Rogério Villafranca

Estrutura e Distribuição de Pesos de Códigos Cíclicos Modulares

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da CAPES

Santo André, 2018

Universidade Federal do ABC

Centro de Matemática, Computação e Cognição

Rogério Villafranca

Estrutura e Distribuição de Pesos de Códigos Cíclicos Modulares

Orientador: Prof. Dr. Francisco César Polcino Milies

Tese de doutorado apresentada ao Centro de Matemática, Computação e Cognição para obtenção do título de Doutor em Matemática

Este exemplar corresponde à versão final da tese
defendida pelo aluno Rogério Villafranca,
e orientada pelo Prof. Dr. Francisco César Polcino Milies.

Santo André, 2018

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Villafranca, Rogério
Estrutura e Distribuição de Pesos de Códigos Cíclicos Modulares / Rogério Villafranca. — 2018.

45 fls.

Orientador: Francisco César Polcino Milies

Tese (Doutorado) — Universidade Federal do ABC, Programa de Pós-Graduação em Matemática, Santo André, 2018.

1. Teoria de Códigos. 2. Álgebras de Grupo. 3. Códigos Cíclicos. 4. Códigos Modulares. I. Polcino Milies, Francisco César. II. Programa de Pós-Graduação em Matemática, 2018. III. Título.

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do autor e com a anuência de seu orientador.

Santo André, 19 de dezembro de 2018.

Assinatura do autor: Rogério Villafranca

Assinatura do orientador:

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Programa de Pós-Graduação em Matemática
Avenida dos Estados, 5001 – Bairro Santa Terezinha – Santo André – SP
CEP 09210-580 · Fone: (11) 4996-0017
ppg.matematica@ufabc.edu.br

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Tese de Doutorado do candidato Rogério Villafranca, realizada em 28 de setembro de 2018:

Prof.(a) Dr.(a) **Francisco Cesar Polcino Milies** (Universidade Federal do ABC) – Presidente

Prof.(a) Dr.(a) **Edson Ryoji Okamoto Iwaki** (Universidade Federal do ABC) – Membro Titular

Prof.(a) Dr.(a) **Raul Antonio Ferraz** (Universidade de São Paulo) – Membro Titular

Prof.(a) Dr.(a) **Anderson Tiago da Silva** (Universidade Federal de Viçosa) – Membro Titular

Prof.(a) Dr.(a) **Thierry Corrêa Petit Lobão** (Universidade Federal da Bahia) – Membro Titular

Prof.(a) Dr.(a) **Maria de Lourdes Merlini Giuliani** (Universidade Federal do ABC) – Membro Suplente

Prof.(a) Dr.(a) **Javier Sánchez Serdà** (Universidade de São Paulo) – Membro Suplente

Prof.(a) Dr.(a) **Irineu Antunes Junior** (Universidade Federal do ABC) – Membro Suplente

AGRADECIMENTOS

Em primeiro lugar agradeço a meu orientador César Polcino por todo apoio, pela paciência e pela grande (e não sei se merecida) confiança e também ao Prof. Raul Ferraz que com muita generosidade esteve sempre presente e fez importantes contribuições a esse trabalho.

Muchísimas gracias, por cierto, ao Prof. Juan Jacobo Simón Pinero, tanto pelo trabalho na Universidade como, e aqui devo estender os agradecimentos a sua esposa Diotila, pela amizade que me ofereceram em minha estada em Múrcia, pelas caronas, pelos passeios e pelas comidas.

Gostaria de agradecer também aos colegas de nosso grupo de Teoria de Códigos USP-UFABC pelo contínuo trabalho nos seminários e eventos e, em particular, ao Samir e à Edite por usarem meus programas e com isso me motivarem a melhorá-los.

Por fim, pelo apoio, confiança e compreensão, agradeço a minha família, especialmente minha querida esposa Tatiana, que sempre me acompanhou com muito amor e comigo enfrentou todas as dificuldades que encontramos.

RESUMO

Neste trabalho estudamos códigos cíclicos modulares sobre corpos finitos utilizando técnicas de álgebras de grupo e alguma análise combinatória. Oferecemos uma abordagem para tratar os códigos modulares de comprimento p^n que nos permite obter novos resultados sobre suas distribuições de pesos. Para os códigos de comprimento $p^n m$, com $p \nmid m$, obtemos informações sobre estrutura e pesos os vendo como códigos sobre anéis de cadeia e os relacionando com códigos semissimples de comprimento m.

Palavras-chave: Teoria de Códigos, Álgebras de Grupo, Códigos Cíclicos, Códigos Modulares

ABSTRACT

In this thesis we use group algebra techniques and some combinatorics to study modular cyclic codes over finite fields. We introduce an approach to deal with codes of length p^n that gives us new results on their weight distributions. We look at codes of length $p^n m$, $p \nmid m$, as codes over chain rings, and by relating them to semisimple codes of length m we obtain information on their structure and weight.

Keywords: Coding Theory, Group Algebras, Cyclic Codes, Modular Codes

LISTA DE TABELAS

LISTA DE SÍMBOLOS

$\langle \alpha \rangle$	Ideal de RC_m gerado por α	36
$a_{[t]}$	t-ésimo coeficiente p-ário do inteiro a	17
$\mathrm{conv}(\mathcal{C})$	Conveniência do código $\mathcal{C}$	10
$\mathrm{d}(\mathcal{C})$	Distância do código $\mathcal{C}$	8
$\mathrm{d_H}(x, y)$	Distância de Hamming entre x e y	7
$\Delta(G)$	Ideal de aumento do anel de grupo RG	6
$\mathbb{F}_q$	Corpo finito com q elementos	3
$\hat{G}$	Idempotente $\frac{1}{\lvert G \rvert} \sum_{g \in G} g$	37
$N^d(t)$	Número de polinômios de grau menor ou igual a d com t raízes distintas	16
$N_k(t)$	Número de polinômios de grau k com t raízes distintas	15
$\mathrm{supp}(x)$	Suporte do elemento x	5
$U(R)$	Grupo de unidades do anel R	3
$\mathrm{w}(\mathcal{C})$	Peso do código $\mathcal{C}$	8
$\mathbb{Z}_m$	Anel dos inteiros módulo m	3

CONTEÚDO

1 INTRODUÇÃO

Códigos cíclicos foram introduzidos em 1957 por E. Prange [Pra57] e, mais adiante, D. S. Berman [Ber67] e F. J. Mac Williams [Mac70] estenderam o conceito, definindo os códigos de grupos em geral.

No já citado artigo [Ber67], Berman estuda códigos de comprimento p^n sobre corpos de característica p, determinando suas estruturas e pesos. Uma classe de códigos de Reed-Muller configura um caso particular dos códigos tratados por Berman. Um tratamento recente dos códigos de Reed-Muller como códigos em uma álgebra de grupo modular pode ser encontrado em [AR17]. Códigos cíclicos modulares são abordados usando técnicas polinomiais e anéis de galois em [DP07] e alguns códigos abelianos modulares com base visível (i. e., uma base que contém um elemento de peso mínimo) são obtidos em [Han17].

Os avanços na teoria entretanto, sobretudo através do tratamento algébrico, são muito mais numerosos para códigos cujos comprimentos não são múltiplos da característica do corpo (ou anel) sobre o qual são construídos. Em particular, Ferraz e Polcino Milies deram em [FP07] início a uma série de resultados obtidos usando técnicas de álgebras de grupos.

Descobertas recentes de que bons códigos binários não lineares estão relacionados com códigos lineares sobre o anel dos inteiros módulo 4 [Cal+93] tem motivado o estudo de códigos sobre anéis em geral. Como uma extensão natural desse anel de coeficientes, Carlderbank e Sloane [CS95] determinaram a estrutura de códigos cíclicos sobre o anel de inteiros módulo p^m e Wan em [Wan11] estendeu esses resultados para códigos cíclicos sobre anéis de Galois. Em 1999, Norton e Salagean-Mandache [NS00] ampliaram ainda estes resultados para códigos cíclicos sobre anéis de cadeia finitos e,

mais adiante, Dinh e López-Permouth [DL04] demonstraram os mesmos resultados de uma maneira diferente. Recentemente, A. T. da Silva obteve os mesmos resultados, de forma bem mais simples, usando técnicas de álgebras de grupo, que permitiram inclusive calcular dimensões e pesos de todos os códigos cíclicos sobre anéis de cadeia sob certas hipóteses naturais [Sil12].

Neste trabalho tratamos códigos cíclicos modulares usando álgebras de grupo. Para isso, consideramos primeiro os códigos de comprimento p^n sob um nova perspectiva que nos permite não somente obter uma nova prova para as fórmulas dadas em [Ber67] para o peso desses códigos, como também determinar toda a distribuição de pesos para parte deles. Em seguida estudamos códigos de comprimento $p^n m$ tratando-os como códigos sobre anéis de cadeia e mostrando que muitas informações sobre suas estruturas e pesos podem ser obtidas a partir de códigos semissimples associados.

Após a apresentação de resultados preliminares sobre anéis, ideais, álgebras de grupo e códigos no capítulo 2, apresentamos no capítulo 3 alguns interessantes resultados sobre relações entre números de polinômios e de suas raízes e sobre combinatória em característica finita que serão usados nos capítulos seguintes.

Os capítulos 4 e 5 trazem nosso tratamento para códigos propriamente dito. O primeiro deles trata do comprimento p^n e o segundo, do comprimento $p^n m$. Finalmente, o capítulo 6 traz exemplos adicionais de códigos modulares, entre os quais figuram muitos códigos ótimos.

Na conclusão, capítulo 7, além de uma breve análise dos resultados obtidos, apresentamos algumas direções em que este trabalho pode ser continuado.

Os pesos de alguns dos códigos dados como exemplos foram obtidos computacionalmente, por isso, na seção 1 do apêndice incluímos a listagem da rotina usada para esse propósito.

2 RESULTADOS PRELIMINARES

2.1 ANÉIS FINITOS E IDEAIS

Nesta seção apresentamos definições e resultados sobre anéis e ideais, em particular, definimos e caracterizamos anéis de cadeia. Todos os anéis tratados são anéis associativos com unidade, fato que assumiremos tacitamente nas definições e resultados. Demonstrações e um tratamento mais detalhado para o conteúdo desta seção podem ser encontrados em [Jac09a], [Jac09b], [Sil12] e [Vil14].

Notação. Utilizaremos as notações $\mathbb{F}_q$ para representar o corpo finito com q elementos e $\mathbb{Z}_m$ para o anel $\mathbb{Z}/m\mathbb{Z}$ de inteiros módulo m.

Definição 2.1. Sejam R um anel comutativo e $r \in R$ um elemento não nulo.

(i) r é uma UNIDADE se é inversível, i. e., se existe $s \in R$ tal que $rs = 1$.

(ii) r é um DIVISOR DE ZERO se existe $s \neq 0$ em R tal que $rs = 0$.

(iii) r é NILPOTENTE se existe um inteiro $m > 0$ tal que $r^m = 0$ (o menor m com essa propriedade é chamado de ÍNDICE DE NILPOTÊNCIA de r)

Definição 2.2. O conjunto das unidades de um anel R forma um grupo com a operação de multiplicação do anel chamado GRUPO DE UNIDADES de R que denotaremos por $U(R)$.

Definição 2.3. Seja I um ideal lateral de um anel R. I é chamado NIL se para todo $x \in I$, existe um inteiro n, que depende de x, tal que $x^n = 0$. I é dito NILPOTENTE se existe um inteiro positivo n tal que $I^n = (0)$, onde I^n é o conjunto de todas as somas finitas de produtos de n elementos de I.

Definição 2.4. Um anel R é chamado LOCAL se o conjunto I de não-unidades de R forma um ideal.

Note-se que o ideal I na definição acima é o único ideal maximal de R, pois todo elemento fora de I é inversível. Por outro lado, se um anel R possui um único ideal maximal I, então R deve ser local, pois todo elemento $a \in R \setminus I$ não pertence a nenhum ideal próprio e, portanto, $Ra = R$, ou seja, a é uma unidade.

Definição 2.5. Um anel R é chamado ANEL DE CADEIA, ou UNISERIAL, se o conjunto de todos os seus ideais forma uma cadeia com a relação de inclusão.

Exemplo 2.6. Dado um inteiro primo p, é fácil ver que o anel $\mathbb{Z}_{p^m}$ dos inteiros módulo p^m é anel de cadeia com ideais $R \supset Rp \supset Rp^2 \supset \cdots \supset Rp^{m-1} \supset (0)$ e que todos os elementos fora do ideal maximal Rp são inversíveis.

Teorema 2.7 ([Vil14], Teorema 1.7)**.** *Para um anel comutativo R as seguintes condições são equivalentes:*

(i) R é um anel local e o ideal maximal M de R é principal.

(ii) R é um anel local de ideais principais.

(iii) R é um anel de cadeia.

Definição 2.8. Um elemento e de um anel R é dito IDEMPOTENTE se $e^2 = e$. Dois idempotentes e_1 e e_2 são chamados ORTOGONAIS se $e_1e_2 = 0$. Um idempotente e é dito CENTRAL se $er = re$ para todo $r \in R$ e é dito PRIMITIVO se sempre que se puder escrever $e = e_1 + e_2$, com e_1 e e_2 ortogonais, então $e_1 = 0$ ou $e_2 = 0$.

Proposição 2.9. *Se $I_1, \ldots, I_s$ são ideais de um anel R tais que $R = I_1 \oplus \cdots \oplus I_s$, então existem idempotentes ortogonais $e_1, \ldots, e_s$ tais que $e_1 + \cdots + e_s = 1$ e $e_kR = I_k$, $1 \leq k \leq s$.*

Definição 2.10. Um ideal I de um anel R é chamado um SOMANDO DIRETO se existir um ideal J tal que $I \oplus J = R$. R é dito SEMISSIMPLES se todos os seus ideais são somandos diretos.

2.2 ÁLGEBRAS DE GRUPO

Nesta seção apresentamos definições e resultados relacionados a álgebras de grupo. As demonstrações desses resultados e um tratamento mais completo podem ser encontrados em [PS02].

Definição 2.11. Dado um anel R e um grupo G, definimos o ANEL DE GRUPO de G sobre R como o conjunto

$$RG \doteq \left\{ \sum_{g \in G} \alpha_g g \;\middle|\; \alpha_g \in R,\ \alpha_g = 0 \text{ exceto um número finito de vezes} \right\}$$

munido das operações

$$\left(\sum_{g \in G} \alpha_g g \right) + \left(\sum_{g \in G} \beta_g g \right) = \sum_{g \in G} (\alpha_g + \beta_g) g$$

$$\left(\sum_{g \in G} \alpha_g g \right) \cdot \left(\sum_{g \in G} \beta_g g \right) = \sum_{g \in G} \left(\sum_{hk = g} \alpha_h \beta_k \right) g$$

$$\lambda \left(\sum_{g \in G} \alpha_g g \right) = \sum_{g \in G} (\lambda \alpha_g) g,\ \lambda \in R$$

Se o anel R for comutativo (e. g. um corpo) RG também é chamado de ÁLGEBRA DE GRUPO de G sobre R.

Definição 2.12. Definimos o SUPORTE de um elemento $x = \sum_{g \in G} \alpha_g g \in RG$ e denotamos por $\operatorname{supp}(x)$ como o conjunto dos elementos de G que comparecem com coeficiente não nulo em x, i. e.,

$$\operatorname{supp}(x) = \{ g \in G \mid \alpha_g \neq 0 \}.$$

Lema 2.13. *Sejam G e H grupos e R um anel comutativo. Então $R(G \times H) \cong (RG)H$.*

Definição 2.14. O homomorfismo

$$\varepsilon : RG \longrightarrow R$$

$$\sum_{g \in G} \alpha_g g \longmapsto \sum_{g \in G} \alpha_g$$

é chamado FUNÇÃO DE AUMENTO de RG e seu núcleo, $\ker(\varepsilon)$, é chamado de IDEAL DE AUMENTO de RG e denotado por $\Delta(G)$.

Proposição 2.15 ([PS02], Proposition 3.2.10)**.** *O conjunto* $\{g-1 \mid g \in G, g \neq 1\}$ *é uma base de* $\Delta(G)$ *sobre* R*. Assim, podemos escrever*

$$\Delta(G) = \left\{ \sum_{\substack{g \in G \\ g \neq 1}} \alpha_g (g-1) \,\middle|\, \alpha_g \in R \right\}$$

As condições para que um anel de grupo seja semissimples são dadas pelo Teorema de Maschke, enunciado a seguir.

Teorema 2.16 (MASCHKE – [PS02], Theorem 3.4.7)**.** *Seja* G *um grupo. O anel de grupo* RG *é simissimples se e somente se as seguintes condições forem satisfeitas:*

(i) R *é um anel semissimples;*

(ii) G *é finito;*

(iii) $|G|$ *é inversível em* R*.*

Corolário 2.17. *Seja* G *um grupo finito e* K *um corpo. Então* KG *é semissimples se e somente se* $\operatorname{car}(K) \nmid |G|$*.*

Definição 2.18. Um álgebra não semissimples é dita MODULAR.

Proposição 2.19 ([Jac09b], Proposition 7.14)**.** *Seja* R *um anel,* N *um ideal nil em* R *e* $\bar{u} = u + N$ *um idempotente de* $\bar{R} = R/N$*. Então existe um idempotente* $e \in R$ *tal que* $\bar{e} = \bar{u}$*. Além disso,* e *é único se* R *é comutativo.*

Teorema 2.20 (COLEMAN – [PS02], Theorem 6.3.1)**.** *Seja* K *um corpo de característica* $p \geq 0$ *e* G *um grupo arbitrário. Então o ideal de aumento* $\Delta(G)$ *de* KG *é nilpotente se e somente se* $p > 0$ *e* G *é um* p*-grupo finito.*

Teorema 2.21. *Seja* R *um anel de cadeia e* M *seu ideal maximal. Então*

$$\frac{RG}{MG} \cong \left(\frac{R}{M}\right) G.$$

2.3 CÓDIGOS

As definições e resultados deste capítulo podem ser encontradas em referências sobre teoria de códigos como [Rom92], [MS77] e [Lin98].

Seja $\mathcal{A}$ um conjunto finito, que chamaremos de ALFABETO , e denotemos por q seu número de elementos. Um CÓDIGO q-ÁRIO $\mathcal{C}$ DE COMPRIMENTO n, será um subconjunto qualquer de $\mathcal{A}^n$ (chamado de ESPAÇO AMBIENTE). Chamaremos, naturalmente, os elementos do alfabeto $\mathcal{A}$ de LETRAS e os elementos de $\mathcal{C}$ de PALAVRAS do código e denotaremos estes últimos como n-uplas ordenadas, como de costume para elementos de um produto cartesiano, ou pela simples justaposição das letras que o formam, i. e., $(x_1, x_2, \ldots, x_n)$ ou $x_1x_2 \ldots x_n$.

Definição 2.22. Dados dois elementos $x = x_1x_2 \ldots x_n$ e $y = y_1y_2 \ldots y_n$ de $\mathcal{A}^n$, chama-se DISTÂNCIA DE HAMMING de x a y ao número letras em que estes elementos diferem, i. e.,

$$\mathrm{d_H}(x, y) = |\{i \mid x_i \neq y_i,\ 1 \leq i \leq n\}| .$$

A função apresentada acima de fato confere ao conjunto $\mathcal{A}^n$ uma estrutura de espaço métrico com as usuais definições de bolas e esferas.

Se no alfabeto $\mathcal{A}$ existe um elemento nulo, podemos fazer a seguinte definição.

Definição 2.23. Dado $x = x_1x_2 \ldots x_n \in \mathcal{A}^n$, o número

$$\mathrm{w_H}(x) = |\{i \mid x_i \neq 0,\ 1 \leq i \leq n\}|$$

chama-se PESO DE HAMMING de x. É claro que $\mathrm{w_H}(x) = \mathrm{d_H}(x, 0)$.

Utilizam-se também outras definições de distância e peso em teoria de códigos como, por exemplo, a distância e o peso de Lee. Pares de funções distância d e peso w devem sempre satisfazer a relação $\mathrm{w}(x) = \mathrm{d}(x, 0)$. Neste texto sempre utilizaremos distância e peso de Hamming, por isso omitiremos a qualificação "de Hamming" e denotaremos simplesmente por d e w.

Definição 2.24. Dado um código $\mathcal{C} \subset \mathcal{A}^n$ e funções distância d e peso w, chama-se DISTÂNCIA MÍNIMA de $\mathcal{C}$ o número

$$\mathrm{d}(\mathcal{C}) = \min\{\mathrm{d}(x, y) \mid x, y \in \mathcal{C},\ x \neq y\}$$

e chama-se PESO MÍNIMO de $\mathcal{C}$, ou simplesmente PESO de $\mathcal{C}$, o número

$$\mathrm{w}(\mathcal{C}) = \min\{\mathrm{w}(x) \mid x \in \mathcal{C},\ x \neq 0\}.$$

Os resultados a seguir lidam com a capacidade de detecção e correção de erros em códigos.

Proposição 2.25. *Todas as esferas de raio r em $\mathcal{A}^n$ possuem o mesmo número de elementos.*

Teorema 2.26. *Seja $\mathcal{C}$ um código com distância mínima d e seja*

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Então é possível detectar até $d-1$ erros e corrigir até κ erros.

Corolário 2.27. *Um código $\mathcal{C}$ pode corrigir até κ erros se e somente se sua distância mínima* $\mathrm{d}(\mathcal{C})$ *verifica a desigualdade*

$$\mathrm{d}(\mathcal{C}) \geq 2\kappa + 1.$$

Definição 2.28. Dado um código $\mathcal{C}$ com distância mínima d, o número

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$$

chama-se a CAPACIDADE de $\mathcal{C}$.

Um código q-ário de comprimento n, com $M = |\mathcal{C}|$ palavras e distância mínima d diz-se um (n, M, d)-CÓDIGO .

Deve parecer claro nesse ponto que é desejável que a distância mínima de um código seja a maior possível para que sua capacidade de detecção e correção também o seja. Por outro lado, é também desejável que o número de palavras no código seja o maior possível para que se possa transmitir a maior densidade de informação possível. Ocorre

que esses objetivos são conflitantes pois uma vez definido o alfabeto e o comprimento das palavras, aumentando-se o número de palavras no código, diminui-se a distância mínima entre elas. A questão de encontrar valores satisfatórios para esses parâmetros é conhecida como o PROBLEMA PRINCIPAL DA TEORIA DE CÓDIGOS e o clássico resultado a seguir nos oferece um primeiro limite.

Teorema 2.29 (COTA DE HAMMING). *Dado um* (n, M, d)*-código, tem-se que*

$$M \leq \frac{q^n}{\sum_{t=0}^{\kappa} \binom{n}{t}(q-1)^t}.$$

A definição a seguir trata do máximo aproveitamento de um código.

Definição 2.30. Um código $\mathcal{C} \subset \mathcal{A}^n$ com distância mínima d e capacidade κ diz-se PERFEITO se

$$\bigcup_{x \in \mathcal{C}} B(x, \kappa) = \mathcal{A},$$

onde $B(x, \kappa) = \{y \in \mathcal{A}^n \mid \mathrm{d}(x, y) \leq \kappa\}$.

Proposição 2.31. *Um* (n, M, d)*-código* $\mathcal{C}$ *é perfeito se e somente se tem-se que*

$$M\left[\sum_{t=0}^{\kappa} \binom{n}{t}(q-1)^t\right] = q^n.$$

2.3.1 Códigos lineares

De modo a dar mais estrutura algébrica a códigos, consideremos como alfabeto $\mathcal{A}$ um corpo (ou anel) finito.

Definição 2.32. Um subespaço vetorial $\mathcal{C}$ de dimensão k do espaço ambiente $\mathbb{F}_q^n$ diz-se um (n, k)-CÓDIGO LINEAR sobre $\mathbb{F}_q$ e, se sua distância mínima d é conhecida, diz-se também um (n, k, d)-CÓDIGO LINEAR sobre $\mathbb{F}_q$.

Caso o alfabeto seja um anel, podemos estender essa definição da seguinte forma:

Definição 2.33. Seja R um anel finito. Um CÓDIGO LINEAR de comprimento n sobre R é um submódulo de R^n. Em particular, um CÓDIGO LINEAR LIVRE sobre R é um código linear sobre R que possui uma R-base.

A estrutura de espaço vetorial (ou módulo) dos códigos lineares nos oferece relações entre uma função distância d e sua correspondente função peso w além da já citada $\mathrm{w}(x) = \mathrm{d}(x, 0)$. Dados elementos x e y de um código linear, uma relação equivalente a esta última é

$$\mathrm{d}(x, y) = \mathrm{w}(x - y).$$

De fato, é bastante comum definir peso a partir de distância ou vice-versa. Há ainda outra importante e facilmente verificável relação entre peso e distância para códigos lineares, a saber, que distância mínima e peso mínimo de um código linear coincidem, i. e.,

$$\mathrm{d}(\mathcal{C}) = \mathrm{w}(\mathcal{C}).$$

Voltando ao problema principal da Teoria de Códigos, fixado q, entre códigos de mesma dimensão, os de maior peso serão considerados melhores e entre códigos de mesmo peso, melhores serão os de maior dimensão. A seguir introduzimos uma medida para comparar códigos ainda que estes difiram tanto na dimensão quanto no peso.

Definição 2.34. [MM13] Definimos a CONVENIÊNCIA de um código $\mathcal{C}$ por

$$\mathrm{conv}(\mathcal{C}) = \mathrm{w}(\mathcal{C}) \cdot \dim(\mathcal{C})$$

Além da estrutura de espaço vetorial ou módulo, podem-se obter importantes resultados acrescentando ainda mais estrutura. Em particular, de importantes propriedade práticas e algébricas é a classe de códigos lineares definida a seguir.

Definição 2.35. Um código linear $\mathcal{C}$ de comprimento n é dito CÍCLICO se sempre que $c_0c_1 \dots c_{n-1}$ pertencer a $\mathcal{C}$, sua permutação cíclica $c_{n-1}c_0c_1 \dots c_{n-2}$ também pertencer.

Tomando o grupo cíclico $G = \langle g \mid g^n = 1 \rangle$, através da associação

$$\phi : \mathcal{C} \longrightarrow RG$$
$$c_0 c_1 \dots c_{n-1} \longmapsto c_0 + c_1 a + \dots + c_{n-1} a^{n-1}$$

é fácil ver que códigos cíclicos de comprimento n sobre R correspondem aos ideais da álgebra de grupo RG.

Definição 2.36. Um código linear $\mathcal{C}$ de comprimento n é dito QUASI-CÍCLICO ou r-QUASI-CÍCLICO se sempre que $c_0 c_1 \dots c_{n-1}$ pertencer a $\mathcal{C}$, sua permutação cíclica $c_{n-r} c_{n-r+1} \cdots c_{n-1} c_0 c_1 \dots c_{n-r-1}$ também pertencer.

2.3.2 Codificação e decodificação

Nesta seção $\mathcal{C}$ será sempre um (n, m)-código linear sobre um corpo (ou anel comutativo) que denotaremos por K.

Definição 2.37. Uma matriz G de dimensão $m \times n$ cujas linhas formam um conjunto de geradores minimal para $\mathcal{C}$ é chamada uma MATRIZ GERADORA OU MATRIZ DE CODIFICAÇÃO de $\mathcal{C}$.

Nessas condições, as palavras de $\mathcal{C}$ são combinações lineares das linhas de G, o que oferece um método de codificação da informação de entrada: dado um vetor de informação u, a palavra correspondente será $c = uG$.

Como $\mathcal{C}$ é um subespaço (ou submodulo) de K^n, pode-se determinar uma função linear sobrejetora $\pi : K^n \to K^{n-m}$ cujo núcleo seja o código $\mathcal{C}$. A partir disso, podemos fazer a seguinte definição.

Definição 2.38. Uma matriz H de dimensão $n \times (n - m)$ que representa nas bases canônicas uma transformação linear $\pi : K^n \to K^{n-m}$ tal que $\ker(\pi) = \mathcal{C}$ é chamada uma matriz de verificação do código $\mathcal{C}$.

Pela definição anterior, o código $\mathcal{C}$ é precisamente o conjunto dos vetores $y \in K^n$ tais que $yH = 0$, de modo que multiplicar pela matriz H é uma maneira de verificar se um

dado vetor é ou não uma palavra do código. Assim, dentro dos limites do código, essa matriz pode ser usada para detectar erros em uma mensagem recebida, i. e., um vetor $y \in K^n$ recebido contém erros se $yH \neq 0$. A expressão yH é uma função de y que definimos abaixo.

Definição 2.39. Seja H a matriz de verificação de $\mathcal{C}$. Dado um vetor $y \in K^n$, o vetor

$$S(y) = yH$$

é chamado de SÍNDROME de y.

Caso erros sejam detectados em um vetor recebido y e considerando-se que a quantidade de erros não supere a capacidade do código, uma maneira de corrigir esses erros é procurar a palavra c do código mais próxima de y. Isso pode ser feito encontrando-se o vetor de menor peso na classe lateral $y + \mathcal{C}$. Esse vetor é chamado de LÍDER DA CLASSE e corresponde exatamente ao VETOR ERRO $e = y - c$. Logicamente, conhecido o vetor erro recupera-se a palavra enviada fazendo $c = y - e$. O método que acabamos de descrever é chamado de DECODIFICAÇÃO POR DISTÂNCIA MÍNIMA.

Além da detecção e correção de erros o processo de decodificação consiste ainda de recuperar o vetor de informação correspondente à palavra do código recebida (e corrigida). Essa etapa, que se poderia chamar de decodificação propriamente dita (i. e., desfazer a codificação) pode ser um problema bastante difícil de tratar de maneira geral. Uma das maneiras de resolvê-lo na prática, desde que o código não seja demasiado grande, é simplesmente ter uma tabela de correspondência entre os vetores de informação e as palavras do código.

3 CONTAGEM E COMBINATÓRIA

Neste capítulo apresentamos alguns resultados sobre contagem de polinômios e suas raízes e algumas identidades combinatoriais que serão usadas nos capítulos seguintes.

3.1 POLINÔMIOS E RAÍZES

Nos resultados a seguir K denota um corpo finito de característica p e $q = |K|$. Em primeiro lugar vamos analisar o número máximo de raízes que um polinômio em várias variáveis com certas limitações de grau pode ter, informação que será usada na determinação do peso de códigos p-ários de comprimento p^n no capítulo 4.

Proposição 3.1. *Seja $f \in K[x_0, \ldots, x_{k-1}]$ um polinômio não nulo em k variáveis com coeficientes em K tal que $d_i \doteq \deg_{x_i}(f) \leq q$, $0 \leq i \leq k-1$. Então f pode ter no máximo*

$$q^k - \prod_{i=0}^{k-1}(q - d_i). \tag{1}$$

raizes distintas $(\alpha_0, \ldots, \alpha_{k-1}) \in K^k$. Ademais, esse número é atingido pelos polinômios da forma

$$f(x_0, \ldots, x_{k-1}) = \lambda \prod_{i=0}^{k-1} \left(\prod_{j=0}^{d_i-1} (x_i - \alpha_{i,j}) \right),$$

onde $\lambda \in K^*$, $\alpha_{i,j} \in K$ e $\alpha_{i,j} \neq \alpha_{i,\ell}$ se $j \neq \ell$.

Demonstração. Vamos provar por indução em k. Para $k = 1$, f é um polinômio de grau $d_0 \leq q$ em apenas uma variável, logo pode ter no máximo d_0 raízes distintas, o que coincide com a expressão (1).

Agora, vamos assumir que o resultado vale para até $k-1$ variáveis. Temos, para k variáveis,

$$f(x_0, \ldots, x_{k-1}) = f_0(x_0, \ldots, x_{k-2}) + f_1(x_0, \ldots, x_{k-2})x_{k-1} + \cdots + f_{d_k}(x_0, \ldots, x_{k-2})x_{k-1}^{d_{k-1}}.$$

Considerando todas as $(k-1)$-uplas $(\alpha_0, \ldots, \alpha_{k-2}) \in K^{k-1}$, denotemos por N o número das que são simultaneamente raízes de $f_0, \ldots, f_{d_k}$. Então, tomando essas $(k-1)$-uplas e todos os $\beta_{k-1} \in K$, temos Nq raízes $(\alpha_0, \ldots, \alpha_{k-2}, \beta_{k-1})$ de f. Para cada uma das $q^{k-1} - N$ outras $(k-1)$-uplas, $f(\alpha_0, \ldots, \alpha_{k-2}, x_{k-1})$ é um polinômio não nulo de grau menor ou igual a $d_{k-1} \leq q$ na variável x_{k-1}, podendo ter então, no máximo, d_{k-1} raízes distintas. Assim, f pode ter até $Nq + (q^{k-1} - N)d_{k-1} = N(q - d_{k-1}) + q^{k-1}d_{k-1}$ raízes. Como $d_{k-1} \leq q$, esse número será máximo quando N for máximo, e, supondo que $f_0, \ldots, f_{d_k}$ tenham as mesmas raízes, pela hipótese de N pode ser, no máximo, $q^{k-1} - \prod_{i=0}^{k-2}(q - d_i)$. Dessa forma, o número máximo de raízes distintas de f será

$$N(q - d_{k-1}) + q^{k-1}d_{k-1} = \left(q^{k-1} - \prod_{i=0}^{k-2}(q - d_i)\right)(q - d_{k-1}) + q^{k-1}d_{k-1} =$$
$$= q^k - \prod_{i=0}^{k-1}(q - d_i).$$

Por fim, dados $\lambda \in K^*$ e $\alpha_{i,j} \in K$ satisfazendo $\alpha_{i,j} \neq \alpha_{i,\ell}$ se $j \neq \ell$,

$$f(x_0, \ldots, x_{k-1}) = \lambda \prod_{i=0}^{k-1}\left(\prod_{j=0}^{d_i-1}(x_i - \alpha_{i,j})\right)$$

tem por raízes as k-uplas $\beta_0, \ldots, \beta_{k-1}$ que tenha $\beta_i = \alpha_{i,j}$ para algum par i, j. Em outras palavras, as k-uplas que não são raízes de tal f devem ter cada β_i distinto de todas as d_i raízes $\alpha_{i,j}$ de f_i, logo, o número de tais k-uplas é trivialmente $(q - d_0) \cdots (q - d_{k-1})$ e o resultado segue. □

De forma complementar ao resultado anterior, nos resultados a seguir determinaremos o número de polinômios, novamente com certa limitação de grau, que possuem um dado número de raízes. Esse resultado será usado também no capítulo 4 para determinar a distribuição de pesos todos os códigos p-ários de comprimento p e de parte dos de comprimento p^n se $n > 1$.

Teorema 3.2. *Denotemos por $N_k(t)$ o número de polinômios de grau k em $K[x]$ que tenham exatamente t raízes distintas. Então*

$$N_k(k) = \binom{q}{k}(q-1),$$
$$N_k(t) = \binom{q}{t}(q-1)q^{k-t} - \sum_{i=t+1}^{k} \binom{i}{t} N_k(i), \text{ for } k < t \leq q.$$

Demonstração. É claro que $N_k(k) = \binom{q}{k}(q-1)$.

Dado $g(x) \in K[x]$, denotemos por $A_{g(x)}$ o conjunto das raízes de $g(x)$ em K. Dados dois subconjuntos de K de mesma cardinalidade $A = \{\alpha_1, \ldots, \alpha_t\}$ e $B = \{\beta_1, \ldots, \beta_t\}$, o número de polinômios $g_1 \in K[x]$ de grau k tais que $A_{g_1(x)} = A$ é o mesmo que o número de polinômios $g_2 \in K[x]$ de grau k tais que $A_{g_2(x)} = B$. Como esse número não depende especificamente dos elementos de A e B, vamos denitá-lo por $n_k(t)$. Agora, o conjunto de todos os polinômios de grau k in $K[x]$ que têm exatamente t raízes distintas é a união disjunta dos conjuntos de polinômios de grau k que tenham como raízes cada um dos subconjuntos de K de cardinalidade t. Então

$$N_k(t) = \binom{q}{t} n_k(t). \tag{2}$$

Dado um conjunto $A = \{\alpha_1, \ldots, \alpha_t\} \subset K$ de cardinalidade t, os polinômios $g(x) \in K[x]$ de grau k para os quais $A \subset A_{g(x)}$ têm a forma

$$g(x) = (x - \alpha_1) \cdots (x - \alpha_t) \cdot g_1(x),$$

onde $g_1(x)$ é um polinômio de grau $k - t$ em $K[x]$. Como existem $(q-1)q^{k-t}$ polinômios de grau $k - t$, o número de polinômios $g(x) \in K[x]$ de grau k tais que $A \subset A_{g(x)}$ é precisamente $(q-1)q^{k-t}$. De modo a computar $n_k(t)$ devemos então subtrair de $(q-1)q^{k-t}$ o número de polinômios de grau k que tenham i raízes, $t+1 \leq i \leq k$, dentre as quais igurem todos os elementos de A. Existem $\binom{q-t}{i-t}$ subconjuntos de K de cardinalidade i contendo A, logo

$$n_k(t) = (q-1)q^{k-t} - \sum_{i=t+1}^{k} \binom{q-t}{i-t} n_k(i),$$

então, tendo em vista a equação (2),

$$N_k(t) = \binom{q}{t}\left[(q-1)q^{k-t} - \sum_{i=t+1}^{k} \frac{\binom{q-t}{i-t}}{\binom{q}{i}} N_k(i)\right].$$

Mas

$$\frac{\binom{q-t}{i-t}}{\binom{q}{i}} = \frac{(q-t)!}{(i-t)!\,(q-i)!} \cdot \frac{i!\,(q-i)!}{q!} \cdot \frac{t!}{t!} = \frac{\binom{i}{t}}{\binom{q}{t}},$$

então

$$N_k(t) = \binom{q}{t}(q-1)q^{k-t} - \sum_{i=t+1}^{k} \binom{i}{t} N_k(i).$$

□

Corolário 3.3. *Definindo $N^d(t)$ como o número de polinômios de grau menor ou igual a d em $K[x]$ que têm exatamente t raízes distintas, temos*

$$N^d(t) = \binom{q}{t}(q^{d-t+1} - 1) - \sum_{i=t+1}^{d} \binom{i}{t} N^d(i).$$

Demonstração. E claro que $N^d(t) = \sum_{k=t}^{d} N_k(t)$. Assim,

$$\begin{aligned}
N^d(t) &= \sum_{k=t}^{d}\left[\binom{q}{t}(q-1)q^{k-t} - \sum_{i=t+1}^{k}\binom{i}{t}N_k(i)\right] = \\
&= \binom{q}{t}(q-1)\sum_{k=t}^{d} q^{k-t} - \sum_{k=t}^{d}\sum_{i=t+1}^{k}\binom{i}{t}N_k(i) = \\
&= \binom{q}{t}(q-1)\sum_{k=0}^{d-t} q^{k} - \sum_{i=t+1}^{d}\sum_{k=i}^{d}\binom{i}{t}N_k(i) = \\
&= \binom{q}{t}(q-1)\frac{q^{d-t+1}-1}{q-1} - \sum_{i=t+1}^{d}\left[\binom{i}{t}\sum_{k=i}^{d} N_k(i)\right] = \\
&= \binom{q}{t}(q^{d-t+1}-1) - \sum_{i=t+1}^{d}\binom{i}{t}N^d(i).
\end{aligned}$$

□

Observação 3.4. Estaremos interessados nas raízes de polinômios em $K[x_0, \ldots, x_{k-1}]$ (ou $K[x]$) que estejam em $\mathbb{F}_p^k \subset K^k$ (ou $\mathbb{F}_p$). A adaptação das demonstrações dos últimos resutados a esse caso é imediata, nos dando a expressão

$$p^k - \prod_{i=0}^{k-1}(p - d_i)$$

para o número máximo de raízes e as fórmulas

$$N_k(t) = \binom{p}{t}(q-1)q^{k-t} - \sum_{i=t+1}^{k}\binom{i}{t}N_k(i)$$

e

$$N^d(t) = \binom{p}{t}(q^{d-t+1}-1) - \sum_{i=t+1}^{d}\binom{i}{t}N^d(i)$$

para os números de polinômios com dado número de raízes.

3.2 COMBINATÓRIA

Nesta seção apresentamos alguns resultados relacionados a coeficientes e expansões binomiais em característica prima. Em tudo que segue p denota um inteiro primo.

Iniciaremos apresentando uma definição e introduzindo uma notação de que faremos uso extensivo tanto aqui quanto nos capítulos que seguem.

Definição 3.5. Dados inteiros a e n tais que $p^n > a$, a pode ser escrito de maneira única na forma

$$a = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1}p^{n-1},$$

com $0 \leq a_0, a_1, \ldots, a_{n-1} \leq p-1$. Tal expressão é chamada de REPRESENTAÇÃO p-ÁRIA ou EXPANSÃO p-ÁRIA de a e os números $a_0, a_1, \ldots, a_{n-1}$ são chamados de COEFICIENTES p-ÁRIOS de a.

Notação. Dado um inteiro a, denotaremos por $a_{[t]}$ o coeficiente de p^t na expansão p-ária de a, i. e., $a = \sum_{i=0}^{n-1} a_{[i]}p^i$.

O teorema a seguir é bastante conhecido em Combinatória (v. [Cam94]) e por isso, embora tenha demonstração razoavelmente simples, não a incluiremos aqui.

Teorema 3.6 (LUCAS)**.** *Sejam a e b inteiros tais que $0 \leq a \leq p^n - 1$ e $0 \leq b \leq p^n - 1$. Então*

$$\binom{a}{b} \equiv \prod_{i=0}^{n-1}\binom{a_{[i]}}{b_{[i]}} \pmod{p}.$$

Lema 3.7. *Dados um primo p e um inteiro positivo n, para quaisquer inteiros a e b, vale a congruência*

$$(-1)^{a-b}\binom{a}{b} \equiv \binom{p^n-1-b}{p^n-1-a} \pmod{p}.$$

Demonstração. De fato,

$$(-1)^{a-b}\binom{a}{b} = (-1)^{a-b}\frac{\prod_{i=b+1}^{a} i}{(a-b)!} = \frac{\prod_{i=b+1}^{a}(-i)}{(a-b)!} \equiv$$
$$\equiv \frac{\prod_{i=b+1}^{a}(p^n-i)}{(a-b)!} = \binom{p^n-1-b}{p^n-1-a} \pmod{p}.$$

□

Corolário 3.8. *Sejam t e n inteiros tais que $t < p^n$. Então*

$$(x-1)^t \equiv \sum_{k=0}^{t}\binom{p^n-1-k}{p^n-1-t}x^k \pmod{p}.$$

Observação 3.9. Com respeito ao Triângulo de Pascal, o corolário 3.8 mostra que os coeficientes da expansão de $(x-1)^t$ em característica p podem ser lidos diretamente na coluna p^n-1-t do triângulo, como ilustra o exemplo a seguir.

Exemplo 3.10. Nos arranjos abaixo temos, à esquerda, um Triângulo de Pascal até a linha 6 e, à direita, um triângulo cujas colunas são formadas, da esquerda para a direita, pelos coeficientes de $(x-1)^6$, $(x-1)^5, \ldots, (x-1)^0$. É fácil ver que os números nos dois arranjos são respectivamente congruentes módulo 7.

1							1						
1	1						−6	1					
1	2	1					15	−5	1				
1	3	3	1				−20	10	−4	1			
1	4	6	4	1			15	−10	6	−3	1		
1	5	10	10	5	1		−6	5	−4	3	−2	1	
1	6	15	20	15	6	1	1	−1	1	−1	1	−1	1

Lema 3.11. *Seja a um inteiro tal que $0 \leq a \leq p^n - 1$. Então*

$$(p^n - 1 - a)_{[k]} = p - 1 - a_{[k]}.$$

Demonstração. De fato,

$$\begin{aligned}(p^n - 1) - a &= (p-1)(1 + p + \cdots + p^{n-1}) - a_{[0]} - a_{[1]}p - \cdots - a_{[n-1]}p^{n-1} = \\ &= (p - 1 - a_{[0]}) + (p - 1 - a_{[1]})p + \cdots + (p - 1 - a_{[n-1]})p^{n-1}.\end{aligned}$$

□

Aplicando o Teorema de Lucas aos últimos resultados, obtemos o seguinte corolário.

Corolário 3.12. *Sejam t e n inteiros tais que $t < p^n$. Então*

$$(x-1)^t \equiv \sum_{k=0}^{t} \left(\prod_{i=0}^{n-1} \binom{p-1-k_{[i]}}{p-1-t_{[i]}} \right) x^k \pmod{p}. \tag{3}$$

Por fim, podemos determinar o número de coeficientes não nulos (ou seja, o peso) de $(x-1)^t$ em característica p.

Corolário 3.13. *Sejam t e n inteiros tais que $t < p^n$. Então o número de coeficientes não nulos, módulo p, na expansão de $(x-1)^t$ é igual ao produto $(t_{[0]}+1)(t_{[1]}+1)\cdots(t_{[n-1]}+1)$.*

Demonstração. O coeficiente de x^k na expressão (3) será nulo se e somente se para algum i, $p - 1 - t_{[i]} > p - 1 - k_{[i]}$, i. e., se $k_{[i]} > t_{[i]}$. Então essa expressão pode ser reescrita na forma

$$(x-1)^t \equiv \sum_{k_{[0]}=0}^{t_{[0]}} \sum_{k_{[1]}=0}^{t_{[1]}} \cdots \sum_{k_{[n-1]}=0}^{t_{[n-1]}} \left[\prod_{i=0}^{n-1} \binom{p-1-k_{[i]}}{p-1-t_{[i]}} \right] x^k \pmod{p},$$

onde incluímos apenas os coeficientes não nulos e há $(t_{[0]}+1)(t_{[1]}+1)\cdots(t_{[n-1]}+1)$ parcelas. □

4 CÓDIGOS PURAMENTE MODULARES

Neste capítulo estudamos a estrutura e a distribuição de pesos de códigos de comprimento p^n sobre um corpo K de característica p. Em todo o capítulo $G = \langle a \mid a^{p^n} = 1 \rangle$ é o grupo cíclico de ordem p^n e $q = |K|$.

Como o comprimento desses códigos é múltiplo da característica do corpo, a álgebra de grupo KG é modular, por isso esses são ditos CÓDIGOS MODULARES. Os códigos no capítulo 5 têm um quociente semissimples do qual extrairemos muita informação, usamos a expressão "puramente modulares" para o presente capítulo em oposição a essa condição, em verdade os códigos aqui apresentados são modulares indecomponíveis.

Vamos começar analisando o ideal de aumento $\Delta(G)$. Sabemos pela proposição 2.15 que $\{a^k - 1 \mid 1 \leq k \leq p^n - 1\}$ é base de $\Delta(G)$ e então, considerando a igualdade $a^k - 1 = (a-1)(a^{k-1} + \cdots + a + 1)$, decorre imediatamente que $\Delta(G) = KG(a-1)$.

Além disso, $(a-1)^{p^n} = a^{p^n} - 1 = 0$, logo $\Delta(G)$ é nilpotente e para todo elemento $m \in \Delta(G)$ temos $m^{p^n} = 0$. Tomemos então $x \in KG \setminus \Delta(G)$. É claro que $\alpha = \varepsilon(x) \neq 0$ e definindo $m = x - \alpha$ temos que $m \in \Delta(G)$, logo

$$x^{p^n} = (\alpha + m)^{p^n} = \alpha^{p^n} + m^{p^n} = \alpha^{p^n} \in K^*,$$

portanto x é inversível e então $\Delta(G)$ contém todos os elementos não inversíveis de KG.

Assim, KG é anel local com ideal maximal principal $\Delta \doteq \Delta(G) = KG(a-1)$ e então, pelo teorema 2.7, é anel de cadeia. Abaixo a cadeia de ideais de KG:

$$KG \supset \Delta \supset \Delta^2 \supset \cdots \supset \Delta^{p^n-1} \supset \Delta^{p^n} = (0).$$

Com isso temos a seguinte caracterização para os códigos cíclicos de comprimento p^n sobre K.

Proposição 4.1. *Todo código cíclico de comprimento p^n sobre K é da forma Δ^ℓ, onde Δ é o ideal de aumento da álgebra do grupo cíclico G sobre K e $1 \leq \ell \leq p^n - 1$.*

É claro que $\mathcal{B} = \{(a-1)^k : \ell \leq k \leq p^n - 1\}$ é uma base de Δ^ℓ, então, usando os corolários 3.8 e 3.12, podemos construir a matriz geradora $(\gamma_{ij})_{(p^n-\ell)\times p^n}$ desse código, cujos elementos são dados por

$$\gamma_{ij} = \binom{p^n - j}{p^n - \ell - i} = \prod_{r=0}^{n-1} \binom{p - j_{[r]}}{p - (\ell + i)_{[r]}}. \tag{4}$$

Exemplo 4.2. Para $\Delta^3 \subset \mathbb{F}_7 C_7$, a matriz (4) assume a forma

$$\begin{pmatrix} \binom{6}{3} & \binom{5}{3} & \binom{4}{3} & \binom{3}{3} & 0 & 0 & 0 \\ \binom{6}{2} & \binom{5}{2} & \binom{4}{2} & \binom{3}{2} & \binom{2}{2} & 0 & 0 \\ \binom{6}{1} & \binom{5}{1} & \binom{4}{1} & \binom{3}{1} & \binom{2}{1} & \binom{1}{1} & 0 \\ \binom{6}{0} & \binom{5}{0} & \binom{4}{0} & \binom{3}{0} & \binom{2}{0} & \binom{1}{0} & \binom{0}{0} \end{pmatrix} = \begin{pmatrix} 6 & 3 & 4 & 1 & 0 & 0 & 0 \\ 1 & 3 & 6 & 3 & 1 & 0 & 0 \\ 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

enquanto para $\Delta^4 \subset \mathbb{F}_3 C_9$, temos a matriz geradora

$$\begin{pmatrix} \binom{2}{1}\binom{2}{1} & \binom{1}{1}\binom{2}{1} & \binom{0}{1}\binom{2}{1} & \binom{2}{1}\binom{1}{1} & \binom{1}{1}\binom{1}{1} & 0 & 0 & 0 & 0 \\ \binom{2}{0}\binom{2}{1} & \binom{1}{0}\binom{2}{1} & \binom{0}{1}\binom{2}{1} & \binom{2}{1}\binom{1}{1} & \binom{1}{0}\binom{1}{1} & \binom{0}{0}\binom{1}{1} & 0 & 0 & 0 \\ \binom{2}{2}\binom{2}{0} & \binom{1}{2}\binom{2}{0} & \binom{0}{2}\binom{2}{0} & \binom{2}{2}\binom{1}{0} & \binom{1}{2}\binom{1}{0} & \binom{0}{2}\binom{1}{0} & \binom{2}{2}\binom{0}{0} & 0 & 0 \\ \binom{2}{1}\binom{2}{0} & \binom{1}{1}\binom{2}{0} & \binom{0}{1}\binom{2}{0} & \binom{2}{1}\binom{1}{0} & \binom{1}{1}\binom{1}{0} & \binom{0}{1}\binom{1}{0} & \binom{2}{1}\binom{0}{0} & \binom{1}{1}\binom{0}{0} & 0 \\ \binom{2}{0}\binom{2}{0} & \binom{1}{0}\binom{2}{0} & \binom{0}{0}\binom{2}{0} & \binom{2}{0}\binom{1}{0} & \binom{1}{0}\binom{1}{0} & \binom{0}{0}\binom{1}{0} & \binom{2}{0}\binom{0}{0} & \binom{1}{0}\binom{0}{0} & \binom{0}{0}\binom{0}{0} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

4.1 ESTRUTURA E CODIFICAÇÃO

A seguir apresentamos outra maneira de obter os elementos de Δ^ℓ que nos oferecerá uma forma de codificação alternativa e permitirá deduzir distribuições de pesos para parte desses códigos.

Proposição 4.3. *Dado ℓ, $0 \leq \ell \leq p^n - 1$, seja r o maior índice tal que $\ell_{[r]} \neq p-1$. Todo elemento $x \in \Delta^\ell$ é da forma*

$$x = \sum_{k=0}^{p^n-1} f(k_{[0]}, k_{[1]}, \ldots, k_{[r]}) a^k,$$

onde $f(x_0, \ldots, x_r)$ é um polinômio em $r+1$ variáveis cujos graus $d_0, \ldots, d_r$ em $x_0, \ldots, x_r$, respectivamente, satisfazem a desigualdade

$$d_0 + d_1 p + \cdots + d_r p^r \leq p^n - 1 - \ell.$$

Demonstração. Temos que

$$x = \lambda_\ell (a-1)^\ell + \lambda_{\ell+1}(a-1)^{\ell+1} + \cdots + \lambda_{p^n-1}(a-1)^{p^n-1},$$

com $\lambda_j \in K$, $\ell \leq j \leq p^n - 1$. Cada potência de $(a-1)$ tem a forma

$$\begin{aligned}(a-1)^j &= \sum_{k=0}^{j} \binom{j}{k} a^k (-1)^{j-k} = \\ &\overset{3.7}{=} \sum_{k=0}^{j} \binom{p^n-1-k}{p^n-1-j} a^k = \\ &\overset{3.6}{=} \sum_{k=0}^{j} \binom{p-1-k_{[0]}}{p-1-j_{[0]}} \binom{p-1-k_{[1]}}{p-1-j_{[1]}} \cdots \binom{p-1-k_{[n-1]}}{p-1-j_{[n-1]}} a^k.\end{aligned}$$

Note-se que o coeficiente de cada a^k na expansão acima se escreve como um produto de fatores da forma

$$\binom{p-1-k_{[i]}}{p-1-j_{[i]}} = \frac{(p-1-k_{[i]})(p-2-k_{[i]})\cdots(j_{[i]}-k_{[i]}+1)}{(p-1-j_{[i]})!} \doteq f_{j,i}(k_{[i]}),$$

onde $f_{j,i}$ e um polinômio de grau $p-1-j_{[i]}$ (o coeficiente de $k^{p-1-j_{[i]}}$ é ± 1). Logo, o coeficiente de a^k em $(a-1)^j$ é um produto

$$f_{j,0}(k_0) f_{j,1}(k_1) \cdots f_{j,n-1}(k_{n-1}).$$

Agora, quando j variar de ℓ a $p^n - 1$, teremos monômios $k_0^{e_0} \cdots k_r^{e_r}$ com expoentes $e_0, \ldots, e_r$ satisfazendo

$$e_0 + e_1 p + \cdots + e_r p^r \leq p^n - 1 - \ell.$$

e o coeficiente de a^k em x será $f(k_0, \ldots, k_r)$, onde f é o polinômio em $r+1$ variáveis, independente de k,

$$f(x_0, \ldots, x_r) \doteq \sum_{j=\ell}^{p^n-1} \lambda_j f_{j,0}(x_0) \cdots f_{j,r}(x_r).$$

□

Corolário 4.4. *Seja ℓ nas condições da proposição 4.3. Consideremos o espaço de polinômios em $r+1$ variáveis*

$$V = \left\{ \sum_{t=0}^{p^n-1-\ell} \alpha_t x_0^{t_{[0]}} \cdots x_r^{t_{[r]}} \;\middle|\; \alpha_t \in K \right\}.$$

A função

$$\begin{aligned} \Gamma : V &\to \Delta^\ell \\ f &\mapsto \sum_{k=0}^{p^n-1} f(k_{[0]}, \ldots, k_{[r]}) a^k \end{aligned} \tag{5}$$

é um isomorfismo de K-espaços vetoriais e, portanto, uma função de codificação para Δ^ℓ.

Demonstração. Basta ver que os monômios $f_{j,0}(x_0) \cdots f_{j,r}(x_r)$ na demonstração da proposição 4.3 geram o espaço V. □

Corolário 4.5. *A matriz $(\gamma_{ij})_{(p^n-\ell)\times p^n}$ cujas entradas são dadas por*

$$\gamma_{ij} = \prod_{k=0}^{r} (j-1)_{[k]}^{(i-1)_{[k]}} \tag{6}$$

é uma matriz geradora para Δ^ℓ.

Demonstração. Seja $\mathcal{B} = \{x_0^{t_{[0]}} \cdots x_r^{t_{[r]}} \mid 0 \leq t \leq p^n - 1 - \ell\}$. Então $\mathcal{B}$ é uma base de V e, considerando a ordem dada por

$$x_0^{t_{[0]}} \cdots x_r^{t_{[r]}} \leq x_0^{s_{[0]}} \cdots x_r^{s_{[r]}} \iff t \leq s, \tag{7}$$

construímos as linhas da matriz (γ_{ij}) a partir das imagens (usando a base canônica de KG) pelo homomorfismo Γ dos elementos de $\mathcal{B}$. Em mais detalhes, o elemento γ_{ij}, será a avaliação do i-ésimo elemento de $\mathcal{B}$, ou seja, $x_0^{(i-1)_{[0]}} \cdots x_r^{(i-1)_{[r]}}$ nos $r+1$ primeiros coeficientes p-ários do expoente do j-ésimo elemento da base canônica de KG, i. e., a^{j-1}. □

Observação 4.6. Para $n = 1$ a matriz (6) se reduz a

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & p-1 \\ 0^2 & 1^2 & 2^2 & \cdots & (p-1)^2 \\ \vdots & \vdots & \vdots & & \vdots \\ 0^{p-1-\ell} & 1^{p-1-\ell} & 2^{p-1-\ell} & \cdots & (p-1)^{p-1-\ell} \end{pmatrix}.$$

Exemplo 4.7. Retomando o exemplo 4.2, para $\Delta^3 \subset \mathbb{F}_7 C_7$ a matriz (6) assume a forma

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0^2 & 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 \\ 0^3 & 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 2 & 2 & 4 & 1 \\ 0 & 1 & 1 & 6 & 1 & 6 & 6 \end{pmatrix},$$

e para $\Delta^4 \subset \mathbb{F}_3 C_9$,

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0^2 & 1^2 & 2^2 & 0^2 & 1^2 & 2^2 & 0^2 & 1^2 & 2^2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0\cdot 0 & 1\cdot 0 & 2\cdot 0 & 0\cdot 1 & 1\cdot 1 & 2\cdot 1 & 0\cdot 2 & 1\cdot 2 & 2\cdot 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \end{pmatrix}.$$

4.2 PESO E CONVENIÊNCIA

O peso dos códigos Δ^ℓ foi determinado por Berman em [Ber67]. Nesta sessão daremos uma nova prova para esse resutado usando os resultados das seções 3.1 e 4.1, relacionaremos o peso desses códigos com os dos geradores canônicos e analisaremos suas conveniências.

Teorema 4.8. *O peso do ideal minimal Δ^{p^n-1} é p^n. Dado ℓ, $0 \leq \ell \leq p^n - 2$, seja r o maior índice tal que $\ell_{[r]} \neq p-1$. Então*

$$\mathrm{w}(\Delta^\ell) = \begin{cases} (\ell_{[r]}+1)p^{n-1-r}, & \text{se } \ell_{[0]} = \cdots = \ell_{[r-1]} = 0; \\ (\ell_{[r]}+2)p^{n-1-r}, & \text{caso contrário.} \end{cases}$$

Demonstração. A primeira parte é imediata, pois Δ^{p^n-1} é o ideal unidimensional gerado por $(a-1)^{p^n-1} = 1 + a + \cdots + a^{p^n-1} = \hat{C}_{p^n}$.

Seja $x \in \Delta^\ell$. Então, pela proposição 4.3, $x = \sum_{k=0}^{p^n-1} f(k_{[0]}, \ldots, k_{[r]})a^k$, onde $f(x_0, \ldots, x_r)$ tem graus $d_0, \ldots, d_r$ em $x_0, \ldots, x_r$, respectivamente, satisfazendo as relações

$$\begin{aligned} 0 \leq d_0, d_1, \ldots, d_r \leq p-1 \\ d_0 + d_1 p + \cdots + d_r p^r \leq p^n - 1 - \ell \end{aligned} \tag{8}$$

É claro que para cada $k = k_{[0]} + k_{[1]}p + \cdots + k_{[r]}p^r + k_{[r+1]}p^{r+1} + \cdots + k_{[n-1]}p^{n-1}$, o coeficiente de a^k em x será nulo se e somente se $(\bar{k}_{[0]}, \ldots, \bar{k}_{[r]}) \in \mathbb{F}_p^{r+1}$ for raiz de f, independentemente dos $n-1-r$ coeficientes restantes $k_{[r+1]}, \ldots, k_{[n-1]}$. Logo, se f tiver exatamente t raízes distintas em $\mathbb{F}_p^{r+1}$, o peso de x será

$$p^n - p^{n-1-r}t. \tag{9}$$

Assim, o peso mínimo que um elemento $x \in \Delta^\ell$ pode assumir está relacionado ao número máximo de raízes distintas que um polinômio $f(x_0, \ldots, x_r)$ nas condições descritas pode ter.

Pela proposição 3.1 (v. também a observação 3.4), esse número é

$$p^{r+1} - \prod_{i=0}^{r}(p - d_i) \tag{10}$$

e só nos resta analisar o máximo valor que essa expressão, condicionada às relações (8), pode assumir. Pelo lema 3.11, sabemos que $p^n - 1 - \ell = (p - 1 - \ell_{[0]}) + \cdots + (p - 1 - \ell_{[r]})p^r$ e devemos considerar dois casos:

(i) Se $\ell_{[0]} = \cdots = \ell_{[r-1]} = 0$, a restrição (8) assume a forma

$$0 \leq d_0, d_1, \ldots, d_{r-1} \leq p - 1$$
$$0 \leq d_r \leq p - 1 - \ell_{[r]}$$

e obtemos imediatamente que o máximo valor que (10) pode assumir é

$$p^{r+1} - (\ell_{[r]} + 1).$$

Agora, substituindo t na equação (9) pela expressão acima, obtemos

$$\mathrm{w}(\Delta^{\ell}) = p^n - p^{n-1-r}(p^{r+1} - (\ell_{[r]} + 1) = p^{n-1-r}(\ell_{[r]} + 1).$$

(ii) Se para algum j, $0 \leq j \leq r - 1$, ocorrer $\ell_{[j]} \neq 0$, então (8) continua impondo $0 \leq d_r \leq p - 1 - \ell_{[r]}$, mas a restrição sobre os outros graus depende do valor que d_r assuma:

$$\begin{cases} 0 \leq d_i \leq p - 1 - \ell_{[i]},\ 0 \leq i \leq r - 1, & \text{se } d_r = p - 1 - \ell_{[r]}; \\ 0 \leq d_0,\ d_1, \ldots, d_{r-1} \leq p - 1, & \text{se } d_r < p - 1 - \ell_{[r]}. \end{cases}$$

É claro que o máximo valor para a expressão (10) ainda virá dos máximos valores que os graus $d_0, \ldots, d_r$ puderem assumir. Resta então apenas comparar as duas situações acima com os máximos valores de $d_0, \ldots, d_r$ em cada. Na primeira situação teremos $d_i = p - 1 - \ell_{[i]}$ para $0 \leq i \leq r$ e

$$\prod_{i=0}^{r}(p - d_i) = \prod_{i=0}^{r}(\ell_{[i]} + 1),$$

enquanto na segunda, $d_0 = d_1 = \cdots = d_{r-1} = p-1$ e $d_r = p-2-\ell_{[r]}$ e

$$\prod_{i=0}^{r}(p-d_i) = \ell_{[r]}+2.$$

Como por hipótese $\ell_{[j]} \neq 0$ para pelo menos um j entre 0 e $r-1$, temos

$$\prod_{i=0}^{r}(\ell_{[i]}+1) \geq (\ell_{[j]}+1)(\ell_{[r]}+1) \geq 2(\ell_{[r]}+1) = 2\ell_{[r]}+2 \geq \ell_{[r]}+2.$$

Note-se que em cada uma das três desigualdades acima pode valer a igualdade se apenas $\ell_{[j]}$ e $\ell_{[r]}$ forem não nulos, se $\ell_{[j]} = 1$ e se $\ell_{[r]} = 0$, respectivamente.

Logo, o máximo valor que (10) pode assumir é

$$p^{r+1} - (\ell_{[r]}+2)$$

e, da mesma forma que no caso (i),

$$\mathrm{w}(\Delta^{\ell}) = p^{n-1-r}(\ell_{[r]}+2).$$

□

A seguir mostramos que o peso desses códigos é determinado por seu gerador (como ideal) e pelos de seus subcódigos.

Proposição 4.9. *O peso de Δ^{ℓ} é o igual ao peso do mais leve entre os geradores $(a-1)^t$, $\ell \leq t \leq p^n-1$.*

Demonstração. Mostramos no corolário a 3.13 que $\mathrm{w}((a-1)^t) = (t_{[0]}+1)\cdots(t_{[n-1]}+1)$. Assim, definindo r como no teorema 4.8 e procedendo da mesma forma que na análise do valor máximo da expressão (10) em sua demonstração, concluímos que

$$\min_{\ell \leq t \leq p^n-1} \mathrm{w}((a-1)^t) = \begin{cases} (\ell_{[r]}+1)p^{n-1-r}, & \text{se } \ell_{[0]} = \cdots = \ell_{[r-1]} = 0; \\ (\ell_{[r]}+2)p^{n-1-r}, & \text{caso contrário.} \end{cases}$$

□

Exemplo 4.10. A tabela a seguir ilustra a proposição 4.9 para os códigos em $\mathbb{F}_5C_{25}$. Na coluna contendo o peso dos geradores, marcamos em vermelho aqueles que determinam os pesos dos códigos que os contém.

Tabela 1. *Relação entre pesos de ideais e de seus geradores.*

ℓ	$w(\Delta^\ell)$	$w((a-1)^\ell)$
1	2	2
2	2	3
3	2	4
4	2	5
5	2	2
6	3	4
7	3	6
8	3	8
9	3	10
10	3	3
11	4	6
12	4	9

ℓ	$w(\Delta^\ell)$	$w((a-1)^\ell)$
13	4	12
14	4	15
15	4	4
16	5	8
17	5	12
18	5	16
19	5	20
20	5	5
21	10	10
22	15	15
23	20	20
24	25	25

A seguir vamos analisar a conveniência dos códigos Δ^ℓ e determinar os códigos de máxima conveniência para dados p e n. O exemplo 4.12 ilustra bem a análise feita na demonstração da proposição a seguir para determinar o código mais conveniente para dados p e n.

Proposição 4.11. *Dado ℓ, $0 \leq \ell \leq p^n - 1$, seja r o maior índice tal que $\ell_{[r]} \neq p-1$. Então*

$$\operatorname{conv}(\Delta^\ell) = \begin{cases} p^{n-1}(\ell_{[r]}+1)(p-\ell_{[r]}), & \text{se } \ell_{[0]} = \cdots = \ell_{[r-1]} = 0; \\ p^{n-1-r}(\ell_{[r]}+2)(p^n-\ell), & \text{caso contrário.} \end{cases}$$

Além disso, se $p \neq 2$, a conveniência é máxima em Δ^{ℓ^*}, onde

$$\ell^* = 1 + \left(\frac{p-3}{2}\right) p^{n-1},$$

e vale

$$\mathrm{conv}_{\max} = \left(\frac{p+1}{2}\right)\left(\left(\frac{p+3}{2}\right) p^{n-1} - 1\right).$$

Para $p = 2$, a conveniência é máxima em Δ e vale

$$\mathrm{conv}_{\max} = 2(2^n - 1).$$

Demonstração. Em primeiro lugar, é fácil ver que

$$\ell = \ell_{[0]} + \ell_{[1]}p + \cdots + \ell_{[r]}p^r + (p^n - p^{r+1})$$

Assim, se $l_{[0]} = \cdots = l_{[r-1]} = 0$, temos $\ell = \ell_{[r]}p^r + (p^n - p^{r+1})$ e então $\dim(\Delta^\ell) = p^n - \ell = p^{r+1} - \ell_{[r]}p^r = p^r(p - \ell_{[r]})$. Logo,

$$\begin{aligned}\mathrm{conv}(\Delta^\ell) &= p^{n-1-r}(\ell_{[r]} + 1) \cdot p^r(p - \ell_{[r]}) = \\ &= p^{n-1}(\ell_{[r]} + 1)(p - \ell_{[r]}).\end{aligned}$$

Note-se que essa expressão é independente de r. Se não ocorre $l_{[0]} = \cdots = l_{[r-1]} = 0$, não desaparece a dependência de r e temos

$$\mathrm{conv}(\Delta^\ell) = p^{n-1-r}(\ell_{[r]} + 2)(p^n - \ell).$$

De modo a determinar a máxima conveniência vamos analisar os dois casos. No primeiro caso, a conveniência é uma expressão quadrática em $\ell_{[r]}$ e para $p \neq 2$ determinamos facilmente que seu máximo ocorre para $\ell_{[r]} = (p-1)/2$ e vale

$$\mathrm{conv}_{\max}(\Delta^\ell) = p^{n-1}\left(\frac{p+1}{2}\right)^2. \tag{11}$$

Para $p = 2$, substituição direta de $\ell_{[r]}$ por 0 e por 1 mostra que em ambos os casos $\mathrm{conv}(\Delta^\ell) = 2^n$.

Considerando agora o segundo caso, o peso continua dependendo apenas de r e $\ell_{[r]}$, enquanto a dimensão será máxima para o mínimo valor de ℓ, ou seja, para $\ell_{[0]} = 1$ e $l_{[1]} = \cdots = l_{[r-1]} = 0$. Assim, teremos $\ell = 1 + \ell_{[r]}p^r + (p^n - p^{r+1})$ e então $\dim(\Delta^\ell) = p^{r+1} - \ell_{[r]}p^r - 1$. Dessa forma,

$$\begin{aligned}\operatorname{conv}(\Delta^\ell) &= p^{n-1-r}(\ell_{[r]} + 2) \cdot (p^{r+1} - \ell_{[r]}p^r - 1) \\ &= (\ell_{[r]} + 2)(p^n - \ell_{[r]}p^{n-1} - p^{n-1-r}). \end{aligned} \tag{12}$$

Vale observar que estamos procurando o valor de ℓ que oferece máxima conveniência e é importante perceber que r e $\ell_{[r]}$ podem ser escolhidos independentemente. Com isso em vista, é claro que a expressão (12) é máxima para $r = n - 1$, o que nos dá $\ell = 1 + \ell_{[n-1]}p^{n-1}$ e $\operatorname{conv}(\Delta^\ell) = (\ell_{[n-1]} + 2)(p^n - \ell_{[n-1]}p^{n-1} - 1)$, que novamente é uma expressão quadrática em $\ell_{[n-1]}$ e terá seu valor máximo no inteiro mais próximo de $(p^n - 2p^{n-1} - 1)/(2p^{n-1})$. Mas

$$\frac{p^n - 2p^{n-1} - 1}{2p^{n-1}} - \frac{p^{n-1} - 1}{2p^{n-1}} = \frac{p-3}{2}$$

e

$$\frac{p^n - 2p^{n-1} - 1}{2p^{n-1}} + \frac{p^{n-1} + 1}{2p^{n-1}} = \frac{p-1}{2},$$

logo

$$\frac{p-3}{2} < \frac{p^n - 2p^{n-1} - 1}{2p^{n-1}} < \frac{p-1}{2}$$

e a cota inferior é a mais próxima. Assim, para $p \neq 2$, devemos tomar $\ell_{[n-1]} = (p-3)/2$, o que conduz a $\ell = 1 + (\frac{p-3}{2})p^{n-1}$ e

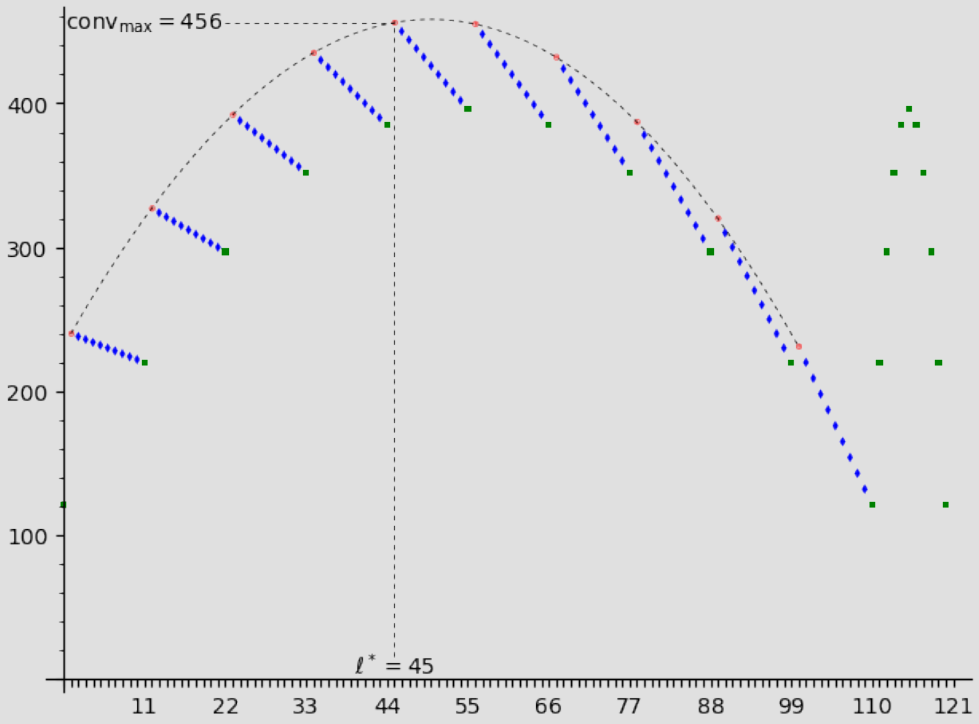
$$\operatorname{conv}_{\max} = \left(\frac{p+1}{2}\right)\left(\left(\frac{p+3}{2}\right)p^{n-1} - 1\right). \tag{13}$$

Para $p = 2$ novamente é mais simples substituir os dois valores possíveis para $\ell_{[n-1]}$, o que nos mostra que a máxima conveniência é $2(2^n - 1)$ e ocorre em $\ell = 1$.

Comparando as expressões (11) e (13), vemos que para $p \neq 2$ a conveniência máxima ocorre para $\ell = 1 + (\frac{p-3}{2})p^{n-1}$ e é dada pela expressão (13). Comparando também os dois casos para $p = 2$, temos que a máxima conveniência é $2(2^n - 1)$ e ocorre para $\ell = 1$. □

Exemplo 4.12. Aplicando as fórmulas demonstradas na proposição 4.11 para $p = 11$ e $n = 2$ obtemos $\ell^* = 45$ e $\text{conv}_{\max} = 456$. A dimensão e o peso do ideal de máxima conveniência são $\dim(\Delta^{45}) = 76$ e $\text{w}(\Delta^{45}) = 6$.

A seguir apresentamos um gráfico da conveniência de Δ^ℓ em função de ℓ para esses valores de p e n.



Os quadrados verdes correspondem ao caso $\ell_{[0]} = \cdots = \ell_{[r-1]} = 0$ enquanto os círculos vermelhos marcam os pontos para os quais $\ell = 1 + \ell_{[n-1]}p^{n-1}$. Os losangos azuis contêm todos os outros casos. A parábola tracejada passando pelos círculos vermelhos corresponde à expressão quadrática $(\ell_{[n-1]} + 2)(p^n - \ell_{[n-1]}p^{n-1} - 1) = (\frac{\ell-1}{p^{n-1}} + 2)(p^n - \ell)$.

4.3 DISTRIBUIÇÃO DE PESOS

A distribuição de pesos dos códigos de comprimento p e de parte dos códigos de comprimento p^n é dada nesta seção. Os pesos presentes em cada código serão de

terminados e o número de palavras de cada peso será calculado utilizando os resultados da seção 3.1.

Teorema 4.13. *Seja ℓ, $p^n - p \leq \ell \leq p^n - 1$. Então Δ^ℓ tem somente palavras de pesos 0 e up^{n-1}, com $\ell_{[0]} + 1 \leq u \leq p$, e o número de palavras de cada peso não nulo é dado recursivamente por*

$$N((\ell_{[0]}+1)p^{n-1}) = \binom{p}{\ell_{[0]}+1}(q-1)$$

$$N(up^{n-1}) = \binom{p}{u}(q^{u-\ell_{[0]}}-1) - \sum_{i=\ell_{[0]}+1}^{u-1}\binom{p-i}{u-i}N(ip^{n-1}), \text{ para } u > \ell_{[0]}+1.$$

Demonstração. Em primeiro lugar, para ℓ na faixa considerada, $\ell = \ell_{[0]} + p^n - p$ e temos $r = 0$ e $\mathrm{w}(\Delta^\ell) = (\ell_{[0]}+1)p^{n-1}$. Como $r = 0$, os coeficientes das palavras desse código vêm de polinômios em apenas uma variável com grau menor ou igual a $p - 1 - \ell_{[0]}$. Mais especificamente, o coeficiente de a^k em uma dada palavra x é da forma $f(k_{[0]})$ e independe de $k_{[1]}, \ldots, k_{[n-1]}$, logo, se f tiver t raízes distintas em $\mathbb{F}_p$, x terá tp^{n-1} coeficientes nulos, ou seja, terá peso $p^n - tp^{n-1} = (p-t)p^{n-1}$ e como $0 \leq \deg(f) \leq p - 1 - \ell_{[0]}$, temos $\ell_{[0]} + 1 \leq p - t \leq p$ e os pesos possíveis são da forma enunciada.

Para ver quantas palavras de peso up^{n-1} existem, basta ver quantos polinômios em K de grau menor ou igual a $p - 1 - \ell_{[0]}$ têm exatamente $p - u$ raízes distintas em $\mathbb{F}_p$. Usando o corolário 3.3 e a observação 3.4, temos então que o número de palavras de peso up^{n-1} é dado por

$$\begin{aligned}
N(up^{n-1}) &= N^{p-1-\ell_{[0]}}(p-u) = \\
&= \binom{p}{p-u}(q^{u-\ell_{[0]}}-1) - \sum_{i=p-u+1}^{p-1-\ell_{[0]}}\binom{i}{p-u}N^{p-1-\ell_{[0]}}(i) = \\
&= \binom{p}{u}(q^{u-\ell_{[0]}}-1) - \sum_{i=\ell_{[0]}+1}^{u-1}\binom{p-i}{p-u}N^{p-1-\ell_{[0]}}(p-i) = \\
&= \binom{p}{u}(q^{u-\ell_{[0]}}-1) - \sum_{i=\ell_{[0]}+1}^{u-1}\binom{p-i}{u-i}N(ip^{n-1}).
\end{aligned}$$

□

A seguir aplicamos as fórmulas dadas no teorema 4.13 para dois códigos, um de comprimento 7 e um de comprimento 5^2.

Exemplo 4.14. Novamente tomando $\Delta^3 \subset \mathbb{F}_7 C_7$, temos $w(\Delta^3) = 4$ e há palavras de pesos 4, 5, 6 e 7 que ocorrem nas seguintes quantidades:

$$N(4) = \binom{7}{4}(7-1) = 210;$$

$$N(5) = \binom{7}{5}(7^2-1) - \binom{7-4}{5-4}N(4) = 378;$$

$$N(6) = \binom{7}{6}(7^3-1) - \binom{7-4}{6-4}N(4) - \binom{7-5}{6-5}N(5) = 1008;$$

$$N(7) = \binom{7}{7}(7^4-1) - \binom{7-4}{7-4}N(4) - \binom{7-5}{7-5}N(5) - \binom{7-6}{7-6}N(6) = 804.$$

Tomando agora $\Delta^{21} \subset \mathbb{F}_5 C_{25}$, temos $w(\Delta^{21}) = 10$ e há palavras de pesos 10, 15, 20 e 25 ocorrendo nas seguintes quantidades:

$$N(10) = \binom{5}{2}(5-1) = 40;$$

$$N(15) = \binom{5}{3}(5^2-1) - \binom{5-2}{3-2}N(10) = 120;$$

$$N(20) = \binom{5}{4}(5^3-1) - \binom{5-2}{4-2}N(10) - \binom{5-3}{4-3}N(15) = 260;$$

$$N(25) = \binom{5}{5}(5^4-1) - \binom{5-2}{5-2}N(10) - \binom{5-3}{5-3}N(15) - \binom{5-4}{5-4}N(20) = 204.$$

5 DECOMPOSIÇÃO DE CÓDIGOS MODULARES

Trataremos neste capítulo de códigos de comprimento $p^n m$ sobre corpos de característica p. Como antes, K será sempre um corpo finito de característica p. Sejam $C_{p^n} = \langle a \mid a^{p^n} = 1 \rangle$ o grupo cíclico de ordem p^n e $C_m = \langle g \mid g^m = 1 \rangle$ o grupo cíclico de ordem m, onde $p \nmid m$.

Vamos considerar a álgebra de grupo $K(C_{p^n} \times C_m) \cong (KC_{p^n})C_m$ (lema 2.13). O anel de coeficientes dessa álgebra, KC_{p^n}, foi o objeto de estudo do capítulo 4 e sabemos tratar-se de um anel de cadeia com ideal máximal Δ gerado por $(a-1)$. De modo a simplificar a notação vamos denotar $R \doteq KC_{p^n}$.

Observe-se que um código $\mathcal{C} \subset RC_m$ é um R-módulo, mas também um K-espaço vetorial e é nesse ponto de vista que estamos interessados, pois desejamos ver $\mathcal{C}$ como um código de comprimento $p^n m$ sobre K, não como um de comprimento m sobre R. Começaremos, entretanto, considerando nossos códigos vistos sobre R e depois mostraremos como o que se sabe sobre R nos oferece muitas informações para o código visto sobre K. Onde uma distinção for necessária, indicaremos explicitamente sobre que estrutura estamos trabalhando, e. g., w_K indicará o peso visto sobre K enquanto w_R, sobre R.

5.1 CÓDIGOS SOBRE ANÉIS DE CADEIA

Nesta seção aplicaremos uma série de resultados mostrados por Silva em [Sil12] considerando a álgebra de grupo $RC_m = (KC_{p^n})C_m$ descrita acima.

Em primeiro lugar, sabemos pelo teorema 2.21 que $RC_m/\Delta C_m \cong \bar{R}C_m$, onde $\bar{R} \doteq R/M$. Note-se que em nosso caso $\bar{R} \cong K$, mas como $KC_m \subset RC_m$, fato que exploraremos na seção 5.2, utilizaremos a notação $\bar{R}$ de modo a claramente diferenciar o que ocorre em RC_m do que ocorre no quociente.

Pelo Teorema de Maschke (teorema 2.16 e corolário 2.17), sabemos que $\bar{R}C_m$ é semissimples, então existem idempotentes primitivos ortogonais $\bar{e}_1, \ldots, \bar{e}_s$ tais que

$$\bar{R}C_m = \bar{R}C_m\bar{e}_1 \oplus \cdots \oplus \bar{R}C_m\bar{e}_s.$$

Sejam $e_1, \ldots, e_s$ os idempotentes de RC_m correspondentes a $\bar{e}_1, \ldots, \bar{e}_s$, respectivamente (v. prop 2.19). Silva mostrou que estes são os idempotentes primitivos ortogonais de RC_m e então

$$RC_m = RC_me_1 \oplus \cdots \oplus RC_me_s.$$

Além disso, cada componente RC_me_i, $1 \leq i \leq m$, é um anel de cadeia com ideais $RC_me_i \supset \Delta C_me_i \supset \Delta^2 C_me_i \supset \cdots \supset \Delta^{p^n-1}C_me_i \supset (0)$ e todo ideal I de RC_m é da forma

$$\begin{aligned} &I = I_0 \oplus \cdots \oplus I_s, \text{ onde} \\ &I_i = \langle (a-1)^{\ell_i}e_i \rangle = \Delta^{\ell_i}C_me_i, \text{ com } 0 \leq \ell_i \leq p^n,\ 1 \leq i \leq s. \end{aligned}$$

Com isso, uma vez conhecida a decomposição de $\bar{R}C_m$, conhecemos a estrutura dos códigos em RC_m. Considerando o tamanho desses códigos, dado $\mathcal{C} = \langle (a-1)^{\ell_1}e_1 \rangle \oplus \cdots \oplus \langle (a-1)^{\ell_s}e_s \rangle$, o número de palavras de $\mathcal{C}$ é

$$|\mathcal{C}| = |\bar{R}|^{\sum_{i=1}^{s}(p^n-\ell_i)r_i},$$

onde $r_i = \dim_{\bar{R}}(\bar{R}C_m\bar{e}_i)$.

Notação. Usaremos a notação $\langle\ \rangle$ apenas para ideais de RC_m, i. .e, $\langle\alpha\rangle$ indica sempre $RC_m\alpha$.

Os idempotentes primitivos de RC_m podem ser obtidos a partir de fórmulas para os idempotentes de $\bar{R}C_m$ dadas por Ferraz e Polcino Milies em [FP07]. Essas fórmulas utilizam apenas a estrutura de subgrupos de C_m e contemplam dois casos:

(i) Para $m = q^s$, onde q é um primo distinto de p e $o(p) = \phi(q^s)$ em $U(\mathbb{Z}_{q^s})$, onde ϕ é a função de Euler;

(ii) Para p ímpar e $m = 2q^s$, onde q é um primo ímpar distinto de p e $o(p) = \phi(q^s)$ em $U(\mathbb{Z}_{2q^s})$.

Além disso, o peso dos códigos nesses casos podem ser determinados a partir das ordens dos subgrupos de C_m. A seguir apresentamos alguns desses resultados, particularizados a nossos códigos.

Notação. Dado um grupo G, denotamos $\hat{G} = \frac{1}{|G|}\sum_{g\in G} g$.

5.1.1 Comprimento q^s

Consideremos primeiro o caso $m = q^s$, onde q é um primo distinto de p e $o(p) = \phi(q^s)$ em $U(\mathbb{Z}_{q^s})$.

Teorema 5.1. *Seja $C_m = G_0 \supset G_1 \supset \cdots \supset G_s = 1$ a cadeia de subgrupos de C_m. Então o conjunto dos idempotentes primitivos de RC_m é dado por*

$$e_0 = \hat{G}_0 \quad e \quad e_i = \hat{G}_i - \hat{G}_{i-1},\ 1 \leq i \leq s.$$

Teorema 5.2. *Seja $I = I_0 \oplus I_1 \oplus \cdots \oplus I_j$, com $0 \leq j \leq s-1$, onde $I_j = \langle (a-1)^{\ell_j} e_j \rangle$, com $0 \leq \ell_j \leq p^n - 1$. Então $\mathrm{w}_R(I) = |G_j|$.*

Teorema 5.3. *Sejam $I_j = \langle (a-1)^{\ell_j} e_j \rangle$, com $0 \leq \ell_j \leq p^n - 1$. Se $I = I_{j_1} \oplus \cdots \oplus I_{j_r}$, $j_k < j_{k+1}$, para $1 \leq k \leq r$ com $\{j_1, \ldots, j_r\} \subsetneq \{0, 1, \ldots, j_r\}$, então $\mathrm{w}(I) = 2|G_{j_r}|$.*

5.1.2 Comprimento $2q^s$

Agora o caso p ímpar e $m = 2q^s$, com q um primo ímpar distinto de p e $o(p) = \phi(q^s)$ em $U(\mathbb{Z}_{2q^s})$.

Teorema 5.4. *Escrevamos $C_m = B \times G$, onde G é um p-subgrupo de Sylow e $B = \{1, t\}$ é um 2-subgrupo de Sylow. Sejam e_i, $0 \leq i \leq s$, os idempotentes primitivos de RG. Então os idempotentes primitivos de RC_m são dados por*

$$\frac{1+t}{2}e_i \quad e \quad \frac{1-t}{2}e_i, \quad 0 \leq i \leq s.$$

Teorema 5.5. *Seja $\mathcal{C} = \langle (a-1)^{\ell_0}(\frac{1+t}{2})e_0\rangle \oplus \langle (a-1)^{\ell_1}(\frac{1+t}{2})e_1\rangle \oplus \cdots \oplus \langle (a-1)^{\ell_r}(\frac{1+d}{2})e_s\rangle$, onde $0 \leq \ell_j \leq p^n - 1$, $0 \leq j \leq r$, então $\mathrm{w}(\mathcal{C}) = 2|G_r|$.*

Teorema 5.6. *Seja $\mathcal{C} = \langle (a-1)^{\ell_{i_1}}(\frac{1+t}{2})e_{i_1}\rangle \oplus \cdots \oplus \langle (a-1)^{\ell_{i_r}}(\frac{1+t}{2})e_{i_r}\rangle$, onde $0 \leq \ell_{i_j} \leq p^n - 1$, $1 \leq j \leq r$ e $\{i_1, \ldots, i_r\} \subsetneq \{0, 1, \ldots, i_r\}$, então $\mathrm{w}(\mathcal{C}) = 4|G_{i_r}|$.*

Observação 5.7. Nos dois últimos resultados também se pode substituir todos os $\frac{1+t}{2}e_i$ por $\frac{1-t}{2}e_i$. Resultados para códigos nos quais comparecem idempotentes de ambas as formas também são tratados por Silva, para mais detalhes v. [Sil12].

Os resultados apresentados nesta seção nos dão informações sobre códigos cíclicos vistos sobre R. A seção seguinte é dedicada a analisar esses códigos como códigos modulares sobre K.

5.2 QUOCIENTE COMO SUBANEL E PESOS SOBRE K

Vamos explorar nesta seção o fato de o quociente $\bar{R}C_m$ ser isomorfo a KC_m, um subanel de RC_m.

Antes de mais nada, $K \subset R$ é uma transversal natural para $\bar{R}$, o que tem algumas consequências imediatas.

Lema 5.8. *Seja $\bar{u} = \bar{\alpha}_0 + \bar{\alpha}_1 g + \cdots + \bar{\alpha}_{m-1}g^{m-1}$ um idempotente de $\bar{R}C_m$. Então, tomando representantes $\alpha_0, \ldots, \alpha_{m-1} \in K$, temos que $e = \alpha_0 + \alpha_1 g + \cdots + \alpha_{m-1}g^{m-1}$ é o idempotente de RC_m tal que $\bar{e} = \bar{u}$. Ademais, se $\bar{u}$ é primitivo, então e também o é.*

Demonstração. A primeira parte é trivial, pois e é idempotente em $KC_m \subset RC_m$. Para a segunda parte, basta ver que se $\bar{u}$ é primitivo, mas $e = e_1 + e_2$ em RC_m, então $\bar{e}_1 = \bar{u}$ ou $\bar{e}_2 = \bar{u}$. Suponhamos que $\bar{e}_1 = \bar{u}$, então $e_2 \in \Delta$ sendo, portanto, nilpotente, logo $e_2 = 0$. □

Observação 5.9. Em geral não existe uma transversal que permita levantar a expressão de um idempotente, ou seja, levantar os coeficientes $\bar{\alpha}_i$, como mostra o exemplo 5.10 a seguir.

Exemplo 5.10. Consideremos o grupo $C_2 = \langle a \rangle$ e os anéis de cadeia $\mathbb{F}_2C_2$, cujo ideal máximal é $\Delta = \langle a - 1 \rangle$ e $\mathbb{Z}_4$, cujo ideal máximal é $M = \bar{2}\mathbb{Z}_4$. Em ambos os casos o corpo de resíduos tem dois elementos, i. e., $(\mathbb{F}_2C_2)/\Delta \cong \mathbb{Z}_4/M \cong \mathbb{F}_2$.

Tomando agora o grupo $C_9 = \langle g \rangle$, temos que os idempotentes primitivos de $\mathbb{F}_2C_9$ são dados por (v. teorema 5.1)

$$\begin{aligned} e_0 &= 1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8; \\ e_1 &= g + g^2 + g^4 + g^5 + g^7 + g^8; \\ e_2 &= g^3 + g^6. \end{aligned}$$

Então, de forma natural, as mesmas expressões nos dão os idempotentes primitivos de $(\mathbb{F}_2C_2)C_9$. Em $\mathbb{Z}_4C_9$, entretanto, os idempotentes primitivos são dados por

$$\begin{aligned} u_0 &= \bar{1} + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8; \\ u_1 &= \bar{2} + \bar{3}g + \bar{3}g^2 + \bar{2}g^3 + \bar{3}g^4 + \bar{3}g^5 + \bar{2}g^6 + \bar{3}g^7 + \bar{3}g^8; \\ u_2 &= \bar{2} + g^3 + g^6. \end{aligned}$$

O resultado a seguir nos permite obter K-bases para os códigos em RC_m a partir de bases das componentes simples de KC_m.

Proposição 5.11. *Sejam $e_1, \ldots, e_s$ os idempotentes primitivos de RC_m e sejam $\mathcal{B}_1, \ldots, \mathcal{B}_s$ bases para $KC_me_1, \ldots, KC_me_s$, respectivamente. Denotemos $\mathcal{B}_i = \{b_{i,1}, b_{i,2}, \ldots, b_{i,r_i}\}$, $1 \leq i \leq s$. Então, para $1 \leq i \leq s$,*

(i) $\mathcal{B}_i$ *é um conjunto de geradores minimal para o* R*-módulo* $\langle e_i \rangle$*;*

(ii) $\text{posto}_R(\langle e_i \rangle) = \dim_K(KC_m e_i) = r_i$.

Além disso, dado $\mathcal{C} = \bigoplus_{i=1}^{s} \langle (a-1)^{\ell_i} e_i \rangle$*, temos*

(iii) O conjunto

$$\mathcal{B}_{\mathcal{C}} = \{(a-1)^{t_i} b_{i,j_i} \mid \ell_i \leq t_i \leq p^n - 1,\ 1 \leq i \leq s,\ 1 \leq j_i \leq r_i\}$$

é uma base para $\mathcal{C}$ *como espaço vetorial sobre* K*;*

(iv) $\dim_K(\mathcal{C}) = \sum_{i=1}^{s} (p^n - \ell_i) r_i$.

Demonstração.

(i) Seja $x \in \langle e_i \rangle$. Então $x = (\sum_{j=0}^{m-1} \alpha_j g^j) e_i$, com $\alpha_j \in R$, ou seja, $\alpha_j = \sum_{k=0}^{p^n-1} \alpha_{j,k} a^k$, com $\alpha_{j,k} \in K$. Logo, $x = \sum_j (\sum_k \alpha_{j,k} a^k g^j) e_i = \sum_k (\sum_j \alpha_{j,k} g^j) e_i a^k$ e, denotando $\beta_k = \sum_j \alpha_{j,k} g^j$, temos que $\beta_k \in KC_m$, portanto, $\beta_k e_i = \sum_{t=1}^{r_i} \beta_{k,t} b_{i,t}$, com $\beta_{k,t} \in K$. Assim, $x = \sum_k (\sum_t \beta_{k,t} b_{i,t}) a^k = \sum_t (\sum_k \beta_{k,t} a^k) b_{i,t}$ e como $\sum_k \beta_{k,t} a^k) \in R$, $\mathcal{B}_i$ gera $\langle e_i \rangle$ como R-módulo. Para ver que esse conjunto de geradores é minimal, basta ver que se se omite algum elemento, o módulo gerado, quando projetado em $\bar{R}C_m$ não pode produzir todo o espaço vetorial $\bar{R}C_m e_i \cong KC_m e_i$.

(ii) Segue imediatamente de (i);

(iii) Temos que $\mathcal{B}_{\mathcal{C}} = \bigcup_{i=1}^{s} \mathcal{B}_{\mathcal{C}_i}$, onde $\mathcal{B}_{\mathcal{C}_i} = \{(a-1)^t b_{i,j} \mid \ell_i \leq t \leq p^n - 1,\ 1 \leq j \leq r_i\}$ e a união é disjunta. Basta então mostrar que $\mathcal{B}_{\mathcal{C}_i}$ é uma K-base de $\mathcal{C}_i = \langle (a-1)^{\ell_i} e_i \rangle$. De fato, dado $x \in \mathcal{C}_i$, temos que $x = \beta e_i = \sum_{j=1}^{r_i} \beta_j b_{i,j}$, onde $\beta_1, \ldots, \beta_{r_i} \in \Delta^{\ell_i}$, ou seja, cada $\beta_j = \sum_{t=\ell_i}^{p^n-1} \gamma_{j,t} (a-1)^t$, com $\gamma_{j,t} \in K$. Dessa forma, $x = \sum_{j=1}^{r_i} \sum_{t=\ell_i}^{p^n 1} \gamma_{j,t} (a-1)^t b_{i,j}$ e mostramos que $\mathcal{B}_{\mathcal{C}_i}$ gera $\mathcal{C}_i$. Da K-independência linear entre os elementos $b_{i,j} \in \mathcal{B}_i$ e entre as distintas potências de $(a-1)$, segue facilmente que $\mathcal{B}_{\mathcal{C}_i}$ é linearmente independente sobre K.

(iv) Segue imediatamente de (iii). □

Exemplo 5.12. Usando a álgebra de grupo $\mathbb{F}_2C_{18} \cong (\mathbb{F}_2C_2)C_9$ do exemplo 5.10, temos que

$$\begin{aligned}
\mathcal{B}_0 &= \{1+g+g^2+g^3+g^4+g^5+g^6+g^7+g^8\},\\
\mathcal{B}_1 &= \{g+g^2+g^4+g^5+g^7+g^8, 1+g^2+g^3+g^5+g^6+g^8\},\\
\mathcal{B}_2 &= \{g^3+g^6, g^4+g^7, g^5+g^8, 1+g^6, g+g^7, g^2+g^8\}
\end{aligned}$$

são bases de $\mathbb{F}_2C_9e_0$, $\mathbb{F}_2C_9e_1$ e $\mathbb{F}_2C_9e_2$ sobre K, e $\langle e_0\rangle$, $\langle e_1\rangle$ e $\langle e_2\rangle$ tem postos 1, 2 e 6, respectivamente.

Então o código $\mathcal{C} = \langle e_1\rangle \oplus \langle (a-1)e_2\rangle$ tem K-base

$$\begin{aligned}
\mathcal{B}_{\mathcal{C}} = \{&g+g^2+g^4+g^5+g^7+g^8,\\
&1+g^2+g^3+g^5+g^6+g^8,\\
&(a-1)(g+g^2+g^4+g^5+g^7+g^8),\\
&(a-1)(1+g^2+g^3+g^5+g^6+g^8),\\
&(a-1)(g^3+g^6), (a-1)(g^4+g^7), (a-1)(g^5+g^8),\\
&(a-1)(1+g^6), (a-1)(g+g^7), (a-1)(g^2+g^8)\}
\end{aligned}$$

e dimensão $(2-0)\cdot 2 + (2-1)\cdot 6 = 10$.

A partir de agora, vamos analisar as relações entre pesos sobre R e sobre K.

Lema 5.13. *Seja $x = \lambda_0 + \lambda_1 g + \cdots + \lambda_{m-1}g^{m-1} \in RC_m$. Então $\mathrm{w}_K(x) = \sum_{j=0}^{m-1} \mathrm{w}_K(\lambda_j)$. Em particular, dados $\lambda \in R$ e $x \in KC_m$, temos que $\mathrm{w}_K(\lambda x) = \mathrm{w}_K(\lambda)\cdot \mathrm{w}_K(x)$.*

Demonstração. Basta ver que cada λ_j é da forma $\lambda_{j,0} + \cdots + \lambda_{j,p^n-1}a^{p-1}$, então o coeficiente de a^ig^j em x é dado por $\lambda_{j,i}$, ou seja, $\mathrm{w}_K(x) = |\{(i,j) \mid \lambda_{j,i} \neq 0\}| = \sum_{j=0}^{m-1} |\{j \mid \lambda_{j,i} \neq 0\}| = \sum_{j=0}^{m-1} \mathrm{w}_K(\lambda_j)$. □

Lema 5.14. *Seja $\mathcal{C} = \langle e\rangle$ um código em RC_m, onde e é um idempotente não necessariamente primitivo e seja $\bar{\mathcal{C}}$ a projeção de $\mathcal{C}$ em $\bar{R}C_m$. Então $\mathrm{w}_K(\mathcal{C}) = \mathrm{w}_R(\mathcal{C}) = \mathrm{w}(\bar{\mathcal{C}})$.*

Demonstração. É claro que $\mathrm{w}(\bar{\mathcal{C}}) \leq \mathrm{w}_R(\mathcal{C}) \leq \mathrm{w}_K(\mathcal{C})$. Seja então $\bar{x} = \sum_{i=0}^{m-1} \bar{\alpha}_i g^i$ uma palavra de peso mínimo em $\bar{R}$. Então tomando representantes $\alpha_0, \ldots, \alpha_{m-1} \in K$ e definindo $x = \sum_{i=0}^{m-1} \alpha_i g^i \in \mathcal{C}$, temos $\mathrm{w}_R(\mathcal{C}) \leq \mathrm{w}_K(\mathcal{C}) \leq \mathrm{w}_K(x) = \mathrm{w}(\bar{x}) = \mathrm{w}(\bar{\mathcal{C}})$ e o resultado segue. □

A seguir mostramos que todos os coeficientes não nulos de uma palavra que tenha peso sobre R mínimo vem da mesma camada $\Delta^\ell \setminus \Delta^{\ell+1}$ de R, o que nos permitirá obter fortes conclusões sobre os pesos de nossos códigos.

Lema 5.15. *Seja $\mathcal{C}$ um código em RC_m. Se $x \in \mathcal{C}$ é uma palavra de peso sobre R mínimo, ou seja, se $\mathrm{w}_R(x) = \mathrm{w}_R(\mathcal{C})$, então existe um único ℓ entre 0 e $p^n - 1$ tal que $x = (a-1)^\ell \sum_{i=0}^{m-1} \alpha_i g^i$, onde cada um dos coeficientes $\alpha_0, \ldots, \alpha_{m-1} \in R$ deve ser inversível ou nulo.*

Demonstração. Seja $x = \beta_0 + \beta_1 g + \cdots + \beta_{m-1} g^{m-1}$, com $\beta_0, \ldots, \beta_{m-1} \in R$. É claro que se pode escrever cada coeficiente não nulo em x na forma $\beta_i = (a-1)^{\ell_i}\alpha_i$, com $\alpha_i \in U(R)$ e $0 \leq \ell_i \leq p^n - 1$. Devemos então provar que os expoentes ℓ_i são todos iguais. Suponhamos que existam índices i e j tais que β_i, $\beta_j \neq 0$ e $\ell_i < \ell_j$. Tomando $y = (a-1)^{p^n - \ell_j} x$, temos que o coeficiente de g^i em y é $\alpha_i (a-1)^{p^n - (\ell_j - \ell_i)} \neq 0$ e que o coeficiente de g^j é $\alpha_j (a-1)^{p^n} = 0$, logo y é uma palavra não nula de $\mathcal{C}$ tal que $\mathrm{w}_R(y) \leq \mathrm{w}_R(x)$, o que contraria a hipótese de minimalidade do peso de x. □

Lema 5.16. *Seja x uma palavra de peso mínimo (sobre R) de um código $\mathcal{C} \subset \langle e \rangle$, onde e é um idempotente em RC_m, não necessariamente minimal. Então existe $y \in KC_m e$ tal que $\mathrm{w}_R(x) = \mathrm{w}_R(y) = \mathrm{w}_K(y)$.*

Demonstração. Seja $I = \{i \mid 0 \leq i \leq m-1,\ g^i \in \mathrm{supp}(x)\}$. Já vimos que podemos escrever $x = (a-1)^\ell \sum_{i \in I} \alpha_i g^i$, com $\alpha_i \in U(R)$ e $0 \leq \ell \leq m-1$. Note-se que como $\alpha_i \in U(R)$, então $\alpha_i = \gamma_i + \delta_i$, com $0 \neq \gamma_i \in K$ e $\delta_i \in \Delta$. Seja então $\check{x} = (a-1)^{p^n - 1 - \ell}$. Temos que $\check{x} = (a-1)^{p^n-1} \sum_{i \in I} \alpha_i g^i = (a-1)^{p^n-1} \sum_{i \in I} \gamma_i g^i$ e que $\check{x} \in \langle e \rangle$ e definimos $y = \sum_{i \in I} \gamma_i g^i \in KC_m$. É claro que $\mathrm{w}_K(y) = \mathrm{w}_R(y) = |I| = \mathrm{w}_R(x)$ e resta apenas ver que $y \in KGe$. Suponha que $y \neq \langle e \rangle$, então podemos escrever $y = y_1 e + y_2(1-e)$, com $y_1, y_2 \in KC_m$, já que tanto y quanto e e $(1-e)$ têm todos os seus coeficientes em K (v. lema 5.8). Mas $\check{x} = (a-1)^{p^n-1} y = (a-1)^{p^n-1} y_1 e + (a-1)^{p^n-1} y_2 (1-e)$ e como $\check{x} \in \langle e \rangle$, deve ocorrer $y_2 = 0$, logo $y \in KC_m e$. □

Teorema 5.17. *Seja I um subconjunto não vazio de $\{0, 1, \ldots, s\}$. Dado $\mathcal{C} = \bigoplus_{i\in I}\langle(a-1)^{\ell_i}e_i\rangle$, com $0 \leq \ell_i \leq p^n - 1$ para todo $i \in I$, sejam $\ell_{\min}$ e $\ell_{\max}$ os valores mínimo e máximo de $\{\ell_i \mid i \in I\}$ e definamos os códigos*

$$\hat{\mathcal{C}} = \bigoplus_{i\in I}\langle(a-1)^{\ell_{\min}}e_i\rangle = \langle(a-1)^{\ell_{\min}}e\rangle;$$
$$\check{\mathcal{C}} = \bigoplus_{i\in I}\langle(a-1)^{\ell_{\max}}e_i\rangle = \langle(a-1)^{\ell_{\max}}e\rangle.$$

onde $e = \sum_{i\in I} e_i$. Então

(i) $\mathrm{w}_R(\hat{\mathcal{C}}) = \mathrm{w}_R(\mathcal{C}) = \mathrm{w}_R(\check{\mathcal{C}}) = \mathrm{w}_R(\langle e\rangle)$;

(ii) $\mathrm{w}_K(\Delta^{\ell_{\min}}) \cdot \mathrm{w}_R(\mathcal{C}) \leq \mathrm{w}_K(\mathcal{C}) \leq \mathrm{w}_K(\Delta^{\ell_{\max}}) \cdot \mathrm{w}_R(\mathcal{C})$,

Demonstração. Em primeiro lugar, é claro que $\langle e\rangle \supset \hat{\mathcal{C}} \supset \mathcal{C} \supset \check{\mathcal{C}}$ e então $\mathrm{w}(\langle e\rangle) \leq \mathrm{w}(\hat{\mathcal{C}}) \leq \mathrm{w}(\mathcal{C}) \leq \mathrm{w}(\check{\mathcal{C}})$, tanto sobre R como sobre K.

O lema 5.16 mostra que existe $y \in KC_m e$ tal que $w_R(y) = \mathrm{w}_R(\langle e\rangle)$, então $\check{y} = (a-1)^{\ell_{\max}}y \in \check{\mathcal{C}}$ e $\mathrm{w}_R(\check{y}) = \mathrm{w}_R(y)$, logo $\mathrm{w}_R(\check{\mathcal{C}}) \leq \mathrm{w}_R(\check{y}) = \mathrm{w}_R(\langle e\rangle)$ e isso prova (i).

Conforme a proposição 4.9, sejam t_1 e t_2 tais que $\ell_{\min} \leq t_1 \leq p^n - 1$ e $\ell_{\max} \leq t_2 \leq p^n - 1$ satisfazendo $\mathrm{w}_K((a-1)^{t_1}) = \mathrm{w}_K(\Delta^{\ell_{\min}})$ e $\mathrm{w}_K((a-1)^{t_2}) = \mathrm{w}_K(\Delta^{\ell_{\max}})$. Consideremos o mesmo elemento $y \in KC_m e$ para demonstrar (ii). Primeiro, $(a-1)^{t_1}y$ é uma palavra de peso sobre R mínimo em $\hat{\mathcal{C}}$ e todos os seus coeficientes não nulos têm peso mínimo sobre K, logo $w_K(\Delta^{\ell_{\min}})\mathrm{w}_R(\mathcal{C}) = \mathrm{w}_K(\hat{\mathcal{C}}) \leq \mathrm{w}_K(\mathcal{C})$ e isso prova a primeira desigualdade. Para a segunda desigualdade basta ver que $(a-1)^{t_2}y \in \check{\mathcal{C}}$, logo $\mathrm{w}_K(\mathcal{C}) \leq \mathrm{w}_K(\check{\mathcal{C}}) \leq w_K((a-1)^{t_2}y) = w_K(\Delta^{\ell_{\max}})w_R(y) = w_K(\Delta^{\ell_{\max}})w_R(\mathcal{C})$. □

O colorário a seguir é imediato.

Corolário 5.18. *Seja $\mathcal{C} = \langle(a-1)^{\ell}e\rangle$ um código em RC_m, onde e é um idempotente não necessariamente primitivo. Então*

$$\mathrm{w}_K(\mathcal{C}) = \mathrm{w}_K(\Delta^{\ell}) \cdot \mathrm{w}_R(\mathcal{C}).$$

Observação 5.19. Vale ressaltar a importância de $KG \subset RG$ nesses resultados. Sem isso não poderíamos localizar os coeficientes da maneira como fizemos, de modo que se R fosse um anel de cadeia comutativo geral, não teríamos resultados tão fortes.

É claro que as cotas para $w_K(\mathcal{C})$ dadas pelo teorema 5.17 são justas já que os próprios códigos $\hat{\mathcal{C}}$ e $\check{\mathcal{C}}$ atingem, respectivamente, a inferior e a superior. Em verdade ambas as cotas são atingidas também por códigos heterogêneos no que se refere aos expoentes de $(a-1)$ em cada componente, como mostra o exemplo a seguir.

Exemplo 5.20. Continuando os exemplos 5.10 e 5.12, temos que $w_R(\langle e_1\rangle \oplus \langle e_2\rangle) = 2$, então para o código $\mathcal{C} = \langle e_1\rangle \oplus \langle (a-1)e_2\rangle$ podemos afirmar que $w_R(\mathcal{C}) = 2$ e

$$2 = w_K(\Delta^0)w_R(\mathcal{C}) \leq w_K(\mathcal{C}) \leq w_K(\Delta^1)w_R(\mathcal{C}) = 4.$$

De fato, determinamos computacionalmente que $w_K(\mathcal{C}) = 4$ e esse é um dos códigos ótimos listados na seção 6.1 (exemplo 6.3).

Considerando agora o código $\mathcal{C}' = \langle (a-1)e_1\rangle \oplus \langle e_2\rangle$, de dimensão 14, novamente temos $w_R(\mathcal{C}') = 2$ e $2 \leq w_K(\mathcal{C}') \leq 4$, mas como $e_2 = g^3 + g^6 \in \mathcal{C}'$, agora temos $w_K(\mathcal{C}') = 2$.

Tanto para $\mathcal{C}$ como para $\mathcal{C}'$ o peso sobre K concide com o peso de uma das componentes, a saber, $w_K(\mathcal{C}) = w_K(\langle (a-1)e_2\rangle)$ e $w_K(\mathcal{C}') = w_K(\langle e_2\rangle)$. Para finalizar essa ilustração da variedade de pesos que se podem encontrar nesses códigos, mesmo em comprimentos baixos, consideremos $\mathcal{C}'' = \langle e_0\rangle \oplus \mathcal{C}$. Suas componentes tem pesos $w_K(\langle e_0\rangle) = 9$, $w_K(\langle e_1\rangle) = 6$ e $w_K(\langle (a-1)e_2\rangle) = 4$, mas $w_K(\mathcal{C}'') = 2$.

5.3 CÓDIGOS NÃO CÍCLICOS

Embora as seções anteriores tenham tratado especificamente de códigos cíclicos, os resultados da seção 5.2 podem ser aplicados a códigos mais gerais, a saber, códigos em $KC_{p^n}G$ onde a única hipótese sobre G é que sua ordem não seja múltipla de p. Tais códigos fogem do escopo deste trabalho e por isso não lhes daremos um tratameto teórico, mas apresentamos um exemplo ilustrativo a seguir.

Exemplo 5.21. Consideremos o grupo não abeliano

$$G = \langle x, y, s \mid x^3 = y^3 = s^3 = 1,\ s = xyx^{-1}y^{-1},\ sx = xs,\ sy = ys \rangle.$$

G tem ordem 27, logo $\mathbb{F}_2 G$ é semissimples. Taufer mostrou em [Tau18] que essa álgebra tem seis componentes simples, das quais uma é não comutativa, de dimensão 18 e gerada por $e = s + s^2$. Exibiu também a forma dos idempotentes não centrais nessa componente e tomando em particular $u = (1 + x + x^2)(1 + y)e$ obteve um código (à esquerda) ótimo $\mathbb{F}_2 Gu$, de dimensão 6 e peso 12. Além dessa componente não comutativa, consideremos a componente unidimensional gerada por $\hat{G}$, que claramente tem peso 27. O código $\mathbb{F}_2 G\hat{G} \oplus \mathbb{F}_2 Gu$ tem peso 11.

Trazendo para nosso contexto, consideremos os códigos gerados por $(a-1)^{\ell_{\hat{G}}}\hat{G}$ e $(a-1)^{\ell_u}u$ em $\mathbb{F}_2 C_4 \times G \cong (\mathbb{F}_2 C_4)G$, para os quais obtivemos os pesos, considerados sobre K, computacionalmente. Note-se que, exceto pelos quatro da forma $\langle (a-1)^{\ell_{\hat{G}}}\hat{G} \rangle$, que são bilaterais, todos os códigos apresentados nesse exemplo são códigos à esquerda.

Os códigos da forma $\langle (a-1)^{\ell_{\hat{G}}}\hat{G} \rangle$ tem pesos 27, 54, 54 e 108 e os da forma $\langle (a-1)^{\ell_u}u \rangle$, pesos 12, 24, 24 e 48, como previsto pelo corolário 5.18, para expoentes 0, 1, 2 e 3, respectivamente.

A tabela a seguir mostra os pesos dos códigos da forma $\langle (a-1)^{\ell_{\hat{G}}}\hat{G} \rangle \oplus \langle (a-1)^{\ell_u}u \rangle$, com $0 \leq \ell_{\hat{G}}, \ell_u \leq 3$. Novamente, os códigos na diagonal, i. e., aqueles com $\ell_{\hat{G}} = \ell_u$, tem pesos como prevê o corolário 5.18. Para os códigos com $\ell_{\hat{G}} \neq \ell_u$, indicamos o peso entre as cotas dadas pelo teorema 5.17, como apresentadas no item (ii).

Tabela 2. *Pesos e cotas para códigos* $\langle (a-1)^{\ell_{\hat{G}}} \hat{G} \rangle \oplus \langle (a-1)^{\ell_u} u \rangle$.

ℓ_u \ $\ell_{\hat{G}}$	0	1	2	3
0	11	$11 \leq 12 \leq 22$	$11 \leq 12 \leq 22$	$11 \leq 12 \leq 44$
1	$11 \leq 22 \leq 22$	22	$22 \leq 22 \leq 22$	$22 \leq 24 \leq 44$
2	$11 \leq 22 \leq 22$	$22 \leq 22 \leq 22$	22	$22 \leq 24 \leq 44$
3	$11 \leq 27 \leq 44$	$22 \leq 44 \leq 44$	$22 \leq 44 \leq 44$	44

6 EXEMPLOS

6.1 CÓDIGOS CÍCLICOS ÓTIMOS

Esta seção contém exemplos de códigos cíclicos modulares ótimos. Os pesos foram determinados computacionalmente utilizando a rotina mostrada na seção 1.1 do apêndice.

Incluímos apenas códigos que atingem a *Upper Bound* da tabela de códigos em `http://www.codetables.de/` [Gra07] e para os quais, apesar de constarem nessa tabela códigos lineares com os mesmos parâmetros, não há construções cíclicas. Ainda assim, nem todos os códigos nessas condições que encontramos foram inclusos.

Todos os exemplos se baseiam na decomposição $KC_{p^n m} \cong (KC_{p^n})C_m$, onde $C_{p^n} = \langle a \rangle$ e $C_m = \langle g \rangle$.

6.1.1 Códigos binários

Exemplo 6.1. $\mathbb{F}_2 C_{12} \cong (\mathbb{F}_2 C_4) C_3$
Idempotentes:

$$e_1 = g + g^2$$
$$e_2 = 1 + g + g^2$$

Tabela 3. *Código binário de comprimento 12.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_1 \rangle \oplus \langle (a-1)^3 e_2 \rangle$	7	4	28

Exemplo 6.2. $\mathbb{F}_2C_{14} \cong (\mathbb{F}_2C_2)C_7$

Idempotentes:

$$e_1 = 1 + g + g^2 + g^4$$
$$e_2 = 1 + g^3 + g^5 + g^6$$
$$e_3 = 1 + g + g^2 + g^3 + g^4 + g^5 + g^6$$

Tabela 4. *Códigos binários de comprimento 14.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_1 \rangle \oplus \langle e_3 \rangle$ $\langle (a-1)e_2 \rangle \oplus \langle e_3 \rangle$	5	6	30

Exemplo 6.3. $\mathbb{F}_2C_{18} \cong (\mathbb{F}_2C_2)C_9$

Idempotentes:

$$e_1 = g^3 + g^6$$
$$e_2 = g + g^2 + g^4 + g^5 + g^7 + g^8$$
$$e_3 = 1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8$$

Tabela 5. *Código binário de comprimento 18.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_1 \rangle \oplus \langle e_2 \rangle$	10	4	40

Exemplo 6.4. $\mathbb{F}_2C_{20} \cong (\mathbb{F}_2C_4)C_5$

Idempotentes:

$$e_1 = g + g^2 + g^3 + g^4$$
$$e_2 = 1 + g + g^2 + g^3 + g^4$$

Tabela 6. *Código binário de comprimento 20.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_1 \rangle \oplus \langle (a-1)^3 e_2 \rangle$	13	4	52

Exemplo 6.5. $\mathbb{F}_2 C_{24} \cong (\mathbb{F}_2 C_8) C_3$

Idempotentes:

$$e_1 = g + g^2$$
$$e_2 = 1 + g + g^2$$

Tabela 7. *Código binário de comprimento 24.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_1 \rangle \oplus \langle (a-1)^5 e_2 \rangle$	17	4	68

Exemplo 6.6. $\mathbb{F}_2 C_{28} \cong (\mathbb{F}_2 C_4) C_7$

Idempotentes:

$$e_1 = 1 + g + g^2 + g^4$$
$$e_2 = 1 + g^3 + g^5 + g^6$$
$$e_3 = 1 + g + g^2 + g^3 + g^4 + g^5 + g^6$$

Tabela 8. *Códigos binários de comprimento 28.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)^3 e_1 \rangle \oplus \langle (a-1)e_2 \rangle$ $\langle (a-1)e_1 \rangle \oplus \langle (a-1)^3 e_2 \rangle$	12	8	96
$\langle e_1 \rangle \oplus \langle (a-1)e_2 \rangle \oplus \langle (a-1)^3 e_3 \rangle$ $\langle (a-1)e_1 \rangle \oplus \langle e_2 \rangle \oplus \langle (a-1)^3 e_3 \rangle$	22	4	88

Exemplo 6.7. $\mathbb{F}_2C_{30} \cong (\mathbb{F}_2C_2)C_{15}$

Idempotentes:

$$e_1 = g + g^2 + g^3 + g^4 + g^6 + g^8 + g^9 + g^{12}$$
$$e_2 = g + g^2 + g^4 + g^5 + g^7 + g^8 + g^{10} + g^{11} + g^{13} + g^{14}$$
$$e_3 = g + g^2 + g^3 + g^4 + g^6 + g^7 + g^8 + g^9 + g^{11} + g^{12} + g^{13} + g^{14}$$
$$e_4 = g^3 + g^6 + g^7 + g^9 + g^{11} + g^{12} + g^{13} + g^{14}$$
$$e_5 = 1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14}$$

Tabela 9. *Códigos binários de comprimento 30.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_4 \rangle \oplus \langle e_5 \rangle$ $\langle (a-1)e_1 \rangle \oplus \langle e_5 \rangle$	6	14	84
$\langle (a-1)e_2 \rangle \oplus \langle (a-1)e_3 \rangle \oplus \langle e_4 \rangle$ $\langle e_1 \rangle \oplus \langle (a-1)e_2 \rangle \oplus \langle (a-1)e_3 \rangle$	14	8	112
$\langle e_1 \rangle \oplus \langle e_2 \rangle \oplus \langle (a-1)e_3 \rangle \oplus \langle (a-1)e_5 \rangle$ $\langle (a-1)e_1 \rangle \oplus \langle e_2 \rangle \oplus \langle e_3 \rangle \oplus \langle (a-1)e_5 \rangle$ $\langle e_2 \rangle \oplus \langle e_3 \rangle \oplus \langle (a-1)e_4 \rangle \oplus \langle (a-1)e_5 \rangle$	17	6	102

Exemplo 6.8. $\mathbb{F}_2C_{34} \cong (\mathbb{F}_2C_2)C_{17}$

Idempotentes:

$$e_1 = g^3 + g^5 + g^6 + g^7 + g^{10} + g^{11} + g^{12} + g^{14}$$
$$e_2 = g + g^2 + g^4 + g^8 + g^9 + g^{13} + g^{15} + g^{16}$$
$$e_3 = 1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{16}$$

Tabela 10. *Códigos binários de comprimento 34.*

Código	Dimensão	Peso	Conveniência
$\langle e_1 \rangle \oplus \langle (a-1)e_2 \rangle$ $\langle (a-1)e_1 \rangle \oplus \langle e_2 \rangle$	24	4	96

Exemplo 6.9. $\mathbb{F}_2C_{36} \cong (\mathbb{F}_2C_4)C_9$

Idempotentes:

$$e_1 = g^3 + g^6$$
$$e_2 = g + g^2 + g^4 + g^5 + g^7 + g^8$$
$$e_3 = 1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8$$

Tabela 11. *Código binário de comprimento 36.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_1 \rangle \oplus \langle e_2 \rangle \oplus \langle (a-1)^3 e_3 \rangle$	27	4	108

Exemplo 6.10. $\mathbb{F}_2C_{40} \cong (\mathbb{F}_2C_8)C_5$

Idempotentes:

$$e_1 = g + g^2 + g^3 + g^4$$
$$e_2 = 1 + g + g^2 + g^3 + g^4$$

Tabela 12. *Código binário de comprimento 40.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_1 \rangle \oplus \langle (a-1)^6 e_2 \rangle$	30	4	120

Exemplo 6.11. $\mathbb{F}_2C_{42} \cong (\mathbb{F}_2C_2)C_{21}$

Idempotentes:

$$
\begin{aligned}
e_1 &= g + g^2 + g^4 + g^7 + g^8 + g^{11} + g^{14} + g^{16} \\
e_2 &= 1 + g + g^2 + g^4 + g^7 + g^8 + g^9 + g^{11} + g^{14} + g^{15} + g^{16} + g^{18} \\
e_3 &= g + g^2 + g^4 + g^5 + g^7 + g^8 + g^{10} + g^{11} + g^{13} + g^{14} + g^{16} + g^{17} + g^{19} + g^{20} \\
e_4 &= 1 + g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} + g^{20} \\
e_5 &= g^5 + g^7 + g^{10} + g^{13} + g^{14} + g^{17} + g^{19} + g^{20} \\
e_6 &= 1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + \\
&\quad g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20}
\end{aligned}
$$

Tabela 13. *Códigos binários de comprimento 42.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_1 \rangle \oplus \langle e_2 \rangle \oplus \langle e_5 \rangle$ $\langle e_1 \rangle \oplus \langle e_4 \rangle \oplus \langle (a-1)e_5 \rangle$	24	8	192

6.1.2 Códigos ternários

Exemplo 6.12. $\mathbb{F}_3C_{12} \cong (\mathbb{F}_3C_3)C_4$

Idempotentes:

$$
\begin{aligned}
e_1 &= 2 + g^2 \\
e_2 &= 1 + g + g^2 + g^3 \\
e_3 &= 1 + 2g + g^2 + 2g^3
\end{aligned}
$$

Tabela 14. *Códigos ternários de comprimento 12.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)^2 e_1 \rangle \oplus \langle (a-1) e_3 \rangle$ $\langle (a-1)^2 e_1 \rangle \oplus \langle (a-1) e_2 \rangle$	4	6	24
$\langle (a-1) e_1 \rangle \oplus \langle e_2 \rangle$ $\langle (a-1) e_1 \rangle \oplus \langle e_3 \rangle$	7	4	28
$\langle (a-1) e_1 \rangle \oplus \langle (a-1)^2 e_2 \rangle \oplus \langle e_3 \rangle$ $\langle (a-1) e_1 \rangle \oplus \langle e_2 \rangle \oplus \langle (a-1)^2 e_3 \rangle$	8	3	24

Exemplo 6.13. $\mathbb{F}_3 C_{24} \cong (\mathbb{F}_3 C_3) C_8$

Idempotentes:

$$
\begin{aligned}
e_1 &= 1 + 2g^2 + g^4 + 2g^6 \\
e_2 &= 2 + g + 2g^2 + g^3 + 2g^4 + g^5 + 2g^6 + g^7 \\
e_3 &= 1 + 2g + 2g^3 + 2g^4 + g^5 + g^7 \\
e_4 &= 1 + g + g^3 + 2g^4 + 2g^5 + 2g^7 \\
e_5 &= 2 + 2g + 2g^2 + 2g^3 + 2g^4 + 2g^5 + 2g^6 + 2g^7
\end{aligned}
$$

Tabela 15. *Códigos ternários de comprimento 24.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_2\rangle \oplus \langle (a-1)^2e_3\rangle$ $\langle (a-1)e_2\rangle \oplus \langle (a-1)^2e_4\rangle$ $\langle (a-1)^2e_3\rangle \oplus \langle (a-1)e_5\rangle$ $\langle (a-1)^2e_4\rangle \oplus \langle (a-1)e_5\rangle$	4	15	60
$\langle e_1\rangle \oplus \langle (a-1)e_2\rangle \oplus \langle e_3\rangle \oplus \langle (a-1)e_4\rangle$ $\langle e_1\rangle \oplus \langle (a-1)e_2\rangle \oplus \langle (a-1)e_3\rangle \oplus \langle e_4\rangle$ $\langle e_1\rangle \oplus \langle e_3\rangle \oplus \langle (a-1)e_4\rangle \oplus \langle (a-1)e_5\rangle$ $\langle e_1\rangle \oplus \langle (a-1)e_3\rangle \oplus \langle e_4\rangle \oplus \langle (a-1)e_5\rangle$	18	4	72
$\langle e_1\rangle \oplus \langle (a-1)e_3\rangle \oplus \langle e_4\rangle \oplus \langle e_5\rangle$ $\langle e_1\rangle \oplus \langle e_3\rangle \oplus \langle (a-1)e_4\rangle \oplus \langle e_5\rangle$ $\langle e_1\rangle \oplus \langle (a-1)e_2\rangle \oplus \langle (a-1)^2e_3\rangle \oplus \langle e_4\rangle \oplus \langle e_5\rangle$ $\langle e_1\rangle \oplus \langle (a-1)e_2\rangle \oplus \langle e_3\rangle \oplus \langle (a-1)^2e_4\rangle \oplus \langle e_5\rangle$ $\langle e_1\rangle \oplus \langle e_2\rangle \oplus \langle e_3\rangle \oplus \langle (a-1)^2e_4\rangle \oplus \langle (a-1)e_5\rangle$ $\langle e_1\rangle \oplus \langle (a-1)^2e_2\rangle \oplus \langle e_3\rangle \oplus \langle (a-1)e_4\rangle \oplus \langle (a-1)e_5\rangle$ $\langle e_1\rangle \oplus \langle e_2\rangle \oplus \langle (a-1)^2e_3\rangle \oplus \langle e_4\rangle \oplus \langle (a-1)e_5\rangle$ $\langle e_1\rangle \oplus \langle (a-1)^2e_2\rangle \oplus \langle (a-1)e_3\rangle \oplus \langle e_4\rangle \oplus \langle (a-1)e_5\rangle$ $\langle e_1\rangle \oplus \langle (a-1)e_2\rangle \oplus \langle (a-1)e_3\rangle \oplus \langle e_4\rangle \oplus \langle (a-1)^2e_5\rangle$ $\langle e_1\rangle \oplus \langle (a-1)e_2\rangle \oplus \langle e_3\rangle \oplus \langle (a-1)e_4\rangle \oplus \langle (a-1)^2e_5\rangle$ $\langle e_1\rangle \oplus \langle e_2\rangle \oplus \langle e_3\rangle \oplus \langle (a-1)e_4\rangle$ $\langle e_1\rangle \oplus \langle e_2\rangle \oplus \langle (a-1)e_3\rangle \oplus \langle e_4\rangle$	19	3	57

6.1.3 Códigos sobre $\mathbb{F}_5$ e $\mathbb{F}_7$

Exemplo 6.14. $\mathbb{F}_5C_{10} \cong (\mathbb{F}_5C_5)C_2$

Idempotentes:

$$e_1 = 3 + 2g$$

$$e_2 = 3 + 3g$$

Tabela 16. *Códigos quinários de comprimento 10.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)^3 e_1 \rangle \oplus \langle (a-1) e_2 \rangle$ $\langle (a-1) e_1 \rangle \oplus \langle (a-1)^3 e_2 \rangle$	6	4	24
$\langle (a-1)^2 e_1 \rangle \oplus \langle (a-1) e_2 \rangle$ $\langle (a-1) e_1 \rangle \oplus \langle (a-1)^2 e_2 \rangle$	7	3	21

Exemplo 6.15. $\mathbb{F}_5C_{15} \cong (\mathbb{F}_5C_5)C_3$

Idempotentes:

$$e_1 = 2 + 2g + 2g^2$$

$$e_2 = 4 + 3g + 3g^2$$

Tabela 17. *Código quinário de comprimento 15.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)^3 e_1 \rangle \oplus \langle (a-1) e_2 \rangle$	10	4	40

Exemplo 6.16. $\mathbb{F}_7C_{14} \cong (\mathbb{F}_7C_7)C_2$

Idempotentes:

$$e1 = 4 + 3g$$

$$e2 = 4 + 4g$$

Tabela 18. *Códigos septários de comprimento 14.*

Código	Dimensão	Peso	Conveniência
$\langle (a-1)^3 e_1 \rangle \oplus \langle (a-1) e_2 \rangle$ $\langle (a-1) e_1 \rangle \oplus \langle (a-1)^3 e_2 \rangle$	10	4	40
$\langle (a-1)^2 e_1 \rangle \oplus \langle (a-1) e_2 \rangle$ $\langle (a-1) e_1 \rangle \oplus \langle (a-1)^2 e_2 \rangle$	11	3	33

6.1.4 Códigos sobre $\mathbb{F}_4$

Nos exemplos a seguir consideramos $\mathbb{F}_4 = \mathbb{F}_2(\zeta)$, onde ζ é uma raíz cúbica primitiva da unidade e satisfaz $\zeta^2 + \zeta + 1 = 0$.

Os códigos apresentados são cíclicos sobre $\mathbb{F}_4$, mas também podem ser vistos como códigos sobre $\mathbb{F}_2$ através da transformação

$$\psi : \mathbb{F}_4^n \to \mathbb{F}_2^{2n}$$
$$(a_1 + b_1\zeta,\, a_2 + b_2\zeta, \ldots,\, a_n + b_n\zeta) \mapsto (a_1,\, b_1,\, a_2,\, b_2, \ldots,\, a_n,\, b_n),$$

onde $a_i,\, b_i \in \mathbb{F}_2$, $1 \leq i \leq n$. É claro que ψ é um homomorfismo de $\mathbb{F}_2$-espaços vetoriais e leva um $(n,\, k)$-código cíclico sobre $\mathbb{F}_4$ em um $(2n,\, 2k)$-código 2-quasi-cíclico sobre $\mathbb{F}_2$.

Exemplo 6.17. $\mathbb{F}_4 C_{12} \cong (\mathbb{F}_4 C_4) C_3$
Idempotentes:

$$e_1 = 1 + (\zeta + 1)g + \zeta g^2$$
$$e_2 = 1 + \zeta g + (\zeta + 1)g^2$$
$$e_3 = 1 + g + g^2$$

Tabela 19. *Código de comprimento 12 sobre* $\mathbb{F}_4$.

Código	Dimensão	Peso	Conveniência
$\langle (a-1)e_1 \rangle \oplus \langle (a-1)e_2 \rangle \oplus \langle (a-1)^3 e_3 \rangle$	7	4	28

Considerado sobre $\mathbb{F}_2$ esse código tem comprimento 24, dimensão 14 e peso 4.

Exemplo 6.18. $\mathbb{F}_4 C_{14} \cong (\mathbb{F}_4 C_2) C_7$

Idempotentes:

$$e_1 = 1 + g + g^2 + g^4$$
$$e_2 = 1 + g^3 + g^5 + g^6$$
$$e_3 = 1 + g + g^2 + g^3 + g^4 + g^5 + g^6$$

Tabela 20. *Códigos de comprimento 14 sobre* $\mathbb{F}_4$.

Código	Dimensão	Peso	Conveniência
$\langle e_1 \rangle \oplus \langle (a-1)e_2 \rangle$ $\langle (a-1)e_1 \rangle \oplus \langle e_2 \rangle$	9	4	36

Considerados sobre $\mathbb{F}_2$ esses códigos são de comprimento 28, dimensão 18 e peso 4.

7 CONCLUSÃO

A obtenção de uma grande quantidade de exemplos de códigos cíclicos ótimos que, mesmo em comprimentos baixos, não constam nas tabelas *online* ([Gra07]) corrobora a idéia de que códigos modulares são ainda relativamente pouco explorados. Os resultados apresentados no capítulo 5 oferecem um método simples para obter códigos modulares para os quais se se conhece a dimensão e se tem boas cotas para os pesos a partir de códigos semissimples. Vale comentar novamente que, embora aqui usados quase exclusivamente para códigos cíclicos, esses resultados podem ser usados para códigos semissimples mais gerais.

Além de aplicar as idéias e resultados desenvolvidos a classes mais gerais de códigos, uma direção natural de continuidade desse trabalho é procurar generalizar as fórmulas para N_k e N^d dadas na seção 3.1 para polinômios com mais do que uma variável, o que consequentemente elimina, ou ao menos afrouxa, a restrição na faixa de códigos para os quais conhecemos toda a distribuição de pesos (v. teorema 4.13). Há ainda em [Sil12] uma série de resultados sobre códigos duais e auto-duais que podem ser naturalmente revisitados usando a abordagem aqui introduzida.

APÊNDICE

1 LISTAGENS DE PROGRAMAS

1.1 Distribuição de Pesos

As rotinas a seguir, escritas em linguagem C, foram usadas para computar a distribuição de pesos dos exemplos apresentados no capítulo 6.

A função `wdp` retorna a distribuição de pesos e o número de palavras computadas de um código de comprimento n e dimensão k sobre um corpo primo $\mathbb{F}_p$, enquanto a função `wde` é usada para códigos sobre uma extensão $\mathbb{F}_{p^e}$ e retorna também a distribuição de pesos do código visto como tendo comprimento $n \cdot e$ sobre $\mathbb{F}_p$. Além dos parâmetros `p`, `n` e `k`, deve-se fornecer uma $\mathbb{F}_p$-base (ou $\mathbb{F}_{p^e}$-base) `B` para o código. O parâmetro `min` inclui um critério de parada: se esse parâmetro for positivo a rotina retorna ao encontrar a primeira palavra (não nula) de peso menor que `min`.

A rotina `free_memory` libera memória alocada por `wdp` e `wde`.

```
1  #include <stdlib.h>
2
3  int *d = NULL;
4
5
6  int *wdp(int p, int n, int k, int *B, int *c0, int min)
7  {
8      int *c, *a, *s;
9      int i, j, w;
10
11     // Weight distribution and number of words computed
12     d = (int*)malloc((n + 2) * sizeof(int));
13     for (j = 0; j <= n + 1; j++)
14         d[j] = 0;
15
```

```
    // Codewords computed
    c = (int*)malloc(n * sizeof(int));
    for (j = 0; j < n; j++)
        c[j] = c0[j];

    // Coefficient and upward/downward vectors
    a = (int*)malloc(k * sizeof(int));
    s = (int*)malloc(k * sizeof(int));
    for (j = 0; j < k; j++) {
        a[j] = 0;
        s[j] = 0;
    }

    i = 0;
    while (i < k) {
        w = 0;
        for (j = 0; j < n; j++)
            if ((c[j] % p) != 0)
                w++;
        d[w]++;
        d[n+1]++;

        if (min && w > 0 && w < min)
            break;

        while (i < k) {
            if (s[i] && a[i] > 0) {
                a[i]--;
                for (j = 0; j < n; j++)
                    c[j] = (c[j] - B[i*n + j]);
                i = 0;
                break;
            }
            else if (!s[i] && a[i] < (p - 1)) {
                a[i]++;
                for (j = 0; j < n; j++)
                    c[j] = (c[j] + B[i*n + j]);
                i = 0;
                break;
            }
            else {
                s[i] = !s[i];
                i++;
            }
        }
    }

```

```
63      free(s);
64      free(a);
65      free(c);
66
67      return d;
68  }
69
70
71  int *wde(int p, int e, int n, int k, int *B, int *c0, int min)
72  {
73      int *c, *a, *s;
74      int i, j, wp, we, z, ne;
75
76      if (n % e != 0)
77          return NULL;
78      ne = n/e;
79
80      // Weight distribution and number of words computed
81      d = (int*)malloc((ne + n + 3) * sizeof(int));
82      for (j = 0; j <= ne + n + 2; j++)
83          d[j] = 0;
84
85      // Codewords computed
86      c = (int*)malloc(n * sizeof(int));
87      for (j = 0; j < n; j++)
88          c[j] = c0[j];
89
90      // Coefficient and upward/downward vectors
91      a = (int*)malloc(k * sizeof(int));
92      s = (int*)malloc(k * sizeof(int));
93      for (j = 0; j < k; j++) {
94          a[j] = 0;
95          s[j] = 0;
96      }
97
98      i = 0;
99      while (i < k) {
100         wp = we = z = 0;
101         for (j = 0; j < n; j++)        {
102             if ((c[j] % p) != 0) {
103                 wp++;
104                 z = 1;
105             }
106             if ((j + 1) % e == 0) {
107                 we += z;
108                 z = 0;
109             }
```

```
110         }
111         d[we]++;
112         d[ne + 1 + wp]++;
113         d[ne + n + 2]++;
114 
115         if (min && we > 0 && we < min)
116             break;
117 
118         while (i < k) {
119             if (s[i] && a[i] > 0) {
120                 a[i]--;
121                 for (j = 0; j < n; j++)
122                     c[j] = (c[j] - B[i*n + j]);
123                 i = 0;
124                 break;
125             }
126             else if (!s[i] && a[i] < (p - 1)) {
127                 a[i]++;
128                 for (j = 0; j < n; j++)
129                     c[j] = (c[j] + B[i*n + j]);
130                 i = 0;
131                 break;
132             }
133             else {
134                 s[i] = !s[i];
135                 i++;
136             }
137         }
138     }
139 
140     free(s);
141     free(a);
142     free(c);
143 
144     return d;
145 }
146 
147 
148 void free_memory()
149 {
150     if (d != NULL) {
151         free(d);
152         d = NULL;
153     }
154 }
```

REFERÊNCIA BIBLIOGRÁFICA

[AR17] H. Andriatahiny e V. H. Rakotomalala. "The Generalized Reed-Muller Codes in a Modular Group Algebra". Em: *British Journal of Mathematics & Computer Science* 20(2) (2017), pp. 1–15.

[Ber67] S. D. Berman. "On the Theory of Group Codes". Em: *Kibernetika* 3 (1967), pp. 31–39.

[Cal+93] A. R. Caldebank et al. "A linear construction for certain Kerdock and Preparata codes". Em: *Bull. Amer. Math.* 29 (1993), pp. 218–222.

[Cam94] P. J. Cameron. *Combinatorics: topics, techniques, algorithms*. Cambridge University Press, 1994.

[CS95] A. R. Caldebank e J. A. Sloane. "Modular and p-adic codes". Em: *Designs, Codes and Cryptography* 6 (1995), pp. 21–35.

[DL04] D. Q. Dinh e S. R. López-Permouth. "Cyclic and negacyclic codes over finite chain rings". Em: *IEEE Transactions on Information Theory* 50 (2004), pp. 1728–1744.

[DP07] S. T. Dougherty e Y. H. Park. "On modular cyclic codes". Em: *Finite Fields and their Applications* 13 (2007), pp. 31–57.

[FP07] R. A. Ferraz e F. C. Polcino Milies. "Idempotents in Group Algebras and Minimal Abelian Codes". Em: *Finite Fields and Their Applications* 13 (2007), pp. 382–393.

[Gra07] Markus Grassl. *Bounds on the minimum distance of linear codes and quantum codes*. Disponível *online* em `http://www.codetables.de`. Acessado em 2018-09-18. 2007.

[Han17] C. Hannusch. "On monomial codes in modular group algebras". Em: *Discrete Mathematics* 340(5) (2017), pp. 957–962.

[Jac09a] N. Jacobson. *Basic Algebra I*. 2ª ed. Dover Publications, Inc, 2009.

[Jac09b] N. Jacobson. *Basic Algebra II*. 2ª ed. Dover Publications, Inc, 2009.

[Lin98] J. H. van Lint. *Introduction to coding theory*. Graduate Texts in Mathematics 86. Springer, 1998.

[Mac70] F. J. MacWilliams. "Binary codes which are ideals in the group algebra of an abelian group". Em: *Bell System Tech. J.* 49 (1970), pp. 987–1011.

[MM13] C. Polcino Milies e F. D. de Melo. "On Cyclic and Abelian Codes". Em: *IEEE Transactions on Information Theory* 59.11 (nov. de 2013), pp. 7314–7319.

[MS77] F. J. MacWilliams e N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Vol. 16. North-Holland Mathematical Library. North-Holland Publishing Company, 1977.

[NS00] G. Norton e A. Salagean-Mandache. "On the structure of linear cyclic codes over finite chain rings". Em: *Appl. Algebra Eng. Commun. Comput.* 10 (2000), pp. 489–506.

[Pra57] E. Prange. "Cyclic error-correcting codes in two symbols, AFCRC-TN-57-103". Em: *Air Force Cambridge research center* (1957).

[PS02] F. C. Polcino Milies e S. K. Sehgal. *An Introduction to Group Rings*. Dordrecht, The Netherlands: Kluwer Academic Publishers, 2002.

[Rom92] S. Roman. *Coding and Information Theory*. Graduate Texts in Mathematics 134. Springer, 1992.

[Sil12] A. T. da Silva. "Códigos cíclicos sobre anéis de cadeia". Tese de doutoramento. IME-USP, 2012.

[Tau18] E. Taufer. "Ideais em anéis de matrizes finitos e aplicações à Teoria de Códigos". Tese de doutoramento. IME-USP, 2018.

[Vil14] R. Villafranca. "Decodificação de códigos sobre anéis de Galois". Tese de mestrado. UFABC, 2014.

[Wan11] Z.-X. Wan. *Finite Fields and Galois Rings*. Singapore: World Scientific, 2011.

ÍNDICE