MENSAGENS CODIFICADAS ATRAVÉS DE ISOMORFISMOS

Natham Cândido de Oliveira(1)

Universidade Federal de Campina Grande, nathan.oliveia_@hotmail.com

RESUMO: Este trabalho é constituído por uma pesquisa bibliográfica que explana sobre o procedimento conhecido como criptografia utilizando alguns estudos das transformações lineares de espaços vetoriais do curso de álgebra linear. Consideramos no presente trabalho que o público alvo já possua algum entendimento sobre os conceitos mais básicos da teoria dos espaços vetoriais de álgebra linear. Entretanto, abordaremos no decorrer do trabalho alguns conceitos que serão de grande estima no entendimento dos processos utilizados nas transformações lineares para a criptografia. No que se trata das transformações lineares iremos abordar ao mesmo tempo os conceitos e propriedades que classificam uma transformação linear realizando exemplificações de operadores no $\mathbb{R}^2$, buscamos também esclarecer um pouco no que diz respeito as propriedades e definições de núcleo e imagem de uma transformação linear, e com isso, definiremos o isomorfismo como uma transformação linear invertível, como a transformação linear é injetora e sobrejetora logo ela é bijetora e portanto, é um isomorfismo, nesse caso, como os espaços vetoriais de saída e chegada são iguais, dizemos que a transformação é um automorfismo. Após trabalhar todos os conceitos necessários para perpetrarmos a criptografia, iremos perceber que a criptografia é um método de gravar e transmitir dados de uma forma que somente os destinatários, possam decodificar e processar. No entanto, a maioria dos algoritmos podem ser quebrados e a informação ser desvendada. O algoritmo é o conjunto de códigos que definem como são feitas as codificações e decodificações. Os algoritmos utilizados em nosso trabalho são por meio de isomorfismo. A aplicação de isomorfismo como algoritmo criptográfico ocorrerá de maneira simples, com objetivo de tornar-se visível a didática do uso dos isomorfismos em criptografia.

Palavras chaves: Transformações Lineares, isomorfismo, criptografia.

INTRODUÇÃO

As transformações lineares é objeto de estudos em álgebra linear e muitas outras áreas da matemática, é também bastante utilizadas em aplicações em diversas áreas, dentre as aplicações das transformações lineares, destacaremos neste trabalho uso como algoritmos de criptografia. Iniciamos o trabalho abordando uma pequena introdução sobre as transformações lineares, apresentado suas propriedades, mostrando as definições de núcleo, imagem, isomorfismo e isomorfismo inverso.

Não iremos realizar demonstrações, pois são vistas nas disciplinas de álgebra linear e também estamos levando em consideração no presente trabalho que, o público alvo já possua algum entendimento sobre os conceitos mais fundamentais da teoria dos espaços vetoriais, iremos apenas apresentar alguns exemplos dos conceitos afim de simplificar a compreensão.

Em nossa volta tem sempre tecnologia, mas não notamos o quanto a matemática está presente concomitante com a mesma. Constantemente estamos tentando proteger informações, arquivos, conta de banco e redes sociais por meios senhas, assim como também

em compras por meio de plataforma online através mensagens e dados indecifráveis para que terceiros não tenha acesso a essas informações.

O algoritmo é o conjunto de regras que definem como são feitas as codificações e decodificações e neste trabalho algoritmo utilizado será isomorfismos. Existem diversos algoritmos criptográficos que utilizam outras áreas da matemática, como por exemplo, a teoria dos números e a matemática discreta. O exemplo que iremos trabalhar embaralha de duas em duas letras. Apesar de ter uma pequena complexidade o algoritmo criptográfico apresentado, os espaços vetoriais no R^n possibilita obter uma infinidade de combinações de números o que dificultaria a decodificação por terceiros.

METODOLOGIA

Trata-se de uma proposta de ensino como base nos estudos de transformações lineares de espaços vetoriais do curso de Álgebra Linear, através de exemplo de criptografia por meio de definições teórica de maneira didática e objetiva. O estudo ocorreu no período de agosto de 2018.

Iremos trabalhar primeiro a teoria de espaços vetoriais sobre $\mathbb{R}$, cuja definição e resultados serão abordados a seguir.

Consideremos uma transformação linear pela seguinte definição: U e V espaços vetoriais sobre K, uma aplicação ou função.

$$T:U \rightarrow V$$

É denominada transformação linear se cumprir as seguintes propriedades:

i) $T(\alpha v) = \alpha T(v)$, $\alpha \in K$ e $v \in V$;

ii) $T(u + v) = T(u) + T(v)$, $\forall\, u, v \in V$.

Quando U = V a transformação linear é chamada operador linear.

Consideremos o exemplo a seguir:

Exemplo 01: seja em $\mathbb{R}^2$ a função T definida por:

$$T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

$$(x, y) \rightarrow T(x, y) = (-x, y)$$

Verifiquemos se a função T cumpri as propriedades necessárias:

Seja $\alpha \in \mathbb{R}$ e $u = (x1, y1)$, $v = (x2, y2) \in \mathbb{R}^2$, temos:

i) $T(\alpha u) = T(\alpha x1, \alpha y1) = (-(\alpha x1), \alpha y1) = \alpha (-x1, y1) = \alpha\, T(x1, y1) = \alpha\, T(u)$

ii) $T(u + v) = T((x1, y1) + (x2, y2)) = (-(x1 + x2) + (y1 + y2)) = (-x1 - x2) + (y1 + y2)) = (-x1 + y1) + (-x2 + y2) = T(x1, y1) + T(x2, y2)$

Logo como foi satisfeito (i) e (ii), segue que T é uma transformação linear.

Definiremos núcleo de uma transformação linear como sendo:

Definição 01: Sejam U e V espaços vetoriais sobre $\mathbb{R}$ e $T:U \rightarrow V$ uma transformação linear, que será titulado por Ker(T) e denomina-se núcleo de T o seguinte subconjunto de U.

$$Ker(T) = \{u \in U / T(u) = 0\}$$

Exemplo 02: Considere T: $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ definida T(x, y) = (x+y, x-y), encontre o Ker(T).

Solução:

Por definição temos: $Ker(T) = \{u \in U / T(u) = 0\}$, logo;

$Ker(T) = \{(x, y) \in \mathbb{R}^2 / T(x, y) = (0, 0)\}$

$Ker(T) = \{(x, y) \in \mathbb{R}^2 / (x + y, x - y) = (0, 0)\}$

$Ker(T) = \{(x, y) \in \mathbb{R}^2 / (x + y = 0) \text{ e } (x - y = 0)\}$

$$\begin{cases} x + y = 0 & (I) \\ x - y = 0 & (II) \end{cases}$$

Por (I) e (II) temos que: $2x = 0$, isto implica que $x = 0$.

Por (II) temos que: $x = y$, segue que $y = 0$.

$$\text{Logo } Ker(T) = \{(0, 0)\}$$

Definiremos imagem de uma transformação linear como sendo:

Definição 02: Sejam U e V espaços vetoriais sobre $\mathbb{R}$ e $T: U \rightarrow V$ uma transformação linear. Indica-se por Im(T) e denomina-se imagem de T, o seguinte subconjunto de V:

$$Im(T) = \{v \in V / V = T(u) \text{ para algum } u \in U\}$$

Exemplo 03: Considere T: $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ definida T(x, y) = (x+y, x-y), encontre o Im(T).

Solução:

Por definição temos: $Im(T) = \{v \in V / V = T(u) \text{ para algum } u \in U\}$, logo;

$Im(T) = \{T(x, y) / (x, y) \in \mathbb{R}^2\}$

$Im(T) = \{(x+y, x-y) / x, y \in \mathbb{R}^2\}$

$Im(T) = [(1, 1) + (1, -1)]$, pois:

$(x+y, x-y) = (x, x) + (y, -y)$

$(x+y, x-y) = x(1, 1) + y(1, -1)$.

$$\text{Segue que } Im(T) = \mathbb{R}^2.$$

Definição 03: Transformação Linear Injetora; Dada uma Transformação Linear $T:U \rightarrow V$, dizemos que T é injetora se dados $u_1 \in U$, $u_2 \in U$ com $T(u_1) = T(u_2)$ tivermos $u_1 = u_2$, ou equivalentemente, T é injetora se dados $u_1, u_2 \in U$ com $u_1 \neq u_2$, então $T(u_1) \neq T(u_2)$.

Teorema 01: A transformação linear T é injetora se, somente se, $Ker(T) = \{0\}$.

Definição 04: Transformação Linear Sobrejetora; Dada uma transformação linear $T:U \rightarrow V$, T é sobrejetora se a imagem de T coincidir com V, ou seja, $T(U) = V$.

Teorema 02: Teorema do Núcleo e da Imagem; Sejam U e V espaços vetoriais sobre $\mathbb{R}$ de dimensões finitas e $T:U \rightarrow V$ uma Transformação Linear então:

$$\dim U = \dim Ker(T) + \dim Im(T).$$

Denominaremos isomorfismo do espaço vetorial U no espaço vetorial V em $\mathbb{R}$ uma Transformação Linear $T:U \rightarrow V$ que seja bijetora.

Teorema 03: Se uma transformação linear $T:U \rightarrow V$, com U e V espaços vetoriais sobre $\mathbb{R}$ é um Isomorfismo, então: $\dim U = \dim V$.

Teorema 04: Transformação Linear Inversa; Se $T:U \rightarrow V$ é uma transformação linear e um isomorfismo, sua inversa $T^{-1}:U \rightarrow V$, também será uma transformação linear e um isomorfismo.

Proposição 01: Imagem Inversa, seja $T:U \rightarrow V$ uma transformação linear e W e Z subespaços de U e V respectivamente. Então:

i) T(W) é subespaço de V;

ii) $T^{-1}(Z)$ é um subespaço de U.

Exemplo 04: Sejam $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ definida por $T(x, y) = (x + y, x - y)$, encontre $T^{-1}(x, y)$.

Solução:

Pelo exemplo 02 e 03, temos que é bijetiva, iremos agora definir $T^{-1}(x, y)$. Dado $(a, b) \in \mathbb{R}^2$, existe um único $(x, y) \in \mathbb{R}^2$, tal que:

$T(x, y) = (a, b) \Leftrightarrow (x, y) = T^{-1}(a, b)$, portanto:

$(x + y, x - y) = (a, b)$

$$\begin{cases} x + y = a & (I) \\ x - y = b & (II) \end{cases}$$

Por (I) temos que:

$$x = a - y \qquad (*)$$

Substituindo $x = a - y$ em (II) temos:

$$(a - y) - y = b$$

$$a - 2y = b$$

$$y = \frac{a-b}{2}$$

Agora substituindo $y = \frac{a-b}{2}$ em (*), temos:

$$x = a - \left(\frac{a-b}{2}\right)$$

$$x = \frac{2a-a+b}{2}$$

$$x = \frac{a+b}{2}$$

Logo

$$(x, y) = T^{-1}(a, b)$$

$$\left(\frac{a+b}{2}, \frac{a-b}{2}\right) = T^{-1}(a, b)$$

$$T^{-1}(x, y) = \left(\frac{x+y}{2}, \frac{x-y}{2}\right)$$

Devemos entender que o algoritmo é o conjunto de regras que definem como são feitas as cifragem e decifragem. Neste trabalho os algoritmos que iremos utilizar será baseado em definições de isomorfismos.

RESULTADOS E DISCUSSÃO

A aplicação do isomorfismo como algoritmo criptográfico ocorrerá de maneira simplificada, com objetivo de revelar a didática do isomorfismo.

Consideremos que tal mensagem a seguir tenha grande valor de especulação, como por exemplo compras feitas pela internet onde é necessário enviar dados pessoas, assim como dados de cartão de credito. Neste processo de criptografia que iremos apresentar é necessário que o remetente e o destinatário sejam conhecidos, assim como todos os outros processo de criptografia.

Iremos exemplificar o processo de criptografia com um simples exemplo:

Mensagem: UFCG CES CUITE

Tabela 01: Tabela de conversão.

A	B	C	D	E	F	G	H	I	J	K	L	M
-1	4	7	3	-2	5	8	2	6	9	12	15	10

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
-3	11	17	-4	0	13	25	29	30	1	-5	22	35

Fonte: Autoria própria

Cada letra está relacionada com um número, iremos realizar a primeira cifragem.

29 5 7 8 7 -2 13 7 29 6 25 -2

O algoritmo que usaremos é da transformação linear do $\mathbb{R}^2$.

$$T(x, y) = (x + 3y, x - 2y)$$

Verifiquemos primeiramente se T é um isomorfismo:

1) $\text{Ker}(T) = \{(x, y) \in \mathbb{R}^2 \ / \ T(x, y) = (0, 0)\}$

$$\text{Ker}(T) = \{(x, y) \in \mathbb{R}^2 \ / \ (x + 3y, x - 2y) = (0, 0)\}$$

$$\text{Ker}(T) = \{0, 0\}$$

Logo a dim Ker(T) = 0

Pelo Teorema do Núcleo e Imagem, temos:

$$\dim V = \dim \text{Ker}(T) + \dim \text{Im}(T)$$

$$2 = 0 + \dim \text{Im}(T)$$

$$\dim \text{Im}(T) = 2$$

Portanto [T] é inversivel, logo T é um isomorfismo.

Agora iremos tomar de dois a dois números primeira cifragem e aplicar em T.

T(29, 5) = (29 + 3*5, 29 – 2*5) = (44, 19);

T(7, 8) = (7 + 3*8, 7 – 2*8) = (31, -9);

T(7, -2) = (7 + 3*(-2), 7 - 2*8) = (1, 11);

T(13, 7) = (13 + 3*7, 13 – 2*7) = (34, -1);

T(29, 6) = (29 + 3*6, 29 – 2*6) = (47, 17);

T(25, -2) = (25 + 3*(-2), 25 – 2*(-2)) = (19, 29).

Logo após da segunda cifragem, temos:

40 19 31 -9 1 11 34 -1 47 17 19 29

Esta é a mensagem recebida pelo destinatário. Como é de domínio comum ao remetente e do destinatário, cabe ao destinatário decifrar a mensagem.

Assim o destinatário deverá encontrar o isomorfismo inverso de da transformação, usaremos um processo rápido e prático.

$$T(x, y) = (a, b) \Leftrightarrow (x, y) = T^{-1}(a, b)$$

$$(x + 3y, x - 2y) = (a, b)$$

$$\begin{cases} x + 3y = a & (1) \\ x - 2y = b & (2) \end{cases}$$

Por (1) temos:

$$x = a - 3y$$

Aplicando $x = a - 3y$ em (2), temos:

$$a - 3y - 2y = b$$

$$-5y = b - a$$

$$y = \frac{a-b}{5}$$

Agora substituindo $y = \frac{a-b}{5}$, em $x = a - 3y$ obtemos:

$$x = a - 3*\left(\frac{a-b}{5}\right)$$

$$x = a - \left(\frac{3a-3b}{5}\right)$$

$$x = \frac{5a - 3a + 3b}{5}$$

$$x = \frac{2a + 3b}{5}$$

Logo, $(x, y) = T^{-1}(a, b)$

$$\left(\frac{2a + 3b}{5}, \frac{a-b}{5}\right) = T^{-1}(a, b)$$

$$T^{-1}(x, y) = \left(\frac{2x + 3y}{5}, \frac{x - y}{5}\right)$$

O destinatário necessitara repeti o mesmo processo, que consiste em tomar dois a dois números e aplicar em $T^{-1}(x, y)$.

$T^{-1}(40, 19) = \left(\frac{2*44 + 3*19}{5}, \frac{44 - 19}{5}\right) = (29, 5)$;

$T^{-1}(31, -9) = \left(\frac{2*31 + 3*(-9)}{5}, \frac{31 - (-9)}{5}\right) = (7, 8)$;

$T^{-1}(1, 11) = \left(\frac{2*1 + 3*11}{5}, \frac{1 - 11}{5}\right) = (7, -2)$;

$T^{-1}(34, -1) = \left(\frac{2*34 + 3*(-1)}{5}, \frac{34 - (-1)}{5}\right) = (13, 7)$;

$T^{-1}(47, 17) = \left(\frac{2*47 + 3*17}{5}, \frac{47 - 17}{5}\right) = (29, 6)$ e

$T^{-1}(19, 29) = \left(\frac{2*19 + 3*29}{5}, \frac{19 - 29}{5}\right) = (25, -2)$.

Após aplicar a mensagem cifrada em T^{-1} o destinatário, obterá:

29 5 7 8 7 -2 13 7 29 6 25 -2

Note que a mensagem que o destinatário obtém, após aplicar em T^{-1} é igual ao da primeira cifragem, utilizando a tabela 01 e finalmente o texto decodificado é:

UFCG CES CUITE

CONSIDERAÇÕES FINAIS

Utilizamos transformações lineares isomórficas na criptografia porque o conceito da criptografia é de criar uma mensagem indecifrável em uma ponta, mas que seja possível de ser decodificada pelo destinatário. Para isso necessitamos que a transformação linear possua uma inversa, logo utilizando o teorema da transformação linear inversa e um isomorfismo inverso, conseguimos realizar as codificações através de exemplificações simples, mas norteando para um trabalho mais elaborado, podendo utilizar matrizes e outros recursos.

Note que o algoritmo que trabalhamos, embaralha duas em duas letras, apesar de ter uma pequena complexidade o algoritmo criptográfico aqui tratado, os espaços vetoriais no $\mathbb{R}^n$ possibilita obter uma infinidade de combinações de números, de dois em dois, até n em n, o que dificultaria a decodificação por terceiros. Logo a utilização do isomorfismo de transformação linear como criptográfico e de real aplicação.

REFERÊNCIAS BIBLIOGRÁFICAS

CALLIOLI, Carlos A. e outros, **Álgebra Linear e Aplicações.** 6. ed. São Paulo - SP: Atual Editora, 1990.

STEINBRUCH, Alfredo e Winterle, Paulo, **Álgebra linear.** 2 ed. São Paulo - SP: Pearson Education do Brasil, 1987.

BOLDRINI, José Luiz e outros, **Álgebra linear.** 3 ed. São Paulo – SP: Editora Harbra LTDA, 1986.