UNIVERSIDADE FEDERAL DO PARANÁ
SETOR DE CIÊNCIAS EXATAS
PÓS-GRADUAÇÃO EM MATEMÁTICA APLICADA

Estrutura Algébrica dos Códigos Quase-Cíclicos e Aplicações

Emidio Santos Portilho Junior

CURITIBA-PR
2008

Estrutura Algébrica dos Códigos Quase-Cíclicos e Aplicações

Emidio Santos Portilho Junior

Orientação:

Prof. Marcelo Muniz Silva Alves

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Matemática Aplicada, Programa de Pós-Graduação em Matemática Aplicada, Setor de Ciências Exatas, Universidade Federal do Paraná.

CURITIBA-PR

2008

Dedicado aos meus pais,
irmãos e amigos, pelo apoio
no decorrer desse percurso.

Agradecimentos

Agradeço a Deus pela vida pelo amor e oportunidades que tem me dado.

À minha família pelo apoio.

Ao meu orientador Marcelo Muniz Silva Alves pela paciência e atenção.

E a todos que, de alguma forma, contribuiram para a realização deste trabalho.

Sumário

Abstract

In this work we observed that Quasi-Cyclic Codes of length $n = lm$ and index l over a finite field $\mathbf{F}$ of characteristic p are submodules of $(R_m)^l$, where R_m is the quotient ring $\dfrac{\mathbf{F}[x]}{x^m - 1}$. This fact motivated us to work in this line of research. One of the important problems in Coding Theory is to find self-dual codes, since among these one finds some of the best codes known to date. An approach proposed by San Ling and Patrick Solé in 2001 shows how to use a well-known algebraic decomposition for Cyclic Codes in studying Quasi-Cyclic Codes. The main idea is to use algebraic techniques in a suitable manner in order to construct self-dual Quasi-Cyclic Codes over $\mathbf{F}^{lm}$ starting from self-dual codes in $(R_m)^l$. With the objective of presenting a complete work, we also show some applications.

Keywords: Codes, Cyclic Codes, Quasi-Cyclic Codes .

Resumo

Neste trabalho observamos que Códigos Quase-Cíclicos de comprimento $n = lm$ indice l sobre um corpo finito $\mathbf{F}$ de caracteristica p são submódulos de $(R_m)^l$ onde $R_m = \dfrac{\mathbf{F}[x]}{x^m - 1}$. Este fato foi o que nos motivou a trabalhar nessa linha de pesquisa.Um dos problemas relacionados a teoria de códigos é encontrar códigos auto-duais, pois entre estes encontramos alguns dos melhores códigos conhecidos.Uma abordagem proposta por San Ling e Patrick Solé em 2001 mostra como utilizar uma decomposição algébrica para Códigos Cíclicos, já conhecida, para estudar Códigos Quase-Cíclicos. A ideia base é usar técnicas Algébricas de forma apropriada a conseguirmos encontrar um meio para construir Códigos Quase-Cíclicos auto-duais sobre $\mathbf{F}^{lm}$ com relação ao produto interno euclidiano a partir de Códigos auto-duais em R_m^l. Afim de completar o trabalho, mostramos algumas aplicações.

Palavras-chave: Códigos, Códigos Cíclicos, Códigos Quase-Cíclicos,

Introdução

Códigos Quase-Cíclicos tem sido estudados há mais ou menos 35 anos. Estes códigos constituem uma generalização de códigos cíclicos. Como veremos no decorrer desse trabalho, esses códigos tem a propriedade de se reduzirem a muitos códigos de menor comprimento.

Neste trabalho, estaremos estudando códigos quase-cíclicos de comprimento $l \cdot m$ e índice l sobre um corpo $\mathbf{F}$ como códigos sobre o anel polinomial

$$R_m = \frac{\mathbf{F}[x]}{x^m - 1}$$

Quando m é coprimo com a característica de $\mathbf{F}$, este último pode ser decomposto em uma soma direta de corpos. Esta decomposição pode ser obtida a partir do teorema chinês dos restos ou da transformada de Fourier discreta, também conhecida como transformada de Mattson-Solomon para códigos cíclicos de comprimento m sobre $\mathbf{F}$. A vantagem desta abordagem é que podemos estudar códigos quase-cíclicos auto-duais por um caminho sistemático e podemos decompor códigos quase-cíclicos em códigos de comprimento menor.

Este trabalho está organizado da seguinte forma. No capítulo 1 fizemos uma abordagem básica da teoria de códigos, demonstramos alguns resultados algébricos que serão de grande importância para o desenvolvimento do trabalho, como o teorema chinês dos restos para anéis de polinômios: se $h(x) \in \mathbf{F}[x]$ é tal que $h(x) = p_1(x) \cdots p_r(x)$, onde os $p_i's$ satisfazem $\text{mdc}(p_i(x), p_j(x)) = 1$, sempre que $i \neq j$. Então:

$$\frac{\mathbf{F}[x]}{h(x)} \cong \frac{\mathbf{F}[x]}{p_1(x)} \oplus \cdots \oplus \frac{\mathbf{F}[x]}{p_r(x)}$$

Também enumeramos alguns resultados como a *Unicidade dos Corpos Finitos* e o *Teorema dos Isomorfismos* para anéis, cujas demonstrações podem ser encontradas em livros elementares de álgebra e teoria de códigos. No capítulo 2, passamos a abordar a teoria de códigos quase-cíclicos, mostramos a correspondência entre códigos quase-cíclicos sobre $\mathbf{F}$ de índice l e comprimento $n = lm$ e códigos lineares sobre o anel R_m, e usamos a decomposição de R_m dada pelo teorema chinês dos restos para decompor os códigos quase-cíclicos em somas diretas de códigos lineares sobre corpos finitos. Ao término do capítulo abordamos o problema utilizando a transformada de Fourier discreta que resulta em uma representação traço para códigos quase-cíclicos. Já no capítulo 3 aplicamos a discussão precedente a códigos quase-cíclicos de índice 2, o caso $m = 3$, o caso $m = 5$ e o caso $m = 7$. Mostramos que, se m é coprimo com q e l ímpar, então não existem códigos auto-duais l-quase-cíclicos sobre $\mathbf{F}_q$ de comprimento lm. Além disso, quando $q \equiv 3 \bmod 4$, códigos l-quase-cíclicos sobre $\mathbf{F}_q$ de comprimento lm existem se, e somente se $l \equiv 0 \bmod 4$. Também mostramos que se q é impar e C_1 e C_2 são códigos de comprimento l sobre $\mathbf{F}_q$, então

$$C = \{(u + v \mid u - v) \mid u \in C_1, v \in C_2\}$$

é um código quase-cíclico de comprimento $2l$ sobre $\mathbf{F}_q$. Além disso, C é auto-dual se, e somente se C_1 e C_2 são auto-duais. Os resultados subsequentes são semelhantes a esses.

Capítulo 1

Preliminares

1.1 Códigos

Fundada por C.E. Shannon, em 1948, a Teoria de Códigos Corretores de Erros foi em príncipo desenvolvida por matemáticos nas décadas de 50 e 60. Com as viagens espaciais e popularização dos computadores na década de 70 os engenheiros começaram a interessar-se pela teoria. Atualmente, códigos corretores de erros são utilizados na transmissão e armazenamento de dados. A exemplo disto, pode-se considerar as fotos de marte enviadas em 1965 e 1972 pela *Mariner 4* e *Mariner 9* respectivamente, além das fotos coloridas de Júpiter enviadas pela nave espacial *Voyager* em 1979 [1].

Observação: Os resultados elementares da teoria de códigos e corpos finitos aqui enunciados, como definições, teoremas, lemas entre outros poderão ser encontrados em [1].

Definição 1.1 *Seja A um conjunto finito com q elementos. Um código corretor de erros sobre A de comprimento n é um subconjunto próprio qualquer não vazio de A^n. O conjunto A é chamado de alfabeto de C. Os elementos de C são chamados de palavras-códigos ou simplesmente palavras.*

Seja $C \subset A^n$ um código a qual denominaremos *código fonte*. Supondo que uma palavra $\mathbf{v}$ de C seja transmitida e que no decorrer do caminho sofra interferência,

gerando vetor $\mathbf{v}'$. Uma das idéias básicas para se obter o vetor $\mathbf{v}$ original é introduzir redundâncias que permitam a detecção e correção dos erros; a tal processo denominaremos recodificação. O novo código obtido nessa recodificação é chamado de *código canal*.

Observação: Para estudarmos a teoria matemática relacionada a códigos corretores de erros é necessário conhecer algumas estruturas algébricas básicas que permitem tratar várias situações matemáticas concretas. Ressaltamos também que quando usarmos a noção de proximidade entre palavras, estaremos nos referindo a *distância de Hamming*.

Definição 1.2 *Dados dois elementos* $\mathbf{u}, \mathbf{v}, \in A^n$*, a distância de Hamming entre* $\mathbf{u}$ *e* $\mathbf{v}$ *é definida como*

$$d(\mathbf{u}, \mathbf{v}) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|.$$

A distância de Hamming entre elementos de A^n tem as propriedades que caracterizam uma *métrica* e por isso é também chamada de *métrica de Hamming*.

Dado $\mathbf{a} \in A^n$ e um número real $t > 0$, definimos a *bola* e a *esfera* de centro $\mathbf{a}$ e raio t como sendo respectivamente os conjuntos

$$D(\mathbf{a}, t) = \{\mathbf{u} \in A^n : d(\mathbf{u}, \mathbf{a}) \leq t\},$$
$$S(\mathbf{a}, t) = \{\mathbf{u} \in A^n : d(\mathbf{u}, \mathbf{a}) = t\}.$$

Definição 1.3 *Seja* C *um código. A distância mínima de* C *é o número*

$$d = \min\{d(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C \text{ e } \mathbf{u} \neq \mathbf{v}\}.$$

Dada distância mínima d de um código C, definiremos

$$t = \left[\frac{d-1}{2}\right],$$

onde $[\alpha]$ representa a parte inteira de um numero real α.

Lema 1.1 *Seja* C *um código com distância mínima* d *e seja* t *como acima. Se* $\mathbf{c}$ *e* $\mathbf{c}'$ *são palavras distintas de* C*, então*

$$D(\mathbf{c}, t) \cap D(\mathbf{c}', t) = \varnothing.$$

Demonstração: De fato, se $\mathbf{x}$ pertencece a $D(\mathbf{c}, t) \cap D(\mathbf{c}', t) = \varnothing$, teríamos $d(\mathbf{x}, \mathbf{c}) \leq t$ e $d(\mathbf{x}, \mathbf{c}') \leq t$, e portanto, pela desigualdade triangular,

$$d(\mathbf{c}, \mathbf{c}') \leq d(\mathbf{x}, \mathbf{c}) + d(\mathbf{x}, \mathbf{c}') \leq 2t \leq d - 1$$

absurdo, pois $d(\mathbf{c}, \mathbf{c}') \geq d$.

□

Chama-se *decodificação* ao procedimento de detecção e correção de erros num determinado código, isto é, se recebemos r, tomamos a palavra v de C que tem a menor distância de r, se houver mais de uma a decodificação não é feita. O teorema a seguir mostra que se cometerem menos que t erros, a palavra decodificada é igual à palavra enviada.

Teorema 1.1 *Seja C um código com distância mínima d. Então C pode corrigir $t = \left[\frac{d-1}{2}\right]$ erros e detectar até $d - 1$ erros.*

Demonstração: Se ao transmitirmos uma palavra $\mathbf{c}$ do código cometemos k erros com $k \leq t$, recebendo a palavra $\mathbf{r}$, então $d(\mathbf{r}, \mathbf{c}) = k \leq t$; enquanto que, pelo lema anterior, a distância de $\mathbf{r}$ a qualquer outra palavra do código é maior que t. Isso determina $\mathbf{c}$ univocamente a partir de $\mathbf{r}$.

Por outro lado, dada uma palavra do código, podemos introduzir nela até $d - 1$ erros sem encontrar outra palavra do código, e assim a detecção do erro será possível.

□

Definição 1.4 *Seja $C \subset A^n$ um código com distância mínima d e seja $t = \left[\frac{d-1}{2}\right]$. O código C será dito perfeito se*

$$\bigcup_{\mathbf{c} \in C} D(\mathbf{c}, t) = A^n.$$

1.2 Noções de Álgebra

Supomos que o leitor tenha uma noção básica da Teoria de Corpos e Anéis e compreenda expressões como classes residuais, domínio de integridade e subcorpo. Ressaltamos também que em todo trabalho, quando nos referirmos a anéis, estaremos nos referindo a anéis comutativos com unidade.

É possivel trocar o alfabeto de um código por outro alfabeto qualquer com um mesmo número de elementos sem alterar os parâmetros do código. Considere A e B dois conjuntos finitos e seja

$$f : A \longrightarrow B$$

uma bijeção. A partir de f podemos definir a função

$$\begin{array}{rccc} \phi : & A^n & \longrightarrow & B^n \\ & (x_1, ..., x_n) & \mapsto & (f(x_1), ..., f(x_n)) \end{array}$$

Essa função é bijetora e preserva as distâncias de Hamming. Sendo assim, um código C em A^n dá origem a um código $C' = \phi(C)$ em B^n com mesma distância mínima e, portanto, mesma capacidade de correção. Por isso podemos considerar, sem perda de generalidade, que A tem estrutura de anel, o que nos permite usar mais ferramentas matemáticas. Mas ainda, costuma-se impor que o alfabeto seja um corpo finito, o que restringe sua cardinalidade a potencias de primos.

No que segue enunciraremos resultados fundamentais para o estudo dos códigos quase-cíclicos.

1.2.1 Anéis, Módulos e Decomposições

Definição 1.5 *Um subconjunto I não vazio de um anel A é um ideal de A se forem verificadas as condições:*
(i) $\forall a, b \in I, a + b \in I$*; e*
(ii) $\forall a \in I$ *e* $\forall c \in A, ca \in I$*.*

É facil ver que um ideal I sempre contém o elemento zero de A, uma vez que dado um elemento $a \in I(\neq \varnothing)$ qualquer, temos que $0 = 0a \in I$. Também é claro que $I = 0$ e $I = A$ são ideais de A. Se $a \in A$, então o conjunto $(a) = \{ca : c \in A\}$ é um ideal de A, mais conhecido como *ideal principal* gerado por a.

Para representar a decomposição de um código quase-cíclico, precisamos de resultados sobre decomposição de anéis e módulos. As definições e resultados a seguir foram adaptados de [7] para o caso que nos interessa, onde R é um anel comutativo com unidade.

Definição 1.6 *Seja R um anel. Diremos que $e \in R$ é idempotente se $e^2 = e$. O conjunto $\{e_1, \ldots, e_m\} \subset R$ é um sistema ortogonal completo de idempotentes de R se*

$$e_i^2 = e_i \ \forall i$$
$$e_i \cdot e_j = 0 \text{ se } i \neq j$$
$$1 = e_1 + \ldots + e_m$$

Teorema 1.2 *Seja R um anel com unidade, $S = \{e_1, \ldots, e_m\}$ um sistema ortogonal completo de idempotentes, e seja $R_i = (e_i)$ o ideal principal de R gerado por e_i. Então:*
(i) $R = R_1 \oplus \cdots \oplus R_m$
(ii) Se $I \lhd R$ então $I_j = e_j I$ é ideal de R_j, e $I = I_1 \oplus \cdots \oplus I_m$

Demonstração: (ii) Vamos provar que I_j é um ideal de R_j. Primeiramente, temos que $I_j \subset R_j$ pela própria definição, pois se $x \in I_j$ então $x = e_j x'$, com $x' \in I$. Se $x = e_j x'$, $y = e_j y'$, com $x', y' \in I$, temos que $x + y = e_j(x' + y')$. Como I é um ideal $x' + y' \in I$ e portanto $x + y \in I_j$. Finalmente, se $c = e_j r \in R_j$ e $x = e_j x' \in I_j$, então $cx = e_j r e_j x' = (e_j)^2 r x' = e_j r x' \in I$, donde I_j é um ideal.

Seja $I_j = e_j I = \{e_j x; x \in I\}$, note que $I_j \subset I$ pois $x \in I$ implica $e_j x \in I$, daí $I_1 + \cdots + I_m \subset I$. Mostremos que essa soma é direta. De fato, seja

$$e_1 x_1 + \cdots + e_m x_m = 0,$$

multiplicando ambos lados dessa igualdade por e_j vem que

$$0 = e_j e_1 x_1 + \ldots + e_j^2 x_j + \ldots + e_j e_m x_m = e_j x_j,$$

logo $I_1 \oplus \cdots \oplus I_m \subset I$. Tome $x \in I$, podemos escrever

$$\begin{aligned} x &= 1 \cdot x \\ &= (e_1 + \cdots + e_m)x \\ &= e_1 x + \cdots + e_m x \end{aligned}$$

e $e_1 x + \cdots + e_m x \in I_1 \oplus \cdots \oplus I_m$, daí $I = I_1 \oplus \cdots \oplus I_m$.
(i) Segue de (ii), com $R = I$.

□

Corolário 1.1 *Se $A_1, A_2, \ldots, A_n$ são anéis comutativos com unidade tal que $R = A_1 \times \ldots \times A_m$ então todo ideal I de R é da forma*

$$I = I_1 \times \cdots \times I_m$$

com $I_j \lhd A_j$

Definição 1.7 *M é um R-módulo (a esquerda) se M é um grupo abeliano com relação a operação*

$$(m, n) \longmapsto m + n$$

que é dotado de uma aplicação $\lambda : R \times M \longrightarrow M$, denotada por $\lambda(r, m) = r \cdot m$, que satisfaz:
(i) $1 \cdot m = m \ \forall m \in M$
(ii) $r(m + n) = rm + rn, \ \forall r \in R, \ \forall m, n \in M$
(iii) $(rs) \cdot m = r \cdot (s \cdot m), \ \forall r, s \in R, \ \forall m \in M$
(iv) $(r + s) \cdot m = rm + sm, \ \forall r, s \in R \ \forall m \in M$

Definição 1.8 *Seja M um R-módulo. Diremos que $N \subset M$, com $N \neq \varnothing$, é um R-submódulo se*
(i) $x, y \in N \Longrightarrow x + y \in N$,
(ii) $\lambda \in R, x \in M \Longrightarrow \lambda x \in M$

Para um anel comutativo R com unidade, um código linear C de comprimento n sobre R é um R-submódulo de R^n.

Teorema 1.3 *Sejam R anel e M um R-módulo. Se $S = \{e_1, \ldots, e_n\}$ é um sistema ortogonal completo de R, com $R_i = e_i R$ e $R = R_1 \oplus \ldots \oplus R_n$ a decomposição de R associado a S, então:*
(i) $e_i M = M_i$ *é R-submódulo de M e $M = M_1 \oplus \ldots \oplus M_n$.*
(ii) Se N é R-submódulo de M, então $N = N_1 \oplus \ldots \oplus N_n$ onde $N_i = e_i N \subset M_i$.
(iii) Se N_i é R_i-módulo de M_i, então $N = N_1 \oplus \ldots \oplus N_n$ é R-submódulo de M.

Demonstração: As demonstrações dos itens (i) e (ii) são análogas ao já feito no teorema 1.2. Demonstraremos então o item (iii). Claramente $N \neq \emptyset$, pois cada N_i contem pelo menos o vetor nulo, e portanto $0 = 0+0+\cdots+0 \in N$. Se $n = n_1+\cdots+n_m$ e $n' = n'_1 + \cdots + n'_m \in N$, então

$$n + n' = (n_1 + n'_1) \cdots + (n_m + n'_m).$$

Como N_i é R_i-módulo de M_i, $n_i + n'_i \in N_i$, para todo i. Portanto, $n + n' \in N$.

Se $n = n_1 + \cdots + n_m \in N$ e $r \in R$, temos

$$rn = rn_1 + \cdots + rn_m$$

onde $rn_i \in M_i$, já que $n_i \in M_i$ e M_i é R-submódulo de M por (i).

Agora temos

$r = e_1 r + \cdots + e_m r$, com $e_i r \in R_i$

daí

$$\begin{aligned} rn_i &= e_1rn_i + \cdots + e_mrn_i \\ &= re_1n_i + \cdots + re_mn_i \end{aligned}$$

Como $n_i \in N_i \subset M_i$, existe $m_i \in M_i$ tal que $n_i = e_im_i$. Portanto,

$$\begin{aligned} rn_i &= r(e_1e_i)m_i + \cdots + r(e_ie_i)m_i + \cdots + r(e_me_i)m_i \\ &= re_in_i \end{aligned}$$

que está em N_i, pois N_i é R_i-submódulo de M_i. Portanto

$$rn = rn_1 + \cdots + rn_m \in N,$$

e N é R-submódulo de M.

□

Lema 1.2 *Seja $S = \{e_1, \ldots, e_n\}$ um sistema ortogonal completo de R e seja $R = R_1 \oplus \ldots \oplus R_m$ a decomposição associada. Se N_i é R_i-módulo para $i = 1, \ldots, m$ então o grupo abeliano*

$$N = N_1 \oplus \ldots \oplus N_m$$

tem estrutura de R-módulo com o produto

$$(r_1 + \ldots + r_m)(x_1 + \ldots + x_m) = r_1x_1 + \ldots + r_mx_m$$

Demonstração: Mostraremos aqui os itens (ii) e (iv) da definição. Note que, para x $= (x_1 + \ldots + x_m)$, y $= (y_1 + \ldots + y_m)$, r $= (r_1 + \ldots + r_m)$ e s $= (s_1 + \ldots + s_m)$, temos que:

$$
\begin{aligned}
(ii)\ \mathrm{r(x+y)} &= (r_1+\ldots+r_m)((x_1+\ldots+x_m)+(y_1+\ldots+y_m)) \\
&= (r_1+\ldots+r_m)((x_1+y_1)+\ldots+(x_m+y_m)) \\
&= r_1(x_1+y_1)+\ldots+r_m(x_m+y_m) \\
&= (r_1x_1+r_1y_1)+\ldots+(r_mx_m+r_my_m) \\
&= (r_1x+\ldots+r_mx)+(r_1y+\ldots+r_my) \\
&= \mathrm{rx+ry}
\end{aligned}
$$

e

$$
\begin{aligned}
(iv)\ \mathrm{(r+s)(x)} &= ((r_1+\ldots+r_m)+(s_1+\ldots+s_m))(x_1+\ldots+x_m) \\
&= ((r_1+s_1)+\ldots+(r_m+s_m))((x_1+\ldots+x_m) \\
&= (r_1+s_1)x_1+\ldots+(r_m+s_m)x_m \\
&= (r_1x_1+s_1x_1)+\ldots+(r_mx_m+s_mx_m) \\
&= (r_1x_1+\ldots+r_mx_m)+(s_1x_1+\ldots+s_mx_m) \\
&= \mathrm{rx+sx}
\end{aligned}
$$

□

Teorema 1.4 *Se $S=\{e_1,\ldots,e_n\}$ é um sistema ortogonal completo de R, com $R_i=(e_i)$ e $R=R_1\oplus\ldots\oplus R_m$ a decomposição de R associada a S, então:*
(i) $M=R_1^l\oplus\ldots\oplus R_m^l$ é R-módulo por

$$(r_1+\ldots+r_m)(x_1+\ldots+x_m)=r_1x_1+\ldots+r_mx_m$$

(ii) A aplicação

$$
\begin{aligned}
\phi : R^l &\longrightarrow R_1^l\oplus\ldots\oplus R_m^l \\
(r_1+\cdots+r_l) &\longmapsto (e_1(r_1+\cdots+r_l),e_2(r_1+\cdots+r_l),\ldots,e_m(r_1+\cdots+r_l))
\end{aligned}
$$

é um isomorfismo de R-módulos.
(iii) N é R-sumódulo de $R_1^l\oplus\ldots\oplus R_m^l$ se, e somente se, $N=N_1\oplus\ldots\oplus N_m$, com N_i sendo R_i-submódulo de R_i^l.

Demonstração: (i) É consequência do lema 1.2 , com $N_i = R_i^l$. (ii) Verificaremos para o produto por escalar, note que

$$\begin{aligned}
&\phi(s(r_1 + \cdots + r_l)) = (e_1 s(r_1 + \cdots + r_l), e_2 s(r_1 + \cdots + r_l), \ldots, e_m s(r_1 + \cdots + r_l)) \\
&= (e_1 s r_1 + \cdots + e_1 s r_l, e_2 s r_1 + \cdots + e_2 s r_l, \ldots, e_m s r_1 + \cdots + e_m s r_l) \\
&= ((e_1 e_1) s r_1 + \cdots + (e_1 e_1) s r_l, (e_2 e_2) s r_1 + \cdots + (e_2 e_2) s r_l, \ldots, (e_m e_m) s r_1 + \cdots + (e_m e_m) s r_l) \\
&= ((e_1 s) e_1 r_1 + \cdots + (e_1 s) e_1 r_l, (e_2 s) e_2 r_1 + \cdots + (e_2 s) e_2 r_l, \ldots, (e_m s) e_m r_1 + \cdots + (e_m s) e_m r_l) \\
&= s(e_1(r_1 + \cdots r_l), \ldots, e_m(r_1 + \cdots + r_l)) \\
&= s\phi(r_1 + \cdots + r_l)
\end{aligned}$$

Mostraremos agora que ϕ é injetora. De fato, note que

$$\phi((r_1 + \cdots r_l)) = (0, \ldots, 0)$$

se, e somente se

$$(e_1(r_1 + \cdots + r_l), e_2(r_1 + \cdots + r_l), \ldots, e_m(r_1 + \cdots + r_l)) = (0, \ldots, 0),$$

ou seja

$$\begin{aligned}
e_1(r_1 + \cdots + r_l) &= 0 \\
e_2(r_1 + \cdots + r_l) &= 0 \\
&\vdots \\
e_m(r_1 + \cdots + r_l) &= 0
\end{aligned}$$

Somando as equações, temos

$$(e_1 r_1 + \cdots + e_m r_1) + \cdots + (e_1 r_l + \cdots + e_m r_l) = 0$$

Agora, $r_i = e_1 r_i + \cdots + e_m r_i$ para todo i, e temos

$$r_1 + \cdots + r_l = 0,$$

o que mostra que $ker(\phi) = \{0\}$. Logo ϕ é injetora. Resta provar que ϕ é sobrejetora. Para facilitar a escrita, provaremos o caso em que $l = 2$, uma vez que a demonstração do caso geral é análoga. Considere $(r_1^1 + \ldots + r_l^1, r_1^2 + \ldots + r_l^2) \in R_1^l \oplus R_2^l$. Tome $x = (r_1^1 + r_1^2) + \ldots + (r_l^1 + r_l^2)$, temos que:

$$\begin{aligned}
\phi(x) &= (e_1((r_1^1 + r_1^2) + \ldots + (r_l^1 + r_l^2)), e_2((r_1^1 + r_1^2) + \ldots + (r_l^1 + r_l^2))) \\
&= (e_1(r_1^1 + \ldots + r_l^1 + r_1^2 + \ldots, +r_l^2), e_2(r_1^1 + \ldots + r_l^1 + r_1^2 + \ldots + r_l^2)) \\
&= (e_1(r_1^1 + \ldots + r_l^1), e_2(r_1^2 + \ldots + r_l^2)) \\
&= (e_1 r_1^1 + \ldots + e_1 r_l^1, e_2 r_1^2 + \ldots + e_2 r_l^2) \\
&= (r_1^1 + \ldots + r_l^1, r_1^2 + \ldots + r_l^2)
\end{aligned}$$

donde ϕ é sobrejetora.

(*iii*) Segue do teorema 1.3 com $N_i = R_i^l$.

□

Observação: Se I é um ideal do anel R, e R/I é o anel quociente correspondente, denotaremos os elementos de R/I por $a + I$ ou $[a]$.

1.2.2 Corpos Finitos

Apresentaremos agora algumas propriedades dos corpos finitos.

Proposição 1.1 *Seja* $\mathbf{K}$ *um corpo e* $P(x) \in \mathbf{K}[x]$. *O elemento* $[f(x)] \in \mathbf{K}[x]/P(x)$ *é invertível se, e somente se,* $MDC(f(x), P(x)) = 1$.

Teorema 1.5 *O anel* $\mathbf{K}[x]/P(x)$ *é um corpo, se e somente se, o polinômio* $P(x)$ *é irredutível sobre* $\mathbf{K}$.

Seja $\mathbf{K}$ um corpo finito com elemento unidade 1. Considere o conjunto

$$\Lambda_{\mathbf{K}} = \{n \in \mathbb{N} : n1 = 0\}.$$

Definição 1.9 *Define-se a característica de um corpo finito* $\mathbf{K}$, *como sendo o inteiro positivo*

$$\text{car}(\mathbf{K}) = \min \Lambda_{\mathbf{K}} = \min\{n \in \mathbb{N} : n1 = 0\} \subset \mathbb{N}.$$

Se o corpo $\mathbf{F}$ é um subcorpo de um corpo $\mathbf{K}$, então $\Lambda_{\mathbf{F}} = \Lambda_{\mathbf{K}}$ e, portanto $\text{car}(\mathbf{K}) = \text{car}(\mathbf{F})$.

Definição 1.10 *Diremos que* $\mathbf{F}$ *é uma extensão de* $\mathbf{K}$ *se* $\mathbf{K}$ *é subcorpo de* $\mathbf{F}$. *Se* $\mathbf{F}$, *considerado como um espaço vetorial sobre* $\mathbf{K}$, *é de dimensão finita, então* $\mathbf{F}$ *é chamado uma extensão finita de* $\mathbf{K}$. *A dimensão do espaço vetorial* $\mathbf{F}$ *sobre* $\mathbf{K}$ *é então chamada de grau de* $\mathbf{F}$ *sobre* $\mathbf{K}$, *em símbolos* $[\mathbf{F} : \mathbf{K}]$

Proposição 1.2 *Seja* $\mathbf{K}$ *um corpo finito, então* $\mathrm{car}(\mathbf{K})$ *é um número primo.*

Demonstração: Seja $m = \mathrm{car}(\mathbf{K})$ e suponhamos que m não seja primo. Então $m = m_1 \cdot m_2$, onde m_1 e m_2 são inteiros maiores do que 1 e menores do que m. Logo,

$$0 = m1 = (m_1 \cdot m_2)1 = m_1(m_2 1) = (m_1 1) \cdot (m_2 1)$$

Como $\mathbf{K}$ é domínio de integridade, temos que $m_1 1 = 0$ ou $m_2 1 = 0$, o que contradiz a minimalidade de m.

□

Proposição 1.3 *Seja* $\mathbf{K}$ *um corpo finito de característica* p, *e seja* $q = p^r$ *para algum inteiro positivo* r. *Se* $a, b \in \mathbf{K}$, *temos que*

$$(a \pm b)^q = a^q \pm b^q.$$

Corolário 1.2 *Se* $\mathbf{K}$ *é um corpo finito então* $|\,\mathbf{K}\,| = p^r$, *onde* $p = \mathrm{car}(\mathbf{K})$ *e* $r = [\mathbf{K} : \mathbb{Z}_p]$.

Proposição 1.4 *Sejam* $\mathbf{F}$ *um corpo de característica* $p > 0$ *e* q *uma potência de* p. *O conjunto* $\mathbf{K} = \{\alpha \in \mathbf{F} : \alpha^q - \alpha = 0\}$ *é um subcorpo de* $\mathbf{F}$.

Lema 1.3 *Seja* $\mathbf{K}$ *um corpo finito com* q *elementos. Para todo* $\alpha \in \mathbf{K}^*$, *onde* $\mathbf{K}^* = \mathbf{K} \setminus \{0\}$, *temos que*

$$\alpha^{q-1} = 1$$

Demonstração: Seja $\alpha \in \mathbf{K}^*$ e considere a aplicação

$$\begin{array}{rccc} \phi_\alpha : & \mathbf{K}^* & \longrightarrow & \mathbf{K}^* \\ & a & \longmapsto & \alpha a \end{array}$$

É imediato que ϕ_α é injetora, e, como $\mathbf{K}^*$ é finito, segue que ϕ_α é bijetora. Se $\mathbf{K}^* = \{a_1, \ldots, a_{q-1}\}$, temos que

$$\{\alpha a_1, \ldots, \alpha a_{q-1}\} = \{a_1, \ldots, a_{q-1}\},$$

e portanto, para cada a_i existe um $a_{j(i)}$ tal que

$$\alpha a_i = a_{j(i)},\ i = 1, 2, \ldots, q-1$$

Multiplicando estas equações, temos

$$\alpha^{q-1} a_1 \ldots a_{q-1} = a_1 \ldots a_{q-1},$$

e consequentemente,

$$\alpha^{q-1} = 1$$

□

Corolário 1.3 *Seja* $\mathbf{K}$ *um corpo finito com* q *elementos. Para todo* $\alpha \in \mathbf{K}$ *e para todo* $i \in \mathbb{N}$*, temos que* $\alpha^{q^i} = \alpha$*.*

Corolário 1.4 *Seja* $\mathbf{K}$ *um corpo finito de de característica* p *com* q *elementos. Seja* $\mathbf{F}$ *uma extensão de* $\mathbf{K}$*. Então os elementos de* $\mathbf{K}$ *são os elementos de* $\mathbf{F}$ *que são raízes de* $x^q - x = 0$*, enquanto que os elementos do subcorpo* $\mathbb{Z}_p$ *de* $\mathbf{F}$ *são raízes do polinômio* $x^p - x = 0$*.*

Demonstração: Segue do corolário anterior que os elementos de $\mathbf{K}$ são raízes do polinômio $x^q - x$. Mas esse polinômio, tendo grau q, tem no máximo q raízes, logo, as suas raízes são todos os elementos de $\mathbf{K}$. A segunda demonstra-se analogamente, considerando $\mathbb{Z}_p$ no lugar de $\mathbf{K}$.

□

Seja $\mathbf{K}$ um corpo finito e seja $\alpha \in \mathbf{K}^*$. Sabemos do lema 1.3 que

$$\{n \in \mathbb{N} : \alpha^n = 1\} \neq \varnothing.$$

Definição 1.11 *A ordem de $\alpha \in \mathbf{K}^*$ é o inteiro positivo*

$$\operatorname{ord} \alpha = \min\{n \in \mathbb{N} : \alpha^n = 1\}.$$

Proposição 1.5 *Seja $\mathbf{K}$ um corpo finito com q elementos e seja $\alpha \in \mathbf{K}^*$. Se para algum inteiro positivo m temos que $\alpha^m = 1$, então $\operatorname{ord}\alpha | m$. Em particular, $\operatorname{ord}\alpha | q-1$.*

Demonstração: Pelo algoritmo da divisão, existem inteiros $s \geq 0$ e r, com $0 < r < \operatorname{ord}\alpha$, tais que $m = (\operatorname{ord}\alpha)s + r$. Portanto,

$$1 = \alpha^m = (\alpha^{\operatorname{ord}\alpha})^s \cdot \alpha^r = 1 \cdot \alpha^r$$

o que pela minimalidade de $\operatorname{ord}\alpha$, implica que $r = 0$; logo, $\operatorname{ord}\alpha \mid m$. Pelo lema 1.3 temos que $\alpha^{q-1} = 1$. Logo, pelo que acabamos de provar, $\operatorname{ord}\alpha \mid q - 1$.

□

Teorema 1.6 *Seja $\mathbf{K}$ um corpo finito qualquer. Para cada número natural n, existe pelo menos um polinômio irredutível de grau n em $\mathbf{K}[x]$.*

Teorema 1.7 *(Existência de Corpos Finitos) Para números inteiros positivos p e n com p primo, existe um corpo com p^n elementos.*

Demonstração: Para todo primo positivo p e todo inteiro positivo natural n, existe, pelo teorema 1.6, um polinômio irredutível $f(x) \in \mathbb{Z}_p[x]$ de grau n; logo, pelo teorema 1.5 o anel $\mathbf{K} = \mathbb{Z}_p[x]/f(x)$ é um corpo com p^n elementos.

□

Teorema 1.8 *Seja $\mathbf{K}$ um corpo finito com $\operatorname{car}(\mathbf{K}) = p$, onde p é um número primo. Então, $\mathbf{K}$ contém um subcorpo isomorfo a $\mathbb{Z}_p$. Em particular, $\mathbf{K}$ tem p^n elementos para algum número natural n.*

O subcorpo de $\mathbf{K}$ que é isomorfo a $\mathbb{Z}_p$ é chamado de subcorpo primo de $\mathbf{K}$.

Teorema 1.9 *(Unicidade dos Corpos Finitos) Dois corpos finitos com mesmo número de elementos são isomorfos.*

Definição 1.12 *Um elemento α de um corpo finito $\mathbf{F}_q$ é chamado de elemento primitivo se* $\operatorname{ord}\alpha = q-1$.

Proposição 1.6 *Seja $\mathbf{K}$ um corpo finito. Sejam α e β elementos de $\mathbf{K}$ tais que* $\mathrm{MDC}(\operatorname{ord}\alpha, \operatorname{ord}\beta) = 1$. *Então* $\operatorname{ord}\alpha\beta = \operatorname{ord}\alpha \operatorname{ord}\beta$.

Demonstração: Sejam $m = \operatorname{ord}\alpha$ e $n = \operatorname{ord}\beta$. Temos então que

$$(\alpha\beta)^{mn} = (\alpha^m)^n(\beta^n)^m = 1.$$

Por outro lado, se $(\alpha\beta)^t = 1$, então

$$\begin{aligned} 1 &= ((\alpha\beta)^t)^m = \alpha^{tm}\beta^{tm} = 1\beta^{tm} = \beta^{tm}, \text{ e} \\ 1 &= ((\alpha\beta)^t)^n = \alpha^{tn}\beta^{tn} = \alpha^{tn}1 = \alpha^{tn}. \end{aligned}$$

Logo, pela proposição 1.5, temos que $n \mid tm$ e $m \mid tn$. Como $\mathrm{MDC}(m,n) = 1$, segue que $m \mid t$ e $n \mid t$. Novamente usando o fato que de que $\mathrm{MDC}(m,n) = 1$, segue que $m \mid t$, o que prova que $mn = \min\{t > 0 : (\alpha\beta)^t = 1\}$; concluimos assim que $\operatorname{ord}\alpha\beta = mn$.

□

Proposição 1.7 *Seja $\mathbf{K}$ um corpo finito e sejam $\alpha \in \mathbf{K}^*$ e $i \in \mathbb{N}$. Suponhamos que* $\operatorname{ord}\alpha = m$, *então*

$$\operatorname{ord}\alpha^i = \frac{m}{\mathrm{MDC}(m,i)}$$

Teorema 1.10 *Todo corpo finito possui elementos primitivos.*

Demonstração: Suponha que $\mathbf{K}$ tenha q elementos. Sabemos pelo lema 1.3 que $y^{q-1} = 1$ para todo $K \in \mathbf{K}^*$. Logo, todos os elementos de $\mathbf{K}^*$ têm ordem $\leq q-1$.

Tome $a \in \mathbf{K}*$ um elemento de ordem máxima m, queremos mostrar que $m = q-1$ o que prova que $\mathbf{K}^*$ possui um elemento de ordem $q-1$. De fato, em princípio provemos que se $b \in \mathbf{K}^*$, então $\operatorname{ord} b$ divide $\operatorname{ord} a = m$. Escrevamos $\operatorname{ord} b = ds$, onde $d = \text{MDC}(\operatorname{ord} b, m)$. Segue que $\text{MDC}(s, m) = 1$. Queremos então provar que $s = 1$. De fato, se $s > 1$, teríamos pela proposição anterior que $\operatorname{ord} b^d = s > 1$ e, portanto, pela proposição 1.6, temos

$$\operatorname{ord}(ab^d) = ms > m$$

contradizendo a maximalidade de $m = \operatorname{ord} a$.

Segue, então, que todo elemento de $\mathbf{K}^*$ satisfaz à equação

$$x^m - 1 = 0,$$

e portanto, $q - 1 =\mid \mathbf{K}^* \mid \leq m$.

Como $m \leq q-1$, pois todos os elementos de $\mathbf{K}^*$ têm ordem $\leq q-1$, segue que

$$m = \operatorname{ord} a = q - 1.$$

□

Teorema 1.11 *Seja* $\mathbf{K}$ *um corpo finito e* n *um inteiro positivo que divide* $\mid \mathbf{K} \mid -1$. *Então, existe um elemento* $\gamma \in \mathbf{K}$ *tal que*

$$X^n - 1 = (X - \gamma^0)(X - \gamma)(X - \gamma^2) \cdots (X - \gamma^{n-1}),$$

com $1, \gamma, \gamma^2, \ldots, \gamma^{n-1}$ *dois a dois distintos.*

Demonstração: Seja α elemento primitivo de $\mathbf{K}$ e $q =\mid \mathbf{K} \mid$. Logo, $\alpha^{q-1} = 1$ e

$$\alpha^m \neq 1, \ \textit{se } 0 < m < q - 1 \tag{1.1}$$

Se $n = 1$, nada temos a provar. Suponhamos $n \geq 2$.

Definamos $\gamma = \alpha^{\frac{q-1}{n}} \in \mathbf{K}$. Temos, então, que $\gamma^0, \gamma, \gamma^2, \cdots, \gamma^{n-1}$ são raízes de $X^n - 1$, e são duas a duas distintas; pois, caso contrário, se $\gamma^i = \gamma^j$ para algum par de inteiros (i, j) tais que $0 \leq i \leq j \leq n-1$, então

$$\alpha^{(j-i)\frac{q-1}{n}} = \gamma^{j-i} = 1,$$

o que contradiz (1.1) pelo fato de $(j-i)\frac{q-1}{n}$ ser um inteiro positivo menor do que $q-1$.

□

Corolário 1.5 *Seja* $\mathbf{K}$ *um corpo finito com* q *elementos e,* n*, um inteiro primo com* q*. Então, existem uma extensão* $\mathbf{F}$ *de* $\mathbf{K}$ *e um elemento* $\gamma \in \mathbf{F}$ *tais que*

$$X^n - 1 = (X - \gamma^0)(X - \gamma)(X - \gamma^2)\cdots(X - \gamma^{n-1})$$

com $1, \gamma, \gamma^2, \ldots, \gamma^{n-1}$ *dois a dois distintos.*

Demonstração: Novamente, se $n = 1$, nada temos a provar. Suponhamos $n \geq 2$. Como n e q são primos entre si, então a classe residual $[q]$ módulo n é invertível em $\mathbb{Z}_n$. Como $\mathbb{Z}_n$ é finito, então, no conjunto

$$\{[q], [q]^2, [q]^3, \ldots\},$$

há certamente repetições. Digamos que $[q]^j = [q]^i$ com $j > i$. Como $[q]$ é invertível em $\mathbb{Z}_n$, segue que $[q]^{-i} = ([q]^{-1})^i \in \mathbb{Z}_n$ e, portanto, existe um inteiro positivo d $(= j - i)$ tal que $[q]^d = 1$.

Seja m um inteiro positivo tal que $[q]^m = 1$. Em virtude do teorema 1.7, sabemos que existe um corpo $\mathbf{F}$, extensão de $\mathbf{K}$, com q^n elementos. Como $[q]^m = 1$, isto é, $q^m \equiv 1 \bmod n$, temos que n divide $q^m - 1$. Sendo assim, o resultado segue do teorema.

□

Não de menor importância é a teoria de traço sobre corpos, uma vez que essa se torna necessária para abordarmos a transformada de Fourier discreta. Os resultados a seguir podem ser encontrados em [4].

Definição 1.13 *Para* $\alpha \in \mathbf{F} = \mathbf{F}_{q^m}$ *e* $\mathbf{K} = \mathbf{F}_q$*, o traço* $Tr_{\mathbf{F}/\mathbf{K}}(\alpha)$ *de* α *sobre* $\mathbf{K}$ *é definido por:*

$$Tr_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}$$

se $\mathbf{K}$ *é o subcorpo primo de* $\mathbf{F}$*, então* $Tr_{\mathbf{F}/\mathbf{K}}(\alpha)$ *é chamado traço absoluto de* α *e simplesmente denotamos por* $Tr(\alpha)$*.*

Teorema 1.12 *Sejam* $\mathbf{K} = \mathbf{F}_q$ *e* $\mathbf{F} = \mathbf{F}_{q^m}$. *Então a função traço* $Tr_{\mathbf{F}/\mathbf{K}}$ *satisfaz as seguintes propriedades:*

(1) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$ *para todo* $\alpha, \beta \in \mathbf{F}$;

(2) $Tr(c\alpha) = cTr(\alpha)$ *onde* $c \in \mathbf{K}, \alpha \in \mathbf{F}$;

(3) A função Tr *de* $\mathbf{F}$ *em* $\mathbf{K}$ *é uma transformação* $\mathbf{K}$*-linear sobrejetora;*

(4) $Tr(a) = ma$ *para todo* $a \in \mathbf{K}$;

(5) $Tr(\alpha^q) = Tr(\alpha)$ *para todo* $\alpha \in \mathbf{F}$.

Demonstração: Demonstraremos aqui os itens(1) e (5). Primeiramente (1). Como $\mathbf{F}$ é um corpo finito, para todo $\alpha, \beta \in \mathbf{F}$ temos que

$$\begin{aligned} Tr(\alpha+\beta) &= \alpha + \beta + (\alpha+\beta)^q + \cdots + (\alpha+\beta)^{q^{m-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \cdots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} \\ &= Tr(\alpha) + Tr(\beta) \end{aligned}$$

De modo análogo para (5). Como $\mathbf{F}$ é um corpo finito com q^m elementos, temos que para todo $\alpha \in \mathbf{F}$ tem-se $\alpha^{q^m} = \alpha$, logo $Tr(\alpha^q) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^m} = \alpha^q + \alpha^{q^2} + \cdots + \alpha = Tr(\alpha)$.

□

Teorema 1.13 *(* ***transitividade do traço****) Seja* $\mathbf{K}$ *um corpo finito,* $\mathbf{F}$ *é uma extensão finita de* $\mathbf{K}$ *e* $\mathbf{E}$ *uma extensão finita de* $\mathbf{F}$. *Então:*

$$Tr_{\mathbf{E}/\mathbf{K}}(\alpha) = Tr_{\mathbf{F}/\mathbf{K}}(Tr_{\mathbf{E}/\mathbf{F}}(\alpha))$$

para todo $\alpha \in \mathbf{E}$.

1.2.3 Anéis de Polinômios e o Teorema Chinês do Resto

Dois resultados de grande importância para o desenvolvimento desse trabalho, o teorema do resto chinês e a decomposição de $\mathbf{K}[x]/(h(x))$ como soma de anéis, serão tratados nesta seção. Antes disso apresentamos resultados técnicos básicos que serão utilizados adiante.

Teorema 1.14 *(Teorema do Isomorfismo) Sejam A e A' anéis e $f : A \longrightarrow A'$ um homomorfismo.*

Então

(i) $Imf = \{f(a) : a \in A\}$ é um subanel de A'.

(ii) $N(f) = \{a \in A : f(a) = 0\}$ é um ideal de A, e f é injetiva $\Longleftrightarrow N(f) = 0$.

(iii) Os anéis $A/N(f)$ e Imf são isomorfos.

Demonstração: Ver [2].

O próximo teorema e seu corolário são fundamentais para o estudo de códigos quase-cíclicos.

Teorema 1.15 *(Teorema chinês dos restos): Seja $\mathbf{K}$ corpo e $f_1(x), f_2(x), \ldots, f_r(x) \in \mathbf{K}[x]$ dois a dois coprimos. Então, dados $a_1(x), \ldots, a_r(x) \in \mathbf{K}[x]$, existe uma solução $g(x)$ do sistema*

$$\begin{aligned} g(x) &\equiv a_1(x) \bmod(f_1(x)) \\ g(x) &\equiv a_2(x) \bmod(f_2(x)) \\ &\vdots \\ g(x) &\equiv a_r(x) \bmod(f_r(x)) \end{aligned}$$

que é única módulo $(f_1(x)f_2(x)...f_r(x))$.

Demonstração: Consideremos o polinômio

$$a_1(x)y_1(x) + \ldots + a_r(x)y_r(x)$$

onde

$$y_i(x) \equiv \begin{cases} 1 \bmod(f_i(x)) \\ 0 \bmod(f_j(x)),\ j \neq i \end{cases}$$

Considerando a primeira equação do sistema temos que $y_j \equiv 0 \bmod f_1(x)$ para todo $j \neq 1$, daí $a_2y_2 + ... + a_ry_r \equiv 0 \bmod f_1(x)$. Ainda $y_1(x) \equiv 1 \bmod f_1(x)$, logo $y_1(x)a(x) \equiv a_1(x) \bmod(f_1(x))$, sendo assim temos

$$y_1(x)a_1(x) + ... + y_ra_r(x) \equiv a_1(x) \bmod(f_1(x)).$$

De modo análogo se verifica para as outras equações.

Resta encontrar um sistema de polinômios que cumpra o papel dos y_i. Façamos $f(x) = f_1(x)...f_r(x)$. Então mdc$(f(x), f(x)/f_1(x)) = 1$, pois um divisor irredutível de $f_1(x)$ e $f(x)/f_1(x)$ teria também de ser divisor de algum $f_j(x)$, com $j \neq 1$, o que é impossível, pela hipótese.

Portanto, a congruência linear

$$(f(x)/f_1(x))z_1(x) \equiv 1 \bmod(f_1(x))$$

tem solução. Se $z_1(x) = b_1(x)$ é uma de suas soluções, então:

$$(f(x)/f_1(x))b_1(x) \equiv 1 \bmod(f_1(x))$$

mas, como $f_2, f_3, ..., f_r$ são divisores distintos de $f(x)/f_1(x)$, então $f(x)/f_1(x) \equiv 0 \bmod(f_2(x))$, $f(x)/f_1(x) \equiv 0 \bmod(f_3(x))$,..., $f(x)/f_1(x) \equiv 0 \bmod(f_r(x))$ e, portanto,

$$\begin{aligned}
(f(x)/f_1(x))b_1(x) &\equiv 0 \bmod(f_2(x)) \\
(f(x)/f_1(x))b_1(x) &\equiv 0 \bmod(f_3(x)) \\
&\vdots \\
(f(x)/f_1(x))b_1(x) &\equiv 0 \bmod(f_r(x))
\end{aligned}$$

De modo análogo, se $b_2(x)$ é solução de de $(f(x)/f_2(x))z_2(x) \equiv 1 \bmod f_2(x)$, então

$$\begin{aligned}
(f(x)/f_2(x))b_2(x) &\equiv 0 \bmod(f_1(x)) \\
(f(x)/f_2(x))b_2(x) &\equiv 1 \bmod(f_2(x)) \\
(f(x)/f_2(x))b_2(x) &\equiv 0 \bmod(f_3(x)) \\
&\vdots \\
(f(x)/f_2(x))b_2(x) &\equiv 0 \bmod(f_r(x))
\end{aligned}$$

E assim por diante. Portanto, $(f(x)/f_1(x))b_1(x), ..., (f(x)/f_r(x))b_r(x)$ cumprem o papel exigido pelos $y_i's$, conforme colocação inicial, e

$b = (f(x)/f_1(x))b_1(x)a_1(x) + (f(x)/f_2(x))b_2(x)a_2(x) + ... + (f(x)/f_r(x))b_r(x)a_r(x)$

é uma solução do sistema.

Se $c(x)$ é uma outra solução então $c(x) \equiv b(x) \bmod(f_i(x))$, $(i = 1, ..., r)$. Portanto, $f_1(x), ..., f_r(x)$ são divisores de $c(x) - b(x)$ mas como $f_1(x), ..., f_r(x)$, são dois a dois

primos entre si, então $f_1(x).f_2(x)...f_r(x)$ também é divisor de $c(x) - b(x)$. De onde $c(x) \equiv b(x) \bmod(f_1(x).f_2(x)...f_r(x))$.

Portanto a solução geral do sistema é

$$f(x) = b(x) + h(x)f(x), h(x) \in \mathbf{K}[x].$$

□

Proposição 1.8 *Se $\phi : A \longrightarrow B$ é homomorfismo de anéis e $b(x) \in B$, existe um único homomorfismo $\overline{\phi} : A[x] \longrightarrow B$ talque*

$$\begin{aligned} \overline{\phi} \mid_A &= \phi \\ \phi(x) &= b \end{aligned}$$

Demonstração: Primeiramente suponhamos que ϕ exista e demonstremos a unicidade. Se $\phi(x) = b$ segue por indução que $\phi(x^n) = b^n$ para todo $n \in \mathbb{N}$. Do fato que, $\overline{\phi} \mid_A = \phi$ temos que

$$\begin{aligned} \overline{\phi}\left(\sum_{i=0}^{n} a_i x^i\right) &= \overline{\phi}(a_0 + a_1 x + \ldots + x^n) \\ &= \overline{\phi}(a_0) + \overline{\phi}(a_1)\overline{\phi}(x) + \ldots + \overline{\phi}(a_n)\overline{\phi}(x^n) \\ &= \phi(a_0) + \phi(a_1)b + \ldots + \phi(a_n)b^n \end{aligned}$$

Vamos provar que a função $\overline{\phi}$ definida como acima é um homomorfismo (existência). Sejam $a(x) = \sum_{i=1}^{n} a_i x^i$ e $c(x) = \sum_{i=1}^{m} c_i x^i$. Temos que

$$\begin{aligned} \overline{\phi}(a(x) + c(x)) &= \overline{\phi}\left(\sum (a_i + c_i)x^i\right) \\ &= \sum \phi(a_i + c_i)b^i \\ &= \sum \left(\phi(a_i) + \phi(c_i)\right) b^i \\ &= \sum \phi(a_i)b^i + \sum \phi(c_i)b^i \\ &= \overline{\phi}\left(a(x)\right) + \overline{\phi}\left(c(x)\right) \end{aligned}$$

e ainda

$$\begin{aligned}
\overline{\phi}(a(x)c(x)) &= \overline{\phi}\left(\sum_{i=0}^{m+n}\sum_{j=0}^{i} a_j c_{i-j} x^i\right) \\
&= \sum_{i=0}^{m+n} \phi\left(\sum_{j=0}^{i} a_j c_{i-j}\right) b^i \\
&= \sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} \phi(a_i)\phi(c_{i-j})\right) b^i \\
&= \overline{\phi}(a(x))\overline{\phi}(c(x))
\end{aligned}$$

segue daí que $\overline{\phi}$ é um homomorfismo.

□

Corolário 1.6 *Se $h(x) \in \mathbf{F}[x]$ é tal que $h(x) = p_1(x)\cdots p_r(x)$, onde os $p_i's$ satisfazem* $\mathrm{mdc}(p_i(x), p_j(x)) = 1$, *sempre que $i \neq j$. Então:*

$$\frac{\mathbf{F}[x]}{h(x)} \cong \frac{\mathbf{F}[x]}{p_1(x)} \oplus \cdots \oplus \frac{\mathbf{F}[x]}{p_r(x)}$$

Demonstração: considere a função ϕ, tal que

$$\phi : \mathbf{F}[x] \longrightarrow \frac{\mathbf{F}[x]}{p_1(x)} \oplus \cdots \oplus \frac{\mathbf{F}[x]}{p_r(x)}$$

$$f(x) \mapsto \left(f(x) + (p_1(x)), \ldots, f(x) + (p_r(x))\right)$$

A função ϕ é um homomorfismo sobrejetor. De fato, dados $f, g \in \mathbf{F}[x]$, temos que

$$\phi((f+g)(x)) = \left(f(x) + g(x) + (p_1(x)), \ldots, f(x) + g(x) + (p_r(x)\right) =$$
$$= \left(f(x) + (p_1(x)), \ldots f(x) + (p_r(x))\right) + \left(g(x) + (p_1(x)), \ldots, g(x) + (p_r(x))\right) =$$
$$= \phi(f(x)) + \phi(g(x))$$

e ainda,

$$\phi((f\cdot g)(x)) = \left(f(x)\cdot g(x) + (p_1(x)), \ldots, f(x)\cdot g(x) + (p_r(x)\right) =$$
$$= \left(f(x) + (p_1(x)), \ldots f(x) + (p_r(x))\right)\cdot\left(g(x) + (p_1(x)), \ldots, g(x) + (p_r(x))\right) =$$
$$= \phi(f(x))\cdot\phi(g(x))$$

Tome $(a_1(x)+(p_1(x))+\cdots+a_r(x)+(p_r(x)))\in \dfrac{\mathbf{F}[x]}{p_1(x)}\oplus\cdots\oplus\dfrac{\mathbf{F}[x]}{p_r(x)}$, queremos determinar $h(x)\in\mathbf{F}[x]$ tal que $\phi(h(x))=(h(x)+(p_1)(x)+\cdots+h(x)+(p_r(x)))=(a_1(x)+(p_1(x))+\cdots+a_r(x)+(p_r(x)))$, o que acontece se, e somente se, o sistema

$$\begin{aligned} h(x) &\equiv a_1(x)\bmod(p_1(x)) \\ h(x) &\equiv a_2(x)\bmod(p_2(x)) \\ &\vdots \\ h(x) &\equiv a_r(x)\bmod(p_r(x)) \end{aligned}$$

tem solução. O que é consequência direta do teorema chinês do resto. Logo, a função ϕ é um homomorfismo sobrejetor.

Note que $ker(\phi)=(p_1(x)\cdots p_r(x))$, visto que $(f(x)+(p_1(x)),\ldots,f(x)+(p_r(x)))=(0,\ldots,0)$ se, e somente se,

$$\begin{aligned} f(x) &\equiv 0\bmod(p_1(x)) \\ f(x) &\equiv 0\bmod(p_2(x)) \\ &\vdots \\ f(x) &\equiv 0\bmod(p_r(x)) \end{aligned}$$

o polinômio $g(x)=0$ é solução do sistema e, pelo teorema do resto chinês, toda solução $f(x)$ do sistema satisfaz $f(x)\equiv 0\bmod(p_1(x)\cdots p_r(x))$. Portanto, $ker(\phi)=(p_1(x)\cdots p_r(x))$. Segue do teorema do isomorfismo que

$$\frac{\mathbf{F}[x]}{h(x)}\cong\frac{\mathbf{F}[x]}{p_1(x)}\oplus\cdots\oplus\frac{\mathbf{F}[x]}{p_r(x)}$$

□

1.3 Códigos Lineares

Os resultados apresentados nesta seção podem ser encontrados em [1].

Considere o corpo finito $\mathbf{K}$ com q elementos tomado como alfabeto. Sendo assim, para cada número natural n, existe um $\mathbf{K}$-espaço vetorial $\mathbf{K}^n$ de dimensão n.

Definição 1.14 *Um código $C \subset \mathbf{K}^n$ será chamado código linear se for um subespaço vetorial de K^n.*

Definição 1.15 *Dado $x \in \mathbf{K}^n$, define-se o peso de x como sendo o número inteiro*

$$\omega(x) = |\{i : x_i \neq 0\}|.$$

Segue daí que

$$\omega(x) = d(x, 0),$$

onde d representa a métrica de Hamming.

Definição 1.16 *O peso de um código linear C é o inteiro*

$$\omega(C) = min\{\omega(x) : x \in C\backslash\{0\}\}.$$

Proposição 1.9 *Seja $C \subset \mathbf{K}^n$ um código linear com distância mínima d. Temos que*
(i) $\forall x, y \in \mathbf{K}^n, d(x, y) = \omega(x - y)$.
(ii) $d = \omega(C)$.

Note que podemos descrever um código C de dimensão k através do núcleo de uma tranformação linear. Considere um subespaço C' de $\mathbf{K}^n$ complementar de C, então,

$$C \oplus C' = \mathbf{K}^n,$$

considere tambem a aplicação linear

$$H : C \oplus C' \longrightarrow \mathbf{K}^{n-k}$$

$$\mathbf{u} + \mathbf{v} \mapsto \mathbf{v}$$

cujo núcleo é C. Segue daí que para determinarmos se $\mathbf{v} \in \mathbf{K}^n$ pertence ou não a C, basta verificar se $H(\mathbf{v})$ é ou não o vetor nulo de $\mathbf{K}^{n-k}$.

Definição 1.17 *Seja $\mathbf{K}$ um corpo finito. Uma transformação linear $T : \mathbf{K}^n \longrightarrow K^n$ é chamada de isometria linear se é bijetora e se $d(\mathbf{u}, \mathbf{v}) = d(T(\mathbf{u}), T(\mathbf{v}))$ para todos $\mathbf{u}, \mathbf{v} \in \mathbf{K}^n$. Dois códigos lineares C e C' são linearmente equivalentes se existir uma isometria linear $T : \mathbf{K}^n \longrightarrow \mathbf{K}^n$ tal que $T(C) = C'$.*

Note que se C e C' são equivalentes então ambos têm mesma dimensão e distância miníma.

Seja $\mathbf{K}$ um corpo finito com q elementos e $C \subset \mathbf{K}^n$ um código linear. Seja $B = \{v_1, ..., v_k\}$ uma base ordenada de C e considere a matriz G, cujas linhas são os vetores $v_i = (v_{i1}, ..., v_{in})$, $i = 1, ..., k$.

A matriz G é chamada de *matriz geradora* de C associada à base B.

Considere a transformação linear definida por

$$T : \mathbf{K}^k \longrightarrow \mathbf{K}^n$$
$$x \mapsto xG$$

se $x = (x_1, ..., x_k)$, temos que

$$T(x) = xG = x_1\mathbf{v}_1 + ... + x_k\mathbf{v}_k,$$

logo $T(\mathbf{K}^k) = C$. Sendo assim podemos considerar $\mathbf{K}^k$ como sendo o código da fonte, C, o código de canal e a transformação T, uma codificação.

Observe que a matriz G não é univocamente determinada por C, pois ela depende da escolha da base B.

Definição 1.18 *Diremos que uma matriz geradora G de um código C está na forma padrão se tivermos*

$$G = (Id_k|A),$$

onde Id_k é a matriz identidade $k \times k$ e A, uma matriz $k \times (n-k)$.

Teorema 1.16 *Dado um código C, existe um código equivalente C' com matriz geradora na forma padrão.*

Demonstração: Ver [1].

Este resultado é uma interpretação do escalonamento de G. As operações de permutar linhas, multiplicar linha por escalar e multiplicar linha por escalar e somar com outra linha deram a nova base de C, a operação de trocar colunas corresponde a permutar coordenadas, que é uma isometria linear, e a matriz obtida é a matriz geradora de um código C' equivalente a C.

Dados $\mathbf{u} = (u_1, ..., u_n)$ e $\mathbf{v} = (v_1, ..., v_n)$ elementos de $\mathbf{K}^n$, definiremos o *produto interno* de $\mathbf{u}$ e $\mathbf{v}$ como sendo

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 + ... + u_n v_n.$$

Essa operação possui as propriedades usuais de um produto interno, simetria e bilinearidade, mas note que podemos ter $\langle \mathbf{u}, \mathbf{u} \rangle = 0$ e $\mathbf{u} \neq 0$. O que vale é que $\langle , \rangle$ é uma forma bilinear **não-degenerada**, isto é, dado $\mathbf{u} \in \mathbf{K}^n$, se $\langle \mathbf{u}, \mathbf{v} \rangle = 0, \forall \mathbf{v}$, então $\mathbf{u} = 0$.

Seja $C \subset \mathbf{K}^n$ um código linear, define-se

$$C^{\perp} = \{\mathbf{v} \in \mathbf{K}^n : \langle \mathbf{v}, \mathbf{u} \rangle = 0, \forall \mathbf{u} \in C\}.$$

Lema 1.4 *Se $C \subset \mathbf{K}^n$ é um código linear, como matriz geradora G, então*
(i) $C^{\perp}$ é um subspaço vetorial de $\mathbf{K}^n$;
(ii) $x \in C^{\perp} \Longleftrightarrow Gx^t = 0$.

Proposição 1.10 *Seja $C \subset \mathbf{K}^n$ um código de dimensão k com matriz geradora $G = (Id_k|A)$, na forma padrão. Então*
(i) $dim C^{\perp} = n - k$;
(ii) $H = (-A^t|Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.

Proposição 1.11 *Sejam C e D códigos lineares em $\mathbf{K}^n$. Se C e D são linearmente equivalentes, $C^{\perp}$ e $D^{\perp}$ são linearmente equivalentes.*

Corolário 1.7 *Se D é um código linear em $\mathbf{K}^n$ de dimensão k, então $D^{\perp}$ é um código de dimensão $n - k$.*

Lema 1.5 *Suponha que C seja um código de dimensão k em $\mathbf{K}^n$ com matriz geradora G. Uma matriz H de ordem $(n - k) \times n$, com coeficientes em $\mathbf{K}$ e com linhas linearmente independentes, é uma matriz geradora de $C^{\perp}$ se, e somente se,*

$$G \cdot H^t = 0.$$

Corolário 1.8 $(C^{\perp})^{\perp} = C$.

Proposição 1.12 *Seja C um código linear e suponhamos que H seja a matriz geradora de $C^{\perp}$. Temos que*

$$v \in C \Longleftrightarrow Hv^t = 0.$$

A matriz geradora de H de $C^{\perp}$ é chamada *matriz teste de paridade* de C ou simplesmente *matriz teste*. Para verificar se um determinado v em $\mathbf{K}^n$ pertence ou não ao código C basta verificar se é nulo o vetor Hv^t.

1.4 Códigos Cíclicos

Os códigos cíclicos constituem uma importante classe de códigos lineares devido a viabilidade de seus algoritmos de codificação e decodificação. No que segue, $\mathbf{K}$ é um corpo finito e representaremos as coordenadas de $\mathbf{K}^n$ por $(x_0, ..., x_{n-1})$.

Definição 1.19 *Um código linear $C \subset \mathbf{K}^n$ será chamado de código cíclico se, para todo $\boldsymbol{c} = (c_0, c_1, ..., c_{n-1})$ pertencente a C, o vetor $(c_{n-1}, c_0, ..., c_{n-2})$ pertence a C.*

Equivalentemente, se $T : \mathbf{F}^n \longrightarrow \mathbf{F}^n$ é tal que $T(c_0, ..., c_{n-1}) = (c_{n-1}, ..., c_{n-2})$, então $C \subset \mathbf{F}^n$ é cíclico se dado $\mathbf{c} \in C$ então $T\mathbf{c} \in C$.

Em sintese, a técnica base ao se lidar com códigos cíclicos é enriquecer a estrutura do espaço vetorial $\mathbf{K}^n$.

Seja R_n o anel das classes residuais em $\mathbf{K}[x]$ módulo $x^n - 1$, ou seja,

$$R_n = \mathbf{K}[x]/(x^n - 1).$$

Sendo assim, um elemento de R_n é um conjunto da forma

$$[f(x)] = \{f(x) + g(x)(x^n - 1) : g(x) \in \mathbf{K}[x]\};$$

usaremos a soma e multiplicação usual em R_n. Ressaltamos ainda que R_n está munido de multiplicação por escalares $\lambda \in \mathbf{K}$, definida por

$$\lambda[f(x)] = [\lambda f(x)],$$

e que é um $\mathbf{K}$-espaço vetorial de dimensão n com base $\{1, [x], ..., [x^{n-1}]\}$, isomorfo a $\mathbf{K}^n$ como $\mathbf{K}$-espaço vetorial pela transformação linear

$$\upsilon : \mathbf{K}^n \longrightarrow R_n$$
$$(a_0, ..., a_{n-1}) \mapsto [a_0 + a_1 x + ... + a_{n-1} x^{n-1}].$$

As vantagens de estarmos trabalhando sobre R_n é que, além de ser um espaço vetorial, este conta com a estrutura adicional de anel e a imagem de um código cíclico por $\mathbf{K}^n$ tem uma estrutura algébrica de ideal, o que será mostrado posteriormente.

Proposição 1.13 *Todo ideal de* $\mathbf{K}[x]$ *é da forma* $(F(x))$*, onde* $F(x) \in \mathbf{K}[x]$.

Demonstração:

Seja I um ideal de $\mathbf{K}[x]$. Se $I = 0$, tomando $F(x) = 0$, temos que $I = (F(x))$. Se $I \neq 0$, seja $F(x) \neq 0$ em I tal que $F(x)$ seja de menor grau possivel, o objetivo é provar que $I = (F(x))$.

Uma vez que $F(x) \in I$, temos claramente que o ideal principal gerado por $F(x)$ está contido em I. Resta provar a outra inclusão. Tome $G(x) \in I$. Segue do algoritmo da divisão que existem polinômios $Q(x)$ e $R(x)$ com $R(x) = 0$ ou $\text{gr}(R(x)) < \text{gr}(F(x))$ tais que

$$G(X) = F(x)Q(x) + R(x).$$

Como $-F(x)Q(x) \in I$, segue que

$$R(x) = G(x) - F(x)Q(x) \in I.$$

Da expressão acima, se $R(x) \neq 0$, teríamos um elemento $R(x)$ em I de grau menor do que o grau de $F(x)$, o que contraria o fato de $F(x)$ ter grau minímo. Portanto $R(x) = 0$ e daí $G(x) = F(x)Q(x) \in (F(x))$.

□

Corolário 1.9 *Seja* $I \neq \{0\}$ *um ideal de* $\mathbf{K}[x]$*. Então, existe um único polinômio mônico* $F(x)$ *em* I *(de grau mínimo) tal que* $I = (F(x))$.

Demonstração: A existência de $F(x)$ é resultado direto da proposição 1.13. Provemos a unicidade. Se $F(x)$ é um gerador de I, então, para toda constante não nula $c \in \mathbf{K}$, temos que $cF(x)$ é um gerador de I. Por outro lado se $F(x)$ e $G(x)$ são geradores de um ideal I, isto é, se

$$I = (F(x)) = (G(x)),$$

então $F(x)$ e $G(x)$ são associados. De fato, na situação acima temos que

$$F(x) = A(x)G(x) \text{ e } G(x) = B(x)F(x).$$

Se $F(x) = 0$, então $G(x) = 0$, e o resultado segue nesse caso. Se $F(x) \neq 0$, das relações acima entre $F(x)$ e $G(x)$, segue que $F(x) = A(x)B(x)F(x)$. Como $\mathbf{K}[x]$ é um domínio, segue que $A(x)B(x) = 1$ e, portanto, $A(x)$ e $B(x)$ são invertíveis, provando que $F(x)$ e $G(x)$ são associados. Segue daí que, se $F(x)$ é mônico e $G(x)$ é outro gerador, então $G(x) = \alpha F(x)$ e $G(x)$ é mônico se, e somente se, $\alpha = 1$ o que acontece se, e somente se $G(x) = F(x)$.

□

Definição 1.20 *Um anel onde todo ideal é principal será chamado anel de ideiais principais.*

Logo, segue da proposição 1.13 e da definição acima que o anel de polinômios $\mathbf{K}[x]$ é um anel de ideias principais. O anel R_n também é um anel de ideais principais, como mostra o resultado a seguir.

Proposição 1.14 *Todo ideal de $\mathbf{K}[x]/(P(x))$ é da forma $([F(x)])$, onde $F(x)$ é um divisor de $P(x)$.*

Demonstração:

Seja I um ideal de $\mathbf{K}[x]/(P(x))$. Considere o conjunto

$$J = \{G(x) \in \mathbf{K}[x] : [G(x)] \in I\}$$

Em princípio, provemos que J é um ideal de $\mathbf{K}[x]$. De fato, se $G_1(x), G_2(x) \in J$, então $[G_1], [G_2] \in I$. E portanto,

$$[G_1(x) + G_2(x)] = [G_1(x)] + [G_2(x)] \in I,$$

conseqüentemente, $G_1(x)+G_2(x) \in J$. Ainda, se $G(x) \in J$ e $H(x) \in \mathbf{K}[x]$, temos que $[G(x)] \in I$, e portanto, $[G(x)H(x)] = [G(x)][H(x)] \in I$. Segue daí que $G(x)H(x) \in J$.

Temos que $J \neq 0$, pois $P(x) \in J$, segue da proposição 1.13 que existe $F(x) \in \mathbf{K}[x] \setminus \{0\}$ tal que $J = (F(x))$.

Uma vez que $P(x) \in J = (F(x))$, segue que $P(x)$ é um múltiplo de $F(x)$, sendo assim, $F(x)$ é um divisor de $P(x)$.

Como $I = \{[G(x)] : G(x) \in J\}$ e $J = (F(x))$, tem-se

$$I = \{[H(x)][F(x)] : [H(x)] \in K[x]/P(x)\} = ([F(x)]).$$

□

Para determinarmos matrizes geradoras e matrizes teste de paridade de códigos cíclicos é necessário caracterizar os códigos cíclicos em R_n, o que será feito na sequência.

Note que a ação de T em $\mathbf{K}^n$, por meio da aplicação υ, é equivalente a multiplicação por $[x]$ em R_n.

Tome $\mathbf{c} = (c_0, ..., c_{n-1})$, temos

$$T(\mathbf{c}) = (c_{n-1}, ..., c_{n-2})$$

e

$$\begin{aligned} \upsilon(T(\mathbf{c})) &= [c_{n-1} + c_0 x + ... + c_{n-2}x^{n-1}] = \\ &= [x][c_0 + c_1 x + ... + c_{n-1}x^{n-1}] = \\ &= [x]\upsilon(\mathbf{c}) \end{aligned}$$

Lema 1.6 *Seja V um subespaço vetorial de R_n. Então, V é um ideal de R_n se, e somente se, V é fechado pela multiplicação por $[x]$.*

Demonstração:

Suponhamos que seja um ideal de R_n. Da definição de Ideal, segue que $[x][f(x)] \in V$ para todo $[f(x)] \in V$.

Reciprocamente, suponhaque V é fechado pela multiplicação por $[x]$. Como V é subspaço é suficiente mostrar que $[g(x)][f(x)] \in V$ para todo $[g(x)] \in R_n$ e todo $[f(x)] \in V$.

Seja $[f(x)] \in V$. Como V é um subespaço de R_n, é claro que $a[f(x)] \in V$, para todo $a \in K$. Da hipótese,

$$[xf(x)] = [x][f(x)] \in V,$$

logo

$$[x^2 f(x)] = [x][xf(x)] \in V$$

e segue por indução que

$$[x^m f(x)] = [x^m][f(x)] \in V$$

para todo $m \in \mathbb{N}$.

A partir disto, segue que, se escrevermos $[g(x)] = [a_0 + a_1 x + ... + a_{n-1}x^{n-1}]$, temos que

$$\begin{aligned} [g(x)][f(x)] &= [g(x)f(x)] = \\ &= [(a_0 + a_1 x + ... + a_{n-1}x^{n-1})f(x)] = \\ &= a_0[f(x)] + a_1[x][f(x)] + ... + a_{n-1}[x^{n-1}][f(x)] \in V \end{aligned}$$

visto que V é um subespaço e cada parcela da ultima expressão pertence a V.

□

Teorema 1.17 *Um subespaço C de $\mathbf{K}^n$ é um código cíclico se, e somente se, $\upsilon(C)$ é um ideal de R_n.*

Demonstração: Dado $(a_0, ..., a_{n-1}) \in C$, temos que $[a_0 + a_1 x + ... + a_{n-1}x^{n-1}] \in \upsilon(C)$; como $\upsilon(C)$ é um ideal temos que

$$[x][a_0 + a_1 x + ... + a_{n-1}x^{n-1}] = [a_{n-1} + a_0 x + ... + a_{n-2}x^{n-1}] \in \upsilon(C)$$

e como υ é bijetora temos que $(a_{n-1}, a_0, \ldots, a_{n-2}) \in C$.

Reciprocamente, se $(a_0, ..., a_{n-1}) \in C$ temos que $(a_{n-1}, a_0, \ldots, a_{n-2}) \in C$, então para todo $[a(x)] \in \upsilon(C)$ temos $[xa(x)] \in \upsilon(C)$, pelo lema anterior $\upsilon(C)$ é um ideal de R_n.

□

Logo, da proposição 1.14 temos que um código C em $\mathbf{K}^n$ é cíclico se, e somente se, $\upsilon(C) = ([g(x)])$, onde $g(x) \in K[x]$ é um divisor de $x^n - 1$.

Se $p = \text{car}(\mathbf{K})$ e $n = mp^s$ com m e p primos entre si, temos que

$$x^n - 1 = ((x^m)^{p^s} - 1) = (x^m - 1)^{p^s}.$$

Afirmamos que $x^m - 1$ admite uma decomposição na forma

$$x^m - 1 = f_1 ... f_r,$$

onde os f_i são irredutíveis e dois a dois distintos.

De fato, temos que $(x^m - 1)' = mx^{m-1} \neq 0$. Se $\text{mdc}(mx^{m-1}, x^m - 1) = g(x) \neq 1$, então $x \mid g(x)$ e daí $x \mid x^m - 1$, e 0 é raiz de $x^m - 1$, o que é um absurdo. Portanto $x^m - 1$ não tem fator em comum com sua derivada.

Suponhamos $x^m - 1 = (g(x))^k h(x)$, com $k \geq 2$, então

$$mx^{m-1} = kg(x)^{k-1} h(x) + (g(x))^k h'(x),$$

o que implicaria em $x^m - 1$ ter fator em comum com sua derivada, o que é um absurdo.

Consequentemente, a decomposição de $x^m - 1$ em irredutíveis em $\mathbf{K}[x]$ não tem fatores repetidos e podemos escrever

$$x^m - 1 = f_1 ... f_r,$$

onde os f_i são irredutíveis e dois a dois distintos. Logo, a decomposição em fatores irredutiveis de $x^n - 1$ é,

$$x^n - 1 = f_1^{p^s} ... f_r^{p^s}.$$

Segue, então, que o polinômio $x^n - 1$ tem exatamente $(p^s + 1)^r$ divisores mônicos. Como existe um bijeção entre os ideais de $\mathbf{K}[x]/(x^n - 1)$ e os divisores mônicos de $x^n - 1$, temos que R_n possui precisamente $(p^s + 1)^r$ ideais.

Observe que R_n não é um domínio de integridade. Daqui por diante, $g(x)$ denotará um divisor de $x^n - 1$, e poremos

$$h(x) = \frac{x^n - 1}{g(x)}.$$

Teorema 1.18 *Seja $I = ([g(x)])$, onde $g(x)$ é um divisor de $x^n - 1$ de grau s. Temos que $[g(x)], [xg(x)], ..., [x^{n-s-1} g(x)]$ é uma base de I como espaço vetorial sobre $\mathbf{K}$.*

Demonstração: Os elementos acima são linearmente independentes. Suponhamos que

$$a_0[g(x)] + a_1[xg(x)] + ... + a_{n-s-1}[x^{n-s-1}] = [0].$$

Logo,

$$[g(x)][a_0 + a_1x + ... + a_{n-s-1}x^{n-s-1}] = [0].$$

Portanto, existe $d(x) \in \mathbf{K}[x]$, tal que

$$g(x)(a_0 + a_1x + ... + a_{n-s-1}x^{n-s-1}) = d(x).(x^n - 1).$$

Daí , temos que

$$(a_0 + a_1x + ... + a_{n-s-1}x^{n-s-1}) = d(x)h(x).$$

visto que o grau de $h(x)$ é $n - s$, devemos ter $d(x) = 0$, e consequentemente, $a_0 = a_1 = ... = a_{n-s-1} = 0$.

Os elementos acima geram I sobre $\mathbf{K}$. De fato, se $[f(x)] \in I$, temos que

$$f(x) \equiv d(x)g(x) \bmod(x^n - 1).$$

Pelo algoritmo da divisão, temos que $d(x) = h(x)c(x) + r(x)$, com $r(x) = a_0 + a_1x + ... + a_{n-s-1}x^{n-s-1}$. Logo,

$$f(x) \equiv d(x).g(x) \equiv c(x).h(x).g(x) + r(x).g(x) \bmod(x^n - 1).$$

e portanto,

$$f(x) \equiv c(x)(x^n - 1) + r(x)g(x) \equiv r(x)g(x) \bmod(x^n - 1).$$

Consequentemente,

$$[f(x)] = a_0[g(x)] + a_1[xg(x)] + ... + a_{n-s-1}[x^{n-s-1}g(x)].$$

□

Corolário 1.10 *Dado um código cíclico C, existe $\mathbf{v} \in C$ tal que $C = \langle \mathbf{v} \rangle$.*

Demonstração:

Seja $I = \upsilon(C)$. Logo, I é gerado como K-espaço vetorial por $[g(x)], [xg(x)], ..., [x^{n-s-1}g(x)]$, onde $g(x)$ é um divisor de $x^n - 1$. Portanto, colocando $\mathbf{v} = \upsilon^{-1}([g(x)])$, temos que C é gerado por $\mathbf{v}, T\mathbf{v}, ..., T^{n-s-1}\mathbf{v}$, e portanto, $C = \langle \mathbf{v} \rangle$.

Corolário 1.11 *Seja $g(x) = g_0 + g_1x + ... + g_sx^s$ um divisor de $x^n - 1$ de grau s. Se $I = I([g(x)])$, então*

$$\dim_{\mathbf{K}} = n - s,$$

e o código $C = \upsilon^{-1}(I)$ tem matriz geradora

$$G = \begin{pmatrix} \upsilon^{-1}([g(x)]) \\ \upsilon^{-1}([xg(x)]) \\ \vdots \\ \upsilon^{-1}([x^{n-s-1}g(x)]) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & ... & g_s & 0 & ... & 0 \\ 0 & g_0 & g_1 & ... & g_s & ... & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & g_0 & \cdots & & g_s \end{pmatrix}$$

Demonstração: Ver [1].

Definição 1.21 *Sejam* $\mathbf{K}$ *um corpo e* $f(x) \in \mathbf{K}[x]$ *de grau* n*. Define-se o polinômio recíproco de* $f(x)$ *como sendo o polinômio*

$$f^*(x) = x^n f\left(\frac{1}{x}\right).$$

Proposição 1.15 *Dados polinômios* f *e* g *temos que:*

(i) $(f.g)^* = f^*.g^*$

(ii) $(f^*)^* = f$

Segue daí que se um polinômio $h(x) = h_0 + h_1x + ... + h_tx^t$ divide $x^n - 1$ então seu recíproco também é um divisor de $x^n - 1$, e portanto gerador de algum código Cíclico.

Teorema 1.19 *Seja* $C = \upsilon^{-1}(I)$ *um código cíclico, onde* $I = ([g(x)])$*, com* $g(x)$ *um divisor de* $x^n - 1$*. Então* $C^\perp$ *é cíclico e* $C^\perp = \upsilon^{-1}(J)$*, onde* $J = ([h^*(x)])$*.*

Demonstração: Ver [1].

Corolário 1.12 *A matriz teste de paridade de* $C = \nu^{-1}(I)$*, em que* $I = ([G(x)])$*, é dada por*

$$H = \begin{pmatrix} h_{n-s} & h_{n-s-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \cdots & h_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & h_{n-s} & \cdots & & h_0 \end{pmatrix}$$

onde

$$\frac{x^n - 1}{g(x)} = h_0 + h_1(x) + \cdots + h_{n-s}x^{n-s}.$$

Demonstração: Ver [1].

Capítulo 2

Códigos Quase-Cíclicos

2.1 Códigos Quase-Cíclicos

Seja $\mathbf{F}$ um corpo finito . Quando for necessário especificar a cardinalidade q de $\mathbf{F}$, escreveremos $\mathbf{F} = \mathbf{F}_q$. O dual $C^{\perp}$ de um código C será entendido com relação ao produto interno padrão. Um código C é *auto-dual* se $C = C^{\perp}$. Denotaremos por T o operador deslocamento ("Shift") padrão em $\mathbf{F}^n$, isto é,

$$T(c_0, c_1, \ldots, c_n) = (c_n, c_0, \ldots, c_{n-1})$$

Definição 2.1 *Um código linear é dito quase-cíclico de índice l ou l-quase-cíclico se, e somente se, é invariante por T^l.*

O caso em que $l = 1$, coincide com o caso que o código é cíclico. Durante todo trabalho assumiremos que o índice l divide o comprimento n.

Seja $\mathbf{F}$ um corpo finito e m um inteiro positivo coprimo com a característica de $\mathbf{F}$. $\mathbf{F}[x]$ denotará os polinômios em uma variável x com coeficientes em $\mathbf{F}$. Como já visto, o anel $R = R(\mathbf{F}, m) = \mathbf{F}[x]/(x^m - 1)$ é usado na representação polinomial de códigos cíclicos de comprimento m sobre $\mathbf{F}$, uma vez que esses são ideais de $R(\mathbf{F}, m)$.

Observação: Daqui para frente neste trabalho, denotaremos o elemento $c(x) + (f(x))$ de $\mathbf{F}[x]/(f(x))$ por $[c(x)]$ ou mesmo $c(x)$.

Seja C um código quase-cíclico sobre $\mathbf{F}$ de índice l e comprimento lm. Denotaremos uma palavra em C como

$$\mathbf{c} = (c_{00}, c_{01}, \ldots, c_{0,l-1}, c_{10} \ldots, c_{1,l-1}, \ldots, c_{m-1,0}, \ldots c_{m-1,l-1}).$$

Seja $\phi : \mathbf{F}^{lm} \to R^l$ definida por

$$\phi(\mathbf{c}) = (\mathbf{c}_0(x), \mathbf{c}_1(x), \ldots, \mathbf{c}_{l-1}(x)) \in R^l$$

onde

$$\mathbf{c}_j(x) = \sum_{i=0}^{m-1} c_{ij} x^i \in R^l.$$

No que segue $\phi(C)$ denota a imagem de C por ϕ.

Lema 2.1 *(San Ling e Patrick Solé) A função ϕ induz uma bijeção entre códigos quase-cíclicos sobre $\mathbf{F}$ de indice l e comprimento lm e códigos lineares sobre R de comprimento l.*

Demonstração: ϕ é claramente bijetora. Como C é um código linear finito, $\phi(C)$ é fechado pela multiplicação por escalares de $\mathbf{F}$ e por soma de vetores, isto é, $\phi(v)$ e $\phi(u) \in \phi(C)$, então $\phi(v) + \phi(u) = \phi(v + u) \in \phi(C)$ (pois $v + u \in C$). Como $x^m = 1$ em R, temos que

$$x\mathbf{c}_j(x) = \sum_{i=0}^{m-1} c_{ij} x^{i+1} = \sum_{i=0}^{m-1} c_{i-1,j} x^i.$$

onde o índice $i - 1$ é tomado em $\{0, 1, \ldots, m-1\}$ módulo m.

A palavra

$$(x\mathbf{c}_0(x), x\mathbf{c}_1(x), \ldots, x\mathbf{c}_{l-1}(x)) \in R^l$$

corresponde a palavra

$$(c_{m-1,0}, c_{m-1,1}, \cdots, c_{m-1,l-1}, c_{00}, c_{01}, \ldots, c_{0,l-1}, \cdots, c_{m-2,0}, \ldots, c_{m-2,l-1}) \in \mathbf{F}^{lm}$$

que está em C, visto que C é quase-cíclico. Portanto, $\phi(C)$ é fechado pela multiplicação por x e desde já $\phi(C)$ é um R-submódulo de R^l.

Revertendo o argumento acima, vemos imediatamente que todo código R-linear R de comprimento l vem de um código quase-cíclico de índice l e comprimento lm sobre $\mathbf{F}$.

□

Afim de estudarmos a dualidade de códigos lineares sobre R, e a relação com códigos lineares sobre $\mathbf{F}$, definiremos a função conjugação $^-$ em R. Note que como $x^m = xx^{m-1} = 1$ em R, x é invertível em R, com $x^{-1} = x^{m-1}$. Definimos a função conjugação$f(x) \mapsto \overline{f(x)}$ como o isomorfismo de R em R que fixa os elementos de $\mathbf{F}$ e envia x em x^{-1}. Ou seja, se $f(x) = a_0 + a_1x + \ldots + a_{m-1}x^{m-1}$, então

$$\begin{aligned}\varphi(a_0 + a_1x + \ldots + a_{m-1}x^{m-1}) &= a_0 + a_1x^{-1} + \ldots + a_{m-1}x^{-m+1} \\ &= a_0 + a_1x^{m-1} + \ldots + a_{m-1}x\end{aligned}$$

Em $\mathbf{F}^{lm}$ usaremos o produto interno Euclidiano usual, isto é, se

$$\mathbf{a} = (a_{00}, a_{01}, \ldots, a_{0,l-1}, a_{10} \ldots, a_{1,l-1}, \ldots, a_{m-1,0}, \ldots a_{m-1,l-1}).$$

e

$$\mathbf{b} = (b_{00}, b_{01}, \ldots, b_{0,l-1}, b_{10} \ldots, b_{1,l-1}, \ldots, b_{m-1,0}, \ldots b_{m-1,l-1}).$$

então

$$\mathbf{a} \cdot \mathbf{b} = \sum_{i=0}^{m-1} \sum_{j=0}^{l-1} a_{ij} b_{ij}.$$

Em R^l, definiremos o produto interno Hermitiano: para $\mathbf{x} = (x_0, \cdots, x_{l-1})$ e $\mathbf{x} = (x_0, \ldots, x_{l-1})$, teremos

$$\langle x, y \rangle = \sum_{i=0}^{m-1} x_j \overline{y_j}.$$

Proposição 2.1 *(San Ling e Patrick Solé) Se* $\mathbf{a}, \mathbf{b} \in \mathbf{F}^{lm}$. *Então* $(T^{lk}(\mathbf{a})).\mathbf{b} = 0$ *para todo* $0 \leq k \leq m-1$ *se, e somente se,* $\langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0$.

Demonstração: A condição $\langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0$ é equivalente a

$$\begin{aligned}0 &= \sum_{j=0}^{l-1} a_j \overline{b_j} = \sum_{j=0}^{l-1} (\sum_{i=0}^{m-1} a_{ij} y^i)(\sum_{k=0}^{m-1} b_{kj} y^{-k}) \\ &= \sum_{j=0}^{l-1} \sum_{i=0}^{m-1} \sum_{k=0}^{m-1} a_{ij} b_{kj} y^{i-k} = (*)\end{aligned} \tag{2.1}$$

fazendo $i - k = h$, temos que

$$(*) = \sum_{h=0}^{m-1} \left[\sum_{j=0}^{l-1} \sum_{k=0}^{m-1} a_{k+h,j} b_{k,j} \right] y^h$$

comparando os coeficientes de y^h em ambos lados , temos que

$$\sum_{i=0}^{l-1}\sum_{i=0}^{m-1} a_{k+h,j}b_{kj} = 0, \text{para todo } 0 \leqslant h \leqslant m-1 \tag{2.2}$$

onde o índice $i+h$ é tomado módulo m. Da equação acima temos mais precisamente que $(T^{-lh}(\mathbf{a})).\mathbf{b} = 0$. Como $T^{-lh} = T^{l(m-h)}$, segue que $\langle\phi(\mathbf{a}), \phi(\mathbf{b})\rangle = 0$, é equivalente a $(T^{lh}(\mathbf{a})).\mathbf{b} = 0$ para todo $0 \leqslant h \leqslant m-1$.

□

Da proposição 2.1 com $\mathbf{a}$ pertencente a um código l-quase cíclico C de comprimento lm sobre F, obtemos o seguinte.

Corolário 2.1 *Se C é um código quase-cíclico sobre $\mathbf{F}$ de comprimento lm e de índice l e se $\phi(C)$ é a imagem em R^l por ϕ, então $\phi(C)^\perp = \phi(C^\perp)$, onde o dual em $\mathbf{F}^{lm}$ é tomado com respeito ao produto interno euclidiano, e o dual em R^l é tomado com respeito ao produto interno Hermitiano. Em particular, um código quase-cíclico C sobre F é auto-dual com respeito ao produto interno euclidiano se, e somente se, $\phi(C)$ é autodual sobre R com respeito ao produto interno Hermitiano.*

Demonstração: Tome $\mathbf{v} \in \phi(C)^\perp$, como ϕ é sobrejetora existe $\mathbf{b} \in \mathbf{F}_q^{lm}$ tal que $\mathbf{v} = \phi(\mathbf{b})$. Daí, se $\langle\phi(\mathbf{a}), \phi(\mathbf{b})\rangle = 0\ \forall \mathbf{a} \in C$, então $T^{lk}(\mathbf{a}).b = 0\ \forall \mathbf{a} \in C$ e $\forall k$, em particular para $k = 0$, $\mathbf{a}.\mathbf{b} = 0$, $\forall \mathbf{a} \in C$, logo $\mathbf{b} \in C^\perp$ implica $\phi(C)^\perp \subset \phi(C^\perp)$. Por outro lado, se $\mathbf{b} \in C^\perp$, dado $\mathbf{a} \in C$ temos que $\mathbf{a}.\mathbf{b} = 0$. Como $\mathbf{a} \in C$ e C é quase-cíclico, temos que $T^{lk}(\mathbf{a}) \in C,\ \forall k$, daí e do fato que $\mathbf{b} \in C^\perp$, vem que $T^{lk}(\mathbf{a}) \cdot \mathbf{b} = 0$, $\forall k$, logo $\langle\phi(\mathbf{a}), \phi(\mathbf{b})\rangle = 0$ para todo $\mathbf{a}$ e portanto $\phi(\mathbf{b}) \in (\phi(C))^\perp$.

□

2.2 Decomposição de Códigos Quase-Cíclicos e Dualidade

Quando $m > 1$, o anel $R = R_m = \mathbf{F}[x]/(x^m - 1)$ não é um corpo. No entanto, do teorema chinês do resto, temos que se m é coprimo com a característica de $\mathbf{F}$, então o anel é um soma direta de corpos finitos. De fato, sob essa hipótese, o polinômio $x^m - 1$ fatora-se em fatores irredutíveis distintos em $\mathbf{F}[x]$, isto é, podemos escrever $x^m - 1 \in \mathbf{F}[x]$ como

$$x^m - 1 = f_1 f_2 \cdots f_r.$$

onde os $f'_j s$ são polinômios irredutíveis não associados dois a dois. Este produto é unico no sentido que, $x^m - 1 = f'_1.f'_2 \cdots f'_s$ é outra decomposição em polinômios, então $r = s$ e, depois de reenumerações adequadas dos f'_j, temos que f_j é um associado de f'_j para cada $1 \leqslant j \leqslant r$. Pelo corolário 1.6 temos

$$\frac{\mathbf{F}[x]}{(x^m - 1)} \cong \frac{\mathbf{F}[x]}{(f_1(x))} \oplus \cdots \oplus \frac{\mathbf{F}[x]}{(f_r(x))}$$

onde cada anel $\mathbf{F}[x]/(f_i)$ é um corpo pois f_i é irredutível.

Para um polinômio f, se f^* denota o polinômio recíproco, então $(f^*)^* = f$. Como $(x^m - 1)^* = -x^m + 1$ e $(f.g)^* = f^*.g^*$, temos que

$$x^m - 1 = -f_1^*.f_2^* \cdots f_r^*.$$

Se f é um polinômio irredutível, f^* também é irredutível. Da unicidade da decomposição de polinômios em fatores irredutíveis, podemos escrever

$$x^m - 1 = g_1 \cdots g_s h_1.h_1^* \cdots h_t.h_t^*.$$

onde $g_1, \ldots, g_s$ são os $f'_j s$ associados aos seus recíprocos, e $h_1, h_1^*, \ldots, h_t, h_t^*$ são os remanescentes $f'_j s$ agrupados em pares.

Segue do corolário 1.6 que podemos escrever

$$R = \frac{\mathbf{F}[x]}{x^m - 1} \cong \left(\bigoplus_{i=1}^{s} \frac{\mathbf{F}[x]}{(g_i)} \right) \oplus \left(\bigoplus_{j=1}^{t} \left(\frac{\mathbf{F}[x]}{(h_j)} \oplus \frac{\mathbf{F}[x]}{(h_j^*)} \right) \right) \tag{2.3}$$

Por simplicidade de notação, fixado m, denotaremos $\mathbf{F}[x]/(g_i)$ por G_i, $\mathbf{F}(x)/(h_j)$

por H'_j e $\mathbf{F}(x)/(h^*_j)$ por H''_j.

Segue da decomposição 2.3 e do teorema 1.4 que

$$R^l \cong \left(\bigoplus_{i=1}^{s} G_i^l\right) \oplus \left(\bigoplus_{j=1}^{t} \left(H_j'^l \oplus H_j''^l\right)\right)$$

como R-módulo.

Por definição, se C é um código R-linear de comprimento l então C é um R-submódulo de R^l. Segue do teorema 1.4 que existem subespaços $C_i, i = 1, ..., s$, $C'_j, j = 1, ..., t$ e $C''_j, j = 1, ..., t$ tais que

$$C = \left(\bigoplus_{i=1}^{s} C_i\right) \oplus \left(\bigoplus_{j=1}^{t} \left(C'_j \oplus C''_j\right)\right)$$

onde, para cada $1 \leqslant i \leqslant s$, C_i é um código linear sobre G_i de comprimento l e, para cada $1 \leqslant j \leqslant t$, C'_j é um código linear sobre H'_j de comprimento l e C''_j é um código linear sobre H''_j de comprimento l.

Todo elemento de R pode ser escrito como $\mathbf{c}(x)$ para algum polinômio $\mathbf{c} \in \mathbf{F}[x]$. A decomposição 2.3 prova que $\mathbf{c}(x)$ pode também ser escrito como uma $(s+2t)$-upla

$$(c_1(x), \ldots, c_s(x), c'_1(x), c''_1(x), \ldots, c'_t(x), c''_t(x)) \tag{2.4}$$

onde $c_i(x) \in G_i (1 \leqslant i \leqslant s)$, $c'_j(x) \in H'_j$, e $c''_j(x) \in H''_j (1 \leqslant j \leqslant t)$

Para qualquer elemento $\mathbf{r} \in R^l$, podemos definir a conjugação $\overline{\mathbf{r}} \in R^l$, induzida pela função $x \mapsto x^{-1}$ em R. Suponha que $\mathbf{r}$ possa ser expresso em termos da decomposição (2.3), como

$$\mathbf{r} = (r_1, \ldots, r_s, r'_1, r''_1, \ldots, r'_t, r''_t),$$

onde $r_i \in G_i (1 \leqslant i \leqslant s), r'_j \in H'_j$, e $r''_j \in H''_j (1 \leqslant j \leqslant t)$.

Nosso objetivo agora é descrever $\overline{\mathbf{r}}$ em termos da decomposição dada por

$$\left(\bigoplus_{i=1}^{s} G_i\right) \oplus \left(\bigoplus_{j=1}^{t} \left(H'_j \oplus H'_j\right)\right)$$

Em princípio note que se f divide x^m-1, então $x^m-1=g(x)f(x)$. Daí $x^m-1\equiv 0 \bmod(f)$ em cada anel $\mathbf{F}[x]/(f)$, e portanto $[x]$ é invertível em $\mathbf{F}[x]/(f)$ com inverso $[x]^{-1}=[x]^{m-1}$.

Teorema 2.1 *Se $f\in\mathbf{F}[x]$ é um fator irredutível de x^m-1, então a aplicação*

$$\frac{\mathbf{F}[x]}{(f)}\longrightarrow\frac{\mathbf{F}[x]}{(f^*)}$$

$$c(x)+(f)\longrightarrow c(x^{-1})+(f^*) \tag{2.5}$$

é um isomorfismo de corpos.

Demonstração: Considere ϕ tal que

$$\mathbf{F}[x]\longrightarrow\frac{\mathbf{F}[x]}{(f^*)}$$
$$c(x)\longrightarrow c(x^{-1})+(f^*)$$

segue da proposição 1.8 que ϕ é um homomorfismo.

Mostremos agora que ϕ é sobrejetora. De fato, dado $c(x)+(f^*)\in\mathbf{F}[x]/(f^*)$, considere o polinômio $c(x^{m-1})$, então

$$\phi(c(x^{m-1}))=c(x^{-(m-1)})+(f^*)=c((x^{m-1})^{-1})+(f^*)=c((x^{-1})^{-1})+(f^*)=c(x)+(f^*),$$

donde ϕ é sobrejetora. Por último temos que $\phi(c(x))=0$ se, se e somente se, $c(x^{-1})+(f^*)=0$, isto é, se $c(x^{-1})\equiv 0\bmod(f^*)$. Façamos $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$ então:

$$\begin{aligned}
\phi(f(x))=f(x^{-1}) &\equiv a_nx^{-n}+a_{n-1}x^{1-n}+\cdots+a_1x^{-1}+a_0x^m \bmod(f^*)\\
&\equiv a_nx^{m-n}+a_{n-1}x^{m-(n-1)}+\cdots+a_1x^{m-1}+a_0x^m \bmod(f^*)\\
&\equiv a_nx^{m-n}+a_{n-1}x^{m-(n-1)}+\cdots+a_1x^{m-1}+a_0x^m \bmod(f^*)\\
&\equiv x^{m-n}\cdot(a_n+a_{n-1}x+\cdots+a_1x^{n-1}+a_0x^n)\bmod(f^*)\\
&\equiv x^{m-n}f^*(x)\equiv 0\ mod(f^*)
\end{aligned}$$

a última passagem se deve ao fato que $f^* \equiv 0 \bmod(f^*)$.

Daí, como f é irredutível, temos que $ker(\phi) = (f)$, logo segue do teorema do isomorfismo que

$$\frac{\mathbf{F}[x]}{(f)} \longrightarrow \frac{\mathbf{F}[x]}{(f^*)}$$
$$c(x) + (f) \longrightarrow c(x^{-1}) + (f^*)$$

é um isomorfismo.

□

Desde já, o fato de f e f^* dividirem $x^m - 1$ implica que $x^m = 1$ em ambos estes anéis. No caso em que f e f^* são associados, vemos da aplicação 2.5 que a aplicação $x \mapsto x^{-1}$ induz um automorfismo de $\mathbf{F}[x]/(f)$. Quando o grau de f é 1, o isomorfismo é a aplicação identidade, isto é $\overline{r} = r$. Denotaremos por $\overline{r}$ a imagem de $r \in \mathbf{F}[x]/(f)$ pelo isomorfismo 2.5.

Como os $g_i's$ são os $f_j's$ associados aos seus recíprocos, temos que o ideal gerado por g_i é igual ao ideal gerado por g_i^*. Logo, dado $r_i \in G_i$, temos do isomorfismo 2.5 que

$$\frac{\mathbf{F}[x]}{(g_i)} \longrightarrow \frac{\mathbf{F}[x]}{(g_i)}$$
$$r_i(x) + (g_i) \longmapsto r_i(x^{-1}) + (g_i)$$

isto é, a imagem de r_i pelo isomorfismo 2.5 é igual a seu conjugado.

A partir do isomorfismo 2.5 definiremos a aplicação ψ, dada por

$$\psi : \left(\bigoplus_{i=1}^{s} G_i\right) \oplus \left(\bigoplus_{j=1}^{t} (H_j' \oplus H_j'')\right) \longrightarrow \left(\bigoplus_{i=1}^{s} G_i\right) \oplus \left(\bigoplus_{j=1}^{t} (H_j' \oplus H_j')\right)$$

onde

$$\psi(r(x)+(g_1), \ldots, r(x)+(g_s), r(x)+(h_1), r(x)+(h_1^*), \ldots, r(x)+(h_t), r(x)+(h_t^*) =$$

$$= (r(x)+(g_1), \ldots, r(x)+(g_s), r(x)+(h_1), r(x^{-1})+(h_1^*), \ldots, r(x)+(h_t), r(x^{-1})+(h_t^*))$$

Segue que temos uma nova decomposição

$$R = \left(\bigoplus_{i=1}^{s} G_i\right) \oplus \left(\bigoplus_{j=1}^{t} \left(H'_j \oplus H'_j\right)\right) \tag{2.6}$$

ψ é claramente um isomorfismo, da maneira como foi definida.

Note que

$$\begin{array}{rccc} \phi_j^{-1}: & \dfrac{\mathbf{F}[x]}{(f_j^*(x))} & \longrightarrow & \dfrac{\mathbf{F}[x]}{(f_j(x))} \\ & r(x) + (f_j^*) & \longrightarrow & r(x^{-1}) + (f_j) \end{array}$$

Conjugando $\mathbf{r}$ temos que o elemento $\overline{\mathbf{r}}$ pode ser expresso como

$$\overline{\mathbf{r}} = (r(x^{-1}) + (g_1), \ldots, r(x^{-1}) + (g_s), r(x^{-1}) + (h_1), r(x^{-1}) + (h_1^*), \ldots, r(x^{-1}) + (h_t), r(x^{-1}) + (h_t^*))$$

Aplicando ψ a $\overline{\mathbf{r}}$ temos que

$$\psi(\overline{\mathbf{r}}) =$$

$$= (r(x^{-1}) + (g_1), \ldots, r(x^{-1}) + (g_s), r(x^{-1}) + (h_1), r((x^{-1})^{-1}) + (h_1^*), \ldots, r(x^{-1}) + (h_t), r((x^{-1})^{-1}) + (h_t^*))$$

$$= (r(x^{-1}) + (g_1), \ldots, r(x^{-1}) + (g_s), r(x^{-1}) + (h_1), r(x) + (h_1^*), \ldots, r(x^{-1}) + (h_t), r(x) + (h_t^*))$$

Comparando $\psi(\mathbf{r})$ e $\psi(\overline{\mathbf{r}})$ vemos que, se

$$\mathbf{r} = (r_1, \ldots, r_s, r'_1, r''_1, \ldots, r'_t, r''_t),$$

com relação a decomposição 2.6, então

$$\overline{\mathbf{r}} = (\overline{r_1}, \ldots, \overline{r_s}, r''_1, r'_1, \ldots, r''_t, r'_t)$$

Quando f e f^* são associados, para vetores $c = (c_1, \ldots, c_l)$, $c' = (c'_1, \ldots, c'_l) \in (\mathbf{F}[x]/(f))^l$, definiremos o produto interno hermitiano em $(\mathbf{F}[x]/(f))^l$ por

$$\langle c, c' \rangle = \sum_{i=1}^{l} c_i \overline{c'_i} \tag{2.7}$$

Sejam $a, b \in R^l$ escreveremos

$$a = (a_0, a_1, \ldots, a_{l-1})$$

e

$$b = (b_0, b_1, \ldots, b_{l-1})$$

Decompondo a_i, b_i usando 2.4, podemos escrever

$$a_i = (a_{i1}, \ldots, a_{is}, a'_{i1}, a''_{i1}, \ldots, a'_{it}, a''_{it}),$$

e

$$b_i = (b_{i1}, \ldots, b_{is}, b'_{i1}, b''_{i1}, \ldots, b'_{it}, b''_{it}),$$

onde $a_{ij}, b_{ij} \in G_j$, $a'_{ij}, b'_{ij} \in H'_j$. Então

$$\langle a, b\rangle = \sum_{i=1}^{l-1} a_i\overline{b_i} = \left(\sum_i a_{i1}\overline{b_{i1}}, \ldots, \sum_i a_{is}\overline{b_{is}}, \sum_i a'_{i1}b''_{i1}, \sum_i a''_{i1}b'_{i1}, \ldots, \sum_i a'_{it}b''_{it}, \sum_i a''_{it}b'_{it}\right)$$

Em particular, $\langle a, b\rangle = 0$ se, e somente se,

$$\sum_i a_{ij}\overline{b_{ij}} = 0 \ (1 \leq j \leq s)$$

e

$$\sum_i a'_{ik}b''_{ik} = 0 = \sum_i a''_{ik}b'_{ik} \ (1 \leq k \leq t)$$

Uma consequência imediata é a seguinte caracterização de código auto-dual sobre R, em termos da decomposição de R em soma de corpos finitos.

Teorema 2.2 *Um código linear C sobre $R(\mathbf{F}, m)$ de comprimento l é auto-dual com respeito ao produto interno Hermitiano, ou equivalentemente, um código l-quase-cíclico de comprimento lm sobre $\mathbf{F}$ é auto dual com respeito ao produto interno euclidiano, se e somonte se,*

$$C = \left(\bigoplus_{i=1}^{s} C_i\right) \oplus \left(\bigoplus_{j=1}^{t} (C'_j \oplus (C'_j)^{\perp})\right)$$

onde para $1 \leq i \leq s$, C_i é um código auto-dual sobre G_i de comprimento l (com respeito ao produto interno Hermitiano) e, para $i \leq j \leq t$, C'_j é um código linear de comprimento l sobre H'_j e $C_j^{\perp}$ é o dual de C_j com respeito ao produto interno Euclidiano.

2.3 Classes de Ciclotomia

Um conceito importante no estudo códigos cíclicos e quase-cíclicos é o estudo da classes de ciclotomia. Apresentaremos este conceito no contexto de ações de grupos.

Definição 2.2 *Se X é um conjunto e G é um grupo, então G age em X se existe uma função $G \times X \longrightarrow X$, denotada por $(g, x) \mapsto gx$, tal que*
(i) $(gh)x = g(hx)$ para todo $g, h \in G$ e $x \in X$;
(ii) $1 \cdot x = x$ para todo $x \in X$, onde 1 é a identidade em G.

Se um grupo G age em um conjunto X, então fixando a primeira variável, digamos g, teremos uma função $\alpha_g : X \longrightarrow X$, tal que, $\alpha_g : x \mapsto gx$. Esta função é uma permutação de X, cuja inversa é $\alpha_{g^{-1}}$: dado $x \in X$,

$$(\alpha_g \alpha_{g^{-1}})(x) = \alpha_g(\alpha_{g^{-1}}(x)) = g(g^{-1}(x)) = (gg^{-1})(x) = 1x = x$$

e temos $\alpha_g \alpha_{g^{-1}} = 1_X$. Analogamente, $\alpha_{g^{-1}} \alpha_g = 1_X$.

Note que $\alpha : G \longrightarrow S_X$, definida por $\alpha : g \longrightarrow \alpha_g$, é um homomorfismo. De fato, dado $g, h \in G$ e $x \in X$ temos que $\alpha_g \circ \alpha_h = \alpha_g(\alpha_h(x)) = g(h(x)) = (gh)(x) = \alpha_{gh}(x)$ Portanto, $\alpha_g \alpha_h = \alpha_{gh}$ para todo $g, h \in G$. Dado qualquer homomorfismo $\phi : G \to S_X$, defina $gx = \phi(g)(x)$. A ação de um grupo G em um conjunto X é outra maneira de vermos um homomorfismo $G \to S_X$.

Definição 2.3 *Se G age em X e $x \in X$, então a **órbita** de x, denotada por $O(x)$, é o subconjunto de X dado por*

$$O(x) = \{gx : g \in G\}$$

*O **estabilizador** de x, denotado por G_x, é o subgrupo $G_x = \{g \in G : gx = x\}$ do grupo G.*

Se G age em um conjunto X, definiremos uma relação em X por $x \equiv y$ no caso onde existe $g \in G$ com $y = gx$. Esta é uma relação de equivalência sobre X cujas classes de equivalência são as órbitas.

Proposição 2.2 *Se G em um conjunto X, então X é a união disjunta de órbitas. Se X é finito, então*

$$|X| = \sum_i |O(x_i)|$$

onde um x_i é tomado em cada órbita.

Demonstração: Como mencionado anteriormente, a relação em X, dada por $x \equiv y$ se existe $g \in G$ com $y = gx$, é uma relação de equivalência cujas classes são as órbitas. Portanto as órbitas particionam X. A contagem dada na segunda declaração é verdadeira visto que as órbitas são disjuntas, não há elementos em X contados duas vezes.

□

Estabeleceremos agora a conexão entre órbitas e estabilizadorares.

Teorema 2.3 *Se G age em um conjunto X e $x \in X$, então*

$$|O(x)| = [G : G_x]$$

isto é o número de elementos na órbita de x é igual ao índice do estabilizador G_x em G.

Demonstração: Se G/G_x denota a família de todas as classes laterais à esquerda de G_x em G. Exi biremos uma bijeção $\phi : G/G_x \to O(x)$, e daí teremos provado o resultado, visto que $|G/G_x| =\mid G \mid / \mid G_x \mid= [G : G_x]$ pelo teorema de Lagrange. Defina $\phi(gG_X) \mapsto gx$. Agora mostraremos que ϕ está bem definida. Se $gG_x = hG_x$, então $h = gf$ para algum $f \in G_x$; isto é, $fx = x$; desde já $hx = gfx = gx$. Temos que ϕ é injetiva; de fato, se $gx = \phi(g(G_x)) = \phi(hG_x) = hx$, então $h^{-1}gx = x$; desde já, $h^{-1}g \in G_x$, e $gG_x = hG_x$. Resta provar que ϕ é uma sobrejeção. Se $y \in O(x)$, então $y = gx$ para algum $g \in G$, e além disso $y = \phi(gG_x)$.

□

Corolário 2.2 *Se um grupo finito G age em um conjunto X, então o número de elementos em qualquer órbita é um divisor de $|G|$.*

O conjunto de todos os elementos inversíveis de $\mathbb{Z}_m$ é um grupo com a operação do produto induzida de $\mathbb{Z}_m$; denotamos este grupo por $U(\mathbb{Z}_m)$. De fato, se $\overline{a}$ e $\overline{b}$ estão em $U(\mathbb{Z}_m)$ então existem $\overline{c}$ e $\overline{d}$ em $\mathbb{Z}_m$ tais que $\overline{ac} = \overline{bd} = \overline{1}$. Logo, $(\overline{a}\overline{b})(\overline{c}\overline{d}) = (\overline{ac})(\overline{bd}) = \overline{1}$, o que mostra que este conjunto é fechado para o produto. As propriedades de grupo seguem das propriedades do produto em $\mathbb{Z}_m$ e da própria definição de $U(\mathbb{Z}_m)$.

Os elementos de $U(\mathbb{Z}_m)$ são conhecidos; prova-se em teoria de números que $U(\mathbb{Z}_m) = \{[a] \in \mathbb{Z}_m; mdc(a, m) = 1\}$.

Seja agora $q = p^n$, p primo, tal que $mdc(q, m) = 1$. Então $[q] \in U(\mathbb{Z}_m)$ e $G = \langle q \rangle$ é um subgrupo cíclico de $U(\mathbb{Z}_m)$. Como $U(\mathbb{Z}_m)$ é finito, a ordem de $[q]$ é finita e

$$G = \{1, q, q^2, \ldots, q^{r-1}\}$$

onde $r = o([q])$; na literatura, costuma-se chamar r de ordem multiplicativa de q módulo m.

Dado $j \in \mathbb{Z}$, $0 \leq j \leq m-1$, a classe q-ciclotômica de j é definida como o conjunto

$$C_j = \{[jq^t] \in \mathbb{Z}_m : t \in \mathbb{Z}, t \geq 0\},$$

Claramente, C_j é a órbita de $[j]$ em $\mathbb{Z}_m$ sob a ação de G. Como as órbitas são as classes da relação de equivalência definida pela ação de G, temos

Proposição 2.3 *Os conjuntos C_i possuem as seguintes propriedades:*
(i) Se $C_i \cap C_j \neq 0$, então $C_i = C_j$.
(ii) A união de todos C_j é igual a $\mathbb{Z}_n$.

Pelo corolário 2.2, o número de elementos em cada classe ciclotômica divide a ordem multiplicativa de q módulo m.

2.4 Traço e Transformada de Fourier

Seja $\mathbf{F} = \mathbf{F}_q$ e assuma m e q coprimos. No caso em que $m \in \mathbf{F}^* = \mathbf{F} - \{0\}$, o isomorfismo 2.3 pode ser descrito mais explicitamente via transformada de Fourier discreta (DFT), também conhecida como transformada de Mattson-Solomon.

Na decomposição 2.3, a soma direta do lado direito corresponde aos fatores irredutíveis de $x^m - 1$ em $\mathbf{F}[x]$.

Existe uma bijeção entre esses fatores e as classes q-ciclotômicas de $\mathbb{Z}/m\mathbb{Z}$ dada pelo seguinte resultado:

Teorema 2.4 *Se f é um polinômio irredutível em $\mathbf{F}_q$ de grau k, então f tem uma raiz ξ em $\mathbf{F}_{q^k}$. Além disso, todas as raízes de f são simples e são dadas pelos k elementos distintos $\xi, \xi^q, \xi^{q^2}, \ldots, \xi^{q^{k-1}}$ de $\mathbf{F}_{q^k}$.*

Demonstração: Ver [4].

Corolário 2.3 *Sejam m e q coprimos, $\mathbf{K}$ um corpo com q elementos, $\mathbf{F} \supset \mathbf{K}$ extensão de $\mathbf{K}$ contendo uma raiz m-ésima primitiva da unidade ξ, e $x^m - 1 = f_1(x) \cdot \ldots \cdot f_r(x)$ a fatoração de $x^m - 1$ em irredutíveis sobre $\mathbf{K}$. Então a aplicação que associa a cada $f_i(x)$ o conjunto $C(i) = \{l \in \mathbb{Z}_m; f(\xi^l) = 0\}$ é uma bijeção entre os fatores irredutíveis de $x^m - 1$ e as classes q-ciclotômicas de $\mathbb{Z}_m$.*

Demonstração: Pelo teorema anterior, se $f_i(\xi^l) = 0$ então as raízes de $f_i(x)$ em $\mathbf{F}$ são

$$\xi^l, \xi^{lq}, \ldots, \xi^{lq^{k-1}},$$

onde $k_i = \partial(f_i(x))$. Logo, se $l \in C(i)$, então

$$C(i) = \{l, lq, \ldots, lq^{k-1}\}$$

Como $f_i(\xi) = 0$ implica em $f_i(\xi^q) = 0$, $C(i)$ é fechado pela ação do grupo multiplicativo $G = \langle q \rangle$. Logo, C_i é a órbita de l por G, ou seja é a classe q-ciclotomica de l em $\mathbb{Z}_m$.

□

Retomando à fatoração na forma

$$x^m - 1 = g_1 \cdots g_s h_1 . h_1^* \cdots h_t . h_t^*$$

denotaremos por U_i $(1 \leq i \leq s)$ a classe q-ciclotômica correspondente a g_i, V_j e W_j as classes ciclotômicas correspondentes a h_j e h_j^* respectivamente.

Como $(m, q) = 1$, existe uma extensão $\mathbf{K} \supset \mathbf{F}$ onde há uma raiz m-ésima primitiva da unidade ξ.

Para

$$\mathbf{c} = \sum_{g \in \mathbb{Z}_m} c_g x^g \in \mathbf{F}[x]/(x^m - 1)$$

a transformada de Fourier é $\widehat{\mathbf{c}} = \sum_{h \in \mathbb{Z}_m} \widehat{c_h} x^h \in \mathbf{K}[x]$, onde o coeficiente de Fourier $\widehat{c_h}$ é definido como

$$\widehat{c_h} = \sum_{g \in \mathbb{Z}_m} c_g \xi^{gh} = c(\xi^h)$$

Lema 2.2 *$\widehat{c}_{qh} = \widehat{c_h}^q$ para todo $h \in \mathbb{Z}_m$.*

Demonstração: Com efeito,

$$\begin{aligned} \widehat{c}_{qh} &= \sum_{g \in \mathbb{Z}_m} c_g \xi^{qgh} = \sum_{g \in \mathbb{Z}_m} c_g^q (\xi^{gh})^q \\ &= \sum_{g \in \mathbb{Z}_m} [c_g \xi^{gh}]^q = [\sum_{g \in \mathbb{Z}_m} c_g \xi^{gh}]^q = \widehat{c_h}^q. \end{aligned}$$

□

Assim, a cada divisor irredutivel de $x^m - 1$ corresponde uma classe q-ciclotomica.

Proposição 2.4 *A transformada inversa é dada por*

$$c_g = m^{-1} \sum_{h \in \mathbb{Z}_m} \widehat{c_h} \xi^{-gh}.$$

Demonstração:

$$\begin{aligned}\sum_{h\in\mathbb{Z}_m}\widehat{c_h}\xi^{-gh} &= \sum_{h\in\mathbb{Z}_m}\left(\sum_{l\in\mathbb{Z}_m}c_l\xi^{lh}\right)\xi^{-gh}\\ &= \sum_l\sum_h c_l\xi^{(l-g)h}\\ &= mc_g+\sum_l c_l\left(\sum_h\xi^{(l-g)h}\right)\end{aligned}$$

Agora, se $t\neq 0$

$$\begin{aligned}\sum_{h\in\mathbb{Z}_m}\xi^{th} &= 1+\xi^t+(\xi^t)^2+\cdots+(\xi^t)^{m-1}\\ &= 0\end{aligned}$$

pois ξ^t é raiz de $x^m-1=(x-1)(1+x+\cdots+x^{m-1})$ e $\xi^t\neq 1$. Portanto

$$mc_g=\sum_{h\in\mathbb{Z}_m}\widehat{c_h}\xi^{-gh}.$$

□

Note agora que, dado $l\in C(i)$, temos um isomorfismo

$$\begin{aligned}\mathbf{F}(x)/(f_i(x)) &\longrightarrow \mathbf{F}[\xi^v]\\ c(x)+(f_i(x)) &\longrightarrow c(\xi^v)=\widehat{c}_v\end{aligned}$$

Sendo

$$x^m-1=f_1\cdots f_s h_1.h_1^*\cdots h_t.h_t^*$$

como na decomposição 2.3, chame de U_i a classe associada a f_i, de V_j a classe associada a h_j e W_j a de h_j^*. Fixe um elemento u_i para cada U_i, $v_i\in V_i$ e $w_i\in W_i$. Temos então isomorfismos

$$\begin{aligned}G_i=\mathbf{F}(x)/(f_i(x)) &\longrightarrow \mathbf{F}[\xi^{u_i}]\\ H_i'=\mathbf{F}(x)/(h_i(x)) &\longrightarrow \mathbf{F}[\xi^{v_i}]\\ H_i''=\mathbf{F}(x)/(h_i^*(x)) &\longrightarrow \mathbf{F}[\xi^{w_i}]\end{aligned}$$

Por isso, identificaremos estes corpos daqui em diante.

Do lema 2.2 segue que se $v \in C_i$ então $\widehat{c}_v \in G_i$, pois $v = u_i q^t$ e $\widehat{c}_v = \widehat{c}_{u_i q^t} = (\widehat{c}_{u_i})^{q^t} \in G_i$. Analogamente para H_i' e H_i''.

Observamos também que estes isomorfismos induzem uma decomposição de $R(m,q)$ em soma de anéis, dado por

$$\begin{aligned} R(m,q) &\longrightarrow \left(\bigoplus_{i=1}^{s} G_i\right) \oplus \left(\bigoplus_{j=1}^{t} (H_j' \oplus H_j'')\right) \\ c(x) + (x^m - 1) &\longrightarrow (\widehat{c}_{u_i}, \ldots, \widehat{c}_{u_s}, \widehat{c}_{v_1}, \widehat{c}_{w_1}, \ldots, \widehat{c}_{v_t}, \widehat{c}_{w_t}) \end{aligned}$$

(onde novamente identificamos G_i com $\mathbf{F}[\xi^{u^i}]$, H_i' com $\mathbf{F}[\xi^{v^i}]$ e H_i'' com $\mathbf{F}[\xi^{w^i}]$). A vantagem de decompor desta forma $R(m,q)$ é que temos uma forma explícita para o isomorfismo inverso.

Sejam $\widehat{c}_i \in G_i$, $\widehat{c}_j{}' \in H_j'$ e $\widehat{c}_j{}'' \in H_j''$ para $i = 1, \ldots, s$ e $j = 1, \ldots, t$. À $s+2t$-upla $(\widehat{c}_1, \ldots \widehat{c}_s, \widehat{c}_1{}', \widehat{c}_1{}'', \ldots, \widehat{c}_t{}', \widehat{c}_t{}'')$, associamos o elemento

$$\sum_{g \in \mathbb{Z}_m} c_g x^g \in \frac{\mathbf{F}[x]}{x^m - 1}$$

onde

$$mc_g = \sum_{g \in \mathbb{Z}_m} \widehat{c}_h \xi^{-gh}$$

Mostraremos agora que

Lema 2.3 *Se $\mathbf{K} \supset \mathbf{F}_q$, ξ é a raiz m-ésima primitiva da unidade em $\mathbf{K}$ então*

$$mc_g = \sum_{i=1}^{s} Tr_{\mathbf{F}(\xi^{u_i})/\mathbf{F}}(\widehat{c}_{u_i} \xi^{-gu_i})$$

onde $x^m - 1 = f_1(x) \cdot \ldots \cdot f_r(x)$.

Demonstração: Seja $\mathsf{C} = \{C_1, C_2, \ldots, C_r\}$ o conjunto das classes q-ciclotômicas em $\mathbb{Z}_m$. Tomando $u_i \in C_i$, com $i = 1, 2, \ldots, r$ e denotando $f_i(x) =$ polinômio minimal

de ξ^{u_i} sobre $\mathbf{K}$, temos que $k_i = [\mathbf{F}(\alpha^{u_i}) : \mathbf{F}] = \partial(f_i(x))$. Daí, a transformada inversa é dada por

$$\begin{aligned}
mc_g &= \sum_{g\in\mathbb{Z}_m} \widehat{c}_h \xi^{-gh} \\
&= \sum_{C\in\mathtt{C}} \left(\sum_{h\in C} \widehat{c}_h \xi^{-gh} \right) \\
&= \sum_{i=1}^{r} \left(\sum_{h\in C_i} \widehat{c}_h \xi^{-gh} \right) \\
&= \sum_{i=1}^{r} \left(\sum_{l=0}^{k_i} \widehat{c}_{u_i q^l} \xi^{-gu_i q^l} \right) \\
&= \sum_{i=1}^{r} \left(\sum_{l=0}^{k_i} (\widehat{c}_{u_i})^{q^l} (\xi^{-gu_i})^{q^l} \right) \\
&= \sum_{i=1}^{r} \left(\sum_{l=0}^{k_i} (\widehat{c}_{u_i} \xi^{-gu_i})^{q^l} \right) \\
&= \sum_{i=1}^{s} Tr_{\mathbf{F}(\xi^{u_i})/\,\mathbf{F}} (\widehat{c}_{u_i} \xi^{-gu_i})
\end{aligned}$$

□

Temos que

$$\theta : \bigoplus_{i=1}^{r} \frac{\mathbf{F}[x]}{(f_i(x))} \longrightarrow \bigoplus_{i=1}^{r} \mathbf{F}(\xi^{u_i})$$

é um isomorfismo de anéis, em coordenadas

$$(c_1(x) + (f_1(x)), \ldots, c_r(x) + (f_r(x)) \longmapsto (c_1(\xi^{u_1}), \ldots, c_r(\xi^{u_r}))$$

Ainda, segue do corolário 1.6 que

$$\phi : R \longrightarrow \bigoplus_{i=1}^{r} \frac{\mathbf{F}[x]}{(f_i(x))}$$

é um isomorfismo de anéis. Compondo, obtemos o isomorfismo

$$\phi \circ \theta : R \longrightarrow \bigoplus_{i=1}^{r} \mathbf{F}(\xi^{u_i})$$

Considere agora

$$\begin{aligned}\psi : \bigoplus_{i=1}^{r} \mathbf{F}(\xi^{u_i}) &\longrightarrow \mathbf{K}^m \\ (c_1, \ldots, c_r) &\longmapsto (c_1, c_1^q, \ldots, c_1^{q^{k_1-1}}, \ldots, c_r, c_r^q, \ldots, c_r^{q^{k_r-1}})\end{aligned}$$

A menos de permutação de coordenadas em $\mathbf{K}^m$,

$$\psi \circ \theta \circ \phi(c(x) + (x^m - 1)) = (\widehat{c}_1, \widehat{c}_2, \ldots, \widehat{c}_m)$$

que é a transformada de Fourier de $c(x) + (x^m - 1)$ escrita vetorialmente. Uma coordenada "tipica"de $\psi \circ \theta \circ \phi(c(x) + (x^m - 1))$ é

$$\begin{aligned}c_i^{q^l} &= c(\xi^{u_i})^{q^l} \\ &= \left(\sum_{g=0}^{m-1} c_g (\xi^{u_i})^g\right)^{q^l} \\ &= \left(\sum_{g=0}^{m-1} c_g \xi^{u_i g}\right)^{q^l} \\ &= \sum_{g=0}^{m-1} c_g^{q^l} \xi^{u_i g q^l} \\ &= \sum_{g=0}^{m-1} c_g \xi^{u_i g q^l} \\ &= \sum_{g=0}^{m-1} c_g \xi^{g(u_i q^l)} \\ &= \widehat{c}_{u_i q^l}.\end{aligned}$$

Seja $S \subset \mathbf{K}^m$ a imagem de ψ.

Chame de $\Im = \psi \circ \theta \circ \phi$. Já temos a expressão de $\Im^{-1} : S \longrightarrow R$ em termos de traços. Compondo $\Im^{-1}$ e ϕ obtemos um isomorfismo

$$\Im^{-1} \circ \psi : \bigoplus_{i=1}^{r} \mathbf{F}(\xi^{u_i}) \longrightarrow R$$

Logo,

$$\begin{aligned}(\Im^{-1}\circ\psi)\circ(\theta\circ\phi)(c(x)+(x^m-1) &= \Im^{-1}(\psi\circ\theta\circ\phi)(c(x)+(x^m-1)= \\ =\Im^{-1}\circ\Im(c(x)+(x^m-1)) &= c(x)+(x^m-1)\end{aligned}$$

mostrando que $\Im^{-1}\circ\psi$ é a inversa do isomorfismo $\theta\circ\phi : R \longrightarrow \bigoplus_{i=1}^{r}\mathbf{F}(\xi^{u_i})$, que é o que procuramos. Calculando $\Im^{-1}\circ\psi$ em $(\widehat{c}_1,\widehat{c}_2,\ldots,\widehat{c}_r)$ obtemos o elemento $\sum_{g=0}^{m-1} c_g x^g$ dado por

$$mc_g = \sum_{i=1}^{s} Tr_{\mathbf{F}(\xi^{u_i})/\mathbf{F}}(\widehat{c}_{u_i}\xi^{-gu_i})$$

□

Considere novamente

$$x^m-1 = g_1g_2\ldots g_s h_1h_1^*\ldots h_th_t^*;$$

Seja U_i a classe ciclotômica associada a g_i, V_j a classe ciclotômica associada a h_j e W_k a classe ciclotômica associada a h_k^*.

Sejam u_i um representante de U_i, v_j e w_j representantes das classes ciclotômicas V_j e W_j respectivamente, $i=1,\ldots,s$, $j=1,\ldots,t$.

Sejam G_i $(1\le i\le s)$, H_j' e H_j'' $(1\le j\le t)$ como antes, e identifique os corpos

$$\begin{aligned}G_i &\cong \mathbf{F}[\xi^{u_i}]\\ H_i' &\cong \mathbf{F}[\xi^{v_i}]\\ H_i'' &\cong \mathbf{F}[\xi^{w_i}]\end{aligned}$$

Então temos $(\theta\circ\phi)^{-1} : \left(\bigoplus_{i=1}^{s} G_i\right)\oplus\left(\bigoplus_{j=1}^{t}(H_j'\oplus H_j'')\right)\longrightarrow R$ dada por

$$(\theta\circ\phi)^{-1}(\widehat{c}_1,\ldots,\widehat{c}_r) = \sum_{g=0}^{m-1} c_g x^g$$

onde

$$mc_g = \sum_{i=1}^{t} Tr_{G_i/\mathbf{F}}(\widehat{c}_i \xi^{-gu_i}) + \sum_{j=1}^{t} (Tr_{H'_j/\mathbf{F}}(\widehat{c}_j \xi^{-gv_j}) + Tr_{H''_j/\mathbf{F}}(\widehat{c}_j \xi^{gw_j}))$$

Deste modo, a transformação de Fourier inversa fornece uma fórmula para a inversa do isomorfismo 2.3 dado pelo teorema chinês do resto. É com esta fórmula que podemos aplicar os resultados de caracterização de códigos quase-cíclicos na construção de exemplos.

Teorema 2.5 *Se $\mathbf{F} = \mathbf{F}_q$ e m e q são coprimos, então, para qualquer l, o códigos quase-cíclicos sobre $\mathbf{F}$ de comprimento lm e índice l são dados pela seguinte construção: Escrevemos $x^m - 1 = \delta g_1 \dots g_s h_1 h_1^* \dots h_t h_t^*$, onde δ é um elemento não nulo de $\mathbf{F}$, $g_1, \dots, g_s$ são os $f'_j s$ associados aos seus recíprocos, e $h_1, h_1^*, \dots, h_t, h_t^*$ são os remanescentes $f'_j s$ irredutíveis agrupados em pares. Tome $G_i = \mathbf{F}[x]/(g_i)$, $H'_j = \mathbf{F}(x)/(h_j)$ e $H''_j = \mathbf{F}(x)/(h_j^*)$. Seja U_i (respectivamente V_j e W_j) a classe ciclotômica de $\mathbb{Z}/m\mathbb{Z}$ correspondente a g_i (respectivamente h'_j e h''_j), e seja $u_i \in U_i$ ($v_j \in V_j$, $w_j \in W_j$) elemento fixo para cada $i = 1, \dots, t$ (para cada $j = 1, \dots, t$). Para cada i, seja C_i um código de comprimento l sobre G_i, e para cada j, seja C'_j é um código de comprimento l sobre H'_j e C'''_j um código de comprimento l sobre H''_j. Para $\mathbf{x_i} \in C_i$, $\mathbf{y_j}' \in C'_j$, e $\mathbf{y_j}'' \in C'''_j$, e para cada $0 \leq g \leq m-1$, tome*

$$\begin{aligned} \mathbf{c}_g((\mathbf{x_i}), (\mathbf{y'_j}), (\mathbf{y''_j})) &= (\Im^{-1} \circ \psi(\mathbf{x_1}, \dots, \mathbf{x_s}, \mathbf{y'_1}, \dots, \mathbf{y'_t}, \mathbf{y''_1}, \dots, \mathbf{y''_t}) \\ &= \sum_{i=1}^{s} Tr_{G_i/\mathbf{F}}(\mathbf{x_i} \xi^{-gu_i}) + \sum_{j=1}^{t} (Tr_{H'_j/\mathbf{F}}(\mathbf{y_j}' \xi^{-gv_j}) + Tr_{H''_j/\mathbf{F}}(\mathbf{y_j}'' \xi^{-gw_j})) \end{aligned}$$

e seja C o código $\mathbf{F}$-linear

$$C = \{\mathbf{c}_0((\mathbf{x_i}), (\mathbf{y'_j}), (\mathbf{y''_j})), \dots, \mathbf{c}_{m-1}((\mathbf{x_i}), (\mathbf{y'_j}), (\mathbf{y''_j})) \mid \mathbf{x_i} \in C_i, \mathbf{y_j}' \in C'_j \text{ e } \mathbf{y_j}'' \in C'''_j\}$$

Então

(i) C é um código quase-cíclico sobre $\mathbf{F}$ de comprimento lm e de indice l. Reciprocamente, todo código quase-cíclico sobre $\mathbf{F}$ de comprimento lm e de indice l é obtido desta construção.

(*ii*) *Além disso, C é auto-dual com respeito ao produto interno Euclidiano se, e somente se C_i são auto-dual com respeito ao produto interno Hermitiano e $C_j'' = (C_j')^{\perp}$ para cada j com respeito ao produto interno Euclidiano.*

Capítulo 3

Aplicações

Aplicaremos a discussão precedente a algumas situações. Serão abordados nesse capítulo códigos quase-cíclico de índice 2, o caso $m = 3$ e a *Construção de Turyn*, o caso $m = 5$, o caso $m = 7$ e a *Construção de Vandermonde*.

3.1 Códigos Quase-Cíclicos de Índice 2

Seja $l = 2$ e $\mathbf{F} = \mathbf{F}_q$ um corpo finito qualquer. Suponhamos em princípio m e q coprimos. A decomposição 2.3 mostra que R pode ser escrito como a soma direta de extensão finitas de $\mathbf{F}_q$.

Códigos auto-duais (com respeito ao produto interno Euclidiano) de comprimento 2 sobre um corpo finito $\mathbf{F}_q$ existem se, e somente se -1 é uma raiz em $\mathbf{F}_q$, que é o caso em que uma das afirmações é verdadeira:
(1) q é potência de 2;
(2) $q = p^b$, onde p é um primo congruente a 1 mod 4; ou
(3) $q = p^{2b}$, onde p é um primo congruente a 3 mod 4.

Este resultado pode ser encontrado em [8]. Neste caso existe um unico código auto-dual de comprimento 2 sobre $\mathbf{F}_q$, a saber um com matriz geradora $(1, i)$, onde i denota a raiz quadrada de -1 em $\mathbf{F}_q$.

Isto permite uma caracterização de códigos quase-cíclicos sobre $\mathbf{F}_q$ de compri-

mento $2m$ e de indice 2, onde m é coprimo com q, onde os fatores irredutíveis de $x^m - 1$ são conhecidos.

Proposição 3.1 *(San Ling e Patrick Solé) Seja m coprimo com q. Então códigos quase-cílicos auto-duais de indice 2 sobre $\mathbf{F}_q$ de comprimento $2m$ existem se, e somente se uma das condições é satisfeita.*
(1) q é potência de 2;
(2) $q = p^b$, onde p é um primo congruente a 1 mod 4; ou
(3) $q = p^{2b}$, onde p é um primo congruente a 3 mod 4.

Demonstração: Se existe um código quase-cílico auto-dual de indice 2 sobre $\mathbf{F}_q$ de comprimento $2m$, então a decomposição 2.3 prova que existe um código auto-dual de comprimento 2 sobre $G_1 = \mathbf{F}_q$, donde as condições na proposição são necessárias.

Reciprocamente, se qualquer uma das condições na proposição é satisfeita, então existe $i \in \mathbf{F}_q$ tal que $i^2+1 = 0$. Consequentemente, toda extensão finita de $\mathbf{F}_q$ tambem contém tal i. Desde já, o código gerado por $(1, i)$ sobre qualquer extensão de $\mathbf{F}_q$ é auto-dual (com respeito ao produto interno Euclidiano e Hermitiano) de comprimento 2. Desde já, o teorema 2.2 assegura a existência de códigos quase-cílicos auto-duais de indice 2 e comprimento $2m$ sobre $\mathbf{F}_q$.

□

Proposição 3.2 *(San Ling e Patrick Solé) Seja m coprimo com q e l ímpar. Então não existem códigos autoduais l-quase-cíclicos sobre $\mathbf{F}_q$ de comprimento lm. Além disso, quando $q \equiv 3 \bmod 4$, códigos l-quase-cíclicos sobre $\mathbf{F}_q$ de comprimento lm existem se, e somente se $l \equiv 0 \bmod(4)$.*

Demonstração: Desde já $Y - 1$ é um fator de $Y^m - 1$, $\mathbf{F}_q$ é sempre um fator direto de R na decomposição 2.3. Como l é ímpar, não existem códigos auto-duais de comprimento l sobre $\mathbf{F}_q$. O resultado menor segue do fato que, quando $q \equiv 3 \bmod 4$, um código auto-dual de comprimento l existe somente quando l é divisivel por 4.

□

3.2 m=2 e m=3

Considereramos nesta seção códigos quase-cíclicos de comprimento $2l$ sobre o corpo finito $\mathbf{F}_q$.

Sabe-se que se C_1 e C_2 são códigos lineares sobre $\mathbf{F}_q$ de comprimento l, então o código

$$C = \{(u+v \mid u-v); u \in C_1, v \in C_2\}$$

é um código quase-cíclico de comprimento $2l$. Mostraremos a seguir que se q é ímpar então todo código quase-cíclico de comprimento $2l$ sobre $\mathbf{F}_q$ é obtido deste modo, usando a construção traço.

Quando q é ímpar e $m = 2$ então $Y^2 - 1$ fatora-se em fatores lineares distintos, sendo que cada um é auto-recíproco. Da decomposição 2.3, R pode ser decomposto na soma direta $\mathbf{F}_q \oplus \mathbf{F}_q$, e um código l-quase-cíclico de comprimento $2l$ sobre $\mathbf{F}_q$ pode ser expresso como $C_1 \oplus C_2$, onde C_1 e C_2 são códigos sobre $\mathbf{F}_q$ de comprimento l. Além disso, são auto-duais com respeito ao produto intermo Euclidiano. As classes de ciclotomia módulo 2 são $\mathrm{C}_0 = \{[0]\}$, $\mathrm{C}_1 = \{[1]\}$. Utilizando o teorema 2.5 temos que se ξ é raiz 2-ésima primitiva da unidade em $\mathbf{F}_q$ então $\xi = -1$ e se $u \in C_1$ e $v \in C_2$, então

$$\begin{aligned} c_0 &= Tr_{\mathbf{F}_q/\mathbf{F}_q}(u\xi^0) + Tr_{\mathbf{F}_q/\mathbf{F}_q}(v\xi^0) \\ &= u + v \end{aligned}$$

ainda

$$\begin{aligned} c_1 &= Tr_{\mathbf{F}_q/\mathbf{F}_q}(u\xi^0) + Tr_{\mathbf{F}_q/\mathbf{F}_q}(v\xi^{-1}) \\ &= u - v \end{aligned}$$

logo a correspondência $C \leftrightarrow C_1 \oplus C_2$ é equivalente à construção $(u+v \mid u-v)$. Portanto, temos a seguinte proposição.

Proposição 3.3 *Seja q um inteiro positivo impar. Se C_1 e C_2 são códigos de comprimento l sobre $\mathbf{F}_q$, então*

$$C = \{(u+v \mid u-v) \mid u \in C_1, v \in C_2\}$$

é um código quase-cíclico de comprimento $2l$ sobre $\mathbf{F}_q$. Todos os códigos l-quase-cíclicos de comprimento $2l$ sobre $\mathbf{F}_q$ são construídos desta forma. Além disso, C é auto-dual se, e somente se C_1 e C_2 são auto-duais.

Assumiremos agora que $m = 3$ e que q não é uma potência de 3. Estudaremos códigos l-quase-cíclicos de comprimento $3l$ sobre $\mathbf{F}_q$.

Seja $q \equiv 2 \bmod(3)$. Quando $q \equiv 2 \mod(3)$, $Y^2 + Y + 1$ é irredutível em $\mathbf{F}_q$, e ainda

$$Y^3 - 1 = (Y-1)(Y^2 + Y + 1)$$

da decomposição 2.3 temos que

$$\frac{\mathbf{F}_q[Y]}{(Y^3-1)} \cong \frac{\mathbf{F}_q[Y]}{(Y-1)} \oplus \frac{\mathbf{F}_q[Y]}{(Y^2+Y+1)} \cong \mathbf{F}_q \oplus \mathbf{F}_{q^2}$$

Este isomorfismo dá uma correspondência entre códigos l-quases-cíclicos de comprimento $3l$ sobre $\mathbf{F}_q$ e um par (C_1, C_2) onde C_1 é um código linear sobre $\mathbf{F}_q$ de comprimento l (com respeito ao produto interno Euclidiano) e C_2 é um código linear sobre $\mathbf{F}_{q^2}$ de comprimento l (com respeito ao produto interno Hermitiano).

As classes de ciclotomia módulo 3 são $\mathrm{C}_0 = \{0\}$ e $\mathrm{C}_1 = \{1, 2\}$. Na primeira classe de ciclotomia C_0 só podemos fixar 0, fixemos 1 na segunda classe de ciclotomia C_1 e seja ξ uma raiz 3-ésima primitiva da unidade em $\mathbf{F}_{q^2} = \{a + b\xi; a, b \in \mathbf{F}_q\}$, então $\xi^2 + \xi + 1 = 0$. Se $x \in \mathrm{C}_1$ e $x \in C_2$ então $y = a + b\xi$, e obtemos do teorema 2.5 que

$$\begin{aligned} c_0 &= Tr_{\mathbf{F}_q/\mathbf{F}q}(x) + Tr_{\mathbf{F}_{q^2}/\mathbf{F}q}(y\xi^{0.1}) \\ &= x + Tr_{\mathbf{F}_{q^2}/\mathbf{F}q}((a+\xi b)\xi^{0.1}) \\ &= x + [(a+\xi b) + (a+\xi b)^q] \\ &= x + 2a + (\xi + \xi^q)b \\ &= x + 2a - b \end{aligned}$$

e ainda

$$\begin{aligned} c_1 &= Tr_{\mathbf{F}_q/\mathbf{F}q}(x\xi^{-1.0}) + Tr_{\mathbf{F}_{q^2}/\mathbf{F}q}(y\xi^{-1.1}) \\ &= x + y\xi^{-1} + (y\xi^{-1}) + (y\xi^{-1})^q \\ &= x + (-2a + 2b) - a(\xi + \xi^q) \\ &= x + (-2a + 2b) - a(-1) \\ &= x - a + 2b \end{aligned}$$

De modo análogo se mostra que,

$$c_3 = x - a - b$$

Portanto, $C = \{(x + 2a - b \mid x - a + 2b \mid x + a + b) \mid x \in C_1, a + \xi b \in C_2\}$ é um código quase-cíclico sobre $\mathbf{F}$ de comprimento $3l$ e de indice l. Segue que todo código quase-cíclico sobre $\mathbf{F}$ de comprimento $3l$ e de indice l é obtida da construção acima.

Em particular, quando $q = 2^t$ (t ímpar) e para qualquer l

$$C = \{(x + a \mid x + a \mid x + a + b) \mid x \in C_1, a + \xi b \in C_2\} \tag{3.1}$$

Se $a, b \in C_2'$ para algum código linear C_2' sobre $\mathbf{F}_q$, então $C_2 = \{a + b\xi \mid a, b \in C_2'\}$ é um código linear sobre $\mathbf{F}_{q^2}$.

Portanto, se começarmos com dois códigos $\mathbf{F}_q$-lineares C_2' e C_1, a construção 3.1 é a própria $(a + x \mid b + x \mid a + b + x)$-construção de Turyn. Em particular obtemos

Teorema 3.1 *A $(a + x \mid b + x \mid a + b + x)$-construção, aplicada a dois códigos sobre $\mathbf{F}_{2^t}$ (t ímpar) de comprimento l, resulta em um $\mathbf{F}_{2^i}$-linear código de comprimento $3l$ que é quase-cíclico de indice l.*

3.3 $m = 5$ e $m = 7$

Teorema 3.2 *Suponha que $m = 5$ e q é tal que $Y^4 + Y^3 + Y^2 + Y + 1$ é irredutível em $\mathbf{F}_q$. Seja $\xi \in \mathbf{F}_{q^4}$ tal que $\xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0$ e se Tr denota o traço de $\mathbf{F}_q^4$ em $\mathbf{F}_q$, então para um código C_1 de comprimento l sobre $\mathbf{F}_q$ e C_2 um código de comprimento l sobre $\mathbf{F}_{q^4}$, o código*

$C = \{(x + Tr(y) \mid x + Tr(y\xi^{-1}) \mid x + Tr(y\xi^{-2}) \mid x + Tr(y\xi^{-3}) \mid x + Tr(y\xi^{-4})) \mid x \in C_1, y \in C_2\}$

é um código l-quase-cíclico de comprimento $5l$ sobre $\mathbf{F}_q$. Todo código l-quase-cíclico de comprimento $5l$ sobre $\mathbf{F}_q$ é construído desta forma.

Alé disso, C é auto-dual se, e somente se C_1 é auto-dual com respeito ao produto interno Euclidiano e C_2 é auto-dual com respeito ao produto interno Hermitiano.

Seja $m = 7$ e $\mathbf{F} = \mathbf{F}_q$. Temos que $Y^7 - 1$ fatora-se em $(Y-1)(Y^3+Y+1)(Y^3+Y^2+1)$ como um produto de fatores irredutiveis. Seja ξ uma raiz primitiva de $Y^3 + Y + 1$ em $\mathbf{F}_{q^3}$, então $\xi^3 + \xi + 1 = 0$. Temos que as classes de ciclotomia módulo 7 são $C_0 = \{0\}$, $C_1 = \{1, 2, 4\}$ e $C_3 = \{3, 5, 6\}$, logo se $y, z \in \mathbf{F}_q$, então $y = a + b\xi + c\xi^2$ e $z = d + e\xi + f\xi^2$, segue do teorema 2.5 que

$$\begin{aligned} c_0 &= Tr_{\mathbf{F}_2/\mathbf{F}_2}(x\xi^0) + Tr_{\mathbf{F}_{2^3}/\mathbf{F}_2}(y\xi^0) + Tr_{\mathbf{F}_{2^3}/\mathbf{F}_2}(z\xi^0) \\ &= x + (y + y^2 + y^4) + (z + z^2 + z^4) = x + a + d \end{aligned}$$

de modo análogo pode-se provar que

$$\begin{aligned} c_1 &= x + a + b + e \\ c_2 &= x + a + b + c + d + f \\ c_3 &= x + b + c + d + e \\ c_4 &= x + a + c + d + e + f \\ c_5 &= x + b + e + f \\ c_6 &= x + c + f \end{aligned}$$

daí

$$C = \{c_0, \ldots, c_6\}$$

3.4 A Construção de Vandermonde

Se $\mathbf{F}$ é um corpo finito e m um inteiro coprimo com a característica de $\mathbf{F}$. Assuma para seção somente que $\mathbf{F}^*$ contem um elemento ξ de ordem m. Então o polinômio $Y^m - 1$ decompõesse completamente em fatores lineares

$$(Y^m - 1 = (Y - 1)(Y - \xi) \cdots (Y - \xi^{m-1})$$

onde $f_i \in \mathbf{F}$ para $0 \leq i \leq m - 1$, então

$$\begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{m-1} \end{pmatrix} = V^{-1} \begin{pmatrix} \widehat{f_0} \\ \widehat{f_1} \\ \vdots \\ \widehat{f}_{m-1} \end{pmatrix}$$

onde os $\widehat{f_i}$ são os coeficientes de Fourier e $V = (\xi^{ij})$ com $0 \leq i, j \leq m - 1$ é a matriz de Vandermonte $m \times m$.

Dado um inteiro positivo l e m vetores $a_0, \ldots, a_{m-1} \in \mathbf{F}^l$. A construção

$$V^{-1} \begin{pmatrix} a_0 \\ \vdots \\ a_i \\ \vdots \end{pmatrix}$$

dara um elemento de R^l. Se C_i $(0 \leq i \leq m - 1)$ são códigos lineares sobre $\mathbf{F}$ de comprimento l, e $a_i \in C_i$ para $0 \leq i \leq m - 1$, então obteremos um código linear sobre R de comprimento l, que então corresponde a um código quase-cíclico sobre $\mathbf{F}$ de comprimento lm e índice l.

Dessa construção obtemos o seguinte teorema

Teorema 3.3 *(San Ling e Patrick Solé) Se* $\mathbf{F}$ *é um corpo finito e* m *um inteiro coprimo com a característica de* $\mathbf{F}$*. Assuma que* $\mathbf{F}^*$ *contem um elemento* ξ *de ordem* m*. Se* $C_0, \ldots, C_{m-1}$ *são códigos lineares de comprimento* l *sobre* $\mathbf{F}$*. Então o produto de* $C_0, \ldots, C_{m-1}$ *pela matriz de Vandermonde é um código quase-cíclico sobre* $\mathbf{F}$ *de comprimento* lm *e índice* l*. Além disso, quando* $\mathbf{F}$ *e* m *são como a cima, todo código* l*-quase-cíclico de comprimento* lm *sobre* $\mathbf{F}$ *é obtido via construção de Vandermonde.*

3.5 Conclusão

Neste trabalho, mostramos que códigos quase-cíclicos de comprimento lm e índice l sobre um corpo $\mathbf{F}$ podem ser tratados como R-submódulos de R_m a partir do isomorfismo $\phi : \mathbf{F}^{lm} \to R^l$ definido por

$$\phi(\mathbf{c}) = (\mathbf{c}_0(x), \mathbf{c}_1(x), \ldots, \mathbf{c}_{l-1}(x)) \in R^l$$

onde

$$\mathbf{c}_j(x) = \sum_{i=0}^{m-1} c_{ij} x^i \in R^l.$$

E a partir disto provamos que um código quase-cíclico C sobre $\mathbf{F}$ é auto-dual com respeito ao produto interno euclidiano se, e somente se, $\phi(C)$ é auto-dual sobre R com respeito ao produto interno Hermitiano.

Também mostramos que quando m é coprimo com a característica de $\mathbf{F}$, este último pode ser decomposto em uma soma direta de corpos dada por

$$R = \frac{\mathbf{F}[x]}{x^m - 1} \cong \left(\bigoplus_{i=1}^{s} \frac{\mathbf{F}[x]}{(g_i)} \right) \oplus \left(\bigoplus_{j=1}^{t} \left(\frac{\mathbf{F}[x]}{(h_j)} \oplus \frac{\mathbf{F}[x]}{(h_j^*)} \right) \right)$$

utilizando-se o teorema chinês dos restos. E utilizamos este resultado para mostrar que um código linear C sobre $R(\mathbf{F}, m)$ de comprimento l é auto-dual com respeito ao produto interno Hermitiano, ou equivalentemente, um código l-quase-cíclico de comprimento lm sobre $\mathbf{F}$ é auto dual com respeito ao produto interno euclidiano, se e somente se,

$$C = \left(\bigoplus_{i=1}^{s} C_i \right) \oplus \left(\bigoplus_{j=1}^{t} (C'_j \oplus (C'_j)^{\perp}) \right)$$

onde para $1 \leq i \leq s$, C_i é um código auto-dual sobre G_i de comprimento l (com respeito ao produto interno Hermitiano) e, para $i \leq j \leq t$, C'_j é um código linear de comprimento l sobre H'_j e $C_j^{\perp}$ é o dual de C_j com respeito ao produto interno Euclidiano.

Nas paginas posteriores utilizamos a teria relacionada a classes de ciclotomia e traço para expressar a transformada inversa de Fourier na forma

$$\mathbf{c}_g((\mathbf{x_i}),(\mathbf{y'_j}),(\mathbf{y''_j})) = \sum_{i=1}^{s} Tr_{G_i/\mathbf{F}}(\mathbf{x_i}\xi^{-gu_i}) + \sum_{j=1}^{t}(Tr_{H'_j/\mathbf{F}}(\mathbf{y_j}'\xi^{-gv_j}) + Tr_{H''_j/\mathbf{F}}(\mathbf{y_j}''\xi^{-gw_j}))$$

e a partir disto mostramos que C é auto-dual com respeito ao produto interno Euclidiano se, e somente se C_i são auto-dual com respeito ao produto interno Hermitiano e $C''_j = (C'_j)^{\perp}$ para cada j com respeito ao produto interno Euclidiano.

A vantagem desta abordagem é que podemos estudar códigos quase-cíclicos auto-duais por um caminho sistemático e podemos decompor códigos quase-cíclicos em códigos de comprimento menor.

Referências Bibliográficas

[1] H. Abramo e T.V. Maria Lucia (2002) *Códigos Corretores de Erros*. Série de Computação e Matemática, Impa.

[2] G. Adilson (2005) *Introdução à álgebra*. Projeto Euclides, Impa.

[3] J.H. Van Lint (1964) *Introduction to Coding Theory*. Aegean Park Press.

[4] R. Lidl & H. Niedeneiter (1983) *Finite Fields*. Addison-Wesley.

[5] R. Joseph J. (2005) *A First Course in Abstract Algebra*. Prentice Hall, 3a edição.

[6] Ling S. & Solé P. (2001) "On the Structure of Quasi-Cyclic Codes I". *IEEE Transactions on Information Theory*. Vol. 47. No 7. 2751-2760.

[7] Frank W. Anderson & Kent R. Fuller(1992) *Rings and Categories of Modules*. Graduate Texts in Mathematics, Hardcover.

[8] S. José Plínio de Oliveira (2005) *Introdução à Teoria dos Números*. Coleção Matemática Universitária, Impa.