Códigos Corretores de Erros e Teoria de Galois

Helena Carolina Rengel Koch
Universidade Federal de Santa Catarina

2016

Sumário

1 Introdução

A Teoria de Códigos Corretores de Erros teve início na década de 1940. Os principais nomes do início do desenvolvimento da teoria são Richard Hamming, Claude Shannon e Marcel Golay, sendo que o último foi o responsável pelo código usado pela espaçonave Voyager para transmitir fotos coloridas de Júpiter e Saturno, no final da década de 1970.

A Teoria de Códigos Corretores de Erros ainda conta com muitas aplicações na prática e garante a confiabilidade de dados transmitidos ou armazenados digitalmente.

Tais códigos são chamados de corretores de erros pois são capazes de detectar e corrigir uma certa quantidade de erros que podem ser cometidos na transmissão das informações. Esses erros, por suas vez, podem acontecer devido a interferências no canal de transmissão, por exemplo, e muitas vezes são chamados de ruídos. Procura-se, então, um código que seja capaz de detectar e corrigir o máximo possível de erros.

Para que os erros possam ser detectados e corrigidos, as palavras que devem ser transmitidas são codificadas de modo que apresentem 'redundâncias'. Obtém-se, então, o que é chamado de código de canal, pois é desenvolvido de acordo com o canal de transmissão das informações. Deve-se ter em mente que cada código deve contar com um modo de decodificação, para que a palavra recebida possa ser entendida pelo receptor. Para isso, o processo de decodificação deve ser feito levando em conta que a palavra recebida nem sempre é uma palavra do código. Quando é possível descobrir qual foi a palavra enviada, apesar dos ruídos, então pode-se dizer que o código detectou e corrigiu todos os erros da transmissão.

Com o objetivo de introduzir a Teoria de Códigos e de fazer uma relação entre tal teoria e a Teoria de Galois, é apresentado este artigo. Aqui, alguns exemplos de códigos de canal serão apresentados e estudados. Entretanto, os detalhes do processo de decodificação não serão trabalhados.

O artigo está dividido em três capítulos. O primeiro vai tratar das noções preliminares de Álgebra e Teoria de Galois necessárias para o desenvolvimento do tema. Entretanto, já considera-se que o leitor tenha alguma base teórica de Álgebra e de Álgebra Linear, tanto que alguns resultados serão apenas enunciados e não provados. Neste primeiro capítulo, serão apresentados alguns tópicos sobre corpos finitos, extensões de corpos e considerações necessárias para a apresentação de alguns códigos e resultados pertinentes a eles.

O segundo capítulo traz uma introdução à Teoria de Códigos. Trata-se de um capítulo repleto de definições e resultados que podem parecer triviais, mas cuja importância no desenvolvimento da teoria é evidente.

Por fim, são apresentados alguns tipos de códigos. Durante a apresentação dos tipos de códigos e dos exemplos, será indicada a aplicação da teoria de extensões de corpos finitos.

2 Corpos finitos e extensões de corpos

2.1 Polinômios

Espera-se do leitor, no início deste capítulo, que já tenha domínio de algumas definições e resultados de Álgebra. Serão trabalhados, aqui, resultados que sucedem o estudo de anéis, ideais e corpos.

Também serão trabalhados alguns resultados referentes ao estudo de polinômios. O anel de polinômios com coeficientes em um corpo K será denotado como $K[x]$. Denotaremos $\langle p(x)\rangle$ os múltiplos do polinômio $p(x) \in K[x]$.

Sabemos que o anel $K[x]$ é um anel principal e o mesmo vale para $K[x]/\langle p(x)\rangle$, onde $p(x) \in K[x]$.

Além disso, para qualquer ideal I não trivial de $K[x]$, existe um único polinômio mônico $p(x) \in K[x]$ tal que $I = \langle p(x)\rangle$.

Proposição 2.1. *Todo ideal de $K[x]/\langle p(x)\rangle$ é da forma $\langle g(x)\rangle$ onde $g(x) \in K[x]$ e $g(x)$ é um divisor de $p(x)$.*

Denotaremos por R_n o conjunto $K[x]/\langle x^n - 1\rangle$.

O conjunto R_n pode ser visto como um K-espaço vetorial de dimensão n, sendo que o conjunto $[1], [x], [x^2], ..., [x^{n-1}]$ formam uma base de R_n.

Definição 2.1. *Dizemos que um polinômio não nulo $p(x)$ em $K[x]$ é irredutível quando:*

- *$p(x)$ não é inversível,*
- *se $p(x)$ pode ser escrito com o produto de dois polinômios $f(x) \in K[x]$ e $g(x) \in K[x]$, então temos que ou $f(x)$ é inversível ou $g(x)$ o é.*

2.2 Corpos finitos

Um corpo que contenha q elementos será denotado, aqui, como $\mathbb{F}_q$.

Teorema 2.1. *Todo corpo finito tem p^m elementos, para algum p número primo e m inteiro positivo.*

Teorema 2.2. *Seja p um número primo. Para qualquer inteiro positivo m, existem polinômios irredutíveis de grau m em $\mathbb{F}_p$.*

Quando calculamos $\mathbb{F}_p[x]/\langle p(x)\rangle$, para um $p(x)$ irredutível em $\mathbb{F}_p[x]$ de grau m, obtemos um corpo com p^m elementos, que pode ser visto como uma extensão de $\mathbb{F}_p$.

Essa informação e o teorema anterior nos garantem que podem ser construídos corpos finitos com um número p^m de elementos para quaisquer números p e m tais que p é primo e m é um inteiro positivo.

Teorema 2.3. *Quaisquer dois corpos finitos com o mesmo número de elementos são isomorfos.*

Proposição 2.2. *Todo corpo finito tem elemento primitivo.*

2.3 Extensões de corpos

Definição 2.2. *Uma extensão de um corpo F é um par (E, i) onde E é um corpo e $i : F \to E$ é um monomorfismo.*

Quando a definição acima é satisfeita, será escrito somente que $F \subset E$ é extensão de corpos, ou ainda que E é extensão de F.

Com isso, podemos enxergar E como um espaço vetorial sobre F. Denotaremos $[E : F]$ a dimensão de E sobre F. Aqui, trataremos somente de extensões finitas, isto é, extensões tais que $dim_F E$ é finita.

Em particular, vamos trabalhar com extensões como $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, que ocorre se, e somente se, m divide n.

Definição 2.3. *Seja $F \subset E$ uma extensão de corpos. Dizemos que um elemento de E é algébrico sobre F se ele é raiz de algum polinômio com coeficientes em F. Se todos os elementos de E forem algébricos sobre F, dizemos que $F \subset E$ é uma extensão algébrica.*

Proposição 2.3. *Todo elemento de $\mathbb{F}_{p^n}$ é raiz do polinômio $f(x) = x^{p^n} - x \in \mathbb{F}_p$.*

Conclui-se que $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ é sempre uma extensão algébrica.

Definição 2.4. *Seja $F \subset E$ uma extensão algébrica de corpos e seja $\beta \in E$. Chamamos de polinômio minimal de β sobre F o polinômio mônico de menor grau em $F[x]$ que tenha β como raiz. Esse polinômio será denotado como $I(\beta, F)$.*

O polinômio minimal será irredutível.

Dado um corpo finito F e um elemento α pertencente a alguma extensão desse corpo. Denotamos como $F(\alpha)$ o menor corpo que contém F e α.

3 Introdução à Teoria de Códigos

3.1 Noções preliminares

Foi dada uma ideia, na introdução deste trabalho, do que é um código de canal. São estes os códigos que serão estudados aqui.

Ilustraremos a necessidade de códigos assim com o exemplo a seguir.

Exemplo 3.1 (Notas do Eliezer)**.** *Suponha que um professor deseja dar três notas possíveis para os alunos de uma turma. Suponha também que ele expresse as notas como elementos de $\mathbb{F}_2 \times \mathbb{F}_2$, da seguinte forma:*

$$8 \mapsto 00$$
$$9 \mapsto 01$$
$$10 \mapsto 10.$$

O conjunto $\{00, 01, 10\}$ é chamado de código da fonte.

O professor vai transmitir as informações com as notas dos alunos por meio de um canal, que pode ter interferências, que causem um erro em cada nota.

Vamos supor que a nota do aluno A era 10 e que aconteceu um erro na transmissão, de modo que a nota recebida foi 00. Nesse caso, o código não vai perceber erro algum, pois a nota poderia ser 00. Nesse caso, o aluno A perderia 2 pontos.

Por outro lado, vamos supor que a nota do aluno B era 10 e a nota recebida foi 11. Nesse caso, o código vai perceber um erro, pois a nota 11 não existe no código da fonte. Entretanto, mesmo que se saiba que houve um erro apenas na transmissão, o código não será capaz de corrigir o erro, pois seria impossível saber se a informação transmitida foi 01 ou 10.

O código da fonte passará, então, pela seguinte transformação:

$$00 \mapsto 0000$$
$$01 \mapsto 0011$$
$$10 \mapsto 1100.$$

O conjunto $\{0000, 0011, 1100\}$ é chamado de código do canal.

Agora, se o canal de transmissão causar um erro em alguma das notas, esse erro poderá ser detectado e corrigido.

Se o receptor da informação se deparar com a informação de que a nota do aluno C é 0111, sabendo que o canal causa apenas um erro por nota, o receptor saberia que a informação enviada teria sido 0011, e que a nota do aluno C é 9.

Definição 3.1. *Um código de comprimento n sobre um alfabeto A é um subconjunto próprio de $A^n = A \times A \times ... \times A$ (n vezes). Cada n-upla do código é dita ser uma palavra.*

O conjunto alfabeto é o conjunto de caracteres disponíveis para formar as palavras. O número n será chamado de comprimento do código.

Nos casos apresentados a seguir, o conjunto A será sempre um corpo finito.

Com essa definição de código, podemos tratar da distância entre duas palavras.

Definição 3.2. *Dadas duas palavras $u = (u_0, u_1, ..., u_{n-1})$ e $v = (v_0, v_1, ..., v_{n-1})$ em A^n, a distância de Hamming é a função $d : A^n \times A^n \to \mathbb{R}$ tal que $d(u, v)$ é a cardinalidade do conjunto $\{i \ / \ u_i \neq v_i, 0 \leq i \leq n-1\}$.*

Proposição 3.1. *A distância de Hammimg é um métrica sobre o conjunto A^n.*

Demonstração. Para que a função seja uma métrica, ela deve satisfazer as 4 propriedades a seguir, para quaisquer u, v e w em A^n:

1. $d(u, v) \geq 0$,
2. $d(u, v) = 0 \Leftrightarrow u = v$,
3. $d(u, v) = d(v, u)$ e
4. $d(u, v) \leq d(u, w) + d(v, w)$.

Vamos provar que a distância de Hamming satisfaz cada um dos itens.

1. A condição está automaticamente satisfeita pois a cardinalidade de um conjunto finito é sempre um número não-negativo.
2. Temos que $d(u, v)$ é a cardinalidade do conjunto $\{i \ / \ u_i \neq v_i, 0 \leq i \leq n-1\}$, que só será igual a 0 se o conjunto for vazio, ou seja, se $u_i = v_i$ para todo $0 \leq i \leq n-1$, o que implica $u = v$.

   Por outro lado, se $u = v$, então para cada i tal que $0 \leq i \leq n-1$, temos $u_i = v_i$, o que significa que a cardinalidade do conjunto $\{i \ / \ u_i \neq v_i, 0 \leq i \leq n-1\}$ é 0, ou seja, que $d(u, v) = 0$.
3. Note que $d(u, v)$ é a cardinalidade do conjunto $\{i \ / \ u_i \neq v_i, 0 \leq i \leq n-1\}$, que é igual à cardinalidade do conjunto $\{i \ / \ v_i \neq u_i, 0 \leq i \leq n-1\} = d(v, u)$.
4. Para provar a desigualdade, podemos pensar na contribuição de uma entrada i das palavras, para algum $0 \leq i \leq n-1$.

   Suponha que $u_i = v_i$. Nesse caso, a contribuição da entrada i no termo $d(u, v)$ será nula, mas no termo $d(u, w) + d(v, w)$, ela pode assumir os valor 0, 1 ou 2.

   Se ocorrer $u_i \neq v_i$, então a contribuição da entrada i no termo $d(u, v)$ será 1. Já em $d(u, w) + d(v, w)$, a contribuição dessa entrada será 1 ou 2, já que não podemos ter $u_i = w_i$ e $v_i = w_i$.

   De qualquer forma, a contribuição da entrada i no termo $d(u, v)$ é sempre menor ou igual do que a sua contribuição do termo $d(u, w) + d(v, w)$. Dessa forma, a desigualdade é satisfeita.

■

Definição 3.3. *Sejam A um alfabeto e $n \in \mathbb{N}$. Uma função $f : A^n \to A^n$ é dito ser uma isometria de A^n se ela preserva as distâncias de Hamming, ou seja, se*

$$d(f(x), f(y)) = d(x, y) \ \forall x, y \in A^n.$$

Exemplo 3.2. *Dada uma bijeção $f : A \to A$, podemos definir a função $F_f^i : A^n \to A^n$ como sendo a função que troca, em todos os elementos de A^n, o elemento da i-ésima coordenada pela sua imagem por f.*

Exemplo 3.3. *Dada uma permutação π de $\{1, 2, ...n\}$, podemos definir a função T_π como sendo a permutação das coordenadas de todos os elementos de A^n. Em outras palavras, a coordenada a_i será substituída por $a_{\pi(i)}$ em todos os elementos de A^n.*

Proposição 3.2. *Toda isometria de A^n é uma bijeção de A^n.*

Demonstração. Seja $f : A^n \to A^n$ uma isometria de A^n. Para verificar que ela é injetora, tome $x, y \in A^n$ tais que $f(x) = f(y)$. Temos então $d(f(x), f(y)) = 0$ Como f é isometria, então $d(x, y) = 0$, o que implica $x = y$ pois a distância de Hamming é uma métrica.

Como toda função injetora de um conjunto nele próprio é sobrejetora, temos que f é uma bijeção de A^n. ■

Definição 3.4. *Sejam C e C' códigos em A^n. Dizemos que C é equivalente a C' se existir uma isometria f de A^n tal que $f(C') = C$.*

Com efeito, a equivalência de códigos é uma relação de equivalência.

3.2 Parâmetros de um código

Definição 3.5. *Seja C um código. A distância mínima d de C é definida por*

$$d = min\{d(u, v); u, v \in C, u \neq v\}.$$

Chamaremos de k a parte inteira do número $\frac{d-1}{2}$.

Definição 3.6. *Sejam $a \in A^n$ e $r \in \mathbb{R}$. O disco de centro a e raio r, denotado por $D(a, r)$, é o conjunto*

$$D(a, r) = \{x \in A^n \ / \ d(a, x) \leq r\}.$$

Proposição 3.3. *Sejam c e c' palavras distintas de um código C. Então*

$$D(c, k) \cap D(c', k) = \emptyset.$$

Demonstração. Suponha, por absurdo, que $D(c, k) \cap D(c', k) \neq \emptyset.$, ou seja, que exista um elemento $x \in A^n$ tal que $x \in D(c, k) \cap D(c', k)$. Nesse caso, teríamos $d(c, x) \leq k$ e $d(c', x) \leq k$. Mas então, pelas propriedades de métrica, teríamos

$$d(c, c') \leq d(c, x) + d(c', x) \leq 2k \leq d - 1.$$

Isso é uma contradição pois d é a distância mínima do código. ■

Teorema 3.1. *Seja C um código com distância mínima d. Então C pode detectar até $d - 1$ erros e corrigir até k erros.*

Demonstração. Seja C um código com distância mínima d e seja k conforme já definido.

Denotemos c a palavra do código que foi enviada e por r a palavra que foi recebida.

Se a transmissão de uma palavra do código provoca um número de erros t tal que $t \leq k$, temos, então que $d(r, c) \leq k$. Pela proposição anterior, sabendo qual foi a palavra recebida, é possível determinar univocamente a palavra enviada.

Por outro lado, dada uma palavra do código, podem ser adicionados até $d - 1$ erros nessa palavra de modo que obtenha-se um elemento de A^n que não pertença ao código. ■

Os parâmetros chamados de fundamentais de um código C sobre um alfabeto A são:

- O número n de coordenadas de cada palavra do código;
- O número M de palavras do código;
- A distância mínima d entre duas palavras do código.

Dois códigos que são equivalentes têm os mesmos parâmetros fundamentais. É natural pensar na possibilidade de, dados três números naturais n, M e d, construir um código corretor de erros com tais parâmetros fundamentais. Entretanto, isso nem sempre é possível, como é explicado em [3].

4 Exemplos de códigos

Pretende-se apresentar, aqui, alguns exemplos de códigos onde é aplicada a Teoria de Galois para corpos finitos.

4.1 Códigos lineares

Nos resultados a seguir, vamos considerar o alfabeto como um corpo K.

Definição 4.1. *Um código $C \subset K^n$ é dito ser um código linear se for um subespaço vetorial de K^n.*

Definição 4.2. *Seja $x \in K^n$. Definimos o peso de x, denotado $w(x)$, como sendo $d(x, 0)$.*

Sabemos então que, dado $x = (x_0, x_1, ..., x_{n-1}) \in K^n$,

$$w(x) = |i \in \{0, 1, ..., n-1\}; x_i \neq 0| .$$

Definição 4.3. *Seja C um código linear. Definimos o peso de C, denotado por $w(C)$ como $w(C) = min\{d(x, 0); x \in C \setminus \{0\}\}$.*

Teorema 4.1. *Seja C um código linear. Então o peso de C é igual a sua distância mínima.*

Demonstração. Seja C um código linear. Então, para quaisquer elementos x e y de C tais que $x \neq y$. Temos que $x - y$ também pertence a C.

Nota-se que $d(x, y) = w(x - y)$, pois o número de coordenadas diferentes entre x e y é igual ao número de coordenadas não nulas da diferença entre x e y. Portanto, minimizar o peso do código é equivalente a minimizar a distância entre quaisquer duas palavras dele. ■

Este fato nos permite calcular a distância mínima d de um código linear C, que tenha M palavras, fazendo $M - 1$ cálculos de distância.

Pois bem, um subespaço vetorial C de um espaço vetorial K^n pode ser descrito como núcleo ou como imagem de uma transformação linear. Aqui, nos interessam somente as transformações lineares injetoras, pois não se deseja que duas palavras diferentes do código da fonte sejam levadas na mesma palavra do código de canal.

Todo código linear, conforme está sendo analisado aqui, é um espaço vetorial de dimensão finita. Note que, quanto aos seus parâmetros, se $K = \mathbb{F}_q$, sabemos que que C tem q^r elementos, onde r é a dimensão de C sobre $\mathbb{F}_q$.

Para obter a representação de C como imagem de uma transformação linear, considere $B = \{v_1, v_2, ...v_r\}$ uma base de C. Queremos que a transformação seja injetora, pois levar duas palavras do código da fonte na mesma palavra do código de canal impossibilitaria a decodificação.

A função

$$T : K^r \to K^n$$

que leva $x = (x_1, x_2, ...x_r) \in K^r$ em $x_1v_1 + x_2v_2 + ... + x_rv_r$ é uma transformação linear injetora. Além disso, a imagem de T é C.

Definição 4.4. *Seja $C \subset K^n$ um código linear. Seja r a dimensão de C. Considere, então, uma base $B = \{v_1, v_2, ...v_r\}$ de C. Escrevemos cada v_i como $(v_{i0}, v_{i1}, ..., v_{in-1})$.*

A matriz

$$G = \begin{pmatrix} v_1 \\ ... \\ v_r \end{pmatrix} = \begin{pmatrix} v_{10} & v_{11} & ... & v_{1n-1} \\ ... & ... & ... & ... \\ v_{r0} & v_{r1} & ... & v_{rn-1} \end{pmatrix}.$$

é chamada de matriz geradora de C associada à base B.

Assim, para um vetor $x = (x_0, x_1, ...x_{r-1}) \in K^r$ qualquer, temos que $T(x) = xG$. Note que G é uma matriz $r \times n$.

Definição 4.5. *Um código linear $C \subset K^n$ é dito ser linearmente equivalente ao código linear $C' \subset K^n$ se C' pode ser obtido de C através de operações do tipo:*

- *Multiplicação de todos os elementos de uma posição fixa de C por um escalar não nulo,*
- *Permutação das posições de todas as palavras de C através de uma mesma permutação de $\{1, 2, ...n\}$.*

A equivalência linear de código também é uma relação de equivalência.

Definição 4.6. *Para dois elementos $u = (u_0, u_1, ...u_{n-1})$ e $v = (v_0, v_1, ...v_{n-1})$ de K^n, o produto interno de u e v, denotado por $\langle u, v\rangle$ é definido como*

$$\langle u, v\rangle = u_0v_0 + u_1v_1 + ... + u_{n-1}v_{n-1}.$$

Definição 4.7. *O complemento ortogonal de um subespaço vetorial de K^n, denotado $C^\perp$ será definido como*

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

Das propriedades de produto interno, sabe-se que $C^\perp$ é um subespaço vetorial de K^n. Portanto, $C^\perp$ também será um código linear. Sua dimensão será $n - r$. Outro ponto importante a ser destacado é que $C^{\perp\perp} = C$.

Definição 4.8. *Seja C um código linear. O código linear $C^\perp$ será chamado de código dual de C.*

Proposição 4.1. *Seja $x \in K^n$. Temos que $x \in C^\perp$ se, e somente se, $Gx^T = 0$.*

Demonstração. Seja $x \in K^n$. Temos que $x \in C^\perp$ se, e somente se, x é ortogonal a todos os elementos de C. Em particular, x deve ser ortogonal aos elementos da base de C. Isso é equivalente a dizer que $Gx^T = 0$, já que as linhas de G são os elementos da base de C. ■

Teorema 4.2. *Seja C um código linear e $C^\perp$ o seu código dual. Seja H uma matriz geradora de $C^\perp$. Nesse caso, temos $v \in C$ se, e somente se, $Hv^T = 0$.*

Esse teorema mostra-se útil pois, a partir dela, para saber se um vetor $x \in K^n$ é uma palavra do código C, basta verificar se $Hv^t = 0$.

Definição 4.9. *Seja $C \subset K^n$ um código linear, $C^\perp$ o seu dual. Uma matriz H geradora de $C^\perp$ é chamada de matriz teste de paridade de C.*

Note que H é uma matriz $n-r \times n$.

Exemplo 4.1 (Código de Hamming)**.** *Considere o código com a seguinte matriz de paridade, com elementos em* $\mathbb{F}_2$*:*

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

Este código tem dimensão 4 e comprimento 7. Ele é denotado como H(7, 4). Sua matriz teste de paridade foi obtida colocando nas colunas os elementos de ${\mathbb{F}_2}^3$ *em qualquer ordem, deixando de fora apenas o elemento nulo.*

Podemos, nesse caso, analisar as colunas de H como elementos de $\mathbb{F}_8 \setminus \{0\}$ *Para cada coluna, considere o elemento mais de cima como o coeficiente de* x^0*, o segundo como o coeficiente de* x *e o terceiro como o coeficiente de* x^2*.*

Considere $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$ *e* α *elemento primitivo de* $\mathbb{F}_8$*. Vamos considerar* α *como a classe de equivalência do polinômio* $p(x) = x$*.*

Nesse caso, H pode ser escrita como

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

Assim, uma palavra do código é um elemento $c = (c_0, c_1, c_2, c_3, c_4, c_5, c_6)$ *de* ${\mathbb{F}_2}^7$ *tal que* $Hc^T = 0$*. Isso implica a igualdade a seguir:*

$$c_0\alpha^0 + c_1\alpha^1 + c_2\alpha^2 + c_3\alpha^3 + c_4\alpha^4 + c_5\alpha^5 + c_6\alpha^6 = 0.$$

Assim, vemos o código como o conjunto de polinômios com coeficientes em $\mathbb{F}_2$ *de grau maior ou igual a 6 tais que admitem* α *como uma raiz em* $\mathbb{F}_8$*.*

Exemplo 4.2 (Códigos de Reed-Salomon)**.** *Considere* $K[x]_{r-1}$ *o conjunto dos polinômios em* $K[x]$ *de grau menor ou igual a* $r-1$*, incluindo o polinômio nulo.*

Vendo o conjunto $K[x]_{r-1}$ *como um* K*-espaço vetorial, observamos que ele tem dimensão* r *e que o conjunto* $\{1, x, x^2, ..., x^{r-1}\}$ *é uma base desse espaço.*

Seja $n \in \mathbb{Z}$ *com* $n \geq r$ *e sejam* $\alpha_1, \alpha_2, ..., \alpha_n$ *elementos distintos de* K*.*

Considere a função:

$$\begin{array}{rccc} T: & K[x]_{r-1} & \to & K^n \\ & p(x) & \mapsto & (p(\alpha_1),\ p(\alpha_2),\ ...,\ p(\alpha_n)) \end{array}$$

Observe que trata-se de uma transformação linear e que é uma função injetora. De fato, um polinômio de grau até $r-1$ *não pode apresentar n raízes distintas, se temos* $n \geq r$*.*

O conjunto $K[x]_{r-1}$ *pode ser visto como o código da fonte, enquanto* $T(K[x]_{r-1}) = C$ *é o código do canal. Nesse caso, C será um código de comprimento n e dimensão r. Esse código será chamado de* ***Código de Reed-Solomon*** *de comprimento n e dimensão r definido por* $\alpha_1, \alpha_2, ..., \alpha_n$*.*

Uma matriz geradora de C será dada por

$$G = \begin{pmatrix} T(1) \\ T(x) \\ ... \\ T(x^{r-1}) \end{pmatrix} = \begin{pmatrix} \alpha_1^0 & \alpha_2^0 & ... & \alpha_n^0 \\ \alpha_1^1 & \alpha_2^1 & ... & \alpha_n^1 \\ ... & ... & ... & ... \\ \alpha_1^{r-1} & \alpha_2^{r-1} & ... & \alpha_n^{r-1} \end{pmatrix}.$$

Um aspecto interessante desse código é que podemos dar uma conta inferior para a distância mínima do código.

Observe que, para qualquer $c \neq 0$ uma palavra do código, temos que existe um polinômio $p(x) \in K[x]$ tal que $c = (p(\alpha_1),\ p(\alpha_2),\ ...,\ p(\alpha_n))$.

Temos que

$$w(c) = |i \in \{0, 1, ..., n-1\};\ c_i \neq 0|$$
$$w(c) = |i \in \{0, 1, ..., n-1\};\ p(\alpha_i) \neq 0|$$
$$w(c) = n - |i \in \{0, 1, ..., n-1\};\ p(\alpha_i) = 0|.$$

E como $|i \in \{0, 1, ..., n-1\};\ p(\alpha_i) = 0| \leq r - 1$, segue que: $w(c) \geq n - (r-1) = n - r + 1$.

Exemplo 4.3 (Código do Mariner 9)**.** *O código utilizado na espaçonave Mariner 9 é um código definido sobre $\mathbb{F}_2$ que faz parte de uma família de códigos definidos como* ***Código de Reed-Muller de Primeira Ordem****.*

Dado um $m \in \mathbb{N}$, considere os elementos de ${\mathbb{F}_2}^m$ vistos como vetores colunas. Organize tais colunas de modo que o elemento nulo seja a última coluna à direita. Obtém-se uma matriz $m \times 2^m$, que será denotada G_m.

Construímos então a matriz $(m+1) \times 2^m$, em que os elementos da primeira linha serão iguais a 1 e, abaixo dessa linha, a matriz G_m aparece como um bloco.

O código gerado pela matriz G será denotado $R(1, m)$.

4.2 Códigos cíclicos

A seguir, serão estudados alguns códigos chamados de códigos cíclicos. Eles constituem uma família particular de códigos lineares. Alguns resultados não serão provados pois tratam-se de generalizações do estudo já feito para códigos lineares.

Definição 4.10. *Um código linear $C \subset K^n$ é chamado de cíclico se para todo $c = (c_0, c_1, ..., c_{n-1}) \in C$, temos que $(c_{n-1}, c_0, ..., c_{n-2})$ também pertence a C.*

Observe que os K-espaços vetoriais K^n e R_n são isomorfos.

Considere o isomorfismo:

$$\begin{array}{rccc} V: & K^n & \to & R_n \\ & (a_0, a_1, ..., a_n) & \mapsto & [a_0x^0 + a_1x^1 + ... + a_nx^n] \end{array}$$

.

Da definição de códigos cíclicos, sabemos que, se temos $c = (c_0, c_1, ..., c_{n-1}) \in C$, então $(c_{n-1}, c_0, ..., c_{n-2})$ também pertence a C.

Analisando a função V, podemos dizer que se $[a_0x^0 + a_1x^1 + ... + a_nx^n] \in R_n$, então $[x]\,[a_0x^0 + a_1x^1 + ... + a_nx^n]$ também pertence a R_n.

Teorema 4.3. *Um código linear $C \subset K^n$ será cíclico se, e somente se, $v(C)$ for um subespaço vetorial de K^n fechado pela multiplicação por $[x]$.*

Em outras palavras, um código linear $C \subset K^n$ será cíclico se, e somente se, $v(C)$ for um ideal de R_n. Teremos, então, que $v(C)$ é gerado por um polinômio $g(x) \in K[x]$ que divide $x^n - 1$.

Definição 4.11. *Seja $C \subset K^n$ um código cíclico tal que $v(C)$ é gerado pelo polinômio $g(x) \in K[x]$ que divide $x^n - 1$. Chamamos $g(x)$ de polinômio gerador de C.*

Proposição 4.2. *Seja $I = \langle g(x) \rangle$ tal que $g(x)$ divide $x^n - 1$. Então $[g(x)], [xg(x)], [x^2 g(x)]$, ... , $[x^{n-s-1} g(x)]$ formam uma base de I como K-espaço vetorial.*

Teorema 4.4. *Seja $C \subset K^n$ um código cíclico com polinômio gerador $g(x) = g_0 x^0 + g_1 x^1 + ... + g_s x^s$ de grau s. Então $dim_K C = n - s$.*

Teorema 4.5. *Seja $g(x) = g_0 x^0 + g_1 x^1 + ... + g_s x^s$ um divisor de $x^n - 1$ de grau s. Seja $I = \langle g(x) \rangle$. O código $C = V^{-1}(I)$ tem matriz geradora*

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

A matriz G é uma matriz $(n - s) \times n$.

Exemplo 4.4 (Código de Golay)**.** *O código de Golay com parâmetros fundamentais $(23, 12, 7)$ é um código cíclico definido em $\mathbb{F}_2$ e gerado por qualquer um dos polinômios $f(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$ ou $g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$.*

Pode-se verificar que $x^{23} + 1 = f(x) \cdot g(x) \cdot (x + 1)$ em $\mathbb{F}_2$

Referências

[1] BAHUT, Richard E. **Theory and Practice of Error Control Codes**, Reading: Addison-Wesley, 1984. 500p.

[2] COUTINHO, Marianda de Almeida N. **Corpos Finitos e Códigos Corretores de Erros**. Juíz de Fora: Universidade Federal de Juiz de Fora, 2014. 73p

[3] HEFEZ, Abramo; VILLELA, Maria Lúcia T. **Códigos Corretores de Erros.** 2.ed. Rio de Janeiro: IMPA, 2008. 216p.

[4] MILES, César P. **Breve introdução à Teoria dos Códigos Corretores de Erros.** Disponível em http://www.sbm.org.br/docs/coloquios/NE-1.04.pdf. Acesso em: 30 jun. 2016.

[5] PLESS, Vera. **Introduction to the Theory of Error-correcting Codes.** John Wiley and Sons, 1982. 169p.

[6] STEWART, Ian. **Galois Theory.** 3.ed. Chapman and Hall, 2004. 288p.