UNIVERSIDADE FEDERAL DE SÃO JOÃO DEL-REI – UFSJ

NÚCLEO DE EDUCAÇÃO À DISTÂNCIA

DEPARTAMENTO DE MATEMÁTICA E ESTATÍSTICA – DEMAT

EDUARDO SCHWARTZ

TRANSFORMAÇÕES LINEARES NO PROCESSAMENTO DE IMAGENS E NA CRIPTOGRAFIA

SÃO JOÃO DEL-REI

2016

EDUARDO SCHWARTZ

TRANSFORMAÇÕES LINEARES NO PROCESSAMENTO DE IMAGENS E NA CRIPTOGRAFIA

Trabalho de conclusão de curso, apresentado como requisito parcial para obtenção do título de Licenciado em Matemática, do curso de Licenciatura em Matemática a Distância, da Universidade Federal de São João Del-Rei.

Orientador: Prof. Me. Stênio Vidal L. R. de Menezes

SÃO JOÃO DEL-REI

2016

EDUARDO SCHWARTZ

TRANSFORMAÇÕES LINEARES NO PROCESSAMENTO DE IMAGENS E NA CRIPTOGRAFIA

Trabalho de conclusão de curso, apresentado como requisito parcial para obtenção do título de Licenciado em Matemática, do curso de Licenciatura em Matemática a Distância, da Universidade Federal de São João Del-Rei.

Os componentes da banca de avaliação, abaixo identificados, consideram este trabalho aprovado.

BANCA EXAMINADORA

_____

Prof.º Me. Stênio Vidal L. R. de Menezes

UFSJ

_____

Prof.ª Ma. Lorena Mara Costa Oliveira

UFSJ

Data da aprovação: São João del-Rei, 26 de novembro de 2016.

A minha esposa e minha filha.

AGRADECIMENTOS

Agradeço a todos aqueles que me apoiaram nesta fase de crescimento da vida. A todos aqueles que de forma direta ou indireta me estenderam sua mão, me incentivaram, perceberam e compreenderam este momento, meus agradecimentos. Agradeço também ao meu orientador Prof. Me. Stênio Vidal L. R. de Menezes pela formidável orientação neste trabalho.

RESUMO

Neste trabalho estudamos as transformações lineares e demonstramos dois tipos de aplicações destas no âmbito computacional. A primeira mostra como as transformações lineares podem ser aplicadas para manipular imagens através de processos como rotação, translação, expansão, reflexão e cisalhamento. A segunda aplicação demonstra como as transformações lineares podem ser utilizadas para criptografar e decifrar mensagens nos diversos espaços vetoriais.

Palavras-chave: Transformação linear, Manipulação de imagem, Criptografia.

ABSTRACT

In this work we study the linear transformations and demonstrate two types of applications in the computational environment. The first shows how the linear transformation can be applied for manipulating images through processes such as rotation, translation, expansion, shearing and reflection. The second application shows how linear transformation can be used to encrypt and decrypt messages in different vector spaces.

Keywords: Linear transformation, Image manipulation, Encryption.

SUMÁRIO

1 – INTRODUÇÃO

As transformações lineares são de fundamental importância nos estudos de Álgebra Linear, Cálculo, Equações Diferenciais, Geometria Diferencial e muitas outras áreas da Matemática, mais também, é de grande utilidade em aplicações nas mais diversas áreas. Alguns exemplos disto são os modelos lineares de regressão utilizados pelo site de buscas na internet Google, onde ajuda os pesquisadores a determinar padrões nas informações coletadas e as pesquisas médicas, que usam as transformações lineares para prever resultados importantes, como os efeitos de medicamentos em pacientes. Possuem importantes aplicações no mundo da computação gráfica, manuseando os pixels na tela do computador dando vida as imagens.

No capítulo 2 iniciaremos o trabalho apresentado uma breve introdução sobre as transformações lineares, apresentado suas propriedades, mostrando as definições de núcleo e imagem e alguns tipos de transformações.

No capítulo 3 veremos como as transformações lineares manipulam objetos, como imagens por exemplo, criando os efeitos de expansão, contração, rotação, reflexão e cisalhamento.

No capítulo 4 focamos em como as transformações lineares podem ser utilizadas para criptografar e decriptografar mensagens dentro de aplicações da informática.

2 – TRANSFOMAÇÕES LINEARES

O objetivo deste capítulo é dar uma visão geral sobre as transformações lineares, ou seja, pretende-se definir uma transformação linear, suas propriedades, seus componentes, as leis de transformação e sua equivalência com as funções.

Os espaços vetoriais, onde ocorrem as transformações lineares, já são bem conhecidos inclusive pela maioria das pessoas que cursaram o ensino médio, dispensando assim a sua apresentação neste trabalho. Não serão feitas provas nem demonstrações, pois estas são vistas nas disciplinas de Álgebra Linear, apenas alguns exemplos dos conceitos serão mostrados afim de simplificar a compreensão.

Segundo (KULDEEP, 2014, P.341), em Matemática, uma **transformação linear** é um tipo particular de função entre dois espaços vetoriais que preserva as operações de adição vetorial e multiplicação por escalar. Uma transformação linear também pode ser chamada de **aplicação linear** ou **mapa linear.**

Sejam V e W espaços vetoriais. Para dizer que T é uma transformação linear do espaço vetorial V no espaço vetorial W, escreve-se $T: V \to W$. Sendo T uma função, cada vetor $v \in V$ tem um único vetor imagem $w \in W$, que será indicado por $w = T(\vec{v})$.

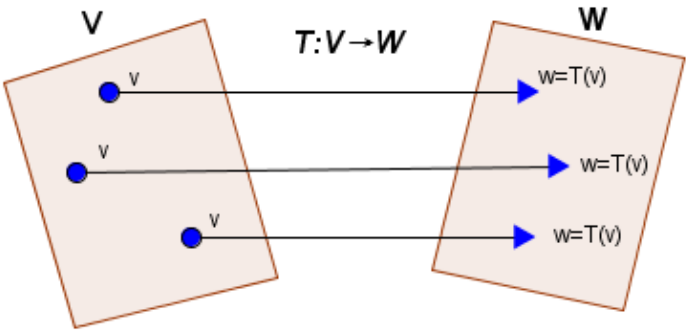


Figura 1- Transformação linear de V em W

Definição

Uma função $T: V \to W$, onde V e W são espaços vetoriais sobre um corpo K, é dita transformação linear se, para todo vetor $u, v \in V$ e para todo $\alpha \in K$, tem-se os seguintes axiomas:

1) $T(u + v) = T(u) + T(v)$

2) $T(\alpha \cdot v) = \alpha \cdot T(v)$

As propriedades 1 e 2 são equivalentes à: $T(u + \alpha \cdot v) = T(u) + \alpha \cdot T(v)$ (Hefez, 2012, P.124)

2.1 Propriedades das transformações lineares

Sejam V e W espaços vetoriais sobre um corpo K, T uma transformação linear de V em W e u e v vetores em V. Então vale o seguinte:

I. $\mathbf{T(0) = 0}$, onde 0 é o vetor nulo

II. $\mathbf{T(-u) = -T(u)}$

III. $\mathbf{T(u - v) = T(u) - T(v)}$

IV. Se $T: V \to W$ for uma transformação linear e $\{v_1, v_2, \dots, v_n\}$ uma base de V existem $k_1, k_2, \dots, k_n$ números escalares, tais que:

$$\boldsymbol{v = k_1 v_1 + k_2 v_2 + \cdots + k_n n_n}$$

$$\mathbf{T(v) = T(k_1 v_1 + k_2 v_2 + \cdots + k_n n_n) = k_1 T(v_1) + k_2 T(v_2) + \cdots + k_n T(v_n)}$$

Sempre é possível obter a imagem T(v) de qualquer $v \in V$, como sendo uma combinação linear dos vetores $\mathbf{T(v_1), T(v_2), \dots, T(v_n)} \in W$.

2.2 Imagem e Núcleo de uma transformação linear

Assim como nas funções com números reais, as transformações lineares possuem os mesmos elementos de domínio, contradomínio e imagem.

Sejam V e W espaços vetoriais sobre um corpo K e T uma transformação linear de V em W, a imagem de T, representado por Im(T), é o conjunto de todos os vetores de W da forma T(v), para algum $v \in V \longrightarrow \text{Im(T)} = \{w \in W | w = T(v)\}$.

Sejam V e W espaços vetoriais sobre um corpo K e T uma transformação linear de V em W, o núcleo de T, representado por N(T) ou Ker(T), é o subconjunto do domínio formado pelos vetores que são levados ao vetor nulo do contradomínio. $N(T) = \{v \in V | T(v) = 0\}$

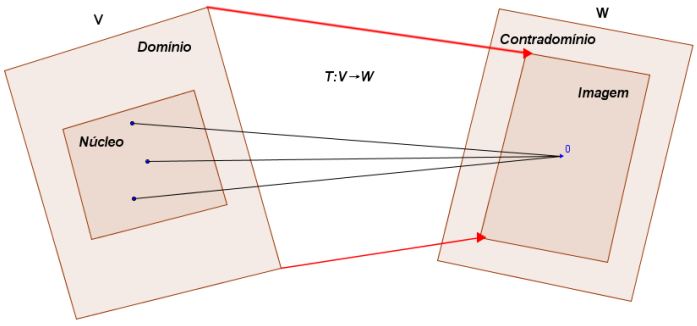


Figura 2

A importância de conhecermos a imagem e o núcleo de uma transformação linear é que através deles conhecemos qual informação foi transformada e qual foi perdida.

Teorema do núcleo e da imagem: Sejam V e W espaços vetoriais de dimensão finita. Seja T: V → W uma transformação linear, então a dimensão do domínio equivale a soma das dimensões do núcleo da transformação com a dimensão da imagem da transformação:

$$\mathbf{dim(V) = dim\big(N(T)\big) + dim\big(Im(T)\big)}$$

2.3 Lei de transformação

A lei de transformação define o valor de cada um dos componentes do vetor na imagem. Tomemos como exemplo a transformação $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ definida pela lei de transformação $T\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{pmatrix} -y \\ x \end{pmatrix}$.

Segundo a lei desta transformação específica, o componente x do vetor deverá ser substituído pelo valor inverso do componente y, e o componente y pelo valor de x.

Digamos que queremos transformar o vetor $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ usando a lei de transformação acima, como ficaria $T\left(\begin{bmatrix} 1 \\ 2 \end{bmatrix}\right)$? Substituindo $x = 1$ e $y = 2$ em:

$$T\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{pmatrix} -y \\ x \end{pmatrix} \rightarrow T\left(\begin{bmatrix} 1 \\ 2 \end{bmatrix}\right) = \begin{pmatrix} \mathbf{-2} \\ \mathbf{1} \end{pmatrix}$$

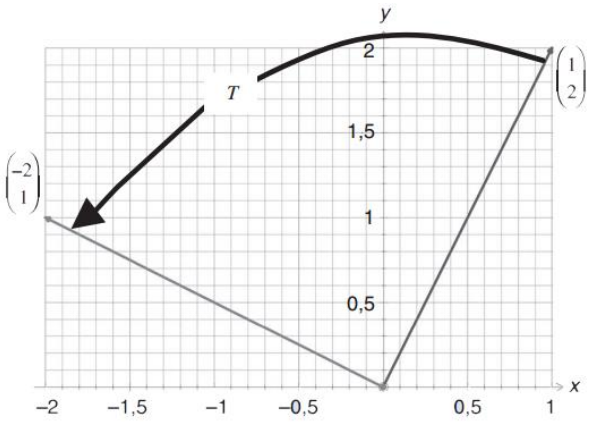


Figura 2 – Desenhando os dois vetores no plano cartesiano
Fonte: (KULDEEP, 2014, P.341)

Verificando se uma transformação é linear ou não

Exemplo 1[1]: Dado uma transformação linear $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, onde a Lei de transformação dos vetores x_1 e x_2 é $T(x_1, x_2) = (x_1 + x_2, 3 \cdot x_1)$. Verifique se é uma transformação linear.

- Verificando a definição 1

[1] Transformações lineares – Khan Academy - https://www.youtube.com/watch?v=wEUj7cZtHYo

Tomemos dois vetores $u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}, v = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$; $u, v \in \mathbb{R}^2$

$u + v = \begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \end{bmatrix} \rightarrow T(u+v) = T\left(\begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \end{bmatrix}\right) = \begin{bmatrix} u_1 + u_2 + v_1 + v_2 \\ 3u_1 + 3v_1 \end{bmatrix}$

como: $T(u) = T\left(\begin{bmatrix} u_1 \\ u_2 \end{bmatrix}\right) = \begin{bmatrix} u_1 + u_2 \\ 3u_1 \end{bmatrix}$ e $T(v) = T\left(\begin{bmatrix} v_1 \\ v_2 \end{bmatrix}\right) = \begin{bmatrix} v_1 + v_2 \\ 3v_1 \end{bmatrix}$

logo: $\mathrm{T}(u) + \mathrm{T}(v) = \begin{bmatrix} \mathrm{u}_1 + \mathrm{u}_2 + v_1 + v_2 \\ 3\mathrm{u}_1 + 3v_1 \end{bmatrix} = \mathrm{T}(\mathrm{u} + v)$

- Verificando a definição 2

Tomemos um vetor $u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$ e um escalar k ; $u \in \mathbb{R}^2, c \in \mathbb{R}$

$k \cdot u = \begin{bmatrix} k \cdot u_1 \\ k \cdot u_2 \end{bmatrix} \rightarrow T(k \cdot u) = \begin{bmatrix} k \cdot u_1 + k \cdot u_2 \\ 3k \cdot u_1 \end{bmatrix} = k \cdot \underbrace{\begin{bmatrix} u_1 + u_2 \\ 3u_1 \end{bmatrix}}_{T(u)}$

logo: $T(k \cdot u) = k \cdot T(u)$

Portanto pela verificação das definições 1 e 2, que *T* é uma transformação é linear.

No exemplo 1, a transformação T: $V \rightarrow$ V ocorre no mesmo espaço vetorial, ou seja o domínio e o contra domínio são os mesmo, este tipo de transformação é chamado de **operação linear** ou **endomorfismo** (morfismo de um objeto matemático nele mesmo).

É importante perceber que nem toda transformação é uma transformação linear, para isso, é necessário que as duas definições de transformações lineares sejam válidas.

Exemplo 2: Verificar se a transformação $T(x, y) = (x^2 + y^2, x)$, é uma transformação linear.

Tomemos dois vetores $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$; $x, y \in \mathbb{R}^2$

- Propriedade aditiva

$T(x_1 + x_2, y_1 + y_2) = ((x_1 + x_2)^2 + (y_1 + y_2)^2, x_1 + x_2)$

$T(x_1 + x_2, y_1 + y_2) = ({x_1}^2 + 2x_1x_2 + {x_2}^2 + {y_1}^2 + 2y_1y_2 + {y_2}^2, x_1 + x_2)$

$T(x_1 + x_2, y_1 + y_2) = ({x_1}^2 + {y_1}^2, x_1) + ({x_2}^2 + {y_2}^2, x_2) + (2x_1x_2 + 2y_1y_2, x_1 + x_2)$

$T(x_1 + x_2, y_1 + y_2) = T(x_1, y_1) + T(x_2, x_2) + (2x_1x_2 + 2y_1y_2, x_1 + x_2)$

A propriedade aditiva não foi satisfeita.

- Multiplicação por escalar

$T(\alpha \cdot x, \alpha \cdot y) = \alpha \cdot T(x, y)$

$T(\alpha \cdot x, \alpha \cdot y) = (\alpha^2 x^2 + \alpha^2 y^2, \alpha \cdot x)$

$T(\alpha \cdot x, \alpha \cdot y) = \alpha(a \cdot x^2 + a \cdot y^2, x)$

A propriedade de multiplicação por escalar não foi satisfeita.

Como nenhuma das propriedades foram satisfeitas, logo não é uma transformação linear, ou seja, o valor da saída da função não se modifica proporcionalmente ao valor da entrada. Como a definição 1 não foi atendida, não era necessário verificar a segunda definição, e podemos concluir que existem transformações que não são lineares.

2.4 Transformações Lineares Compostas

A transformação linear composta ocorre quando é efetuada uma transformação, não de um vetor de origem, mas sim de um vetor criado por uma outra transformação. Sejam $T: \mathbb{R}^m \to \mathbb{R}^n$ e $S: \mathbb{R}^n \to \mathbb{R}^p$ duas transformações lineares, podemos aplicar T e depois S para formar a composta das duas transformações que denotamos por $S \circ T$. Notemos que para que $S \circ T$ faça sentido, o contradomínio de T e o domínio de S devem ser o mesmo (neste caso $\mathbb{R}^n$), e a transformação resultante $S \circ T$ vai do domínio de T ao contradomínio de S, neste caso $S \circ T: \mathbb{R}^m \to \mathbb{R}^p$. Definimos a transformação composta como sendo:

$$S \circ T : \begin{array}{c} \mathbb{R}^m \to \mathbb{R}^p \\ v \longmapsto S(T(v)) \end{array}$$

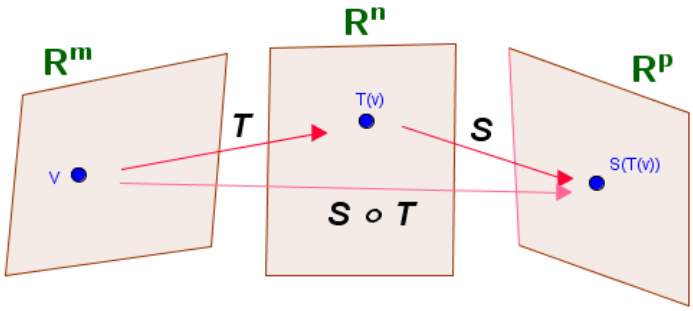


Figura 3 - A transformação composta $S \circ T$

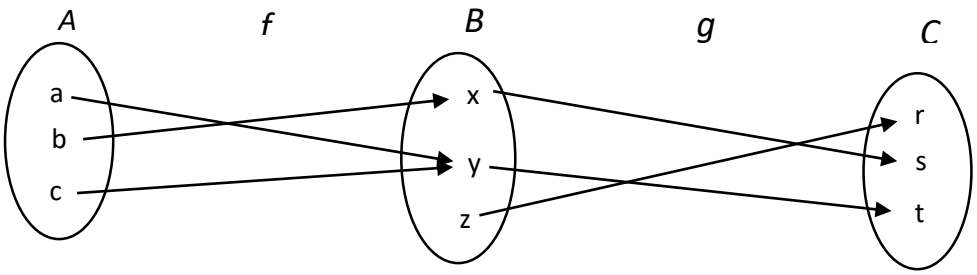
Definição:

Função composta g após f de duas funções $f: A \to B$ e $g: B \to C$ ($g \circ f: A \to C$). Função que aplica cada objeto x, pertencente ao domínio de f, à função f, obtendo uma imagem, $f(x)$, aplicando-a depois à função g, para obter a sua imagem, $g(f(x))$.

$g \circ f: A \to D$

$\forall x \in A, (g \circ f)(x) = g(f(x))$

Sejam as transformações $f: A \to B$ e $g: B \to C$ definidas pelo diagrama abaixo



Para encontrar a transformação composta $(g \circ \mathrm{f}) : \mathrm{A} \to \mathrm{C}$, usamos a definição de transformação para calcular:

$(g \circ f)(a) = g(f(a)) = g(y) = t$

$(g \circ f)(b) = g(f(b)) = g(x) = s$

$(g \circ f)(c) = g(f(c)) = g(y) = t$

Poderíamos ter chegado a mesma resposta se "seguirmos as flechas" no diagrama:

$$a \to y \to t\,,\ \ b \to x \to s\,,\ \ c \to y \to t$$

Para encontrar a imagem de cada transformação: f, g e $g \circ f$ podemos utilizar o diagrama, onde os valores imagem pela transformação f são x e y, e os valores imagem por g são r, s e t, portanto:

Imagem de $f = \{x, y\}$ e imagem de $g = \{r, s, t\}$

Pelo cálculo anterior os valores imagem pela transformação composta são t e s, portanto:

Imagem de $g \circ f = \{s, t\}$

Podemos notar que as imagens de $g\ e\ g \circ f$ são diferentes.

2.5 Transformação Linear Injetora

Definição: Uma transformação linear $T: V \to W$, é injetora, se para quaisquer $u, v \in V$ se $u \neq v$ então $T(u) \neq T(v)$. O que equivalente a, se $T(u) = T(v)$ então $u = v$.

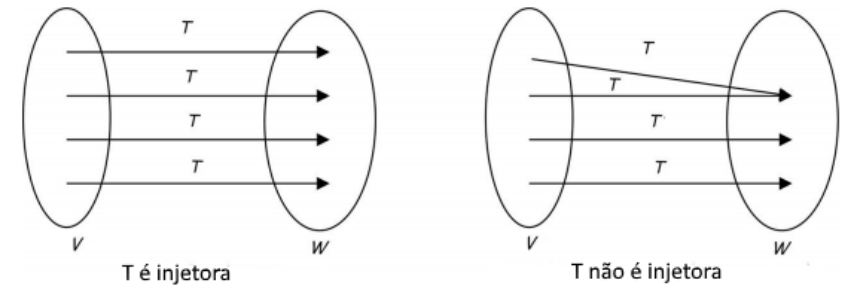


Figura 5 – Transformação linear injetora e não injetora
Fonte: adaptado de (KULDEEP, 2014, P.373)

T é injetora se as imagens de dois vetores distintos são distintas. Uma transformação linear $T: V \to W$ é injetora se, e somente se, $N(T) = \{0\}$.

No diagrama da figura 6, vamos demonstrar que a transformação $f: A \to B$ é injetora mas não sobrejetora.

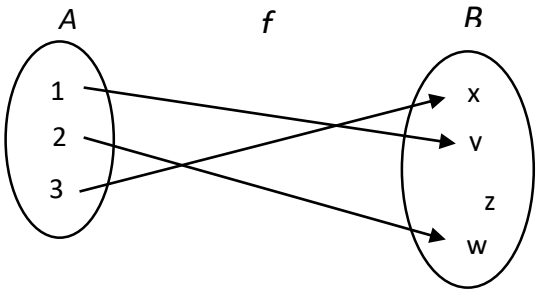


Figura 6

A transformação $f: A \to B$ é injetora, pois cada elemento de A tem uma imagem distinta, porém, não é sobrejetora, pois $z \in B$ não é imagem de nenhum elemento de A. Logo a transformação é injetora e não sobrejetora.

2.6 Transformação Linear Sobrejetora

Uma transformação linear $T: V \to W$ é sobrejetora se o conjunto imagem de T é o conjunto W, isto é. $Im(T) = W$. Conforme ilustrado na figura 7.

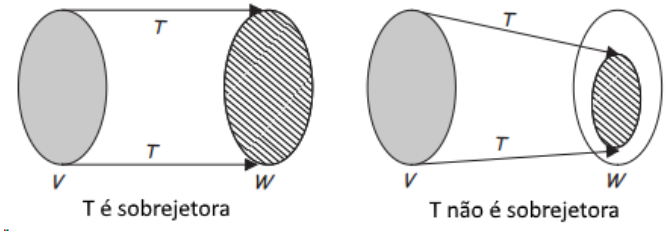


Figura 7 - Transformação linear sobrejetora e não sobrejetora
Fonte: adaptado de (KULDEEP, 2014, P.377)

Seja a transformação $f: A \to B$ definida pelo diagrama da figura 8, vamos mostrar que a transformação é sobrejetora mas não injetora

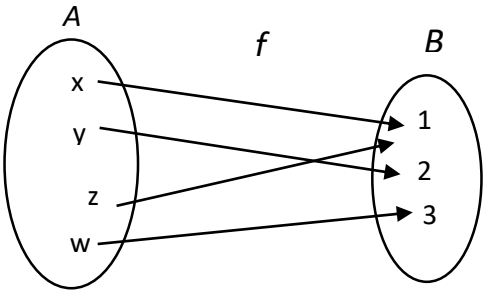


Figura 8

A transformação $f: A \to B$ não é injetora, pois x e z são transformados no mesmo elemento 1, porém, é sobrejetora, pois, cada elemento de B é imagem de algum elemento de A. Logo a transformação é sobrejetora e não injetora.

2.7 Transformação Linear Bijetora - Isomorfismo

Uma transformação linear $T: V \to W$ é bijetora quando for injetora e sobrejetora. Transformações lineares bijetoras são também denominadas **isomorfismos** e, consequentemente, V e W são denominados espaços vetoriais isomorfos. Dizemos que dois espaços vetoriais V e W são isomorfos quando existe algum isomorfismo $T: V \to W$.

Segundo Steinbrusch(1987, p.181), "Chama-se isomorfismo do espaço vetorial V no espaço vetorial W a uma transformação linear $T: V \to W$, que é bijetora. Neste caso, os espaços vetoriais V e W são ditos isomorfos. Sendo que todo espaço vetorial V de dimensão n é isomorfo a $\mathbb{R}^n$, assim, dois espaços vetoriais de dimensão finita são isomorfos se tiverem a mesma dimensão."

Por exemplo, para verificar a existência de isomorfismo na transformação linear T: $P_2(\mathbb{R}) \to \mathbb{R}^3$ definida por $T(a_2t^2 + a_1t + a_2) = (a_0 + a_1, a_1 - a_2, a_0 + a_1 + a_2)$.

Temos que analisar primeiro o núcleo da transformação para ver se é injetora:

$N(T) = T(a_2t^2 + a_1t + a_2) = 0 \Rightarrow (a_2t^2 + a_1t + a_2) = (0,0,0)$

Obtém-se, assim, o sistema linear:

$$\begin{cases} a_0 + a_1 = 0 \\ a_1 - a_2 = 0 \\ a_0 + a_1 + a_2 = 0 \end{cases}$$

Do qual se conclui que $a_0 = a_1 = a_2 = 0$. Logo $N(T) = 0$, logo T é injetora.

Sendo T pertencente ao $\mathbb{R}^3$ e uma vez que $\dim(P_2(\mathbb{R})) = \dim(\mathbb{R}^3) = 3$, logo T é sobrejetora e, assim, concluímos que T é um isomorfismo.

2.8 Operadores Lineares Inversíveis

As transformações lineares inversas são importantes, pois é através delas que conseguimos reverter uma transformação ao seu ponto de início. Exemplos de aplicações com transformações lineares inversas podem ser encontradas em transformação de uma imagem como na Figura , ou em criptografia, quando uma mensagem codificada por uma transformação T necessita ser decodifica pela transformação inversa de T conforme será demonstrado no capítulo 3.

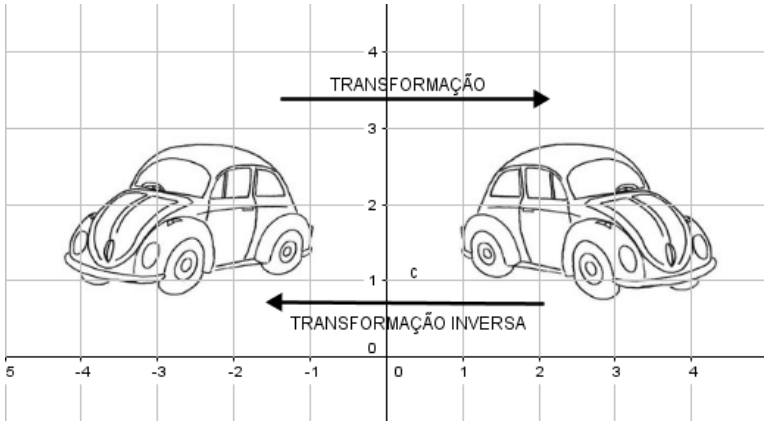


Figura 9 – Transformação inversa

O conceito de operadores lineares inversos é o mesmo de função inversa, onde uma função é inversível quando existe uma outra que, composta a ela, resulta na função identidade, lembrando que uma função é inversível se, e somente se, é injetora e bijetora.

Definição: Seja V espaço vetorial, o espaço vetorial de todos os operadores lineares definidos em V será representado por $L(V)$. Um operador linear $T \in L(V)$ é inversível se existe $T^{-1} \in L(V)$ tal que $T \circ T^{-1} = T^{-1} \circ T = I$ (operador identidade de *V*).

Para efeitos de demonstração[2] considere a matriz:

$$A_\theta = \begin{bmatrix} cos\ \theta & -sen\ \theta \\ sen\ \theta & \cos\theta \end{bmatrix}$$

Fixada a base canônica em $\mathbb{R}^2$, esta matriz define a transformação linear $T_\theta: \mathbb{R}^2 \to \mathbb{R}^2$ para cada $(x_1, x_2) \in \mathbb{R}^2$, por $T_\theta(x_1, x_2) = (x_1 \cos\theta - x_2\ sen\ \theta,\ x_1\ sen\ \theta + x_2 \cos\theta)$.

T_θ pode ser interpretado geometricamente como uma rotação dos vetores do plano em θ radianos (figura 10). Podemos verificar que θ é o ângulo formado pelo vetor (x_1, x_2) e pela sua imagem $T_\theta(x_1, x_2)$. A imagem (y_1, y_2) é o resultado da rotação do vetor (x_1, x_2).

O que queremos demonstrar aqui é se existe uma transformação inversa, ou seja, que nos permita obter (x_1, x_2) a partir de (y_1, y_2).

[2] Exemplo adaptado de LUZ, C., MATOS, A., & NUNES, S. (2004/2005, pag. 16/17)

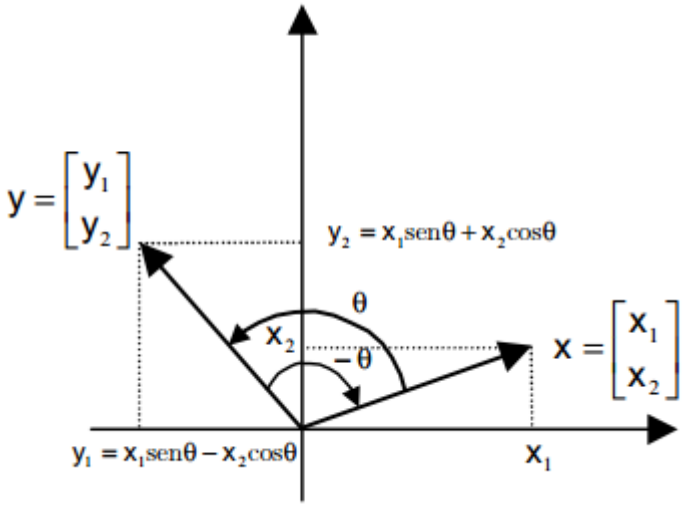


Figura 10 – Rotação de θ rad e a sua inversa
Fonte: LUZ, C., MATOS, A., & NUNES, S. (2004/2005, pag.17)

O que procuramos é a transformação inversa de T_θ representado por ${T_\theta}^{-1}$.

Nota-se que $A_{-\theta}$ é a matriz inversa de A_θ é, pois $A_\theta A_{-\theta} = I$, que pode ser facilmente verificado, e é definida por:

$$A_{-\theta} = \begin{bmatrix} \cos(-\theta) & -sen\,(-\theta) \\ sen\,(-\theta) & \cos(-\theta) \end{bmatrix} = \begin{bmatrix} cos\,\theta & sen\,\theta \\ -sen\,\theta & \cos\theta \end{bmatrix}$$

Este fato revela o paralelismo existente entre a operação de inversão de matrizes e a operação de inversão de transformações lineares.

3 – TRANSFORMAÇÕES GEOMÉTRICAS NO PLANO

Algumas transformações lineares podem ser representadas geometricamente, e algumas destas representações possuem aplicações nas mais diversas áreas da computação gráfica, onde encontramos a necessidade de manipular o conteúdo de uma cena. Animações, por exemplo, são efeitos criados pelo movimento da câmera ou dos objetos presentes na cena. Mudanças no formato, tamanho e orientação estão ligadas às transformações geométricas. Estas aplicações são aplicadas à cena para alterar a geometria dos objetos que compõem a cena sem fazer alterações topológicas.

Todas as transformações geométricas podem ser representadas na forma de equações. O problema é que manipulações de objetos gráficos normalmente envolvem muitas operações de aritmética simples. As matrizes são muito usadas nessas manipulações porque são mais fáceis de usar e entender do que as equações algébricas, o que explica por que programadores e engenheiros as usam extensivamente.

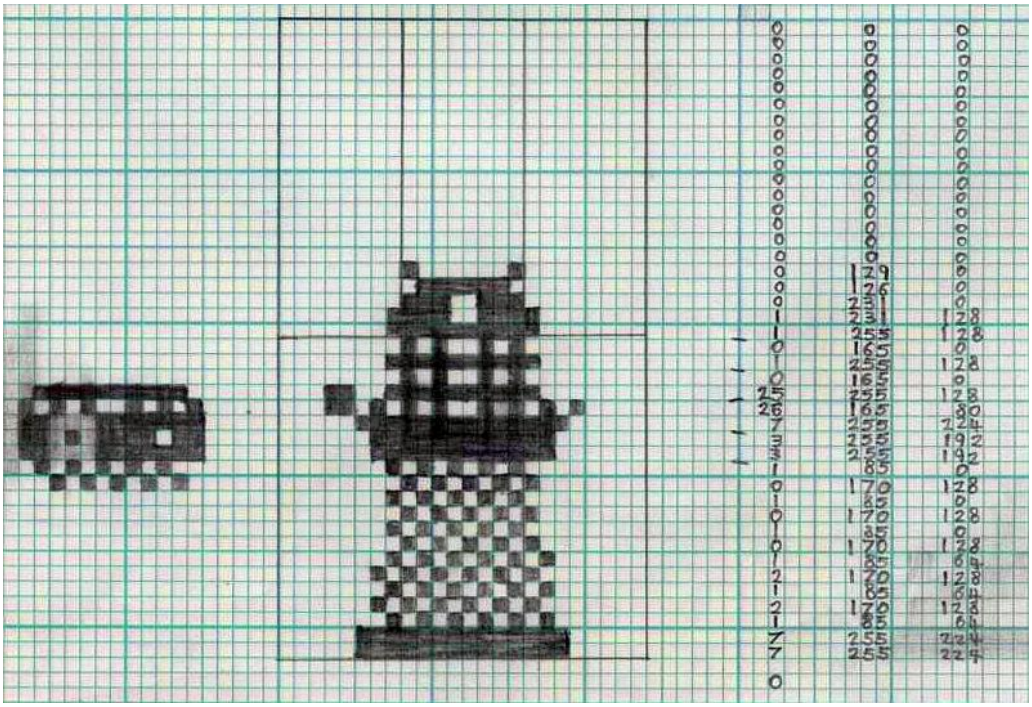


Figura 11 - Esboço para criação de um personagem de vídeo game nos anos 80, a imagem desenhada em papel quadriculado é convertida para uma matriz para sua posterior manipulação
Fonte: http://cronodon.com/Programming/c64_programming.html - Acessado em 19/05/2016

Uma transformação geométrica é uma função cujo domínio e imagem são formados por um conjunto de pontos. Geralmente, tanto o domínio como a imagem pertencem ambos ao $\mathbb{R}^2$ ou ao $\mathbb{R}^3$. Frequentemente as transformações geométricas necessitam ser funções um para um, ou seja, sempre que $f(a) = f(b)$ então $a = b$.

As mais comuns transformações geométricas no Plano, como escala, rotação, translação, espelhamento e cisalhamento, serão discutidas neste capítulo.

3.1 Escala (Resize)

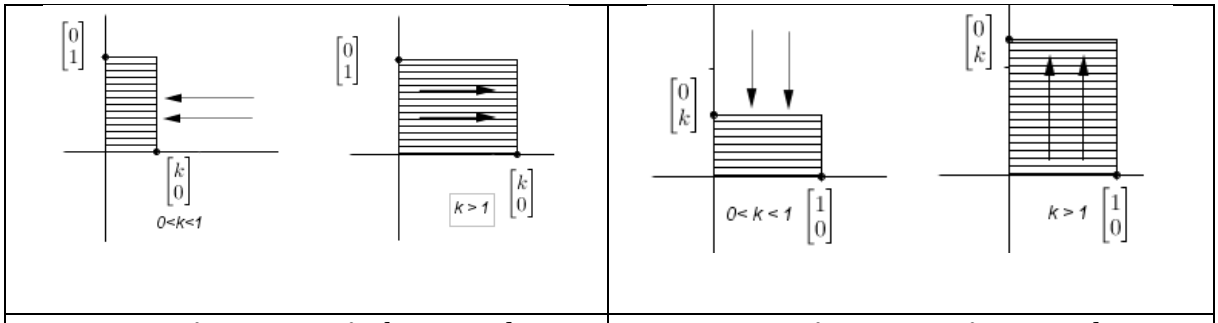
Esta transformação também conhecida como expansão, dilatação ou contração, é bastante utilizada quando queremos fazer um objeto parecer maior ou menor, em outras palavras, mudar sua escala. Quando damos um zoom em uma fotografia para ampliá-la ou diminui-la estamos aplicando uma transformação de escala. Seja um ponto $P(x, y)$ sobre o qual queremos efetuar a transformação e α e β números reais não nulos, podemos definir a função T como sendo:

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

$T(x, y) \longmapsto (\alpha x, \beta y)$

Matriz da transformação;

$$A = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$$



Expansão e contração horizontal	Expansão e contração vertical

Figura 12

Esta transformação faz com que os objetos sejam esticados ou encolhidos na direção dos eixos x e y. O redimensionamento $S(S_x, S_y)$ mapeia o ponto (x, y) ao ponto (x', y') dado por:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} S_x \cdot x \\ S_y \cdot y \end{pmatrix} = \begin{pmatrix} S_x & 0 \\ 0 & S_y \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

S_x é o fator de escala na direção do eixo x. Se $|S_x| > 1$, então ocorre uma expansão da direção do eixo x. Se $|S_x| < 1$, então ocorre uma contração no lugar. Se S_x for negativo, além da expansão ou contração na direção do eixo x, uma reflexão neste eixo também ocorre (figura 14). Os mesmos resultados obtemos com S_y que é o fator de escala na direção do eixo y.

Podemos analisar estas propriedades em um objeto utilizando por exemplo uma transformação cujos fatores de redimensionamento são $S_x = 2$ e $S_y = 0{,}5$, ou seja, expandindo o objeto ao

longo do eixo x em um fator de 2 e contraindo-o na direção do eixo y por um fator de 0,5 (Figura 13) .

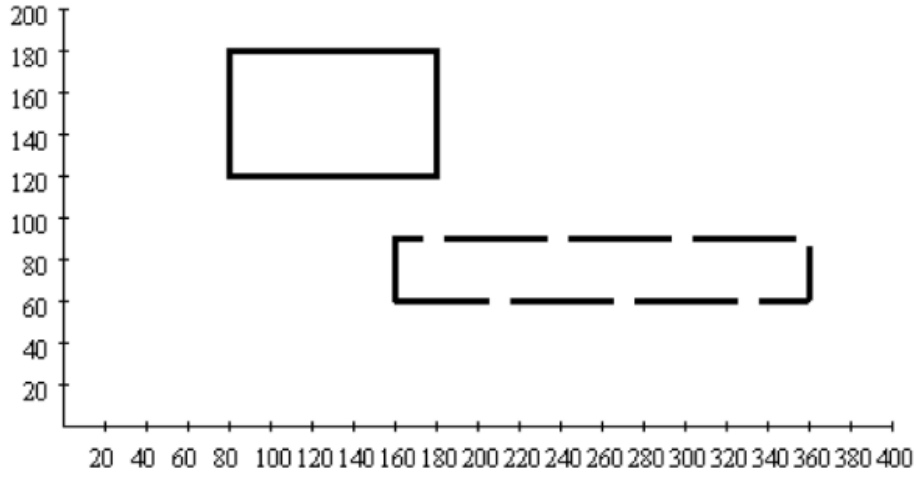


Figura 13 – Escala aplicada a um retângulo gerando uma transformação adicional de translação
Fonte: KLAWONN, F. (2008,pág.24)

A aplicação desta transformação ao retângulo cujo vértice inferior esquerdo está localizado no ponto (80,120) e seu vértice superior direito está em (180,180) gerou um retângulo cuja largura dobrou com metade da altura original (figura tracejada). Além disso, o retângulo também sofreu uma translação para uma posição inferior direita em relação ao retângulo original. O redimensionamento sempre é realizado com respeito a origem do sistema de coordenadas. Aplicando um redimensionamento em um objeto que não está centralizado na origem deste sistema conduzirá a uma translação do objeto além de seu redimensionamento.

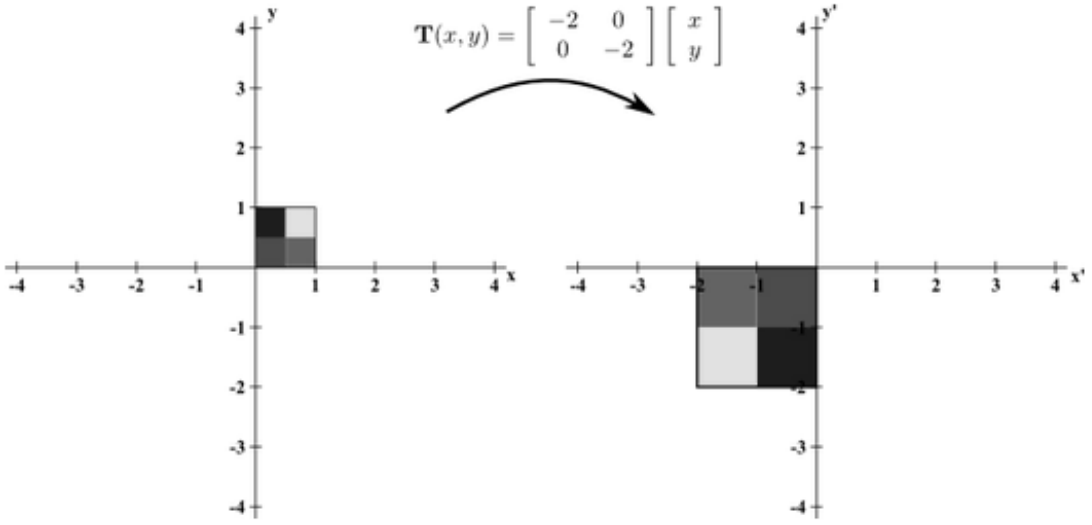


Figura 14 – Escala aplicada a um quadrado gerando uma transformação adicional de reflexão
Fonte: http://mathinsight.org/determinant_linear_transformation (Acessado em 25/10/2016)

3.2 Rotação (Rotation)

Esta transformação rotacional objetos no plano tanto no sentido horário como no sentido anti-horário a partir de um ponto base que pode ser um dos vértices do objeto um ponto externo a ele. Quando uma fotografia está de ponta cabeça ou de lado e queremos coloca-la na posição correta, aplicamos a transformação de rotação. Outra utilidade da rotação é que através desta transformação podemos fazer com que os eixos de elipses, hipérboles ou parábolas fiquem paralelos aos eixos cartesianos e, assim simplificamos suas equações. Seja um ponto externo $P(x, y)$ sobre o qual queremos girar o objeto, podemos definir a função T como sendo:

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

$T(x, y) \longmapsto (x \cdot \cos\theta - y \cdot \text{sen}\,\theta\,, x \cdot sen\ \theta + y \cdot \cos\theta)\ tal\ que\ 0 \leq \theta \leq 2\pi$

Matriz da transformação

$$T_\theta = \begin{bmatrix} cos\ \theta & -sen\ \theta \\ sen\ \theta & \cos\theta \end{bmatrix}$$

Esta transformação é determinada por um único parâmetro, o ângulo de rotação. Se o ângulo for positivo então a rotação será no sentido anti-horário em relação a origem do sistema de coordenadas. Já um ângulo negativo fará com que a rotação seja no sentido horário.

A rotação $R(\theta)$ definida pelo ângulo θ mapeia o ponto (x, y) ao ponto (x', y') dado por:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \cdot \cos(\theta) - y \cdot \text{sen}(\theta) \\ x \cdot \text{sen}(\theta) + y \cdot \cos(\theta) \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -sen\ (\theta) \\ sen\ (\theta) & \cos(\theta) \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

A rotação sempre é executada em torno da origem do sistema de coordenadas. Como consequência disso, um efeito de deslocamento semelhante como ao caso de escalonamentos acontece, quando um objeto não está centrado em torno da origem.

Na figura 15 aplicando uma rotação de 45º em um objeto que não está centrado na origem podemos observar que além da rotação o objeto sofre uma translação.

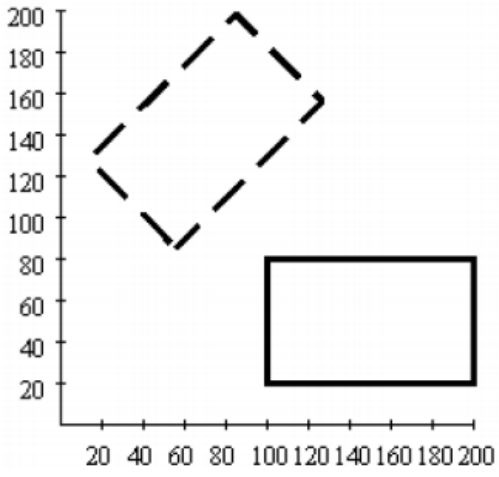


Figura 15 – Rotação aplicada a um retângulo gerando uma transformação adicional de translação
Fonte: KLAWONN, F. (2008,pág.25)

Quando o objeto está posicionado na origem do sistema de coordenadas, ele não sofre com o efeito da translação.

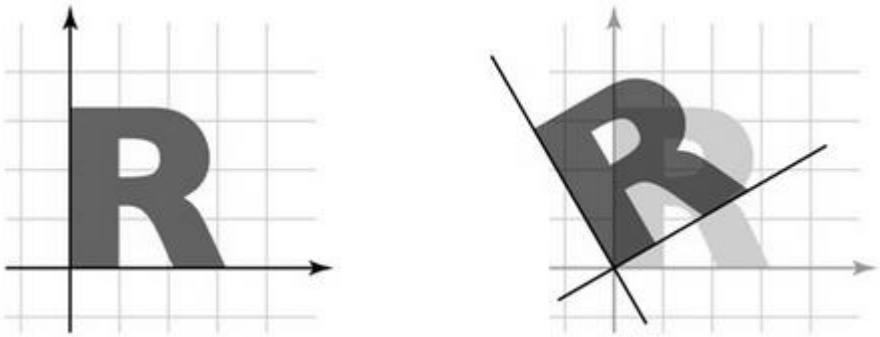


Figura 16 – Rotação aplicada a uma imagem posicionada na origem do sistema de coordenadas.
Fonte: http://slideplayer.com/slide/4875172/ (Acessado em 25/10/2016)

3.3 Translação (Translation)

Através da translação podemos deslocar objetos no plano, nos sentidos horizontal e/ou vertical. As translações não alteram as medidas das distâncias, nem alteram as amplitudes dos ângulos dos objetos. O objeto transformado por translação mantém tamanho e forma, modificando sua localização, como por exemplo, podemos ver na figura 14. A utilização cotidiana desta transformação nos meios digitais, está no simples clicar em cima de um objeto e arrastá-lo para uma nova posição. Já na matemática, esta transformação é bastante utilizada para simplificar equações, definindo um novo sistema cartesiano de forma que o objeto a ser estudado, neste novo sistema, tenha uma equação mais simples. Para calcular a nova posição dos pontos (A,B,C,D) da imagem apresentada na figura 14, podemos descrever na forma matricial:

$$\begin{bmatrix} A_X{}' \\ A_Y{}' \end{bmatrix} = \begin{bmatrix} A_X \\ A_Y \end{bmatrix} + \begin{bmatrix} \Delta A_X \\ \Delta A_Y \end{bmatrix}$$

$$\begin{bmatrix} B_X{}' \\ B_Y{}' \end{bmatrix} = \begin{bmatrix} B_X \\ B_Y \end{bmatrix} + \begin{bmatrix} \Delta B_X \\ \Delta B_Y \end{bmatrix}$$

$$\begin{bmatrix} C_X{}' \\ C_Y{}' \end{bmatrix} = \begin{bmatrix} C_X \\ C_Y \end{bmatrix} + \begin{bmatrix} \Delta C_X \\ \Delta C_Y \end{bmatrix}$$

$$\begin{bmatrix} D_X{}' \\ D_Y{}' \end{bmatrix} = \begin{bmatrix} D_X \\ D_Y \end{bmatrix} + \begin{bmatrix} \Delta D_X \\ \Delta D_Y \end{bmatrix}$$

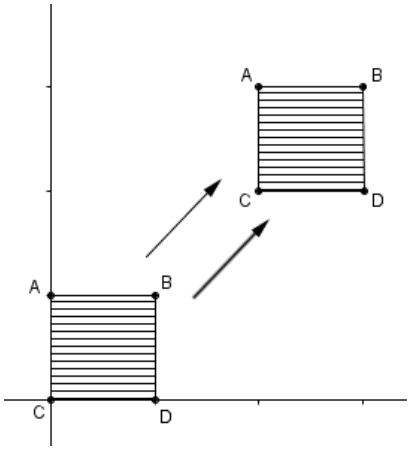


Figura 47 - Translação de um objeto

É importante perceber que diferente das outras transformações mostradas neste trabalho, a translação, segundo (KLAVONN, 2008, pg.44) "não é uma aplicação linear, portanto não pode ser representada em termos de multiplicação de matrizes. Uma multiplicação de matriz mantém sempre o vetor nulo sem modificações, enquanto que a translação afeta todos os pontos, incluindo a origem que corresponde ao vetor zero."

A figura 17 mostra um exemplo desta transformação, aonde um quadrado localizado em $P = \{A(0,1); B(1,1); C(0,0); D(1,0)\}$, é movimentado 2 unidades a direita e 2 unidades para cima.

$$\begin{bmatrix} A_X{}' \\ A_Y{}' \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix} \rightarrow A' = P(2,3)$$

$$\begin{bmatrix} B_X{}' \\ B_Y{}' \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \end{bmatrix} \rightarrow B' = P(3,3)$$

$$\begin{bmatrix} C_X{}' \\ C_Y{}' \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \end{bmatrix} \rightarrow C' = P(2,2)$$

$$\begin{bmatrix} D_X{}' \\ D_Y{}' \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix} \rightarrow D' = P(3,2)$$

Após a transformação o quadrado ficará em $P = \{A(2,3); B(3,3); C(2,2); D(3,2)\}$

Na figura 18 podemos ver um exemplo de aplicação de translação no movimento de arrastar e soltar (drag-and drop) realizado com o mouse em cima de um objeto gráfico. O computador apaga o objeto e o recria com suas novas coordenadas, dando assim a impressão que ele está se movimentando. O mesmo acontece com o simples movimento do mouse na tela.

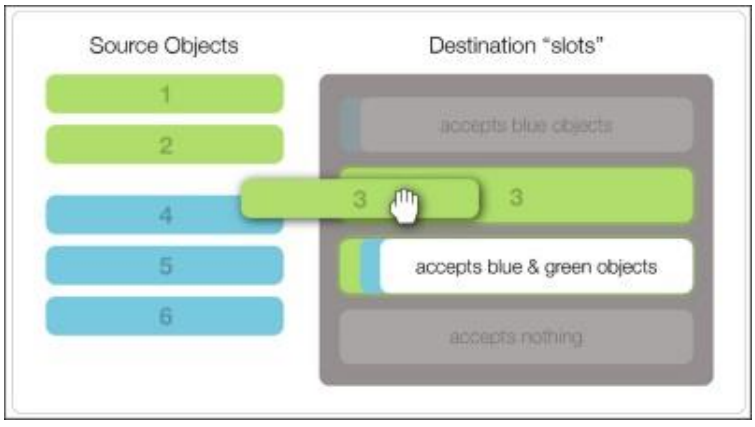


Figura 58 – Amostra de Translação
Fonte: http://kentwilliam.com/articles/rich-drag-and-drop-in-react-js

3.4 Reflexão/Espelhamento (Mirror)

A transformação de reflexão aplicada a um objeto, produz um objeto espelhado com relação a um dos eixos ou ambos. Muito utilizado em desenho gráfico quando se deseja criar uma cópia inversa da imagem. Podemos definir a função T dependendo de sua aplicação como sendo:

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

Reflexão em torno do eixo x:

$T(x, y) \longmapsto (x, -y)$

A reflexão $R(R_x, R_y)$ mapeia o ponto (x, y) ao ponto (x', y') dado por:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} R_x \cdot x \\ R_y \cdot (-y) \end{pmatrix} = \begin{pmatrix} R_x & 0 \\ 0 & -R_y \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

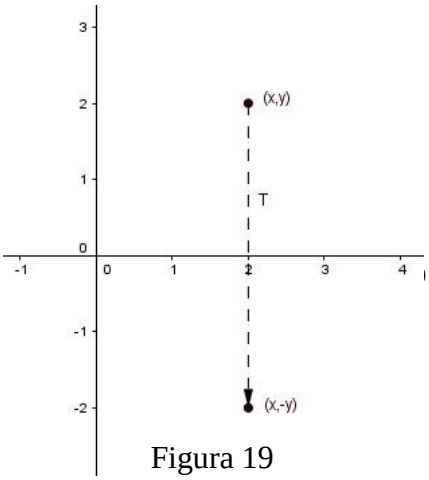


Figura 19

Reflexão em torno do eixo y:

$T(x, y) \longmapsto (-x, y)$

A reflexão $R(R_x, R_y)$ mapeia o ponto (x, y) ao ponto (x', y') dado por:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} R_x \cdot (-x) \\ R_y \cdot y \end{pmatrix} = \begin{pmatrix} -R_x & 0 \\ 0 & R_y \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

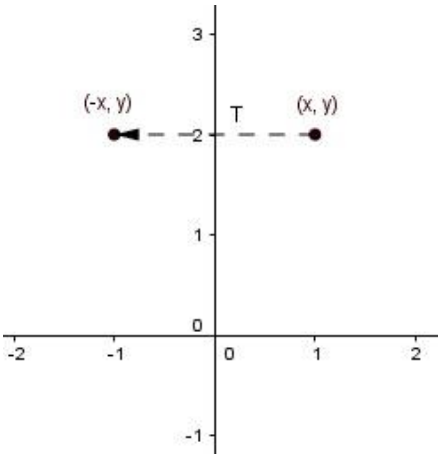


Figura 20

Reflexão na origem:

$T(x, y) \longmapsto (-x, -y)$

A reflexão $R(R_x, R_y)$ mapeia o ponto (x, y) ao ponto (x', y') dado por:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} R_x \cdot (-x) \\ R_y \cdot (-y) \end{pmatrix} = \begin{pmatrix} -R_x & 0 \\ 0 & -R_y \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

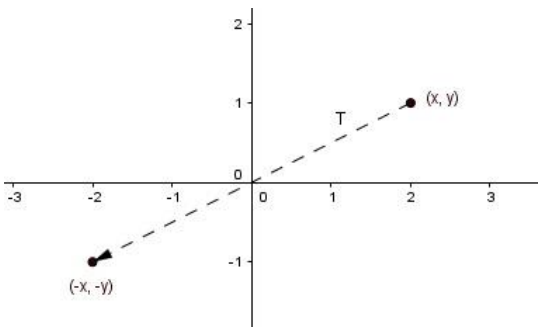


Figura 21

Reflexão em torno da reta $y = x$:

$T(x, y) \longmapsto (y, x)$

A reflexão $R(R_x, R_y)$ mapeia o ponto (x, y) ao ponto (x', y') dado por:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} R_x \cdot x \\ R_y \cdot y \end{pmatrix} = \begin{pmatrix} R_x & 0 \\ 0 & R_y \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

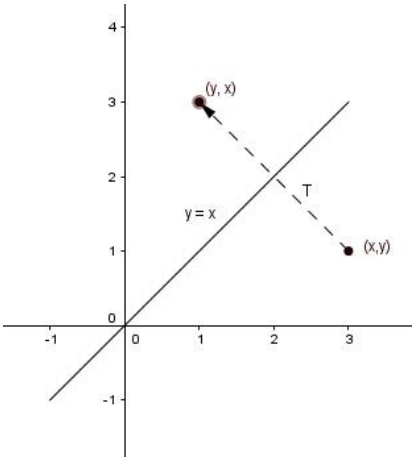


Figura 22

Figura 23 - A transformação de reflexão é vista sempre que olhamos para uma superfície espelhada, como a deste lago na foto
Fonte: Adaptado de http://www.imgrum.net/media/1275063377630865061_3415119872 - Acessado em 13/05/2016

3.5 Cisalhamento (Shearing)

A transformação de cisalhamento provoca uma distorção do objeto em uma de suas coordenadas ou em ambas. Utilizado amplamente nos filtros de distorção de imagens em programas gráficos.

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

Cisalhamento horizontal:

$$A = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \quad T(x, y) \longmapsto (x + \alpha y, y)$$

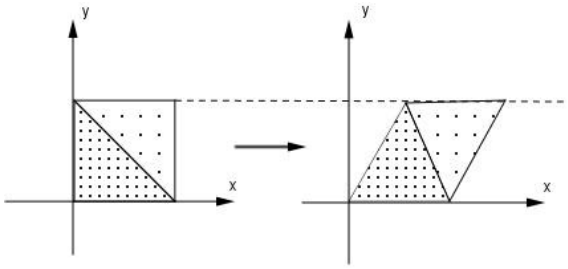


Figura 24

Cisalhamento vertical:

$$A = \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix} \quad T(x,y) \longmapsto (x, y + \alpha x)$$

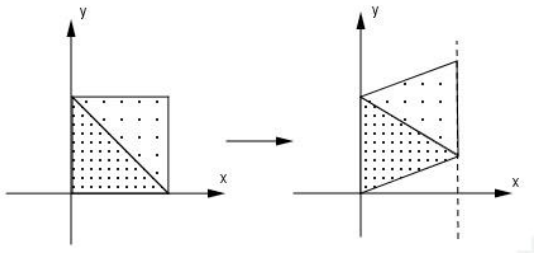


Figura 25

Similar a transformação de escala, o cisalhamento necessita também de dois parâmetros, porém, não na diagonal principal da matriz de transformação, mas nas outras posições.

Aplicando a transformação de cisalhamento $Sh(S_x, S_y)$ ao ponto (x, y) gera o ponto (x', y') com as novas coordenadas:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x + S_x \cdot y \\ y + S_y \cdot x \end{pmatrix} = \begin{pmatrix} 1 & S_x \\ S_y & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

Assim como ocorre nas transformações de escala e rotação, a transformação de cisalhamento é realizada em respeito à origem do sistema de coordenadas, isso implica que se o objeto não estiver centrado em torno da origem, ele não apenas sofrerá deformação através da transformação de cisalhamento como também ocorrerá um deslocamento do mesmo.

Figura 26 – Cisalhamento aplicado a um retângulo gerando uma transformação adicional de translação
Fonte: KLAWONN, F. (2008,pág.26)

Na figura acima o objeto tracejado foi obtido do retângulo , aplicando uma transformação de cisalhamento com os parâmetros $S_x = 1$ e $S_y = 0$. Como $S_y = 0$, o cisalhamento ocorreu na direção do eixo y.

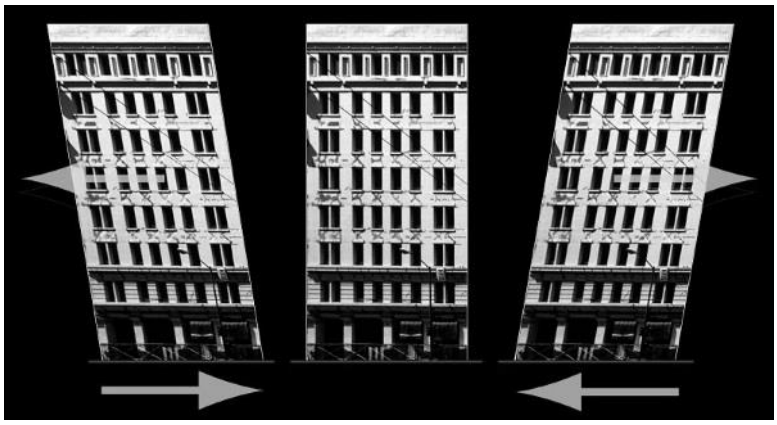


Figura 67 - Transformação de cisalhamento aplicado a uma imagem para demonstrar os efeitos do tremor de terra sobre a estrutura de um edifício.
Fonte: Digital Imaging and the Web in Teaching Structures - http://www.arch.virginia.edu/~km6e/tti/tti-summary/part-2.html - Acessado em 15/05/2016

4 – ISOMORFISMO APLICADO À CRIPTOGRAFIA

Dentre as inúmeras aplicações das transformações lineares, podemos destacar o seu uso cotidiano no desenvolvimento de algoritmos de criptografia. A tecnologia atual não está imune às ameaças que a envolvem, e não conseguimos pensar em um mundo, onde não haja sistemas protegidos por senhas e mensagens indecifráveis para aqueles que não deveriam ter acesso a elas. Claro que existem diversos algoritmos criptográficos que utilizam outras áreas da matemática, como por exemplo, a teoria dos números e a matemática discreta. Apesar de existirem trabalhos específicos sobre criptografia, queremos mostrar aqui, a utilização das transformações lineares isomórficas na criptografia.

Mas porque as transformações lineares aplicadas a criptografia têm que ser isomórficas? Porque a ideia principal da criptografia é a habilidade de criar uma mensagem indecifrável em uma ponta, mas que seja possível de ser decifrada na outra ponta através da reversão do código utilizado como chave. Para isso necessitamos que a transformação linear possua uma inversa, logo utilizando o *Teorema da Transformação Linear Inversa* que afirma que se $T: V \to W$ é uma Transformação Linear e um Isomorfismo, sua inversa $T^{-1}: W \to V$, também será uma Transformação Linear e um Isomorfismo.

4.1 Um pouco de história

Reis, imperadores e generais buscavam formas eficientes de se comunicar com seus exércitos, e o temor de que suas ordens fossem interceptadas pelo inimigo fez com que as mensagens fossem mascaradas através de códigos e cifras, tornando-as ilegíveis para outros além do destinatário, como podemos observar na própria etimologia da palavra criptografia, que é composta dos termos gregos “kryptos” (secreto) e “grapho” (escrita). Ao longo da história os códigos vieram a ser fundamentais no sucesso das batalhas e o trabalho dos criptógrafos e matemáticos eram cada vez mais valorizados. Podemos dar como exemplo o sucesso na decodificação feita por matemáticos poloneses a serviço das tropas aliadas, das mensagens geradas pela máquina “Enigma” criada por Arthur Scherbius em 1918 e amplamente utilizada durante a segunda guerra mundial pelo exército alemão.

O primeiro registro que se tem de alguém que utilizou um sistema criptográfico foram os hebreus utilizando um alfabeto invertido para “esconder” as mensagens. O método utilizado substituía cada letra do alfabeto por outro do alfabeto invertido.

Um exemplo utilizando o alfabeto hebraico:

ת	ש	ר	ק	ץ צ	ף פ	ע	ס	נ	ם מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	ם מ	נ	ס	ע	ף פ	ץ צ	ק	ר	ש	ת

Logo a mensagem em hebraico: לתקוף את האויב (ATACAR O INIMIGO)

Ficaria escrita de modo invertido: ביואה תא חוקתל (INDECIFRÁVEL NA ÉPOCA?)

Este tipo de criptografia ficou conhecida como cifra de substituição monoalfabética, onde cada letra do alfabeto original é substituída por outra letra ou por um símbolo. Esta cifra permaneceu invulnerável por séculos.

A partir do ano 600 AC, a técnica de codificação assíria é provavelmente a primeira prova da utilização de meios de codificação na Grécia, para dissimular mensagens escritas em bandas de papiros.

A técnica consistia em enrolar uma banda de papiros num cilindro chamado scytale, escrever o texto longitudinalmente na faixa enrolada e levada na cintura como se fosse um cinto com as letras para dentro. (A mensagem no exemplo ao lado é "Matar rei amanhã a meia noite"). A mensagem, uma vez desenrolada, já não ficaria mais compreensível. Basta que o destinatário tenha um cilindro do mesmo diâmetro para poder decifrar a mensagem.

Figura 26
Fonte: FIARRESGA, p.7

Diversas variantes destes métodos de criptografia forma criados ao longo dos séculos, como por exemplo a codificação César onde Simon Singh, (2002) em sua obra descreveu como que "César deslocava as letras em três casas, ficando claro que, empregando-se qualquer deslocamento entre uma das 25 casas, é possível criar 25 códigos distintos"(p.27)., a codificação Vigenere que utilizava uma tabela contendo 26 alfabetos e a utilizava tanto para criptografar como para decriptografar, a codificação ROT13, etc.. até que no final do século XVIII, os sistemas de criptografia já eram amplamente usados para as comunicações militares utilizando dispositivos que evoluíram bastante com a tecnologia eletromecânica (comunicação via telégrafo e rádio). (SILVA, p.25)

É claro que nunca existiu um sistema e criptografia que não pudesse ser quebrado, mas o objetivo principal era tornar o método de acesso a informação tão trabalhoso que o invasor perdesse o interesse e desistisse.

4.2 Aplicação do Isomorfismo em R^2 na criptografia

Após uma breve introdução na história da criptografia, podemos perceber como que as transformações isomórficas podem atuar como um tradutor entre a mensagem legível e a mensagem codificada. Vamos iniciar representando abaixo uma tabela de substituição das letras do alfabeto por números aleatórios (Para efeitos de simplificação não utilizaremos os acentos neste exemplo).

Tabela 1 - Tabela de Conversão

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
3	12	-3	7	2	5	4	8	-4	-12	0	20	1	-6
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**SPC**	**.**
-5	10	14	-17	-1	-2	-13	15	11	-14	18	-8	6	-10

Digamos agora que utilizando esta tabela nós quiséssemos escrever a seguinte mensagem: GRADUACAO MATEMATICA UFSJ.

Fazendo as substituições de cada caractere pelo seu respectivo número teremos:

Tabela 2- Substituindo a mensagem pelos seus respectivos códigos.

G	**R**	**A**	**D**	**U**	**A**	**C**	**A**	**O**	**SPC**	**M**	**A**	**T**
4	-17	3	7	13	3	-3	3	-5	6	1	3	-2
E	**M**	**A**	**T**	**I**	**C**	**A**	**SPC**	**U**	**F**	**S**	**J**	**.**
2	1	3	-2	-4	-3	3	6	-13	5	-1	-12	-10

Até o momento apenas substituímos as letras por uma tabela de números aleatórios assim como era feito antigamente na cifra de substituição monoalfabética, porém é agora que entrará a função das transformações lineares. Convertidos as letras em números, utilizaremos uma regra de transformação para transformar esta mensagem em outra, onde apenas o destinatário que conheça tanto a tabela de substituição como a regra de transformação poderá decifrar a mensagem.

A regra de transformação que utilizaremos a seguir será do espaço R^2

$$\boxed{T(x,y) = (2x - y, x + 3y)}$$

Antes de começarmos a codificar a mensagem, precisamos nos certificar de que a regra de transformação nos garanta uma transformação isomórfica, conforme vimos no capítulo 1.8 sobre transformações lineares bijetoras.

$[T]_{can} = \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix} \rightarrow \det[T] = 6 - (-1) = 7$, logo T é um isomorfismo.

Como nossa transformação é do espaço R^2, aplicaremos a transformação a cada par de caracteres da nossa mensagem:

$T(4,-17) = \big(2 \cdot 4 - (-17), 4 + 3 \cdot (-17)\big) = (\mathbf{25}, \mathbf{-47})$

$T(3,7) = (2 \cdot 3 - 7,3 + 3 \cdot 7) = (\mathbf{-1}, \mathbf{24})$

$T(13,3) = (2 \cdot 13 - 3,13 + 3 \cdot 3) = (\mathbf{23}, \mathbf{22})$

$T(-3,3) = (2 \cdot (-3) - 3, (-3) + 3 \cdot 3) = (\mathbf{-9}, \mathbf{6})$

$T(-5,6) = (2 \cdot (-5) - 6, (-5) + 3 \cdot 6) = (\mathbf{-16}, \mathbf{13})$

$T(1,3) = (2 \cdot 1 - 3,1 + 3 \cdot 3) = (\mathbf{-1}, \mathbf{10})$

$T(-2,2) = (2 \cdot (-2) - 2, (-2) + 3 \cdot 2) = (\mathbf{-6}, \mathbf{4})$

$T(1,3) = (2 \cdot 1 - 3,1 + 3 \cdot 3) = (\mathbf{-1}, \mathbf{10})$

$T(-2,-4) = (2 \cdot (-2) - (-4), (-2) + 3 \cdot (-4)) = (\mathbf{0}, \mathbf{-14})$

$T(-3,3) = (2 \cdot (-3) - 3, (-3) + 3 \cdot 3) = (\mathbf{-9}, \mathbf{6})$

$T(6,-13) = \big(2 \cdot 6 - (-13), 6 + 3 \cdot (-13)\big) = (\mathbf{25}, \mathbf{-33})$

$T(5,-1) = \big(2 \cdot 5 - (-1), 5 + 3 \cdot (-1)\big) = (\mathbf{11}, \mathbf{2})$

$T(-12,-10) = (2 \cdot (-12) - (-10), (-12) + 3 \cdot (-10)) = (\mathbf{-14}, \mathbf{-42})$

Após a transformação de nossa mensagem ela ficaria da seguinte forma:

?	**?**	**S**	**?**	**?**	**?**	**?**	**SPC**	**?**	**?**	**S**	**P**	**N**
25	-47	-1	24	23	22	-9	6	-16	13	-1	10	-6
G	**S**	**P**	**K**	**X**	**?**	**SPC**	**?**	**?**	**W**	**E**	**X**	**?**
4	-1	10	0	-14	-9	6	25	-33	11	2	-14	-42

Podemos notar que além da mensagem ficar indecifrável, alguns números ficaram sem um caractere correspondente na tabela de substituição e por isso não possuem uma representação para eles.

Como a pessoa que irá receber a mensagem possui tanto a tabela de substituição utilizada como também a regra da transformação, basta que ela encontre o isomorfismo inverso da transformação para conseguir decifrar a mensagem.

Como a nossa transformação $T(x, y) = (2x - y, x + 3y)$ é uma matriz $2x2$, então poderemos encontrar a inversa T^{-1} multiplicando o inverso do determinante de T pela sua matriz adjunta.

$$T = \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix} \rightarrow T^{-1} = \frac{1}{\det(T)} \cdot adj(T^T) \rightarrow \boldsymbol{T^{-1}} = \mathbf{\frac{1}{7}} \cdot \begin{pmatrix} \mathbf{3} & \mathbf{1} \\ \mathbf{-1} & \mathbf{2} \end{pmatrix}$$

Assim, $\left(\mathbf{\frac{1}{7}}(\boldsymbol{3x + y}), \mathbf{\frac{1}{7}}(\boldsymbol{-x + 2y})\right)$ será a regra para descriptografar a mensagem.

$$T^{-1}(25, -47) = \left(\frac{1}{7}(3 \cdot 25 - 47), \frac{1}{7}(-25 + 2 \cdot (-47))\right) = (\mathbf{4}, \mathbf{-17})$$

$$T^{-1}(-1{,}24) = \left(\frac{1}{7}(3 \cdot (-1) + 24), \frac{1}{7}(1 + 2 \cdot 24)\right) = (\mathbf{3}, \mathbf{7})$$

$$T^{-1}(23{,}22) = \left(\frac{1}{7}(3 \cdot 23 + 22), \frac{1}{7}((-23) + 2 \cdot 22)\right) = (\mathbf{13}, \mathbf{3})$$

$$T^{-1}(-9{,}6) = \left(\frac{1}{7}(3 \cdot (-9) + 6), \frac{1}{7}(9 + 2 \cdot 6)\right) = (\mathbf{-3}, \mathbf{3})$$

$$T^{-1}(-16{,}13) = \left(\frac{1}{7}(3 \cdot (-16) + 13), \frac{1}{7}(16 + 2 \cdot 13)\right) = (\mathbf{-5}, \mathbf{6})$$

$$T^{-1}(-1{,}10) = \left(\frac{1}{7}(3 \cdot (-1) + 10), \frac{1}{7}(1 + 2 \cdot 10)\right) = (\mathbf{1}, \mathbf{3})$$

$$T^{-1}(-6{,}4) = \left(\frac{1}{7}(3 \cdot (-6) + 4), \frac{1}{7}(6 + 2 \cdot 4)\right) = (\mathbf{-2}, \mathbf{2})$$

$$T^{-1}(-1{,}10) = \left(\frac{1}{7}(3 \cdot (-1) + 10), \frac{1}{7}(1 + 2 \cdot 10)\right) = (\mathbf{1}, \mathbf{3})$$

$$T^{-1}(0, -14) = \left(\frac{1}{7}(3 \cdot 0 - 14), \frac{1}{7}(0 + 2 \cdot (-14))\right) = (\mathbf{-2}, \mathbf{-4})$$

$$T^{-1}(-9{,}6) = \left(\frac{1}{7}(3\cdot(-9)+6), \frac{1}{7}(9+2\cdot 6)\right) = (\mathbf{-3}, \mathbf{3})$$

$$T^{-1}(25, -33) = \left(\frac{1}{7}(3\cdot 25-33), \frac{1}{7}((-25)+2\cdot(-33))\right) = (\mathbf{6}, \mathbf{-13})$$

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

$$T^{-1}(-14, -42) = \left(\frac{1}{7}(3\cdot(-14)-42), \frac{1}{7}((-(-14))+2\cdot(-42))\right) = (\mathbf{-12}, \mathbf{-10})$$

Conseguindo assim decodificar a mensagem retornando ao texto de origem.

G	**R**	**A**	**D**	**U**	**A**	**C**	**A**	**O**	**SPC**	**M**	**A**	**T**
4	-17	3	7	13	3	-3	3	-5	6	1	3	-2
E	**M**	**A**	**T**	**I**	**C**	**A**	**SPC**	**U**	**F**	**S**	**J**	**.**
2	1	3	-2	-4	-3	3	6	-13	5	-1	-12	-10

4.3 Aplicando o mesmo exemplo no espaço vetorial R^3.

Sabendo que não existe sistema criptográfico a prova de invasão, fica a missão do criptógrafo criar chaves cada vez mais complexas, levando cada vez mais tempo para decifrá-la e assim desestimular o invasor. No exemplo anterior vimos a criação de uma chave através de uma Transformação $T: R^2 \to R^2$.

Utilizando a tabela 1 de conversão, veremos como ficaria a codificação da mesma mensagem GRADUACAO MATEMATICA UFSJ. Só que desta vez faremos a transformação do espaço vetorial R^3 para o espaço vetorial R^3. Na tabela 2 já temos a mensagem convertida para seus respectivos códigos. Vamos criar agora uma regra de transformação para esta mensagem que será a chave de codificação:

$$\boxed{T(x, y, z) = (2x - 3y + z, x + y - 2z, -x + 2y + 2z)}$$

Assim como fizemos no exemplo anterior, precisamos nos certificar de que a regra de transformação nos garanta uma transformação isomórfica, ou seja, que sua matriz associada na base canônica possua uma inversa, e para isso verificaremos se seu determinante é diferente de zero.

$$[T]_{can} = \begin{pmatrix} 2 & -3 & 1 \\ 1 & 1 & -2 \\ -1 & 2 & 2 \end{pmatrix}$$

Novamente, precisamos nos certificar de que a regra de transformação nos garanta uma transformação isomórfica, verificando se seu determinante é diferente de zero.

$\begin{vmatrix} 2 & -3 & 1 \\ 1 & 1 & -2 \\ -1 & 2 & 2 \end{vmatrix} \begin{matrix} 2 & -3 \\ 1 & 1 \\ -1 & 2 \end{matrix} = 4 - 6 + 2 + 1 + 8 + 6 = \mathbf{15}$, logo T é um isomorfismo.

Como nossa transformação é do espaço R^3, aplicaremos a transformação a cada três caracteres da nossa mensagem:

$T(4,-17,3) = (2 \cdot 4 - 3 \cdot (-17) + 3, 4 - 17 - 2 \cdot 3, -4 + 2 \cdot (-17) + 2 \cdot 3)$
$= (\mathbf{62}, \mathbf{-19}, \mathbf{-32})$

$T(7,13,3) = (2 \cdot 7 - 3 \cdot 13 + 3, 7 + 13 - 2 \cdot 3, -7 + 2 \cdot 13 + 2 \cdot 3) = (\mathbf{-22}, \mathbf{14}, \mathbf{25})$

$T(-3,3,-5) = (2 \cdot (-3) - 3 \cdot 3 - 5, -3 + 3 - 2 \cdot (-5), 3 + 2 \cdot 3 + 2 \cdot (-5))$
$= (\mathbf{-20}, \mathbf{10}, \mathbf{-1})$

$T(6,1,3) = (2 \cdot 6 - 3 \cdot 1 + 3, 6 + 1 - 2 \cdot 3, -6 + 2 \cdot 1 + 2 \cdot 3) = (\mathbf{12}, \mathbf{1}, \mathbf{2})$

$T(-2,2,1) = (2 \cdot (-2) - 3 \cdot 2 + 1, (-2) + 2 - 2 \cdot 1, 2 + 2 \cdot 2 + 2 \cdot 1) = (\mathbf{-9}, \mathbf{-2}, \mathbf{8})$

$T(3,-2,-4) = (2 \cdot 3 - 3 \cdot (-2) - 4, 3 - 2 - 2 \cdot (-4), -3 + 2 \cdot (-2) + 2 \cdot (-4))$
$= (\mathbf{8}, \mathbf{9}, \mathbf{-15})$

$T(-3,3,6) = (2 \cdot (-3) - 3 \cdot 3 + 6, (-3) + 3 - 2 \cdot 6, 3 + 2 \cdot 3 + 2 \cdot 6) = (\mathbf{-9}, \mathbf{-12}, \mathbf{21})$

$T(-13,5,-1) = (2 \cdot -13 - 3 \cdot 5 - 1, -13 + 5 - 2 \cdot (-1), 13 + 2 \cdot 5 + 2 \cdot (-1))$
$= (\mathbf{-42}, \mathbf{-6}, \mathbf{21})$

$T(-12,-10,6) = (2 \cdot -12 - 3 \cdot -10 + 6, -12 - 10 - 2 \cdot 6, 12 + 2 \cdot (-10) + 2 \cdot 6)$
$= (\mathbf{12}, \mathbf{-34}, \mathbf{4})$

A mensagem fica indecifrável.

?	**?**	**?**	**?**	**Q**	**?**	**?**	**P**	**S**	**B**	**M**	**E**	**?**
62	-19	-32	-22	14	25	-20	10	-1	12	1	2	-9
T	**Z**	**H**	**?**	**?**	**?**	**J**	**?**	**?**	**N**	**?**	**B**	**?**
-2	-8	8	9	-15	-9	-12	21	-42	-6	21	12	-34

Novamente encontraremos a inversa T^{-1} multiplicando o inverso do determinante de T pela adjunta da matriz transposta.

$$T = \begin{pmatrix} 2 & -3 & 1 \\ 1 & 1 & -2 \\ -1 & 2 & 2 \end{pmatrix} \rightarrow T^{-1} = \frac{1}{\det(T)} \cdot adj(T^T)$$

Calcularemos a matriz adjacente através dos cofatores da matriz transposta de T.

$$T^T = \begin{pmatrix} 2 & 1 & -1 \\ -3 & 1 & 2 \\ 1 & -2 & 2 \end{pmatrix}$$

$$adj(T^T) = \begin{pmatrix} \begin{vmatrix} 1 & 2 \\ -2 & 2 \end{vmatrix} & \begin{vmatrix} -3 & 2 \\ 1 & 2 \end{vmatrix} & \begin{vmatrix} -3 & 1 \\ 1 & -2 \end{vmatrix} \\ \begin{vmatrix} 1 & -1 \\ -2 & 2 \end{vmatrix} & \begin{vmatrix} 2 & -1 \\ 1 & 2 \end{vmatrix} & \begin{vmatrix} 2 & 1 \\ 1 & -2 \end{vmatrix} \\ \begin{vmatrix} 1 & -1 \\ 1 & 2 \end{vmatrix} & \begin{vmatrix} 2 & -1 \\ -3 & 2 \end{vmatrix} & \begin{vmatrix} 2 & 1 \\ -3 & 1 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} 6 & 8 & 5 \\ 0 & 5 & 5 \\ 3 & -1 & 5 \end{pmatrix}$$

$$T^{-1} = \frac{1}{\det(T)} \cdot adj(T^T) = \frac{1}{15} \cdot \begin{pmatrix} 6 & 8 & 5 \\ 0 & 5 & 5 \\ 3 & -1 & 5 \end{pmatrix} = \begin{pmatrix} \frac{6}{15} & \frac{8}{15} & \frac{5}{15} \\ 0 & \frac{5}{15} & \frac{5}{15} \\ \frac{3}{15} & \frac{-1}{15} & \frac{5}{15} \end{pmatrix} = \begin{pmatrix} \mathbf{\frac{2}{5}} & \mathbf{\frac{8}{15}} & \mathbf{\frac{1}{3}} \\ \mathbf{0} & \mathbf{\frac{1}{3}} & \mathbf{\frac{1}{3}} \\ \mathbf{\frac{1}{5}} & \mathbf{\frac{-1}{15}} & \mathbf{\frac{1}{3}} \end{pmatrix}$$

Assim, $\left(\mathbf{\frac{2x}{5} + \frac{8y}{15} + \frac{z}{3}, \frac{y}{3} + \frac{z}{3}, \frac{x}{5} - \frac{y}{15} + \frac{z}{3}}\right)$ será a regra para descriptografar a mensagem.

$$T^{-1}(62,-19,-32) = \left(\frac{2(62)}{5} + \frac{8(-19)}{15} - \frac{32}{3}, \frac{-19}{3} - \frac{32}{3}, \frac{62}{5} + \frac{19}{15} - \frac{32}{3}\right) = (\mathbf{4,-17,3})$$

$$T^{-1}(-22,14,25) = \left(\frac{2(-22)}{5} + \frac{8(14)}{15} + \frac{25}{3}, \frac{14}{3} + \frac{25}{3}, \frac{-22}{5} - \frac{14}{15} + \frac{25}{3}\right) = (\mathbf{7,13,3})$$

$$T^{-1}(-20,10,-1) = \left(\frac{2(-20)}{5} + \frac{8(10)}{15} - \frac{1}{3}, \frac{10}{3} - \frac{1}{3}, \frac{-20}{5} - \frac{10}{15} - \frac{1}{3}\right) = (\mathbf{-3,3,-5})$$

$$T^{-1}(12,1,2) = \left(\frac{2(12)}{5} + \frac{8(1)}{15} + \frac{2}{3}, \frac{1}{3} + \frac{2}{3}, \frac{12}{5} - \frac{1}{15} + \frac{2}{3}\right) = (\mathbf{6,1,3})$$

$$T^{-1}(-9,-2,8) = \left(\frac{2(-9)}{5} + \frac{8(-2)}{15} + \frac{8}{3}, \frac{-2}{3} + \frac{8}{3}, \frac{-9}{5} + \frac{2}{15} + \frac{8}{3}\right) = (\mathbf{-2,2,1})$$

$$T^{-1}(8,9,-15) = \left(\frac{2(8)}{5} + \frac{8(9)}{15} + \frac{-15}{3}, \frac{9}{3} - \frac{15}{3}, \frac{8}{5} - \frac{9}{15} - \frac{15}{3}\right) = (\mathbf{3,-2,-4})$$

$$T^{-1}(-9,-12,21) = \left(\frac{2(-9)}{5} + \frac{8(-12)}{15} + \frac{21}{3}, \frac{-12}{3} + \frac{21}{3}, \frac{-9}{5} + \frac{12}{15} + \frac{21}{3}\right) = (\mathbf{-3,3,6})$$

$$T^{-1}(-42,-6,21) = \left(\frac{2(-42)}{5} + \frac{8(-6)}{15} + \frac{21}{3}, \frac{-6}{3} + \frac{21}{3}, \frac{-42}{5} + \frac{6}{15} + \frac{21}{3}\right) = (\mathbf{-13,5,-1})$$

$$T^{-1}(12,-34,4) = \left(\frac{2(12)}{5} + \frac{8(-34)}{15} + \frac{4}{3}, \frac{-34}{3} + \frac{4}{3}, \frac{12}{5} + \frac{34}{15} + \frac{4}{3}\right) = (\mathbf{-12,-10,6})$$

Conseguindo assim decodificar a mensagem retornando ao texto de origem.

G	**R**	**A**	**D**	**U**	**A**	**C**	**A**	**O**	**SPC**	**M**	**A**	**T**
4	-17	3	7	13	3	-3	3	-5	6	1	3	-2
E	**M**	**A**	**T**	**I**	**C**	**A**	**SPC**	**U**	**F**	**S**	**J**	**.**
2	1	3	-2	-4	-3	3	6	-13	5	-1	-12	-10

5 – CONSIDERAÇÕES FINAIS

Chegamos ao final deste trabalho mostrando a importância das transformações lineares, não somente em aplicações teóricas dentro da álgebra linear, onde ela é mais conhecida pelos alunos, mas pudemos, além de relembrar seus conceitos básicos, demonstrar dois exemplos de aplicações reais.

Foram escolhidos dois exemplos de aplicações em que os alunos, mesmo sem perceber, utilizam quase que diariamente quando estão em frente do computador movimentando o mouse ou acessando o e-mail.

A primeira aplicação mostrou como as transformações lineares mudam a aparência e/ou a posição de cada elemento gráfico no computador, apesar das demonstrações deste trabalho serem básicas elas servem de base para transformações mais avançadas, como os filtros em softwares gráficos ou transformações em 3D.

Já na segunda aplicação demonstramos uma aplicação computacional que poucos alunos imaginariam que pudesse ser realizada através das transformações lineares, a criptografia de dados. Pois sempre que se fala em criptografia a primeira coisa que vem na cabeça são os números primos. Apesar da pequena complexidade de nosso algoritmo criptográfico, se determinarmos várias rodadas no processo, chegaremos a uma intratabilidade considerável, pois o espaço vetorial nos dá uma infinidade de combinação de números, de um em um, de dois em dois, até de n em n, o que dificulta em muito a decriptografia por pessoas não autorizadas, sendo assim, nosso objetivo de utilizar o Isomorfismo de Transformações Lineares como um método criptográfico, se mostra possível e de aplicação real.

6 – REFERÊNCIAS BIBLIOGRÁFICAS

ANTON, H., & RORRES, C. (2004). *Elementary Linear Algebra - Applications Version.* Wiley.

BOLDRINI, J. L., COSTA, S. I., FIGUEIREDO, V. L., & WETZELR, H. G. (1980). *Álgebra Linear 3ª Edição.* São Paulo: Harper & Row do Brasil.

FIARRESGA, V. M. (2010). *Criptografia e Matemática.* Universidade de Lisboa, Departamento de Matemática.

FIGUEIREDO, L. M., & CUNHA, M. O. (2009). *Álgebra Linear 1 - Módulo 3* (2ª ed., Vol. 2). Fundação CECIERJ.

HEFEZ, A., & FERNANDEZ, C. d. (2012). *Introdução á Àlgebra Linear.* Rio de Janeiro: Coleção PROFMAT.

KLAWONN, F. (2008). *Introduction to Computer Graphics using Java 2D and 3D.* London: Spinger-Verlag London Limited.

KOLMAN, B., & Hill, D. (2008). *Linear Algebra with Applications.* New Jersey: Pearson Education.

KULDEEP, S. (2014). *Linear Algebra Step by Step.* New York: Oxford University Press.

LUZ, C., MATOS, A., & NUNES, S. (2004/2005). Transformações Lineares. *Escola Superior de Tecnologia - Departamento de Matemática*. Setúbal, Portugal.

MEYER, C. D. (2000). *Matrix Analysis and Applied Linear Algebra.* Siam.

SILVA, L. H. (2009). *Transformações lineares e isomorfismos: um exemplo em criptografia.* Imperatriz: MA.

SINGH, S. (2002). *O Livro dos Códigos.* Rio de Janeiro: Record.

STEINBRUCH, A., & WINTERLE, P. (1987). *Álgebra Linear.* Makron.

VINCE, J. (2006). *Mathematics for Computer Graphics 2ª Edition.* London: Springer-Verlag.