3
Corpos de Funções Algébricas e Códigos de Goppa

Neste capítulo serão apresentados alguns resultados básicos da teoria de corpos de funções algébricas necessários para poder definir códigos de Goppa e estudar suas propriedades. Todos os resultados e demonstrações deste capítulo podem ser encontrados em (Sti). Algumas vezes a linguagem das curvas algébricas também será utilizada, assim estabeleceremos uma equivalência entre os corpos de funções e as curvas.

3.1
Corpos de Funções Algébricas

K denotará um corpo arbitrário.

Definição 3.1 *Seja $F \supseteq K$ uma extensão de K. Se F é uma extensão algébrica finita de $K(x)$, onde $x \in F$ é transcendente sobre K, dizemos que F/K é um corpo de funções algébricas de uma variável sobre K.*

Chamaremos F/K simplesmente de corpo de funções sobre K.

O conjunto $\tilde{K} = \{z \in F \mid z \text{ é algébrico sobre } K\}$ é um subcorpo de F, já que a soma, produto e inverso de elementos algébricos são também algébricos. $\tilde{K}$ é chamado o corpo de constantes de F/K. Podemos notar que $K \subseteq \tilde{K} \subseteq F$ e é facilmente verificado que $F/\tilde{K}$ é um corpo de funções sobre $\tilde{K}$. E ainda, se $\tilde{K} = K$, dizemos que K é algebricamente fechado em F.

Exemplo 3.1.1 *O exemplo mais simples de um corpo de funções algébricas é o chamado corpo de funções racionais F onde $F = K(x)$ com $x \in F$ transcendente sobre K. Todo elemento $z \in K(x)^*$ possui uma única representação do tipo:*

$$z = a \prod_i p_i(x)^{n_i} \tag{3-1}$$

onde $a \in K^*$, $p_i(x) \in K[x]$ são polinômios mônicos, distintos dois a dois e $n_i \in \mathbb{Z}$.

Um corpo de funções F/K sempre pode ser representado como uma extensão algébrica de um corpo de funções racionais $K(x)$, isto é, $F = K(x, y)$ onde $\phi(y) = 0$ para algum polinômio irredutível $\phi(T) \in K(x)[T]$.

Se F/K não é um corpo de funções racionais, não é fácil encontrar a decomposição em irredutíveis como em 3-1. Outro problema que temos com a representação de um elemento de um corpo qualquer é: tomando $\alpha_1, \alpha_2, ..., \alpha_n \in K$, encontrar todas as funções racionais $f(x) \in K(x)$, tais que $\alpha_1, \alpha_2, ..., \alpha_n$ sejam seus zeros ou polos. A fim de solucionar tais problemas, introduziremos a noção de *anéis de valorização* e *lugares*.

Definição 3.2 *Um anel de valorização O de um corpo de funções F/K é um anel $O \subseteq F$ satisfazendo as seguintes propriedades:*

(1) $K \subsetneqq O \subsetneqq F$, *e*

(2) *se $z \in F$, então $z \in O$ ou $z^{-1} \in O$.*

Exemplo 3.1.2 *Consideremos novamente o corpo de funções racionais $K(x)/K$. Dado um elemento irredutível $p(x) \in K[x]$ tomemos o seguinte conjunto:*

$$O_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}.$$

$O_{p(x)}$ assim definido é um anel de valorização, pois temos:

(1) *Claramente $K \subsetneqq O_{p(x)} \subsetneqq K(x)$.*

(2) *Seja $h(x) \in K(x)$ tal que $h(x) = \dfrac{t(x)}{s(x)}$, onde $t(x), s(x) \in K[x]$ e $s(x) \neq 0$. Suponhamos, sem perda de generalidade, que $t(x)$ e $s(x)$ não possuem fatores em comum. Assim:*

(a) *Se $p(x) \nmid s(x)$ então $h(x) \in O_{p(x)}$.*

(b) *Se $p(x) \mid s(x)$ então $s(x) = p(x)^a q(x)$ onde $q(x) \in K[x]$ e $a \in \mathbb{N}$ e logo $h(x)^{-1} = \dfrac{p(x)^a q(x)}{t(x)}$, e segue-se do fato que $t(x)$ e $s(x)$ não possuem fatores em comum e da hipótese que $p(x) \mid s(x)$, que $p(x) \nmid t(x)$. Portanto, $h(x)^{-1} \in O_{p(x)}$.*

Note que se $q(x)$ é um elemento irredutível diferente de $p(x)$, então temos que $O_{p(x)} \neq O_{q(x)}$.

Vejamos agora um outro anel de valorização de $K(x)/K$:

$$O_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], deg\, f(x) \leq deg\, g(x) \right\}.$$

Neste caso teremos o seguinte ideal maximal:

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], deg\, f(x) < deg\, g(x) \right\}.$$

O lugar P_∞ é chamado lugar no infinito de $K(x)$.

Note que todos esses anéis e ideais dependem do elemento gerador x de $K(x)/K$. Por exemplo, $K(x) = K(1/x)$, e o lugar infinito relacionado a $1/x$ é o lugar P_0 relacionado a x.

De fato, pode-se mostrar que os únicos lugares do corpo de funções racionais são $P_{p(x)}$ e P_∞ definidos acima.

A seguir enumeraremos algumas propriedades dos corpos de funções (as demonstrações podem ser encontradas em (Sti)).

Proposição 3.1.3 *Seja O um anel de valorização de um corpo de funções F/K. Então:*

(a) *O é um anel local, isto é, O possui um único ideal maximal $P = O \setminus O^*$, onde $O^* = \{z \in O \mid$ existe $w \in O$ com $zw = 1\}$ é o grupo das unidades de O.*

(b) *$\tilde{K} \subseteq O$ e $\tilde{K} \cap P = \{0\}$.*

Lema 3.1.4 *Sejam O um anel de valorização de um corpo de funções F/K, P seu ideal maximal e $0 \neq x \in P$. Sejam $x_1, x_2, ..., x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$ para $i = 1, ..., n-1$. Então $n \leq [F : K(x)] \leq \infty$.*

Teorema 3.1.5 *Seja O um anel de valorização de um corpo de funções F/K e P seu único ideal maximal. Então*

(a) *P é um ideal principal;*

(b) *Se $P = tO$ então, para todo $0 \neq z \in F$, z possui uma única representação da forma $z = t^n u$ para $n \in \mathbb{Z}$ e $u \in O^*$;*

(c) *O é um domínio de ideais principais. Mais precisamente, se $P = tO$ e $\{0\} \neq I \subseteq O$ é um ideal, então $I = t^n O$ para algum $n \in \mathbb{N}$.*

Definição 3.3 *Um anel que possui as propriedades acima é chamado de anel de valorização discreta.*

Definição 3.4 *Sejam O um anel de valorização do corpo de funções F/K e P seu ideal maximal. Diremos que o ideal P é um lugar de F/K. Um elemento $t \in P$ tal que $P = tO$ é chamado um elemento primo de P, ou parâmetro local em P.*

Denotaremos por $\mathbb{P}_F$ o conjunto de todos os lugares da extensão F/K.

Se O é um anel de valorização de F/K e P seu ideal maximal então, para $0 \neq x \in F$, temos que $x \in P$, se e somente se, $x^{-1} \notin O$. Daí podemos concluir que O é unicamente determinado por P, isto é, $O = \{z \in F \mid z^{-1} \notin P\}$. Chamaremos $O_P = O$ de anel de valorização do lugar P.

Uma segunda definição de lugar será dada através de valorizações.

Definição 3.5 *Seja F/K um corpo de funções. Dizemos que a função $v : F \to \mathbb{Z} \cup \{\infty\}$ é uma valorização discreta de F/K se satisfaz as seguintes propriedades:*

(1) $x \in F$ *e* $v(x) = \infty \Leftrightarrow x = 0$.

(2) $v(xy) = v(x) + v(y)$ *para todo* $x, y \in F$.

(3) $v(x + y) \geq min\{v(x), v(y)\}$ *para todo* $x, y \in F$.

(4) *Existe um elemento* $z \in F$ *com* $v(z) = 1$.

(5) $v(a) = 0$ *para todo* $0 \neq a \in K$.

Neste contexto, o símbolo ∞ significa um elemento que não pertence a $\mathbb{Z}$ tal que $\infty + \infty = \infty + n = n + \infty = \infty$ e $\infty > m$ para todo $m, n \in \mathbb{Z}$.

Pelas condições (2) e (4) segue imediatamente que $v : F \to \mathbb{Z} \cup \{\infty\}$ é sobrejetiva. A condição (3) é chamada de desigualdade triangular.
Das propriedades de uma valorização segue que se $x, y \in F$ e $v(x) \neq v(y)$, então $v(x + y) = min\{v(x), v(y)\}$.

Definição 3.6 *Sejam $P \in \mathbb{P}_F$ e t um elemento primo de P. Definamos a função $v_P : F \to \mathbb{Z} \cup \{\infty\}$ tal que $v_P(0) = \infty$ e para todo $z \in F^*$ $v_P(z) = n$, onde temos $z = t^n u$ com $u \in {O_P}^*$ e $n \in \mathbb{Z}$.*

Podemos observar que esta definição depende apenas de P, e não da escolha do parâmetro local t.

Teorema 3.1.6 *Seja F/K um corpo de funções.*

(a) *Para todo lugar $P \in \mathbb{P}_F$, a função definida acima é uma valorização discreta de F/K. Além disso,*

$$O_P = \{z \in F \mid v_P(z) \geq 0\}$$

$$O_P^* = \{z \in F \mid v_P(z) = 0\}$$

$$P = \{z \in F \mid v_P(z) > 0\}.$$

Um elemento $x \in F$ é um elemento primo ou um parâmetro local em P se, e somente se, $v_P(x) = 1$.

(b) *Seja v uma valorização discreta de F/K. Então $P = \{z \in F \mid v(z) > 0\}$ é um lugar de F/K e $O_P = \{z \in F \mid v(z) \geq 0\}$ é seu correspondente anel de valorização.*

(c) *Todo anel de valorização O de F/K é um subanel maximal próprio de F.*

De acordo com o teorema que acabamos de demonstrar, lugares e valorizações são essencialmente a mesma coisa.

Sejam P um lugar de F/K e O_P seu anel de valorização. Como P é um ideal maximal, O_P/P é um corpo. Para $x \in O_P$ definimos $x(P) \in O_P/P$ como a classe residual de x módulo P. Para $x \in F \setminus O_P$ diremos que $x(P) := \infty$. Pela proposição 3.1.3 sabemos que $K \subseteq O_P$ e $K \cap P = \{0\}$, logo $O_P \longrightarrow O_P/P$ induz uma aplicação quociente de K em O_P. Portanto, daqui por diante, sempre consideraremos K como um subcorpo de O_P/P, via esta imersão. Podemos notar que o mesmo argumento é válido para $\tilde{K}$, logo também podemos considerar $\tilde{K}$ como um subcorpo de O_P/P.

Definição 3.7 *Seja $P \in \mathbb{P}_F$.*

(a) *Dizemos que $F_P := O_P/P$ é o corpo da classe residual de P. E a aplicação*

$$F \longrightarrow F_P \cup \{\infty\}$$

$$x \longmapsto x(P)$$

é chamada a aplicação quociente com relação a P. Também poderemos usar a seguinte notação: $x + P = x(P)$ para $x \in O_P$.

(b) $deg\, P := [F_P : K]$ *é chamado o grau de* P *e pode se mostrar que* $deg\, P \leq [F : K(x)] < \infty$.

Definição 3.8 *Seja* $z \in F$ *e* $P \in \mathbb{P}_F$. *Diremos que* P *é um zero de* z *se, e somente se,* $v_P(z) > 0$ *e que* P *é um pólo de* z *se, e somente se,* $v_P(z) < 0$. *E ainda, se* $v_P(z) = m > 0$, P *é um zero de* z *de ordem* m; *e se* $v_P(z) = -m < 0$, P *é um pólo de ordem* m.

O seguinte teorema nos dá como corolário que todo elemento $z \in F$ transcendente sobre K possui pelo menos um zero e um pólo. Em particular $\mathbb{P}_F \neq \emptyset$. Mais ainda, possui o mesmo número de zeros e pólos, e esse número é finito.

Teorema 3.1.7 *Sejam* F/K *um corpo de funções e* R *um subanel de* F, *tal que* $K \subseteq R \subseteq F$. *Suponha que* $0 \neq I \subsetneq R$ *é um ideal próprio de* R. *Então existe um lugar* $P \in \mathbb{P}_F$ *tal que* $I \subseteq P$ *e* $R \subseteq O_P$.

Já vimos que o corpo de constantes $\tilde{K}$ de um corpo de funções algébricas F/K é uma extensão finita sobre K e $F/\tilde{K}$ é um corpo de funções sobre $\tilde{K}$.

A partir de agora, F/K denotará sempre um corpo de funções algébricas de uma variável, onde K é um corpo algebricamente fechado em F, isto é, $\tilde{K} = K$.

Definição 3.9 *O grupo dos divisores de* F/K *é o grupo abeliano livre gerado pelos lugares de* F/K *e será denotado por* $\mathcal{D}_F$. *Os elementos de* $\mathcal{D}_F$ *são chamados divisores de* F/K. *Em outras palavras, um divisor* $D \in \mathcal{D}_F$ *é uma soma formal*

$$D = \sum_{P \in \mathbb{P}_F} n_P P,$$

onde $n_P \in \mathbb{Z}$ *e quase todos* n_P *são nulos.*

O *suporte* de D é definido por

$$supp\, D := \{P \in \mathbb{P}_F \mid n_P \neq 0\}.$$

No conjunto $\mathcal{D}_F$ podemos definir uma operação de soma como segue: dados $D = \sum n_P P$ e $D' = \sum n_P{}' P$ dois divisores em $\mathcal{D}_F$, definimos

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n_P{}')P.$$

O *elemento neutro* do grupo de divisores $\mathcal{D}_F$ é o seguinte divisor

$$0 = \sum_{P \in \mathbb{P}_F} n_P P, \text{ onde todos } n_P = 0.$$

Para $Q \in \mathbb{P}_F$ e $D = \sum n_P P \in \mathcal{D}_F$, definimos $v_Q(D) := n_Q$, consequentemente temos

$$supp\, D := \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\}$$

e

$$D = \sum_{P \in supp\, D} v_P(D) P.$$

Existe uma relação de ordem parcial em $\mathcal{D}_F$, definida por

$$D_1 \leq D_2 \Longleftrightarrow v_P(D_1) \leq v_P(D_2), \quad \forall P \in \mathbb{P}_F.$$

Um divisor $D \geq 0$ é dito *positivo*.

O *grau* de um divisor é definido por

$$deg\, D = \sum_{P \in \mathbb{P}_F} v_P(D) \cdot deg\, P$$

e na verdade $deg : \mathcal{D}_F \longrightarrow \mathbb{Z}$ é um homomorfismo.

Como já dizemos anteriormente, todo elemento $x \in F^*$ tem um número finito de pólos e zeros em $\mathbb{P}_F$, então podemos definir o que se segue.

Definição 3.10 *Sejam $0 \neq x \in F$, Z o conjunto de zeros de x em $\mathbb{P}_F$ e N o conjunto de pólos de x em $\mathbb{P}_F$. Então*

$$(x)_0 := \sum_{P \in Z} v_P(x) P \quad \textit{é chamado o divisor de zeros de } x,$$

$$(x)_\infty := \sum_{P \in N} (-v_P(x)) P \quad \textit{é chamado o divisor de pólos de } x$$

e finalmente

$$(x) := (x)_0 - (x)_\infty \quad \textit{é o divisor principal de } x.$$

É claro que $(x)_0$ e $(x)_\infty$ são divisores positivos pela própria definição e temos que

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P. \tag{3-2}$$

Os elementos de K podem ser caracterizados pela seguinte propriedade, já que K é algebricamente fechado em F

$$x \in K \Longleftrightarrow (x) = 0.$$

Definição 3.11 *O grupo*

$$\mathcal{P}_F := \{(x) \mid 0 \neq x \in F\}$$

é chamado o grupo dos divisores principais de F/K.

Note que $\mathcal{P}_F$ é um subgrupo de $\mathcal{D}_F$, já que se $x, y \in F$ e $x \neq 0$, $y \neq 0$ então $(xy) = (x) + (y)$ pela equação 3-2 e pelas propriedades de valorização.

Definição 3.12 *O grupo quociente $\mathcal{C}_F := \mathcal{D}_F/\mathcal{P}_F$ é chamado o grupo das classes dos divisores.*

A imagem de um divisor $D \in \mathcal{D}_F$ no grupo quociente será denotada por $[D]$. $[D]$ será chamada a classe do divisor D.

Definição 3.13 *Dizemos que $D, D' \in \mathcal{D}_F$ são equivalentes, ou seja, $D \sim D'$, se $[D] = [D']$. Logo $D = D' + (x)$ para algum $x \in F\backslash\{0\}$. Esta é um relação de equivalência, que pode ser verificada facilmente.*

Para cada divisor $A \in \mathcal{D}_F$, podemos considerar o conjunto $\mathcal{L}(A)$ dado por

$$\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\}.$$

Temos que $x \in \mathcal{L}(A)$ se, e somente se, $v_P(x) \geq -v_P(A)$, para todo $P \in \mathbb{P}_F$. Os elementos de $\mathcal{L}(A)$ podem ser caracterizados em termos dos zeros e dos pólos de A, mais precisamente, se

$$A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$$

com $n_i > 0, m_j > 0$ então $\mathcal{L}(A)$ consiste dos elementos $x \in F$ tais que

1. x tem zeros de ordem $\geq m_j$ em Q_j para $j = 1, ..., s$ e
2. x pode ter pólos somente nos lugares $P_1, ..., P_r$, onde a ordem dos pólos em P_i é limitada por n_i, para $i = 1, ..., r$.

Estes conjuntos $\mathcal{L}(A)$ são K-espaços vetorias e temos que se A' é divisor equivalente a A então $\mathcal{L}(A) \simeq \mathcal{L}(A')$ (são isomorfos como K-espaço vetoriais). De fato, se $A = A' + (z)$ com $z \in F^*$, o isomorfismo está dado por:

$$\begin{array}{rccc} \varphi & : & \mathcal{L}(A) & \longrightarrow & F \\ & & x & \longmapsto & xz \end{array}$$

Note que esta é uma função K-linear, cuja imagem está contida em $\mathcal{L}(A')$.

Outras propriedades dos espaços $\mathcal{L}(A)$ são:

1. $\mathcal{L}(A) \neq \{0\}$ se, e somente se, existe um divisor $A' \sim A$ com $A' \geq 0$.
2. $\mathcal{L}(0) = K$.
3. Se $A < 0$ então $\mathcal{L}(A) = \{0\}$.
4. Se A, B são dois divisores de F/K tais que $A \leq B$, então $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ e $dim\,(\mathcal{L}(B)/\mathcal{L}(A)) \leq deg\, B - deg\, A$.

O nosso objetivo é mostrar que $\mathcal{L}(A)$ é um espaço vetorial de dimensão finita para todo $A \in \mathcal{D}_F$.

Dado qualquer divisor $A \in \mathcal{D}_F$, sempre podemos escrevé-lo como $A = A_+ - A_-$, onde A_+ e A_- são divisores positivos.

Proposição 3.1.8 *Com a notação anterior temos que para todo divisor $A \in \mathcal{D}_F$, $\mathcal{L}(A)$ é um espaço vetorial de dimensão finita sobre K. Mais precisamente,*

$$dim\, \mathcal{L}(A) \leq 1 + deg\, A_+.$$

Definição 3.14 *Para todo divisor $A \in \mathcal{D}_F$, o inteiro $dim\, A := dim\, \mathcal{L}(A)$ é chamado a dimensão do divisor A.*

Um dos problemas mais importantes na teoria de corpos de funções algébricas é calcular a dimensão de um divisor (conhecer a dimensão será essencial para calcular os parâmetros de um código de Goppa que definiremos posteriormente). A próxima seção nos dará ferramentas extremamente importantes para tal cálculo, entre elas está o Teorema de Riemann-Roch.

Teorema 3.1.9 *Todo divisor principal possui grau 0. Mais precisamente, se $x \in F/K$, $(x)_0$ o divisor dos zeros de x e $(x)_\infty$ o divisor dos pólos de x, então*

$$deg\,(x)_0 = deg\,(x)_\infty = [F : K(x)].$$

A prova do teorema pode ser encontrada em (Sti).

O seguinte corolário, nos permite caracterizar divisores principais:

Corolário 3.1.10 *Valem as propriedades:*

1. *Sejam A e A' divisores tais que $A \sim A'$. Então $dim\, A = dim\, A'$ e $deg\, A = deg\, A'$.*
2. *Se $deg\, A < 0$ então $dim\, A = 0$.*
3. *Para um divisor A de grau 0 as seguintes afirmações são equivalentes:*
   (a) *A é principal;*
   (b) *$dim\, A \geq 1$;*
   (c) *$dim\, A = 1$.*

Exemplo 3.1.11 *Mais uma vez vamos considerar o corpo de funções racionais $F = K(x)$. Para $z \in K(x)$ temos $z = a \cdot f(x)/g(x)$ com $a \in K\backslash\{0\}$, $f(x), g(x) \in K[x]$ polinômios mônicos e primos entre si.*

Sejam

$$f(x) = \prod_{i=1}^{n} p_i(x)^{n_i}$$

e

$$g(x) = \prod_{j=1}^{s} q_j(x)^{m_j}$$

onde $p_i(x), q_j(x) \in K[x]$ são polinômios mônicos irredutíveis e distintos dois a dois. Logo o divisor principal em $\mathcal{D}_{K(x)}$ é da seguinte forma

$$(z) = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (deg\, g - deg\, f) P_\infty,$$

onde P_i, Q_j são os lugares correspondentes a $p_i(x)$ e $q_j(x)$ respectivamente.

Da proposição 3.1.8 temos que

$$dim\, A \leq 1 + deg\, A \quad \text{para todo divisor } A \geq 0. \tag{3-3}$$

Na verdade a equação 3-3 vale para divisores de grau ≥ 0. De fato, se $dim\, A > 0$, existe $A' \geq 0$ tal que $A \sim A'$. Logo, pelo corolário 3.1.10 temos:

$$dim\, A = dim\, A' \leq 1 + deg\, A' = 1 + deg\, A.$$

Como veremos na próxima seção, para poder calcular os parâmetros de um código de Goppa, será necessário calcular a dimensão de alguns divisores.

Existe uma relação entre o grau e a dimensão do divisor, esta relação está dada pelo teorema de Riemann-Roch. Para poder enunciá-lo precisaremos introduzir alguns conceitos, entre eles o gênero de um corpo de funções.

Proposição 3.1.12 *Existe $\gamma \in \mathbb{Z}$ tal que, para todo divisor $A \in \mathcal{D}_F$, temos o seguinte:*

$$deg\, A - dim\, A \leq \gamma.$$

Note que γ depende somente de F/K e não de A.

Definição 3.15 *Definimos o gênero g de F/K por*

$$g = max\{deg\, A - dim\, A + 1 \mid A \in \mathcal{D}_F\}.$$

Observe que esta definição faz sentido pela proposição 3.1.12.
Para qualquer corpo de funções F/K, o gênero é um inteiro não-negativo.

Um primeiro passo na direção do teorema de Riemann-Roch é o seguinte teorema:

Teorema 3.1.13 (Riemann) *Seja F/K um corpo de funções de gênero g.*

1. *Para $A \in \mathcal{D}_F$, temos*

$$dim\, A \geq deg\, A + 1 - g.$$

2. *Existe um inteiro c, dependendo de F/K, tal que*

$$dim\, A = deg\, A + 1 - g$$

sempre que $deg\, A \geq c$.

Exemplo 3.1.14 *Vamos mostrar que o corpo de funções racionais $K(x)/K$ possui $g = 0$.*

Seja P_∞ o divisor do pólo de x e considere o espaço vetorial $\mathcal{L}(rP_\infty)$ para $r \geq 0$. Claramente $1, x, ..., x^r$ pertencem a $\mathcal{L}(rP_\infty)$, portanto para r suficientemente grande devemos ter:

$$r + 1 \leq dim\,(rP_\infty) = deg\,(rP_\infty) + 1 - g = r + 1 - g.$$

Logo $g \leq 0$.

Como $g \geq 0$ para todo corpo de funções, temos o que queríamos.

Em geral é difícil determinar o gênero de um corpo de funções, mas foge ao nosso objetivo discutir tal problema.

Definição 3.16 *Seja F/K um corpo de funções de gênero g. Para cada divisor A de F, definimos o índice de especialidade $i(A)$ de A como segue:*

$$i(A) = dim\, A - deg\, A + g - 1.$$

O teorema de Riemann 3.1.13 nos diz que $i(A)$ é um inteiro não-negativo e que $i(A) = 0$ se $deg\, A$ é suficientemente grande.

Para chegarmos ao teorema de Riemann-Roch ainda temos que definir a noção de divisor canônico, isto é feito utilizando diferenciais de Weil, mas aqui vamos tentar simplificar a sua definição.

Definição 3.17 *Um divisor W é chamado de divisor canônico se, e somente se, vale que $deg\, W = 2g - 2$ e $dim\, W \geq g$.*

Agora já podemos enunciar o teorema.

Teorema 3.1.15 (Riemann-Roch) *Seja W um divisor canônico de F/K. Então, para todo $A \in \mathcal{D}_F$,*

$$dim\, A = deg\, A + 1 - g + dim\, (W - A).$$

Corolário 3.1.16 *Para um divisor canônico W temos*

$$deg\, W = 2g - 2 \;\; e \;\; dim\, W = g.$$

Pelo teorema de Riemann $i(A) = 0$ se $deg\, A \geq c$ para c uma constante. Vamos agora dar uma descrição precisa dessa constante.

Teorema 3.1.17 *Se A é um divisor de F/K de grau $\geq 2g - 1$ então*

$$dim\, A = deg\, A + 1 - g.$$

Podemos observar que a limitação $2g - 1$ neste teorema é a melhor possível e ainda para um divisor canônico W

$$dim\, W > deg\, W + 1 - g.$$

3.2
Curvas Algébricas versus Corpos de Funções

Como vimos, toda curva algébrica projetiva irredutível não-singular $\mathcal{C}$ definida sobre $\mathbb{F}_q$ tem associado, de um modo natural, um corpo de funções $\mathbb{F}_q(\mathcal{C})$. Começando com um corpo de funções $F/\mathbb{F}_q$, queremos associar uma curva. Para isto escolhemos um elemento transcendente $x \in F$ sobre $\mathbb{F}_q$. Como $F/\mathbb{F}_q(x)$ é uma extensão finita, então existe um elemento $y \in F$ tal que $F = \mathbb{F}_q(x, y)$ e seja $g(X, Y) \in \mathbb{F}_q[X, Y]$ um polinômio irredutível com $g(x, y) = 0$. Associamos a $F/\mathbb{F}_q$ o modelo não-singular da curva projetiva definida pela homogenização do polinômio g.

Teorema 3.2.1 *Seja $\mathcal{C}$ definida sobre $\mathbb{F}_q$ uma curva algébrica projetiva irredutível não-singular e seja F seu corpo de funções, então existe uma correspondência 1-1 entre os pontos $P \in \mathcal{C}$ e os lugares de $F/\mathbb{F}_q$ dada por:*

$$P \mapsto M_P$$

onde M_p é o ideal maximal do anel local da curva $\mathcal{C}$ em P.

3.3
Códigos Geométricos de Goppa

Vamos definir RS-códigos sobre $\mathbb{F}_q$ e depois faremos sua generalização, obtendo assim os códigos geométricos de Goppa.

Sejam $n = q-1$ e $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, isto é, $\mathbb{F}_q^* = \{\beta, \beta^2, ..., \beta^n = 1\}$. Seja $k \in \mathbb{Z}$ tal que $1 \leq k \leq n$ e consideremos o seguinte espaço vetorial de dimensão k:

$$\mathcal{L}_k = \{f \in \mathbb{F}_q[X] \mid deg\, f \leq k-1\}$$

e a aplicação de avaliação (a mesma aplicação estudada em 2-1), ou seja, $av : \mathcal{L}_k \longrightarrow \mathbb{F}_q^n$ dada por

$$av(f) = (f(\beta), f(\beta^2), ..., f(\beta^n)). \tag{3-4}$$

Essa é uma aplicação injetiva já que $deg\, f < n$. Agora podemos definir um código de Reed-Solomon sobre $\mathbb{F}_q$, que é um $[n, k]$-código tal que

$$C_k = \{(f(\beta), f(\beta^2), ..., f(\beta^n)) \mid f \in \mathcal{L}_k\}.$$

Neste caso, o peso de $0 \neq c = av(f) \in C_k$ é dado por

$$\begin{aligned} w(c) &= n - |\{i \in \{1, ..., n\}; f(\beta^i) = 0\}| \\ &\geq n - deg\, f \\ &\geq n - (k-1) \\ &\geq n - k + 1. \end{aligned}$$

Portanto a distância mínima d de C_k satisfaz

$$d \geq n - k + 1.$$

Por outro lado a proposição 2.1.7 nos diz que $d \leq n-k+1$. Logo $d = n-k+1$ para RS-códigos, o que implica que RS-códigos são MDS-códigos sobre $\mathbb{F}_q$.

Vamos fixar algumas notações:

$F/\mathbb{F}_q$ é um corpo de funções de gênero g.
$P_1, ..., P_n$ são pares distintos de lugares de $F/\mathbb{F}_q$ de grau 1.
$D = P_1 + \cdots + P_n$.
G é um divisor de $F/\mathbb{F}_q$ tal que $supp\, G \cap supp\, D = \emptyset$.

Definição 3.18 *O código geométrico de Goppa $C_{\mathcal{L}}(D, G)$ associado aos divisores D e G é definido por*

$$C_{\mathcal{L}}(D, G) = \{(x(P_1), ..., x(P_n)) \mid x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Note que esta definição faz sentido, pois se $x \in \mathcal{L}(G)$ e $supp\, G \cap supp\, D = \emptyset$, temos $v_{P_i}(x) \geq 0$. A classe residual $x(P_i)$ de x modulo P_i é um elemento do corpo quociente de P_i. Como $deg\, P_i = 1$, o corpo quociente é $\mathbb{F}_q$, logo $x(P_i) \in \mathbb{F}_q$.

Como em 2-1, podemos considerar uma função de avaliação

$$av_D(x) : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$$

dada por

$$av_D(x) = (x(P_1), ..., x(P_n)) \in \mathbb{F}_q^n.$$

Esta função de avaliação é $\mathbb{F}_q$-linear, e $C_{\mathcal{L}}(D,G)$ é a imagem de $\mathcal{L}(G)$ por esta função. A analogia com o RS-código é óbvia. Na verdade, tomando um corpo de funções $F/\mathbb{F}_q$ e divisores D e G, RS-códigos são facilmente vistos como um caso especial dos códigos geométricos de Goppa. Na verdade, a definição 3.18 é uma forma complicada de definir certos subespaços de $\mathbb{F}_q^n$.

O próximo teorema mostrará porque tais códigos são interessantes, pois pode-se calcular, ou no mínimo estimar, seus parâmetros n, k e d através do teorema de Riemann-Roch e obter uma limitação inferior para suas distâncias mínimas em uma situação geral.

Teorema 3.3.1 *$C_{\mathcal{L}}(D,G)$ é um $[n,k,d]$-código onde*

$$k = dim\, G - dim\,(G - D)$$

e

$$d \geq n - deg\, G.$$

Prova:

Tome a aplicação de avaliação

$$\begin{array}{rccc} av_D & : & \mathcal{L}(G) & \longrightarrow & C_{\mathcal{L}}(D,G) \\ & & x & \longmapsto & (x(P_1),...,x(P_n)) \end{array}$$

Claramente av_D é sobrejetora e o núcleo de av_D é dado por

$$\begin{aligned} Ker(av_D) &= \{x \in \mathcal{L}(G) \mid (x(P_1),...,x(P_n)) = (0,...,0)\} \\ &= \{x \in \mathcal{L}(G) \mid v_{P_i}(x) > 0 \ para\ i = 1,...,n\} \\ &= \mathcal{L}(G - D). \end{aligned}$$

Segue-se que $k = dim\, C_{\mathcal{L}}(D,G) = dim\, G - dim\,(G - D)$. Suponhamos que $C_{\mathcal{L}}(D,G) \neq 0$, do contrário não faria sentido falar em d. Seja $x \in \mathcal{L}(G)$ com $w(av_D(x)) = d$. Note que existem $n - d$ lugares $P_{i_1},...,P_{i_{n-d}} \in supp\, D$ que são zeros de x, então

$$0 \neq x \in \mathcal{L}(G - (P_{i_1} + ... + P_{i_{n-d}})).$$

Pelo corolário 3.1.10 temos

$$0 \leq deg\,(G - P_{i_1} + ... + P_{i_{n-d}}) \;=\; deg\, G - deg\,(P_{i_1} + ... + P_{i_{n-d}})$$

$$\begin{aligned} &= deg\, G - (n-d) \\ &= deg\, G - n + d. \end{aligned}$$

Portanto $d \geq n - deg\, G$.

□

Corolário 3.3.2 *Se $deg\, G < n$ então é injetiva a aplicação de avaliação $av_D : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D,G)$ é e ainda:*

1. *$C_{\mathcal{L}}(D,G)$ é $[n,k,d]$-código com $k = dim\, G \geq deg\, G + 1 - g$ e $d \geq n - deg\, G$. Portanto, $k + d \geq n + 1 - g$.*
2. *Se, além disso, $2g - 2 < deg\, G < n$ então $k = deg\, G + 1 - g$.*
3. *Se $\{x_1, ..., x_k\}$ é uma base de $\mathcal{L}(G)$ então a matriz*

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{pmatrix}$$

é uma matriz geradora de $C_{\mathcal{L}}(D,G)$.

Prova:

Como $deg\,(G-D) = deg\, G - n < 0$ então $\mathcal{L}(G-D) = 0$. Como $\mathcal{L}(G-D)$ é o núcleo de av_D temos que av_D é injetiva.

1. Pelo teorema 3.3.1 temos $k = dim\, G - dim\,(G-D) = dim\, G$,
   pois $\mathcal{L}(G-D) = 0$. Pelo teorema de Riemann-Roch temos

$$k = dim\, G = deg\, G + 1 - g + dim\,(W - G) \geq deg\, G + 1 - g$$

   pois $dim\,(W-G) \geq 0$. Logo

$$k + d \geq deg\, G + 1 - g + n - deg\, G,$$

   isto é,

$$k + d \geq n + 1 - g.$$

2. Pelo teorema 3.1.34, $k = deg\, G + 1 - g$.

3. Trivial.

□

Pelo item 2 do corolário anterior e pela limitação de Singleton temos que se $deg\, G < n$:

$$n + 1 - g \leq k + d \leq n + 1.$$

Note que $k+d = n+1$ se F é um corpo de funções de gênero $g = 0$. Logo códigos geométricos de Goppa construídos sobre corpos de funções racionias $\mathbb{F}_q(z)$ são sempre MDS-códigos. Isto será discutido com mais detalhes na próxima seção.

Vamos sempre assumir que $deg\, G < n$.

Definição 3.19 *O inteiro $d^* = n - deg\, G$ é chamado a distância prescrita de um código $C_{\mathcal{L}}(D, G)$.*

O teorema 3.3.1 nos mostra que a distância mínima de um código geométrico de Goppa não pode ser menor que sua distância prescrita. Quanto a $d^* = d$ ou $d^* < d$, veja a proposição a seguir.

Proposição 3.3.3 *Se $dim\, G > 0$ e $d^* > 0$ então $d = d^*$ se, e somente se, existe um divisor D' tal que $0 \leq D' \leq D$, $deg\, D' = deg\, G$ e $dim\,(G - D') > 0$.*

Prova:

($\Longrightarrow$) Suponhamos $d = d^*$. Então existe $x \in \mathcal{L}(G)$ tal que a palavra-código $(x(P_1), ..., x(P_n)) \in C_{\mathcal{L}}(D, G)$ tem precisamente $n - d = n - d^* = deg\, G$ componentes 0, isto é, $x(P_{i_j}) = 0$ para $j = 1, ..., deg\, G$.
Tomemos

$$D' = \sum_{j=1}^{deg\, G} P_{i_j}.$$

Então $0 \leq D' \leq D$, $deg\, D' = deg\, G$ e $dim\,(G - D') > 0$, pois $x \in \mathcal{L}(G - D')$.

($\Longleftarrow$) Seja D' um divisor tal que $0 \leq D' \leq D$, $deg\, D' = deg\, D$ e $dim\,(G - D') > 0$.
Tome $0 \neq y \in \mathcal{L}(G - D')$. O peso de $(y(P_1), ..., y(P_n))$ é $deg\,(D' - G) = deg\, D' - deg\, G = n - deg\, G$. Logo $d \leq n - deg\, G = d^*$, isto implica que $d = d^*$.

□

Definição 3.20 *Dizemos que dois códigos $C_1, C_2 \in \mathbb{F}_q^n$ são equivalentes se existe um vetor $a = (a_1, ..., a_n) \in (\mathbb{F}_q \setminus \{0\})^n$ tal que $C_2 = aC_1$, isto é,*

$$C_2 = \{(a_1c_1, ..., a_nc_n) \mid (c_1, ..., c_n) \in C_1\}.$$

Evidentemente códigos equivalentes possuem a mesma dimensão, a mesma distância mínima e o mesmo peso. Mas, note que, esta equivalência não preserva todas as propriedades de um código.

Proposição 3.3.4 *Valem as seguintes propriedades:*

1. *Suponhamos que dois divisores G_1 e G_2 são tais que $G_1 \sim G_2$ e $supp\, G_1 \cap supp\, D = supp\, G_2 \cap supp\, D = \emptyset$. Então os códigos $C_{\mathcal{L}}(D, G_1)$ e $C_{\mathcal{L}}(D, G_2)$ são equivalentes.*

2. *Reciprocamente se um código $C \subseteq \mathbb{F}_q^n$ é equivalente a $C_{\mathcal{L}}(D, G)$, então existe um divisor $G' \sim G$ tal que $supp\, G' \cap supp\, D = \emptyset$ e $C = C_{\mathcal{L}}(D, G')$.*

   Prova:

1. Tome $G_2 = G_1 - (z)$ com $v_{P_i}(z) = 0$, para $i = 1, ..., n$.

   Se $a = (z(P_1), ..., z(P_n)) \in \mathbb{F}_q \setminus \{0\}$ então a aplicação

$$\begin{array}{rccc} f & : & \mathcal{L}(G_1) & \longrightarrow & \mathcal{L}(G_2) \\ & & x & \longmapsto & xz \end{array}$$

   é bijetiva pelo obsevado após a definição 3.13. Logo temos $C_{\mathcal{L}}(D, G_2) = aC_{\mathcal{L}}(D, G)$.

2. Seja $C = aC_{\mathcal{L}}(D, G)$ com $a = (a_1, ..., a_n) \in (\mathbb{F}_q \setminus \{0\})^n$. Escolha $z \in F$ com $z(P_i) = a_i$ se $i = 1, ..., n$ e $G' = G - (z)$. Então $C = C_{\mathcal{L}}(D, G')$.

□

Observação: Se G é um divisor cujo suporte não é disjunto do suporte de D, podemos definir o código geométrico de Goppa $C_{\mathcal{L}}(D, G)$ associado a D e G da seguinte forma: Escolha um divisor $G' \sim G$ com $supp\, G' \cap supp\, D = \emptyset$ e então $C_{\mathcal{L}}(D, G) = C_{\mathcal{L}}(D, G')$.

3.3.1
Códigos Geométricos de Goppa associados a Corpos de Funções Racionais

Nesta seção estudaremos códigos geométricos de Goppa associados a corpos de funções racionais. Decreveremos tais códigos de forma muito explícita através de geradores e matriz de paridade. Na teoria de códigos, esta classe de códigos é chamada de *Códigos de Reed-Solomon Generalizados.*

Definição 3.21 *Um código geométrico de Goppa $C_{\mathcal{L}}(D,G)$ associado aos divisores G e D de um corpo de funções racionais $\mathbb{F}_q(z)/\mathbb{F}_q$ é chamado de racional (como na seção anterior, $D = P_1 + \cdots + P_n$, onde P_i são lugares distintos de grau 1 e $supp\, G \cap supp\, D = \emptyset$).*

Observe que o comprimento de um código geométrico racional de Goppa é limitado por $q+1$, pois $\mathbb{F}_q(z)$ possui apenas $q+1$ lugares de grau 1: o pólo P_∞ de z e para cada $\alpha \in \mathbb{F}_q$, os zeros P_α de $z-\alpha$.

Proposição 3.3.5 *Seja $C = C_{\mathcal{L}}(D,G)$ um código geométrico racional de Goppa sobre $\mathbb{F}_q$, e n,k,d os parâmetros de C. Então:*

1. *$n \leq q+1$.*
2. *$k = 0 \iff deg\, G < 0$; e $k = n \iff deg\, G > n-2$.*
3. *Para $0 \leq deg\, G \leq n-2$, temos $k = 1 + deg\, G$ e $d = n - deg\, G$. Em particular, C é um MDS-código.*
4. *$C^{\perp}$ também é um código geométrico racional de Goppa.*

Agora determinaremos especificamente uma matriz geradora de códigos racionais.

Proposição 3.3.6 *Seja $C = C_{\mathcal{L}}(D,G)$ um código geométrico racional de Goppa sobre $\mathbb{F}_q$ e n,k,d seus parâmetros.*

1. *Se $n \leq q$ então existem pares de elementos distintos $\alpha_1, ..., \alpha_n \in \mathbb{F}_q$ e $v_1, ..., v_n \in \mathbb{F}_q \backslash \{0\}$ (não necessariamente distintos) tais que*

$$C = \{(v_1 \cdot f(\alpha_1), ..., v_n \cdot f(\alpha_n)) \mid f \in \mathbb{F}_q[z] \ \text{ e } deg\, f \leq k-1\}.$$

A matriz

$$M = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_n v_n \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \cdots & \alpha_n^2 v_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \cdots & \alpha_n^{k-1} v_n \end{pmatrix}$$

é a matriz geradora de C.

2. *Se $n = q + 1$, C tem a seguinte matriz geradora*

$$M = \begin{pmatrix} v_1 & v_2 & \cdots & v_{n-1} & 0 \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_n v_{n-1} & 0 \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \cdots & \alpha_n^2 v_{n-1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \cdots & \alpha_n^{k-1} v_{n-1} & 1 \end{pmatrix}$$

onde $\mathbb{F}_q = \{\alpha_1, ..., \alpha_{n-1}\}$ e $v_1, ..., v_{n-1} \in \mathbb{F}_q \backslash \{0\}$.

Prova:

1. Como $D = P_1 + \cdots + P_n$ e $n \leq q$ existe pelo menos um lugar P de grau 1 que não está em $supp\, D$ (existem $q + 1$ lugares de grau 1).

   Tome um lugar $Q \neq P$ de grau 1 (pode ser $Q = P_1$). Pelo teorema de Riemann-Roch, $dim\,(Q - P) = 1$, portanto pelo corolário 3.1.10 $Q - P$ é principal.

   Seja $Q - P = (z)$, então z é um elemento gerador do corpo das funções racionais sobre $\mathbb{F}_q$ e P é o divisor dos pólos de z, isto é, $P = P_\infty$. Pela proposição anterior, podemos assumir que $deg\, G = k - 1 \geq 0$. Logo o divisor $(k-1)P_\infty - G$ tem grau 0, então ele é principal (pelo teorema de Riemann-Roch e pelo corolário) 3.1.10. Sendo $(k-1)P_\infty - G = (u)$ com $0 \neq u \in \mathbb{F}_q(z)$ pois $dim\,((k-1)P_\infty - G) = 1$.

   Os elementos do conjunto $\{z^i u; i = 0, ...k-1\}$ pertencem a $\mathcal{L}(G)$ pois

   – Se $\overline{P} = P_\infty$ então $v_{\overline{P}}(u) = k - 1 - v_{\overline{P}}(G)$,

$$\begin{aligned} v_{\overline{P}}(z^i u) &= i v_{\overline{P}}(z) + v_{\overline{P}}(u) \\ &= -i + k - 1 - v_{\overline{P}_\infty}(G) \\ &\geq 0 - v_{\overline{P}_\infty}(G) \end{aligned}$$

$$= \quad -v_{\overline{P}_\infty}(G)$$

– Se $\overline{P} = P_\infty$ então $v_{\overline{P}}(u) = -v_{\overline{P}}(G)$, $v_{\overline{P}}(z) \geq 0$ e

$$\begin{aligned} v_{\overline{P}}(z^i u) &= i v_{\overline{P}}(z) + v_{\overline{P}}(u) \\ &\geq 0 - v_{\overline{P}}(G) \\ &= -v_{\overline{P}}(G) \end{aligned}$$

Mais ainda, eles são linearmente independentes sobre $\mathbb{F}_q$ em virtude de toda combinação linear sobre $\mathbb{F}_q$ de $\{z^i u; i = 0, \ldots, k-1\}$ dar origem a uma combinação linear sobre $\mathbb{F}_q$ de $\{z^i; i = 0, \ldots, k-1\}$ que é linearmente independente sobre $\mathbb{F}_q$.

Como $dim\, G = k$, $\{u, zu, ..., z^{k-1}u\}$ é uma base de $\mathcal{L}(G)$, isto é,

$$\mathcal{L}(G) = \{u \cdot f(z) \mid f \in \mathbb{F}_q[z] \text{ e } deg\, f \leq k-1\}.$$

Tome $\alpha_i = z(P_i)$ e $v_i = u(P_i)$. Daí,

$$(u \cdot f(z))(P_i) = u(P_i) \cdot f(z(P_i)) = v_i \cdot f(\alpha_i)$$

para $i = 1, ..., n$. Logo

$$C = C_{\mathcal{L}}(D, G) = \{(v_1 \cdot f(\alpha_i), ..., v_n \cdot f(\alpha_n) \mid deg\, f \leq k-1\}.$$

A palavra código em C correspondente a uz^j é $(v_1\alpha_1^j, ..., v_n\alpha_n^j)$ com $j = 0, ..., k-1$. Logo a matriz geradora de C é dada por

$$M = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_n v_n \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \cdots & \alpha_n^2 v_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \cdots & \alpha_n^{k-1} v_n \end{pmatrix}$$

2. O caso $n = q + 1$ é análogo ao anterior. Tome z tal que $P_n = P_\infty$ é um pólo de z. Como antes $(k-1)P_\infty - G = (u)$ com $0 \neq u \in \mathbb{F}_q(z)$

e $\{u, zu, ..., z^{k-1}u\}$ é uma base de $\mathcal{L}(G)$. Para $1 \leq i \leq n-1 = q$ os elementos $\alpha_i = z(P_i)$ são distintos, logo $\mathbb{F}_q = \{\alpha_1, ..., \alpha_{n-1}\}$. Além disso, $v_i = u(P_i) \in \mathbb{F}_q \backslash \{0\}$ para $i = 1, ..., n-1$. Para $0 \leq j \leq k-2$ obtemos

$$((uz^j)(P_1), ..., (uz^j)(P_n)) = (\alpha_1^j v_1, ..., \alpha_{n-1}^j v_{n-1}, 0),$$

e para $j = k-1$ temos

$$((uz^{k-1})(P_1), ..., (uz^{k-1})(P_n)) = (\alpha_1^{k-1} v_1, ..., \alpha_{n-1}^{k-1} v_{n-1}, \gamma)$$

com $\gamma \neq 0$. Substituindo u por $\gamma^{-1} \cdot u$ temos o desejado.

□

Definição 3.22 *Sejam $\alpha = (\alpha_1, ..., \alpha_n)$ onde α_i são elementos distintos de $\mathbb{F}_q$, e $v = (v_1, ..., v_n)$ onde $0 \neq v_i \in \mathbb{F}_q$ e não necessariamente distintos. Então o código de Reed-Solomon generalizado denotado por $GRS_k(\alpha, v)$ consiste de todos os vetores $(v_1 \cdot f(\alpha_1), ..., v_n \cdot f(\alpha_n))$ com $f(z) \in \mathbb{F}_q[z]$ e $\deg f \leq k-1$ (para $k \leq n$ fixo).*

No caso de $\alpha = (\beta, \beta^2, ..., \beta^n)$ (onde $n = q-1$ e β é uma raiz n-ésima da unidade) e $v = (1, ..., 1)$ temos que $GRS_k(\alpha, v)$ é um código de Reed-Solomon como na seção anterior.

Claramente os $GRS_k(\alpha, v)$ são $[n, k]$-códigos e, pela proposição 3.3.6 temos que todos os códigos geométricos racionais de Goppa sobre $\mathbb{F}_q$ de comprimento $n \leq q$ são códigos de Reed-Solomon generalizados. Vamos agora ver se a recíproca é verdadeira.

Proposição 3.3.7 *Todo código de Reed-Solomon generalizado $GRS_k(\alpha, v)$ pode ser representado como um código geométrico racional de Goppa.*

Prova:

Sejam $\alpha = (\alpha_1, ..., \alpha_n)$ com $\alpha_i \in \mathbb{F}_q$ e $v = (v_1, ..., v_n)$ com $0 \neq v_i \in \mathbb{F}_q$. Consideremos o corpo de funções racionais $F = \mathbb{F}_q(z)$. Sejam P_i o zero de $z - \alpha_i$ $(i = 1, ..., n)$ e P_∞ o polo de z. Tome $u \in F$ tal que

$$u(P_i) = v_i \ para \ i = 1, ..., n. \tag{3-5}$$

Este elemento existe pelo teorema de aproximação ou podemos utilizar interpolação de Lagrange para determinar $u(z) \in \mathbb{F}_q[z]$. Sejam $D = P_1 + \cdots + P_n$

e $G = (k-1)P_\infty - (u)$. A prova da proposição 3.3.6 nos mostra que $GRS_k(\alpha, v) = C_{\mathcal{L}}(D, G)$.

□

O mesmo argumento se aplica a códigos de comprimento $n = q+1$ sobre $\mathbb{F}_q$ que têm a matriz geradora da proposição 3.3.5 e esses códigos também podem ser representados como códigos geométricos racionais de Goppa.

Definição 3.23 *Considere uma extensão de corpos $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ e um código C sobre $\mathbb{F}_{q^m}$ de comprimento n. Então*

$$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n$$

é chamado o subcorpo do subcódigo de C (ou a restrição de C a $\mathbb{F}_q$).

Sendo assim $C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n$ é um código sobre $\mathbb{F}_q$. E sua distância mínima não pode ser menor que a distância mínima de C e, trivialmente, vemos que $dim\, C|_{\mathbb{F}_q} \leq dim\, C$.

Definição 3.24 *Sejam $n|q^m - 1$, $\beta \in \mathbb{F}_{q^m}$ uma raiz primitiva n-ésima da unidade, $l \in \mathbb{Z}$ e $\delta \geq 2$. Defina um código $C(n, l, \delta)$ sobre $\mathbb{F}_{q^m}$ pela matriz geradora*

$$H = \begin{pmatrix} 1 & \beta^l & \beta^{2l} & \cdots & \beta^{(n-1)l} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \cdots & \beta^{(n-1)(l+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{l+\delta-2} & \beta^{2(l+\delta-2)} & \cdots & \beta^{(n-1)(l+\delta-2)} \end{pmatrix}$$

O código $C = C(n, l, \delta)^{\perp}|_{\mathbb{F}_q}$ é chamado um código BCH com distância prescrita δ. Em outras palavras temos

$$C = \{c \in \mathbb{F}_q^n \mid H \cdot c^t = 0\}.$$

Proposição 3.3.8 *Sejam $n|q^m - 1$, $\beta \in \mathbb{F}_{q^m}$ uma raiz primitiva n-ésima da unidade, $F = \mathbb{F}_{q^m}(z)$ um corpo de funções racionais sobre $\mathbb{F}_{q^m}$ e P_0 (respectivamente P_∞) o zero (respectivamente o polo) de z. Para $i = 1, ..., n$ denotamos por P_i o zero de $z - \beta^{i-1}$, e $D_\beta = P_1 + P_2 + \cdots + P_n$. Sejam $a, b \in \mathbb{Z}$ tais que $0 \leq a + b \leq n - 2$. Então temos*

1. *$C_{\mathcal{L}}(D_\beta, aP_0+bP_\infty) = C(n,l,\delta)$ com $l=-a$ e $\delta = a+2+b$, onde $C(n,l,\delta)$ é como na definição 3.24;*

2. *O dual de $C_{\mathcal{L}}(D_\beta, aP_0+bP_\infty)$ é dado por*

$$C_{\mathcal{L}}(D_\beta, aP_0+bP_\infty)^\perp = C_{\mathcal{L}}(D_\beta, rP_0+sP_\infty)$$

com $r=-(a+1)$ e $s=n-b-1$. Daí o BCH-código $C(n,l,\delta)^\perp|_{\mathbb{F}_q}$ é uma restrição do código $C_{\mathcal{L}}(D_\beta, rP_0+sP_\infty)$ a $\mathbb{F}_q$, com $r=l-1$ e $s=n+1-\delta-l$.

Definição 3.25 *Sejam $L=\{\alpha_1,...,\alpha_n\} \subseteq \mathbb{F}_{q^m}$ com $|L|=n$, $g(z)\in\mathbb{F}_{q^m}[z]$ um polinômio de grau t tal que $1\leq t\leq n-1$ e $g(\alpha_i)\neq 0$, $\forall \alpha_i \in L$.*

1. *O código $C(\mathcal{L}, g(z)) \subseteq (\mathbb{F}_{q^m})^n$ tem a seguinte matriz geradora*

$$H = \begin{pmatrix} g(\alpha_1)^{-1} & g(\alpha_2)^{-1} & \cdots & g(\alpha_n)^{-1} \\ \alpha_1\cdot g(\alpha_1)^{-1} & \alpha_2\cdot g(\alpha_2)^{-1} & \cdots & \alpha_n\cdot g(\alpha_n)^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{t-1}\cdot g(\alpha_1)^{-1} & \alpha_2^{t-1}\cdot g(\alpha_2)^{-1} & \cdots & \alpha_n^{t-1}\cdot g(\alpha_n)^{-1} \end{pmatrix}$$

2. *O código $\Gamma(L,g(z)) = C(L,g(z))^\perp|_{\mathbb{F}_q}$ é chamado um código clássico de Goppa com polinômio de Goppa $g(z)$. Isto siginifica que*

$$\Gamma(L,g(z)) = \{c\in\mathbb{F}_q^n \mid H\cdot c^t = 0\}$$

onde H é a matriz acima.

Note que H é um caso especial da matriz M da proposição 3.3.6. Basta tomarmos $v_i = g(\alpha_i)^{-1}$, então $C(L,g(z))$ e $C(L,g(z))^\perp$ são códigos de Reed-Solomon generalizados.

Proposição 3.3.9 *Além da notação da definição anterior, sejam P_i o zero de $z-\alpha_i$ (para $\alpha_i\in L$), P_∞ o polo de z e $D_L = P_1+P_2+\cdots+P_n$. Seja G_0 o divisor dos zeros de g(z) (no grupo dos divisores do corpo de funções racionais $F=\mathbb{F}_{q^m}(z)$). Então*

$$C(L,g(z)) = C_{\mathcal{L}}(D_L, G_0-P_\infty) = C_{\mathcal{L}}(D_L, A-G_0)^\perp \tag{3-6}$$

e

$$\Gamma(L, g(z)) = C_L(D_L, G_0 - P_\infty)^\perp|_{\mathbb{F}_q} = C_L(D_L, A - G_0)|_{\mathbb{F}_q},$$

onde o divisor A é determinado como se segue

$$h(z) = \prod_{\alpha_i \in L} (z - \alpha_i) \quad e \quad A = (h'(z)) + (n-1)P_\infty. \tag{3-7}$$

Corolário 3.3.10 *Valem as seguintes propriedades:*

1. *(BCH-limitado) A distância mínima de códigos BCH com distância prescrita δ é no mínimo δ.*

2. *(Limitação de Goppa) A distância mínima de um código clássico de Goppa $\Gamma(L, g(z))$ é no mínimo $1 + deg\, g(z)$.*

   Prova:

1. Representamos um BCH-código na forma $C = C_{\mathcal{L}}(D_\beta, rP_0 + sP_\infty)|_{\mathbb{F}_q}$. A distância mínima de $C_{\mathcal{L}}(D_\beta, rP_0 + sP_\infty)$ é, pela proposição 3.3.5 e pela proposição 3.3.8, dada por

   $$d = n - deg\,(rP_0 + sP_\infty) = n - ((l-1) + (n+1-\delta-l)) = \delta.$$

   Como a distância mínima de um subcódigo de um subcorpo não pode ser menor que a distância mínima do código original, a distância mínima de C é $\geq \delta$.

2. Pela proposição 3.3.9 temos $\Gamma(L, g(z)) = C_{\mathcal{L}}(D_L, A - G_0)|_{\mathbb{F}_q}$, onde A é como em 3-7. Mas $C_{\mathcal{L}}(D_L, A - G_0)$ tem distância mínima

   $$d = n - deg\,(A - G_0) = n - ((n-1) - deg\, g(z)) = 1 + deg\, g(z).$$

   Como a distância mínima de um subcódigo de um subcorpo não pode ser menor que a distância mínima do código original, a distância mínima de $\Gamma(L, g(z))$ é $\geq 1 + deg\, g(z)$.

□

Sob o ponto de vista algébrico,o corpo de funções racionais $\mathbb{F}_q(z)$ é o exemplo mais simples de um corpo de funçoes algébricas. No entanto, o código geométrico de Goppa associado a divisores de $\mathbb{F}_q(z)$ são interessantes.
É de se esperar que estudar códigos de Goppa construídos sobre um corpo de funções $F/\mathbb{F}_q$ não-racional seja ainda mais interessante.

Considere $F/\mathbb{F}_q$ dado por

$$F = \mathbb{F}_q(x, y) \quad \text{com } \varphi(x, y) = 0$$

onde $\varphi \in \mathbb{F}_q[x, y]$ é um polinômio não-constante, irredutível. F pode ser pensado como uma extensão finita do corpo de funções racionais $\mathbb{F}_q(x)$. Mas, neste caso, alguns problemas surgem:

1. É $\mathbb{F}_q$ o corpo total de constante de F?
2. Calcular o gênero de F.
3. Como descrever os lugares de F explicitamente? Em particular, quais lugares têm grau um?
4. Construir uma base para $\mathcal{L}(G)$.

Outra pergunta interessante é: Quantos lugares de grau um pode ter um corpo de funções de gênero g ?

Esta pergunta é importante em teoria de códigos já que com freqüência estamos interessados em construir "códigos longos"e o comprimento de um código de Goppa está limitado pelo número de lugares de grau um.