e neste caso ρ será também uma função peso.

Um exemplo importante para o assunto deste trabalho é o seguinte:

Exemplo 4.1.4 *Seja $\mathcal{C}$ uma curva projetiva, não-singular, irredutível definida sobre $\mathbb{F}_q$ e seja P um ponto racional de $\mathcal{C}$. Considere R o anel das funções racionais de $\mathcal{C}$ regulares fora de P (i.e.; se $f \in R$, f não-constante, então P é o único polo de f) e portanto temos que $v_P(f) \leq 0$ para toda $f \in R$ não-nula. Definamos $\rho(f) = -v_p(f)$ para $f \in R$, então ρ é uma função peso.*
O objetivo é mostrar que pode ser desenvolvida a teoria dos códigos geométricos sem usar a teoria das curvas algébricas.

Lema 4.1.5 *Seja ρ uma função de ordem em R. Então temos:*

1. *se $\rho(f) = \rho(g)$ então $\rho(fh) = \rho(gh)$ para todo $h \in R$;*
2. *se $f \in R$ e $f \neq 0$ então $\rho(1) \leq \rho(f)$;*
3. *$\mathbb{F} = \{f \in R \mid \rho(f) \leq \rho(1)\}$;*
4. *se $\rho(f) = \rho(g)$ então existe um único $\lambda \in F^*$ tal que $\rho(f - \lambda g) < \rho(g)$.*

Prova:

1. Seja $\rho(f) = \rho(g)$. Então $(O.4)$ nos diz que existe $\lambda \in F^*$ tal que $\rho(f - \lambda g) < \rho(g)$. Por $(O.3)$ temos $\rho(fh - \lambda gh) < \rho(gh)$. Mas $fh = (fh - \lambda gh) + \lambda gh$, então $\rho(fh) = \rho(\lambda gh) = \rho(gh)$ por $(O.2)$ e $(O.1)$ respectivamente.

2. Seja $0 \neq f \in R$ tal que $\rho(f) < \rho(1)$. Então $\rho(1) > \rho(f) > \rho(f^2) > ...$ é uma sequência estritamente decrescente pela condição $(O.3)$, mas isto contradiz o fato de que $\mathbb{N} \cup \{-\infty\}$ é ordenado. Logo $\rho(1) \leq \rho(f)$ para todo $0 \neq f \in R$.

3. É claro que $\mathbb{F}$ é um subconjunto de $\{f \in R \mid \rho(f) \leq \rho(1)\}$, pelas condições $(O.0)$ e $(O.1)$. Se $f \neq 0$ e $\rho(f) \leq \rho(1)$ então $\rho(f) = \rho(1)$ pelo item anterior. Logo existe $\lambda \in \mathbb{F}$ tal que $\rho(f - 1\lambda) < \rho(1)$ por $(O.4)$. Então $f - \lambda = 0$ e $f \in \mathbb{F}$.

4. A existência de λ está garantida por $(O.4)$. Vamos ver somente a unicidade. Suponhamos que existem $0 \neq \lambda, \mu \in \mathbb{F}$ tais que $\rho(f - \lambda g) < \rho(g)$ e $\rho(f - \mu g) < \rho(g)$. Por $(O.2)$ temos $\rho(f - \lambda g - (f - \mu g)) < \rho(g)$. Logo $\rho((\mu - \lambda)g) < \rho(g)$. A condição $(O.1)$ mostra que $\mu - \lambda = 0$.

□

Proposição 4.1.6 *Se existe uma função de ordem em R, então R é um domínio*

Prova:

Sejam $f, g \in R$ tais que $fg = 0$. Sem perda de generalidade suponhamos que $\rho(f) \leq \rho(g)$. Então $\rho(f^2) \leq \rho(fg) = \rho(0) = -\infty$, o que implica que $\rho(f^2) = -\infty$, e $f^2 = 0$. Mas, se $f \neq 0$, pelo lema 4.1.5 temos que $\rho(1) \leq \rho(f)$, então $\rho(f) \leq \rho(f^2) = \rho(0) = -\infty$. Logo $f = 0$, que é uma contradição. Logo R não possui divisores de zero.

□

A recíproca não é verdadeira como mostra o exemplo a seguir:

Exemplo 4.1.7 *A $\mathbb{F}$-álgebra $R = \mathbb{F}[X_1, X_2]/(X_1X_2 - 1)$ é um domínio, mas R não possui nenhuma função de ordem.*
Denotaremos por x_i a classe do elemento $X_i \in R$. Se ρ é uma função de ordem em R, então $\rho(1) \leq \rho(x_1)$, logo $\rho(x_2) \leq \rho(x_1x_2) = \rho(1)$. Portanto $\rho(x_2) = \rho(1)$ e analogamente $\rho(x_1) = \rho(1)$. Daí, $\rho(f) \leq \rho(1)$ para todo $f \in R$. Então $\mathbb{F} = R$ pelo lema 4.1.5, que é uma contradição já que $x_1 \notin \mathbb{F}$.

A próxima proposição e o próximo teorema nos mostrarão que existe uma base para R com certas propriedades sempre que existir uma função de ordem e que reciprocamente, se tal base existe, então é possível definir uma função de ordem. Embora a formulação de tal fato seja extremamente técnica, é fácil de ser aplicado.

Proposição 4.1.8 *Seja R uma $\mathbb{F}$-álgebra tal que $R \neq \mathbb{F}$, com função de ordem ρ. Então existe uma base $\{f_i \mid i \in \mathbb{N}\}$ de R sobre $\mathbb{F}$ tal que $\rho(f_i) < \rho(f_{i+1})$ para todo i. Tal base tem a seguinte propriedade: se i é o menor inteiro positivo tal que f pode ser escrito como combinação linear dos i primeiros elementos da base, então $\rho(f) = \rho(f_i)$. Seja $l(i, j)$ o inteiro l tal que $\rho(f_if_j) = \rho(f_l)$, então $l(i, j) < l(i + 1, j)$ para todo i e j. Seja $\rho_i = \rho(f_i)$. Se ρ é uma função peso, então $\rho_{l(i,j)} = \rho_i + \rho_j$.*

Prova:

Pela hipótese, existe $f \in R \setminus \mathbb{F}$. Pelo lema 4.1.5 $\rho(1) < \rho(f)$ e assim já que $\rho(f^n) < \rho(f^{n+1})$ para todo $n \in \mathbb{N}$ temos que o conjunto dos valores de ρ é infinito. Seja $(\rho_i \mid i \in \mathbb{N})$ a sequência crescente de todos os inteiros não-negativos que aparecem como $\rho(f)$ sendo $f \in R$ não-nulo. Por definição para todo $i \in \mathbb{N}$ existe $f_i \in R$ tal que $\rho(f_i) = \rho_i$ e, além disso, temos que $\rho(f_i) < \rho(f_{i+1})$ para todo i, e para todo $f \in R$ não-nulo, existe i tal que $\rho(f) = \rho(f_i)$. O fato de que $\{f_i \mid i \in \mathbb{N}\}$ forma uma base, é provado por indução e pelo lema 4.1.5 (4) e, por $(O.2)$, possui a propriedade desejada. De $(O.3)$ podemos ver que $l(i,j)$ é estritamente crescente. E ainda se ρ é uma função peso, então $\rho_{l(i,j)} = \rho_i + \rho_l$ pela condição $(O.5)$.

□

Exemplo 4.1.9 *Considere a ordem lexicográfica graduada como no exemplo 4.1.2 para $m = 2$. Sejam $X = X_1$, $Y = X_2$ e considere $R = \mathbb{F}[X,Y]$ com a seguinte base*

$$\{X^\alpha Y^\beta \mid \alpha, \beta \in \mathbb{N}_0\}.$$

Considere a base de monômios e seus correspondentes índices organizados (diagonalmente da esquerda para direita) nas seguintes tabelas:

$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
Y^6	·	·	·	·	·	…
Y^5	XY^5	·	·	·	·	…
Y^4	XY^4	X^2Y^4	·	·	·	…
Y^3	XY^3	X^2Y^3	X^3Y^3	·	·	…
Y^2	XY^2	X^2Y^2	X^3Y^2	·	·	…
Y^1	XY	X^2Y	X^3Y	X^4Y	·	…
1	X	X^2	X^3	X^4	X^5	…

E ainda,

$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
22	·	·	·	·	·	…
16	23	·	·	·	·	…
11	17	24	·	·	·	…
7	12	18	25	·	·	…
4	8	13	19	·	·	…
2	5	9	14	20	·	…
1	3	6	10	15	21	…

Note que $f_8 = XY^2$ e $f_9 = X^2Y$. Então $f_8 f_9 = XY^2 \cdot X^2Y = X^3Y^3 = f_{25}$. Logo $l(8,9) = 25$.

Teorema 4.1.10 *Sejam R uma $\mathbb{F}$-álgebra e $\{f_i \mid i \in \mathbb{N}\}$ uma base de R como o espaço vetorial sobre $\mathbb{F}$ com $f_1 = 1$, L_i um espaço vetorial gerado por $f_1, ..., f_i$ e $l(i,j)$ o menor inteiro positivo l tal que $f_i f_j \in L_l$. Suponhamos que $l(i,j) < l(i+1,j)$ para todo $i,j \in \mathbb{N}$. Seja $(\rho_i \mid i \in \mathbb{N})$ uma sequência estritamente crescente de inteiros não-negativos. Definamos $\rho(0) = -\infty$ e $\rho(f) = \rho_i$ se i é o menor inteiro positivo tal que $f \in L_i$. Então ρ é uma função de ordem em R. Se, além disso, vale que $\rho_{l(i,j)} = \rho_i + \rho_j$, então ρ é uma função peso.*

Prova:

As condições $(O.0), (O.1), (O.2)$ e $(O.4)$ são consequências direta da definição. Para todo elemento não-nulo $f \in R$, associamos $\iota(f)$, o menor inteiro positivo tal que $f \in L_{\iota(f)}$. Sejam f e g elementos diferentes de zero de R.

$$f = \sum_{i \leq \iota(f)} \lambda_i f_i, \qquad g = \sum_{j \leq \iota(g)} \nu_j f_j \quad \text{então temos}$$

$$fg = \sum_{l \leq \iota(fg)} \mu_l f_l \quad \text{com } \lambda_{\iota(f)}, \nu_{\iota(g)}, \mu_{\iota(fg)} \neq 0.$$

Logo existe $\mu_{ijl} \in \mathbb{F}$ tal que

$$f_i f_j = \sum_{l \leq l(i,j)} \mu_{ijl} f_l \quad \text{onde } \mu_{ijl} \neq 0,$$

então

$$\mu_l = \sum_{l(i,j)=l} \lambda_i \nu_j \mu_{ijl}.$$

A função $l(i,j)$ é estritamente crescente em i e em j por definição e simetria. Note que $l(i,j) < l(\iota(f), \iota(g))$ se $i < \iota(f)$ ou $j < \iota(g)$ e, além disso, se $i = \iota(f)$ e $j = \iota(g)$, vale que

$$\lambda_i \nu_j \mu_{ijl(i,j)} \neq 0,$$

e é igual a $\mu_{\iota(fg)}$, e portanto temos que $\iota(fg) = l(\iota(f), \iota(g))$. Mais ainda, se $\rho_{l(i,j)} = \rho_i + \rho_j$, então

$$\rho(fg) = \rho_{\iota(fg)} = \rho_{l(\iota(f),\iota(g))} = \rho_{\iota(f)} + \rho_{\iota(g)} = \rho(f) + \rho(g).$$

$\square$

Exemplo 4.1.11 *Seja $w = (w_1, ..., w_m)$ uma m-upla de inteiros positivos chamada peso. O grau com peso de $\alpha \in \mathbb{N}^m$ e do seu monômio correspondente X^α é definido por*

$$wdeg\,(X^\alpha) = wdeg\,(\alpha) = \sum_{l=1}^{m} \alpha_l w_l,$$

e de um polinômio não-nulo $F = \sum \lambda_\alpha X^\alpha$ por

$$wdeg\,(F) = max\{wdeg\,(X^\alpha) \mid \lambda_\alpha \neq 0\}.$$

A função grau é de fato uma função grau no anel $R = \mathbb{F}[X_1, ..., X_m]$. A ordem lexicográfica graduada com peso $\prec_w$ em $\mathbb{N}^m$ é definida por

$$\alpha \prec_w \beta \text{ se, e somente se,}$$

$$wdeg\,(\alpha) < wdeg\,(\beta) \;\text{ ou }\; wdeg\,(\alpha) = wdeg\,(\beta) \text{ e } \alpha \prec_L \beta,$$

e de maneira similar para monômios. Isto é realmente uma relação de ordem de redução que é isomorfa a $\mathbb{N}$.

Considere a ordem lexicográfica graduada com peso para $m = 2$ com $X = X_1$, $Y = X_2$, $wdeg\,(X) = 4$ e $wdeg\,(Y) = 5$.

Seja $R = \mathbb{F}_q[X, Y]$ e $\{X^\alpha Y^\beta \mid \alpha, \beta \in \mathbb{N}_0\}$ como uma base com o $\mathbb{F}_q$-álgebra. Considere o grau com peso $4\alpha + 5\beta$ desta base e seu correspondente índice dados nas seguintes tabelas.

$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
25	·	·	·	·	·	$\cdots$
20	24	·	·	·	·	$\cdots$
15	19	23	·	·	·	$\cdots$
10	14	18	22	·	·	$\cdots$
5	9	13	17	21	25	$\cdots$
0	4	8	12	16	20	24

E ainda,

$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
22	·	·	·	·	·	$\cdots$
15	20	·	·	·	·	$\cdots$
10	14	19	·	·	·	$\cdots$
6	9	13	18	·	·	$\cdots$
3	5	8	12	17	23	$\cdots$
1	2	4	7	11	16	21

Os elementos da base X^6 e XY^4 possuem o mesmo grau com peso, 24. Mas XY^4 é menor que X^6 na ordem lexicográfica. Logo $f_{20} = XY^4$ e $f_{21} = X^6$.

4.2 Existência de Funções Peso

Exemplo 4.2.1 *Seja I o ideal em $\mathbb{F}[X,Y]$ gerado por um polinômio da forma*

$$X^aY^c + Y^{b+c} + G$$

com $G \in \mathbb{F}[X,Y]$, $deg_X(G) = d < a$, $deg(G) < b+c$ e $mdc(a,b) = 1$, onde o grau de $G \in \mathbb{F}[X,Y]$ como polinômio em X é denotado por $deg_X(G)$. Seja $S = \mathbb{F}[X,Y]/I$. Denotaremos as classes de X, Y e G módulo I por x, y e g respectivamente. Logo $x^ay^c = -y^{b+c} - g$, o que implica que, x^ay^c é uma combinação linear de elementos da forma $x^\alpha y^\beta$ com $\alpha < a$, já que $deg_X(G) < a$. Por indução vemos que

$$\{x^\alpha y^\beta \mid \alpha, \beta \in \mathbb{N}_0,\ \alpha < a \text{ ou } \beta < c\}$$

é uma base de S. Suponhamos que exista uma função peso ρ em S tal que $mdc(\rho(x), \rho(y)) = 1$. Mostraremos que $\rho(x) = b$ e $\rho(y) = a$. Seja $X^\alpha Y^\beta$ o monômio em G com o maior peso. Então $\alpha + \beta < a + c$.
Daí, $\rho(g) \leq \alpha\rho(x) + \beta\rho(y)$ por $(O.2)$ e $(O.5)$.

– *Se $\rho(y) \leq \rho(x)$, então*

$$\begin{aligned} \alpha\rho(x) + \beta\rho(y) &= \alpha\rho(x) + (\beta - c)\rho(y) + c\rho(y) \\ &\leq (\alpha + \beta - c)\rho(x) + c\rho(y) \\ &< a\rho(x) + c\rho(y). \end{aligned}$$

Logo $\rho(g) < \rho(x^ay^c)$ e portanto $\rho(x^ay^c) = \rho(x^ay^c + g)$. Como $\rho(y^{b+c}) = \rho(x^ay^c + g)$, então temos que $\rho(y^{b+c}) = \rho(x^ay^c)$ e logo $a\rho(x) = b\rho(y)$.

– *Se $\rho(x) \leq \rho(y)$ obtemos analogamente que $a\rho(x) = b\rho(y)$.*

Logo, em ambos os casos $a\rho(x) = b\rho(y)$. Como $mdc(\rho(x), \rho(y)) = 1$, então $\rho(x) = b$ e $\rho(y) = a$.

A seguinte proposição nos mostra que a $\mathbb{F}$-álgebra S admite uma função peso como a descrita anteriormente se $c = 0$. Mas se $c > 0$, então x^a e y^b são dois elementos que possuem o mesmo peso ab e são independentes módulo elementos de peso estritamente menor que ab. Isto contradiz a condição $(O.4)$. Logo não existe função peso se $c > 0$.

Exemplo 4.2.2 *O polinômio $X^3Y + Y^3 + Y$ é redutível com $a = 3, b = 2, c = 1, d = 0$ e $G = Y$. Pela proposição 4.1.6 não existe uma função de ordem.*

Considere o subespaço R de S que é gerado por

$$\{x^\alpha y^\beta \mid \alpha, \beta \in \mathbb{N}_0, \alpha < a \text{ e } c\alpha \leq (a-d)\beta\}.$$

Provaremos que R é uma $\mathbb{F}$-álgebra e que podemos definir uma função peso em R tal que $\rho(x) = b$ e $\rho(y) = a$.

Proposição 4.2.3 *Seja I o ideal em $\mathbb{F}[X,Y]$ gerado por um polinômio da forma $X^aY^c + uY^{b+c} + G$ com $u \in \mathbb{F}^*$, $G \in \mathbb{F}[X,Y]$, $deg_X(G) = d < a$, $deg(G) < b + c$ e $mdc(a,b) = 1$. Sejam $S = \mathbb{F}[X,Y]/I$ e R o espaço vetorial gerado por $\{x^\alpha y^\beta \mid \alpha, \beta \in \mathbb{N}_0, \alpha < a \, e \, c\alpha \leq (a-d)\beta\}$. Então R é uma $\mathbb{F}$-álgebra com uma função peso ρ tal que $\rho(x) = b$ e $\rho(y) = a$.*

Prova:

O conjunto $\{x^\alpha y^\beta \mid \alpha < a \text{ ou } \beta < c\}$ é uma base para S sobre $\mathbb{F}$ então $\{x^\alpha y^\beta \mid \alpha < a \text{ e } c\alpha \leq (a-d)\beta\}$ é uma base para R. Sejam $f_1, ..., f_n, ...$ uma enumeração desta base de R. Se $f_i = x^\alpha y^\beta, \alpha < a$ e $c\alpha \leq (a-d)\beta$, então definamos $\rho_i = \alpha b + \beta a$. A função $(\alpha, \beta) \longmapsto \alpha b + \beta a$ é injetiva no domínio $\{(\alpha, \beta) \in \mathbb{N}^2 \mid \alpha < a\}$, pois $mdc(a,b) = 1$. Logo se $i \neq j$, então $\rho_i \neq \rho_j$. Podemos assumir que a enumeração $(\rho_i \mid i \in \mathbb{N})$ forma uma sequência estritamente crescente.

Seja $L_l = < f_1, ..., f_l >$. Provaremos que para todo i, j existe um inteiro não-negativo l tal que $f_i f_j \in L_l$. Então R é uma $\mathbb{F}$-álgebra. Além disso, mostraremos que se $l(i,j)$ é o menor inteiro não-negativo l tal que $f_i f_j \in L_l$ então $\rho_{l(i,j)} = \rho_i + \rho_j$ e portanto vai existir uma função peso ρ em R tal que $\rho(x^\alpha y^\beta) = \alpha b + \beta a$ pelo teorema 4.1.10.
Sejam

$$\begin{aligned} f_i &= x^\alpha y^\beta, \quad \rho_i = \alpha b + \beta a \quad \text{com } \alpha < a \text{ e } c\alpha \leq (a-d)\beta, \\ f_j &= x^\gamma y^\delta, \quad \rho_j = \gamma b + \delta a \quad \text{com } \gamma < a \text{ e } c\gamma \leq (a-d)\delta. \end{aligned}$$

Então

$$f_i f_j = x^{\alpha+\gamma} y^{\beta+\delta}, \quad \rho_i + \rho_j = (\alpha+\gamma)b + (\beta+\delta)a \quad \text{e } c(\alpha+\gamma) \leq (a-d)(\beta+\delta).$$

– Se $\alpha+\gamma<a$ então $f_i f_j$ é um elemento da base de R. Então $f_{l(i,j)} = f_i f_j$ e $\rho_{l(i,j)} = \rho_i + \rho_j$.

– Se $\alpha+\gamma \geq a$ então $\alpha+\gamma = a+\epsilon$ com $\epsilon < a$. Logo

$$ca \leq c(\alpha+\gamma) \leq (a-d)(\beta+\delta),$$

e $\beta+\delta = c+\eta$ para algum inteiro não-negativo η. Como $c(a+\epsilon) \leq (a-d)(c+\eta)$ isto implica que $c(d+\epsilon) \leq (a-d)\eta$, então $\epsilon < a$ e $c\epsilon \leq (a-d)(b+c+\eta)$. Logo

$$f_i f_j = x^a y^c x^\epsilon y^\eta = -ux^\epsilon y^{b+c+\eta} - x^\epsilon y^\eta g.$$

Sendo assim $x^\epsilon y^{b+c+\eta}$ é um elemento f_l da base de R e

$$\rho_i + \rho_j = (\alpha+\gamma)b + (\beta+\delta)a = \epsilon b + (b+c+\eta)a = \rho_l.$$

Vamos mostrar agora que $x^\epsilon y^\eta \in L_{l-1}$. Isto implicará que $f_i f_j \in L_l \setminus L_{l-1}$ e portanto que $l(i,j) = l$.

Note que um monômio de G com coeficientes não-nulos é da forma $X^k Y^\lambda$ com $k \leq d$ e $k+\lambda < b+c$, já que $deg_X\,(G) = d$ e $deg\,(G) < b+c$.

Afirmação: Se $(\epsilon,\eta),(k,\lambda) \in \mathbb{N}_0^2$ satisfazem

$$\epsilon < a, \quad c(\epsilon+d) \leq (a-d)\eta,$$

$$k \leq d, \quad k+\lambda < b+c \quad \text{e}$$

$$\rho_l = \epsilon b + (b+c+\eta)a,$$

então $x^{\epsilon+k} y^{\eta+\lambda} \in L_{l-1}$.

Prova da Afirmação: Se $\epsilon+k < a$ então $x^{\epsilon+k}y^{\eta+\lambda}$ é elemento da base de R, pois $c(\epsilon+k) \leq (a-d)(\eta+\lambda)$. Logo,

$$\begin{aligned}(\epsilon+k)b + (\eta+\lambda)a &= \epsilon b + (kb+\lambda a) + \eta a \\ &< \epsilon b + (b+c+\eta)a = \rho_l\end{aligned}$$

já que $b<a$ e $k+\lambda < b+c$. Então $x^{\epsilon+k}y^{\eta+\lambda} \in L_{l-1}$.

Por outro lado, se $\epsilon+k \geq a$ então $\epsilon+k = a+\epsilon'$ para algum inteiro não-negativo ϵ', onde $\epsilon' < \epsilon$, pois $k \leq d < a$. Analogamente ao caso anterior temos $\eta+\lambda = c+\eta'$, para algum inteiro não-negativo η', e $c\epsilon' \leq (a-d)\eta'$. Logo,

$$x^{\epsilon+k}y^{\eta+\lambda} = x^a y^c x^{\epsilon'} y^{\eta'} = -ux^{\epsilon'} y^{b+c+\eta'} - x^{\epsilon'} y^{\eta'} g.$$

Então, o termo $x^{\epsilon'} y^{b+c+\eta'}$ é um elemento $f_{l'}$ da base de R e vale que

$$\rho_{l'} = \epsilon' b + (b + c + \eta')a = (a + \epsilon')b + (c + \eta')a = (\epsilon + k)b + (\eta + \lambda)a,$$

que é estritamente menor que ρ_l, como vimos anteriormente. Disto segue que $x^{\epsilon'} y^{\eta'} g \in L_{l'-1}$ e $l' < l$. Logo $x^{\epsilon+k}y^{\eta+\lambda} \in L_{l-1}$.

□

Corolário 4.2.4 *Seja F um polinômio da forma $X^aY^b + uY^{b+c} + G$ com $u \in \mathbb{F}^*$, $G \in \mathbb{F}[X, Y]$, $deg_X(G) = d < a$, $deg(G) < b + c$ e $mdc(a, b) = 1$. Se G não é divisível por Y, então F é absolutamente irredutível.*

Prova:

Suponhamos que existam dois polinômios U e V tais que $F = UV$. Sejam u o elemento de $S = \mathbb{F}[X, Y]/(F)$ correspondente a U módulo (F) e v o elemento de S correspondente a V módulo (F). Então $uv = 0$. Seja R um subespaço de S gerado pelos elementos $x^\alpha y^\beta$ tal que $\alpha < a$ e $c\alpha \leq (a - d)\beta$. Então R é uma $\mathbb{F}$-álgebra com uma função peso pela proposição 4.2.3. Logo R é um domínio pela proposição 4.1.6. Consideremos os dois casos a seguir:

(i) Se $c = 0$, então $R = S$. Logo $u = 0$ ou $v = 0$.

(ii) Suponhamos $c > 0$. Por um argumento análogo ao da demonstração da proposição anterior, é possível mostrar que existem inteiros r e s tais que $y^r u, y^s v \in R$. Então $y^r u \cdot y^s v = y^{r+s}uv = 0$ o que implica que $y^r u = 0$ ou $y^s v = 0$. Se $y^r u = 0$ então $Y^r U \in (F)$. Sendo assim existe um polinômio A tal que

$$Y^r U = AF = A(X^aY^b + uY^{b+c} + G).$$

F não é divisível por Y, já que $c > 0$ e G não é divisível por Y. Logo A é divisível por Y^r. Então $U \in (F)$ e $u = 0$. Analogamente $v = 0$ se $y^s v = 0$.
Em ambos os casos $u = 0$ ou $v = 0$. Daí S é um domínio, (F) é um ideal primo logo F é irredutível. Estes resultados ainda são válidos se estendermos $\mathbb{F}$ a seu fecho algébrico. Logo F é absolutamente irredutível.

□

OBS.: Se $c = 0$ então $R = S$ e $\{x^\alpha y^\beta \mid \beta < b\}$ é também uma base da $\mathbb{F}$-álgebra R, por simetria.

Exemplo 4.2.5 *Vamos agora fazer uma generalização da proposição 4.2.3 para mais que duas variáveis no caso $c = 0$. Seja wdeg o grau pesado em $\mathbb{F}[X_1, ..., X_m]$, onde X_i tem peso $a_1...a_{i-1}b_i...b_{m-1}$. Seja I o ideal em $\mathbb{F}[X_1, ..., X_m]$ gerado por*

$$X_i^{a_i} + X_{i+1}^{b_i} + G_i \ \ para \ \ i = 1, ..., m-1$$

onde $G_i \in \mathbb{F}[X_1, ..., X_{i+1}]$, wdeg $(G_i) < a_1...a_ib_i...b_{m-1}$ e mdc$(a_i, b_j) = 1$ para todo $i \leq j$. Então o anel $R = \mathbb{F}[X_1, ..., X_m]/I$ possui a seguinte base

$$\{x^\alpha \mid \alpha \in \mathbb{N}_0^m, \alpha_i < a_i \ para \ todo \ i < m\}.$$

O anel R tem uma função peso ρ tal que

$$\rho(x_i) = a_1...a_{i-1}b_i...b_{m-1}.$$

Logo R é um domínio e o ideal I é primo.

Nosso próximo objetivo é definir códigos de avaliação e obter limitações para a distância mínima dos códigos duais através de função de ordem.

4.3 Códigos de Avaliação e seu duais

Nesta seção R será sempre uma $\mathbb{F}_q$-álgebra com função de ordem ρ e $(f_i \mid i \in \mathbb{N})$ será uma base de R sobre $\mathbb{F}_q$ com as seguintes propriedades:

- $\rho(f_i) < \rho(f_{i+1})$ para todo $i \in \mathbb{N}$.
- Para todo elemento não-nulo f em R existe j com $\rho(f) = \rho(f_j)$.

A existência de tal base foi provada pela proposição 4.1.8.
Considere L_l o espaço vetorial gerado por $f_1, ..., f_l$. Então para todo $0 \neq f \in R$ temos $\rho(f) = \rho(f_l)$, se e somente se, l é o menor inteiro tal que $f \in L_l$. Seja $l(i, j)$ o menor inteiro positivo l tal que $f_i f_j \in L_l$, então $l(i, j) < l(i+1, j)$ para todo $i, j \in \mathbb{N}$.

Vamos definir uma operação de multiplicação em $\mathbb{F}_q^n$ simplesmente fazendo a multiplicação coordenada a coordenada, isto é: $a*b := (a_1b_1, ..., a_nb_n)$

onde $a = (a_1, ..., a_n)$ e $b = (b_1, ..., b_n)$ são elementos em $\mathbb{F}_q^n$. O espaço vetorial $\mathbb{F}_q^n$ com a multiplicação $*$ é um anel comutativo com unidade $(1, ..., 1)$. Identificamos o subanel unitário $\{(\lambda, ..., \lambda) \mid \lambda \in \mathbb{F}_q\}$ com $\mathbb{F}_q$. Desta forma $\mathbb{F}_q^n$ é uma $\mathbb{F}_q$-álgebra.

Definição 4.6 *A aplicação*

$$\varphi : R \longrightarrow \mathbb{F}_q^n,$$

é chamada um morfismo de $\mathbb{F}_q$-álgebras se φ é $\mathbb{F}_q$-linear e vale que

$$\varphi(fg) = \varphi(f) * \varphi(g).$$

Para cada elemento f_i da base de R seja $h_i \in \mathbb{F}_q^n$ a imagem deste elemento pelo morfismo φ, isto é, $h_i = \varphi(f_i)$.

Definição 4.7 *Definimos o código de avaliação E_l e seu dual C_l por*

$$E_l = \varphi(L_l) =< h_1, ..., h_l >,$$

$$C_l = \{c \in \mathbb{F}_q^n \mid c \cdot h_i = 0 \ \textit{para todo} \ i \leq l\}.$$

A sequência de códigos $(E_l \mid l \in \mathbb{N})$ é crescente com respeito a inclusão. Como tais códigos são subespaços do espaço vetorial $\mathbb{F}_q^n$ que tem dimensão finita, logo existe um N tal que $E_l = E_N$ para todo $l \geq N$. O código E_N é a imagem de R por φ.

Consideraremos apenas os morfismos que são sobrejetivos. Então $E_l = \mathbb{F}_q^n$ e $C_l = 0$ para $l \geq N$.

Exemplo 4.3.1 *Seja $\mathcal{P}$ o conjunto formado por n pontos racionais distintos $P_1, ..., P_n$ de $\mathbb{F}_q^m$. Seja $R = \mathbb{F}_q[X_1, ..., X_m]$. Considere a seguinte função avaliação*

$$\begin{array}{rcccc} av_{\mathcal{P}} & : & R & \longrightarrow & \mathbb{F}_q^n \\ & & f & \longmapsto & (f(P_1), ..., f(P_n)) \end{array}$$

$av_{\mathcal{P}}$ assim definida é um morfismo de $\mathbb{F}_q$-álgebras de R em $\mathbb{F}_q^n$, já que $FG(P) = F(P)G(P)$ para todo par de polinômios F e G e para todo ponto racional $P \in \mathbb{F}_q^n$.

Lema 4.3.2 *A função $av_{\mathcal{P}}$ é sobrejetiva.*

Prova:

Seja $P_j = (x_{j1}, ..., x_{jm})$. Seja $A_{il} = \{x_{jl} \mid j = 1, ..., n\} \backslash \{x_{il}\}$ e seja G_i o polinômio dado por

$$G_i = \prod_{l=1}^{m} \prod_{x \in A_{il}} (X_l - x).$$

Então $G_i(P_j) = 0$ para todo $i \neq j$. Mais ainda, $G_i(P_i) \neq 0$ já que $P_1, ..., P_n$ foram escolhidos distintos. A imagem do polinômio $G_i/G_i(P_i)$ pelo morfismo $av_{\mathcal{P}}$ é o i-ésimo elemento da base canônica de $\mathbb{F}_q^n$. Logo $av_{\mathcal{P}}$ é sobrejetora.

□

Suponhamos que I seja um ideal do anel $\mathbb{F}_q[X_1, ..., X_m]$. Seja $\{P_1, ..., P_n\}$ o conjunto de zeros do ideal I com coordenadas em $\mathbb{F}_q$. Como $f(P_j) = 0$ para todo $f \in I$ e $j = 1, ..., n$, a função avaliação induz uma função linear no quociente $\mathbb{F}_q[X_1, ..., X_m]/I$ que está bem definida e também é um morfismo sobrejetivo de $\mathbb{F}_q$-álgebras.

4.4
Limitação da distância mínima de códigos duais

Como na seção anterior, seja R é uma $\mathbb{F}_q$-álgebra com função de ordem ρ. e $\{f_i \mid i \in \mathbb{N}\}$ uma base de R sobre $\mathbb{F}_q$ tal que $\rho(f_i) < \rho(f_{i+1})$ para todo $i \in \mathbb{N}$ e considere L_l o espaço vetorial com $f_1, ..., f_l$ como base.
O número $l(i, j)$ foi definido como o menor inteiro positivo tal que $f_i f_j \in L_l$. A função $l(i, j)$ é estritamente crescente em ambos os argumentos.

Seja $\varphi : R \longrightarrow \mathbb{F}_q^n$ um morfismo sobrejetivo de $\mathbb{F}_q$-álgebras e sejam $h_i = \varphi(f_i)$, $E_l = \varphi(L_l)$ e C_l seu dual como definidos anteriormente.
Sabemos que existe um inteiro positivo N tal que $E_l = \mathbb{F}_q^n$ para todo $l > N$. Então $C_l = 0$ para $l > N$.

Seja H a matriz $N \times n$ com h_i como sua i-ésima linha para $1 \leq i \leq N$.

Definição 4.8 *Seja $y \in \mathbb{F}_q^n$. Definimos as síndromes s_i e s_{ij} por*

$$s_i(y) = y \cdot h_i \ e \ s_{ij}(y) = y \cdot (h_i * h_j).$$

Dessa forma $S(y) = (s_{ij}(y) \mid 1 \leq i, j \leq N)$ é a matriz das síndromes de y.

Lema 4.4.1 *Sejam $y \in \mathbb{F}_q^n$ e $D(y)$ a matriz diagonal com y na diagonal principal. Então*

$$S(y) = HD(y)H^t$$

e

$$posto(S(y)) = w(y), \text{ onde } w \text{ é o peso em } \mathbb{F}_q^n.$$

Prova:

A matriz das síndromes $S(y)$ é igual a $HD(y)H^t$, pois

$$s_{ij}(y) = y \cdot (h_i * h_j) = \sum_l y_l h_{il} h_{jl},$$

onde h_{il} é a l-ésima entrada de h_i. O posto da matriz diagonal $D(y)$ é igual ao número de coordenadas diferentes de zero de y, que é por definição $w(y)$. As linhas de H geram $\mathbb{F}_q^n$, já que $E_N = \mathbb{F}_q^n$. Portanto ambas as matrizes H e H^t possuem posto n. Logo $posto(S(y)) = posto(D(y)) = w(y)$.

□

Definição 4.9 *Para cada $l \in \mathbb{N}$, definimos o conjunto N_l como segue:*

$$N_l = \{(i,j) \in \mathbb{N}^2 \mid l(i,j) = l+1\}.$$

e denotamos por ν_l a cardinalidade deste conjunto.

Lema 4.4.2 *1. Se $y \in C_l$ e $l(i,j) \leq l$, então $s_{ij}(y) = 0$.*

2. Se $y \in C_l \backslash C_{l+1}$ e $l(i,j) = l+1$, então $s_{ij}(y) \neq 0$.

Prova:

1. Seja $y \in C_l$. Se $l(i,j) \leq l$ então $f_i f_j \in L_l$. Daí, $h_i * h_j = \varphi(f_i f_j)$ é um elemento de $\varphi(L_l)$, que é o dual de C_l. Logo $s_{ij}(y) = y \cdot (h_i * h_j) = 0$.

2. Seja $y \in C_l \backslash C_{l+1}$. Se $l(i,j) = l+1$, então $f_i f_j \in L_{l+1} \backslash L_l$. Então $f_i f_j \equiv \mu f_{l+1}$ módulo L_l para algum $0 \neq \mu \in \mathbb{F}_q$. Logo $h_i * h_j \equiv \mu h_{l+1}$ módulo $\varphi(L_l)$. Mas $y \notin C_{l+1}$, então $s_{l+1}(y) \neq 0$. Portanto $s_{ij}(y) \neq 0$.

□

Lema 4.4.3 *Se $t = \nu_l$ e $(i_1, j_1), ..., (i_t, j_t)$ é uma enumeração de elementos de N_l em ordem crescente com respeito a ordem lexicográfica de $\mathbb{N}^2$, então $i_1 < ... < i_t$ e $j_t < ... < j_1$. Se, além disso, $y \in C_l \backslash C_{l+1}$, então*

$$s_{i_u j_v}(y) = \begin{cases} 0, & se \quad u < v \\ \neq 0, & se \quad u = v \end{cases}$$

Prova:

A sequência $(i_1, j_1), ..., (i_t, j_t)$ é ordenada da seguinte forma $i_1 \leq ... \leq i_t$ e $j_u < j_{u+1}$ se $i_u = i_{u+1}$. Se $i_u = i_{u+1}$ então $j_u < j_{u+1}$ e além disso,

$$l + 1 = l(i_u, j_v) < l(i_u, j_{u+1}) = l(i_{u+1}, j_{u+1}) = l + 1,$$

que é uma contradição. Logo a sequência $i_1, ..., i_t$ é estritamente crescente. Um argumento análogo mostra que $j_{u+1} < j_u$ para todo $u < t$.

Seja $y \in C_l$. Se $u < v$, então $l(i_u, j_v) < l(i_v, j_v) = l + 1$. Logo, pelo lema 4.4.2, temos $s_{i_u j_v}(y) = 0$.

Seja $y \notin C_{l+1}$. Se $u = v$, então $l(i_u, j_v) = l + 1$. Logo, pelo lema 4.4.2, temos $s_{i_u j_v}(y) \neq 0$.

□

Proposição 4.4.4 *Se $y \in C_l \backslash C_{l+1}$ então $w(y) \geq \nu_l$.*

Prova:

Segue imediatamente dos lema 4.4.3 e 4.4.1.

□

Definição 4.10

$$d(l) = min\{\nu_m \mid m \geq l\},$$

$$d_\varphi(l) = min\{\nu_m \mid m \geq l, C_m \neq C_{m+1}\}.$$

Os números $d(l)$ e $d_\varphi(l)$ serão chamados de ordem de limitação.

Se R é uma álgebra afim da forma $\mathbb{F}_q[X_1, ..., X_m]/I$ e φ uma função avaliação $av_{\mathcal{P}}$ do conjunto $\mathcal{P}$ de n pontos em $\mathbb{F}_q^m$, então denotaremos d_φ por $d_{\mathcal{P}}$.

Teorema 4.4.5 *Os números $d(l)$ e $d_\varphi(l)$ são limitações inferiores da distância mínima de C_l da seguinte maneira*

$$d(C_l) \geq d_\varphi(l) \geq d(l).$$

Prova:

Segue imediatamente da definição 4.10 e da proposição 4.4.4.

□

OBS.: O conjunto N_l e os números ν_l e $d(l)$ dependem somente da função de ordem ρ e não da escolha da base $\{f_i \mid i \in \mathbb{N}\}$ nem do conjunto de pontos. O número $d_{\mathcal{P}}$ depende da função de ordem e da escolha do conjunto de pontos, mas não da escolha da base.
Note que se $\mathcal{P} \subseteq \mathcal{P}'$, então $d_{\mathcal{P}} \geq d_{\mathcal{P}'}$.

Exemplo 4.4.6 *Sejam $R = \mathbb{F}_q[X]$ e ρ, tal que $\rho(f) = deg\,(f)$, a função de ordem do exemplo 4.1.5. Sejam $f_i = X^{i-1}$, α um elemento primitivo de $\mathbb{F}_q$, $n = q-1$ e $\varphi : R \longrightarrow \mathbb{F}_q^n$ definida por $\varphi(f) = (f(\alpha^0), f(\alpha^1), ..., f(\alpha^{n-1}))$. Então $C_l = \{c \in \mathbb{F}_q^n \mid c \cdot \varphi(f_i) = 0, 1 \leq i \leq l\}$, que é um código cíclico com respeito ao conjunto $\alpha^0, \alpha^1, ..., \alpha^{l-1}$. A ordem de limitação é dada por $d(l) = l + 1$.*

Exemplo 4.4.7 (Códigos de Reed-Muller.) *Sejam $R = \mathbb{F}_q[X_1, ..., X_m]$ e ρ a função de ordem associada à ordem lexicográfica especial para monômios de R. Seja f_i o i-ésimo monômio com respeito a essa ordem. Sejam $n = q^m$ e $P_1, ..., P_n$ uma enumeração de n pontos de $\mathbb{F}_q^m = \mathcal{P}$. Então o código de Reed-Muller $RM_q(r, m)$ é obtido avaliando todos os polinômios $f \in \mathbb{F}_q[X_1, ..., X_m]$ de grau no máximo r em todos pontos de $\mathcal{P}$. Se $f_l = {X_1}^r$, então $f_{l+1} = X_m^{r+1}$ e $\{f_i \mid i \leq l\}$ é o conjunto de todos os monômios de grau no máximo r. Então $RM_q(r, m) = av_{\mathcal{P}}(L_l) = E_l$.*

A distância mínima para códigos de Reed-Muller é bem conhecida e pode ser calculada com as ferramentes desenvolvidas acima, obtendo o seguinte teorema:

Teorema 4.4.8 *Sejam r e m dois inteiros positivos tais que $0 \leq r < (q-1)m$, então a distância mínima do código $RM_q(r, m)$ é igual a $(\mu + 1)q^\nu$ onde $\nu, \mu \in \mathbb{N}_0$ são tais que $(q-1)m - r = \nu(q-1) + \mu$ com $\mu < q-1$.*

4.5 Funções peso e semigrupos

Seja ρ uma função peso definida sobre uma $\mathbb{F}_q$-álgebra R. A condição $(O.5)$, vista anteriormente, implica que o subconjunto

$$\Lambda = \{\rho(f) \mid f \in R, f \neq 0\}$$

de inteiros não-negativos possui as seguintes propriedades

$$0 \in \Lambda \text{ e } x + y \in \Lambda, \forall x, y \in \Lambda.$$

Definição 4.11 *Um subconjunto Λ de $\mathbb{N}_0$ é chamado semigrupo se $0 \in \Lambda$ e $\forall x, y \in \Lambda$, $x + y \in \Lambda$.*

Elementos de $\mathbb{N} \backslash \Lambda$ são chamados *lacunas* de Λ e os elementos de Λ são chamados *não-lacunas* de Λ. Se todos os elementos de Λ são divisíveis por $d > 1$, então existem infinitas lacunas. O número de lacunas é denotado por $g = g(\Lambda)$.

Se $g < \infty$, então existe $n \in \mathbb{N}$ tal que se $x \in \mathbb{N}$ e $x \geq n$, então $x \in \Lambda$. O condutor de Λ é o menor $n \in \Lambda$ tal que $\{x \in \mathbb{N} \mid x \geq n\}$ está contido em Λ, denotado por $c = c(\Lambda)$. Então $c - 1$ é a maior lacuna de Λ se $g > 0$.

Exemplo 4.5.1 *Se ρ é uma função peso, então $\Lambda = \{\rho(f) \mid f \in R, f \neq 0$ é o semigrupo de ρ. Em particular, se $\rho = -v_P$ do exemplo 4.1.4, então Λ é o semigrupo de Weierstrass de P.*

Proposição 4.5.2 *Seja Λ um semigrupo com g lacunas e condutor c.*

1. *$g = 0 \Longleftrightarrow c = 0$.*
2. *Seja $g > 0$. Então $c \geq g + 1$, e $\Lambda = \{x \in \mathbb{N} \mid x \geq g + 1\} \cup \{0\} \Longleftrightarrow c = g + 1$.*
3. *Existe exatamente uma lacuna se, e somente se, 1 é a única lacuna.*
4. *Se 2 é uma não-lacuna, então $\{1, 3..., 2g - 1\}$ é o conjunto das lacunas. E ainda $c = 2g$.*

Definição 4.12 *Os elementos de um semigrupo Λ serão enumerados pela sequência $(\rho_l \mid l \in \mathbb{N})$ tal que $\rho_l < \rho_{l+1}$ para todo l. O número de lacunas menores que ρ_l será denotado por $g(l)$.*

Lema 4.5.3 *Seja Λ um semigrupo com finitas lacunas.*

1. *Se $l \in \mathbb{N}$ então $g(l) = \rho_l - l + 1$.*
2. *Se $l \in \mathbb{N}$ então $\rho_l \leq l + g - 1$ e a igualdade é válida se, e somente se, $\rho_l \geq c$.*
3. *Se $l > c - g$, então $\rho_l = l + g - 1$.*
4. *Se $l \leq c - g$, então $\rho_l < c - 1$.*

Prova:

1. A não lacuna ρ_l é o (ρ_l+1)-ésimo elemento de $\mathbb{N}$. Então ρ_l é o $(\rho_l+1-g(l))$-ésimo elemento do subgrupo Λ. Logo $l = \rho_l + 1 - g(l)$.
2. Claramente $g(l) \leq g$ e $g(l) = g \Longleftrightarrow \rho_l \geq c$.
3. O condutor c é o $(c + 1)$-ésimo elemento de $\mathbb{N}$. Todas as lacunas são estritamente menores que c. Então c é o $(c + 1 - g)$-ésimo elemento de Λ. Logo $c = \rho_{c+1-g}$. Seja $l > c - g$. Então $\rho_l \geq \rho_{c-g+1} = c$, o que implica que $\rho_l = l + g - 1$ pelo item 2.
4. Seja $l \leq c - g$. Então $\rho_l \leq l + g - 1 \leq c - 1$. Mas $c - 1$ é uma lacuna ou é negativo, logo $\rho_l < c - 1$.

□

No lema anterior usamos somente o fato de que $\{n \in \mathbb{N} \mid n \geq c\}$ está contido em Λ e $c - 1 \notin \Lambda$. Na próxima proposição usaremos que um semigrupo é fechado com relação à adição.

Proposição 4.5.4 *Suponhamos que o número de gaps é finito. Então vale*

$$c \leq 2g.$$

$c = 2g$ se, e somente se, para todo inteiro não-negativo s, se s é uma lacuna, então $c - 1 - s$ é uma não-lacuna.

Prova:

Consideremos um par de inteiros não-negativos (s, t) tal que $s + t = c - 1$. No mínimo um destes dois números é uma lacuna, já que $c - 1$ é uma lacuna e a soma de duas não-lacunas é uma não-lacuna. Mas existem c de tais pares, que implica no que queríamos.

A igualdade é válida se, e somente se, para todo par de inteiros não-negativos (s, t) com $s + t = c - 1$ exatamente um desses dois números é uma não-lacuna e o outro é uma lacuna. □

Exemplo 4.5.5 *O semigrupo da função peso de curvas planas definidas pela equação $X^aY^c + Y^{b+c} + g = 0$ como no proposição 4.2.3 é igual a*

$$< a, b > \backslash \{\alpha b + \beta a \,|\, \alpha, \beta \in \mathbb{N}_0, \alpha < a,\, c\alpha > (a-d)\beta\},$$

onde $< a, b >$ denota o semigrupo gerado por a e b,

$$< a, b >= \{ma + nb\,|m, n \in \mathbb{N}_0\}.$$

Lema 4.5.6 *Sejam Λ um semigrupo com finitas lacunas e $s \in \Lambda$. A cardinalidade de $\Lambda \backslash (s + \Lambda)$ é igual a s.*

Prova:

Seja c o condutor de Λ. Seja $T = \{t \in \mathbb{N} \mid t \geq s + c\}$. Então T está contido em Λ e em $s + \Lambda$. Seja $U = \{u \in \Lambda \mid u < s + c\}$. Então o número de elementos de U é igual a $s + c - g$ e Λ é a união disjunta de U e T. Seja $V = \{v \in s + \Lambda \mid s \leq v < s + c\}$. Então o número de elementos de V é igual a $c - g$ e $s + \Lambda$ é a união disjunta de V e T. Além disso $V \subseteq U$, já que $s \in \Lambda$ e Λ é um semigrupo. Logo

$$\#(\Lambda \setminus (s + \Lambda)) = \#U - \#V = (s + c - g) - (c - g) = s.$$

□

Lema 4.5.7 *Seja f um elemento não-nulo da $\mathbb{F}_q$-álgebra R com função peso ρ. Então*

$$dim\,(R/(f)) = \rho(f).$$

Prova:

Seja Λ o semigrupo da função peso ρ. Sejam $s = \rho(f)$ e $(\rho_i \mid i \in \mathbb{N})$ a sequência dos elementos de Λ com ordem crescente. A imagem por ρ do conjunto dos elementos não-nulos do ideal (f) é igual a $s + \Lambda$. Logo para todo $\rho_i \in \Lambda$ existe um $f_i \in R$ tal que $\rho(f_i) = \rho_i$. Se além disso $\rho_i \in s + \Lambda$, então podemos tomar $f_i \in (f)$. Os conjuntos $\{f_i \mid i \in \mathbb{N}\}$ e $\{f_i \mid i \in \mathbb{N}, \rho_i \in s + \Lambda\}$ são bases da álgebra R e do ideal (f) respectivamente. Logo as classes de f_i

módulo (f) com $i \in \mathbb{N}$ e $\rho_i \in \Lambda \setminus (s + \Lambda)$ formam uma base de $R/(f)$. Logo a dimensão de $R/(f)$ é igual ao número de elementos de $\Lambda \setminus (s + \Lambda)$, que é $\rho(f)$ pelo lema 4.5.6.

$\square$

Lema 4.5.8 *Seja R uma álgebra afim com função peso ρ e função avaliação av_P. Seja $0 \neq f \in R$. Então o número de zeros de f é no máximo $\rho(f)$.*

Prova:

Seja $\mathcal{Q}$ o conjunto de zeros de f e $t = |\mathcal{Q}|$. A função $av_Q : R \longrightarrow \mathbb{F}_q^t$ é linear e sobrejetiva pelo lema 4.3.2. Além disso $g(Q) = 0$ para todo $Q \in \mathcal{Q}$ e $g \in (f)$. Isto induz uma aplicação $av_{\mathcal{Q}} : R/(f) \longrightarrow {\mathbb{F}_q}^t$ que é linear e sobrejetiva. Então o número de zeros de f é no máximo a dimensão de $R/(f)$ que é igual a $\rho(f)$ pelo lema 4.5.7.

$\square$

Seja ρ uma função peso em $R = \mathbb{F}_q[X_1, ..., X_m]/I$. Seja $(\rho_i \mid i \in \mathbb{N})$ a enumeração de elementos do semigrupo de ρ em ordem crescente. Seja $\mathcal{P}$ um conjunto de n pontos distintos de ${\mathbb{F}_q}^m$ contido no conjunto dos zeros de I e seja $av_{\mathcal{P}} : R \longrightarrow \mathbb{F}_q^m$ a correspondente função de avaliação. O código de avaliação E_l é o que já definimos anteriormente. Então $E_l = \{av_{\mathcal{P}}(f) \mid f \in R, \rho(f) \leq \rho_l\}$.

Teorema 4.5.9 *A distância mínima de E_l é no mínimo $n - \rho_l$. Se $\rho_l < n$ então $dim\,(E_l) = l$.*

Prova:

Seja c um elemento não nulo de E_l. Então existe um elemento $0 \neq f \in R$ tal que $\rho(f) \leq \rho_l$ e $c = av_{\mathcal{P}}(f)$. Então $c_i = f(P_i)$ para todo i. O número de zeros de f é no máximo ρ_l pelo lema 4.5.8. Então $w(c) \geq n - \rho_l$.

Suponhamos além disso que $\rho_l < n$. E_l é a função de avaliação do espaço vetorial L_l de dimensão l. Se $f \in L_l$ e $av_{\mathcal{P}}(f) = 0$, então f tem no mínimo n zeros. Logo $f = 0$ pelo lema 4.5.8, já que $\rho_l < n$. Então a função $av_{\mathcal{P}} : L_l \longrightarrow E_l$ é um isomorfismo, logo $dim\, E_l = l$.

$\square$

Corolário 4.5.10 *Seja ρ uma função peso com g lacunas. Se $\rho_k < n$ então E_k é um $[n, k, d]$ código tal que $k + d \geq n + 1 - g$.*

Prova:

Segue imediatamente do teorema 4.5.9 e do fato de que $\rho_k \leq k + g - 1$ que foi mostrado em 4.5.3.

$\square$