Matriz Geradora de Códigos Diedrais

João Antonio Camargo Neto[1] **Alonso Sepúlveda Castellanos**[1,2]

1. Faculdade de Matemática, UFU, Uberlândia-MG

Contato: joao.camargo@ufu.br

Introdução

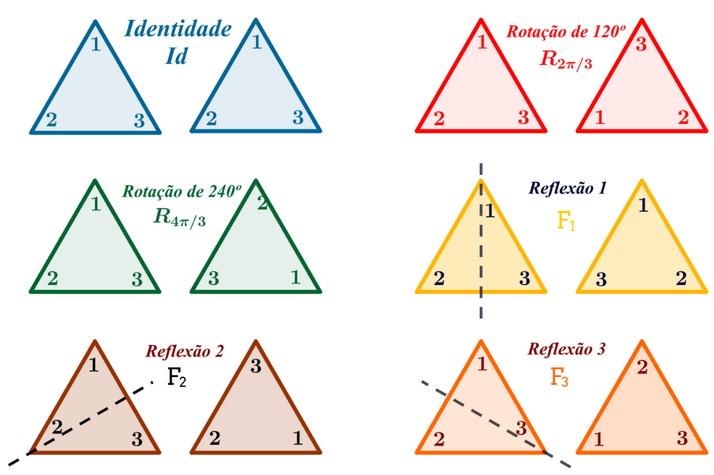
Neste trabalho estudamos uma estrutura de códigos corretores de erros, onde é necessária uma abordagem à teoria de anéis de grupos e, especificamente usaremos os anéis de grupos sobre o grupo Diedral, o qual será o foco para construção de códigos por meio de divisores de zero do anel de grupo.

O objetivo deste trabalho é estabelecer um isomorfismo entre anéis de grupos e o conjunto das matrizes $n \times n$ e, com isso, construir códigos por meio das matrizes correspondentes a elementos divisores de zero do anel de grupo e, em especial, obter códigos auto-duais através de divisores de zero nilpotentes de ordem 2.

Preliminares

Grupo Diedral

Observe o grupo gerado pelas simetrias de um triângulo equilátero: [1]



Onde Id , $R_{\frac{2\pi}{3}}$, $R_{\frac{4\pi}{3}}$ são rotações no sentido anti-horário e F_1, F_2 e F_3 são reflexões. O grupo $S_\triangle$ é formado então por 3 rotações e 3 reflexões.

O grupo de simetrias de um polígono regular será chamado de **Grupo Diedral**, o qual será denotado por $\mathbf{D_n}$ e possui $2n$ elementos, onde n elementos são rotações e n são reflexões.

Ainda podemos ver que $D_n = \langle R, F\rangle$, onde $R = R_{\frac{360^o}{n}}$ e F uma reflexão qualquer, então $R^n = F^2 = Id$ e $FRF = R^{-1}$. A forma geral de um grupo diedral será dado então por:

$$D_n = \langle R, F : R^n = F^2 = Id; FRF = R^{-1}\rangle$$

$$D_n = \{Id, R, R^2, R^3, \ldots, R^{n-1}, F, FR, FR^2, \ldots, FR^{n-1}\}.$$

Anéis de Grupo

Sejam R um anel com unidade e G um grupo qualquer, definimos o anel de grupo RG como o conjunto de combinações lineares formais do tipo:

$$\alpha = \sum_{g\in G} \alpha_g g$$

Note que, dados dois elementos, $\alpha, \beta \in RG$, $\alpha = \sum_{g\in G} \alpha_g g$ e $\beta = \sum_{g\in G} \beta_g g$, eles são iguais se, e somente se, $\alpha_g = \beta_g, \forall g \in G$.
As operações definidas são: [2]

- Soma: Dados dois elementos $\alpha = \sum_{g\in G} \alpha_g g$ e $\beta = \sum_{g\in G} \beta_g g$

$$\alpha + \beta = \sum_{g\in G} (\beta_g + \alpha_g) g.$$

- Produto: Dados dois elementos $\alpha = \sum_{g\in G} \alpha_g g$ e $\beta = \sum_{h\in G} \beta_h h$

$$\alpha\beta = \sum_{g,h\in G} (\alpha_g \beta_h) gh.$$

- Produto por escalar: Se $\lambda \in R$ e $\alpha = \sum_{g\in G} \alpha_g g$

$$\lambda\alpha = \sum_{g\in G} \lambda(\alpha_g) g.$$

Verifica-se que RG é um R-módulo com identidade $1_R.1_G = 1$. Se R for comutativo, segue que RG é uma álgebra sobre R.

Considere, então, o anel de grupo $\mathbb{Z}_2D_3$. Vejamos como é um elemento do anel de grupo: Seja $u \in \mathbb{Z}_2D_3$

$$u = \sum_{g\in D_3} \alpha_g g = 1Id + 1R_{120} + 0R_{270} + 1F + 0FR + 0FR^2 = Id + R_{120} + F$$

Códigos Diedrais

Código de Anel de Grupo

Definição 1. *Sejam RG um anel de grupo e $u \in RG$ não nulo, dizemos que u é um **divisor de zero à esquerda** de RG se existe $v \in RG$, $v \neq 0$, tal que, $uv = 0$. De maneira análoga, u é chamado **divisor de zero à direita** de RG se $vu = 0$. Se u é divisor de zero à direita e à esquerda de RG, então dizemos que u é **divisor de zero** de RG.*

Seja u um divisor de zero do anel de grupo RG e, seja W um submódulo de RG com base $S \subseteq G$. O submódulo Wu é chamado de código à esquerda do divisor de zero u. No caso em que RG não é comutativo, podemos também definir no anel de grupo o código à direita uW. O elemento u é chamado de gerador do código Wu e, este submódulo tem base Su. Os elementos de Wu são chamados de palavras do código.

Matriz Geradora

Seja $u = \sum_{g\in G} \alpha_g g \in RG$. Construímos, então, a RG-matriz sobre u, a qual denotamos por $M(RG, u)$ definida da forma:

$$M(RG,u) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}$$

Teorema 2. *Dada uma lista dos elementos de um grupo G de ordem n, existe um isomorfismo de anéis entre o anel de grupo RG e as G-matrizes de tamanho $n \times n$ sobre R. Este isomorfismo é dado por $\sigma(w) = M(RG, w)$.*

Proof. A demonstração pode ser encontrada em [2]. ∎

Código sobre o grupo Diedral

Definimos anteriormente o Grupo Diedral de um polígono de n lados como sendo: $D_n = \langle F, R : F^2 = R^n = e, FR = R^{-1}F\rangle$. Onde **F** é uma reflexão qualquer e **R** é a rotação de $\frac{360^o}{n}$, os elementos de D_n são:

$$D_n = \{Id, R, R^2, \ldots, R^{n-1}, F, FR, FR^2, \ldots, FR^{n-1}\}$$

Note que o inverso de FR^i é ele mesmo. A matriz relativa aos elementos de D_n será: [3]

$$\left[\begin{array}{ccccc|ccccc} Id & R & R^2 & \ldots & R^{n-1} & F & FR & FR^2 & \ldots & FR^{n-1} \\ R^{n-1} & Id & R & \ldots & R^{n-2} & FR & FR^2 & FR^3 & \ldots & F \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ R & R^2 & R^3 & \ldots & Id & FR^{n-1} & F & FR & \ldots & FR^{n-2} \\ \hline F & FR & FR^2 & \ldots & FR^{n-1} & Id & R & R^2 & \ldots & R^{n-1} \\ FR & FR^2 & FR^3 & \ldots & F & R^{n-1} & Id & R & \ldots & R^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ FR^{n-1} & F & FR & \ldots & FR^{n-2} & R & R^2 & R^3 & \ldots & Id \end{array}\right]$$

Assim, o espaço das matrizes da forma $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$, onde A é uma matriz circulante e B é uma matriz circulante reversa (Matriz de Hanke), é isomorfo ao anel de grupo sobre D_n.

Conhecendo, então, um elemento divisor de zero no anel de grupo sobre D_n, podemos facilmente construir uma matriz geradora de um código tomando as linhas linearmente independentes de sua matriz. Se o elemento for nilpotente de ordem 2 no anel de grupo teremos um código auto-dual.

Código Binário de Golay Extendido

Vamos verificar os parâmetros do código sobre o Anel de Grupo $\mathbb{Z}_2D_{12}$, a partir do elemento $u = 1 + F(R + R^2 + R^4 + R^5 + R^6 + R^7 + R^9) \in \mathbb{Z}_2D_{12}$, que é um divisor de zero em $\mathbb{Z}_2D_{12}$. Observe a submatriz B, circulante reversa, da matriz geradora construida com base na estrutura enunciada acima:

$$B = \begin{bmatrix} 0&1&1&0&1&1&1&1&0&1&0&0 \\ 1&1&0&1&1&1&1&0&1&0&0&0 \\ 1&0&1&1&1&1&0&1&0&0&0&1 \\ 0&1&1&1&1&0&1&0&0&0&1&1 \\ 1&1&1&1&0&1&0&0&0&1&1&0 \\ 1&1&1&0&1&0&0&0&1&1&0&1 \\ 1&1&0&1&0&0&0&1&1&0&1&1 \\ 1&0&1&0&0&0&1&1&0&1&1&1 \\ 0&1&0&0&0&1&1&0&1&1&1&1 \\ 1&0&0&0&1&1&0&1&1&1&1&0 \\ 0&0&0&1&1&0&1&1&1&1&0&1 \\ 0&0&1&1&0&1&1&1&1&0&1&0 \end{bmatrix}$$

Este código será o código binário de Golay extendido, cuja a distância mínima calculamos utilizando o programa SageMath:

```
sage:  C = codes.GolayCode(GF(2))
sage:  C.minimum_distance()
8
```

Os parâmetros do código gerado serão [24,12,8].

Conclusão

Obtemos uma estrutura geral para construção de diversos códigos com variadas características, em especial códigos auto-duais, utilizando a teoria de anéis de grupo juntamente com a estrutura de grupos de simetrias de polígonos regulares.

Agradecimentos

Agradeço ao PIC-ME e ao CNPQ pelo subsídio por meio da bolsa de estudos para o desenvolvimento do trabalho.

References

[1] CASTELLANOS, A. S. **Estruturas Algébricas e Aplicações**. 2017. 85 p. Universidade Federal de Uberlândia, Uberlândia, 2017.

[2] HURLEY, T. **G**roup rings and rings of matrices. 31^a ed. Galway: International Journal of Pure and Applied Mathematics, 2006.

[3] MCLOUGHLIN I. **Di**hedral codes. Galway:National University of Ireland, 2009. Dísponível em: <https://aran.library.nuigalway.ie/handle/10379/6401>. Acesso em: 05 jan. 2018.