UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

INSTITUTO DE MATEMÁTICA

A INVERSA DE DRAZIN, EM EQUAÇOES SINGULARES E CRIPTOGRAFIA

CYNTHIA FEIJÓ SEGATTO

Dissertação realizada sob orientação do Prof. Dr. Julio Cesar Ruiz Clayssen. Essa dissertação é requisito parcial para obtenção do título de Mestre em Matemática pelo Curso de Pós-Graduação em Matemática da UFRGS. (Defendida em 22/08/88)

PORTO ALEGRE

1988

SUMARIO

AGRADECIMENTOS

Ao Prof. Julio pelo seu apoio e orientação.

Ao Flávio por sua paciência e incentivo.

ABSTRACT

The inverse of Drazin is developed for rings and then restrict to the case of equare matrices over complex field and over finite fields or congruence rings. Applications to singular differential and diference equation and cryptography are considered in this work.

RESUMO

A inversa de Drazin é apresentada, sendo primeiramente estudada sobre anéis comutativos e após, esta noção é particularizada para o caso de matrizes quadradas definidas sobre o corpo dos complexos e sobre os anéis Z_t. Também são vistas aplicações da inversa de Drazin em Equações Diferenciais e em Diferenciação Matriciais com coeficientes singulares e em Criptografia.

INTRODUÇÃO:

No capítulo I, "A inversa de Drazin, em anéis", a inversa de Drazin é apresentada e é feito um estudo de suas propriedades em um anel qualquer, como sua unicidade quando existir.

Além disto, é feita uma rápida comparação com a π-regularidade de Azumaya.

No capítulo II, "A inversa matricial de Drazin", a noção de inversa de Drazin é particularizada para o anel das matrizes quadradas n x n definidas sobre o corpo dos complexos. Para este anel, é garantida a existência da inversa de Drazin para qualquer elemento A, isto é, existe uma única matriz A^D tal que:

$$A^D A = A A^D$$

$$A^D A A^D = A^D$$

$$A^{m+1} A^D = A^m, \quad \text{para algum } m > 0$$

No capítulo III, "A inversa matricial de Drazin em corpos e anéis finitos", é feita uma extensão do estudo da inversa de Drazin para corpos e anéis finitos, visando aplicações em criptografia.

Nos capítulos IV e IV são feitas aplicações da inversa de Drazin em sistemas de equações diferenciais matriciais, codificação e decodificação criptográfica.

CAPITULO I

I - INVERSAS DE DRAZIN EM ANÉIS

I.1 - INTRODUÇÃO

"As únicas álgebras com divisão sobre o corpo dos números reais são a menos de isomorfismos, o próprio corpo dos números reais, o corpo dos números complexos e os quartenios reais" (1).

Este clássico teorema de Frobenius, estabelece que não existe outro sistema hipercomplexo além dos reais e dos complexos, que possua simultaneamente as propriedades de comutatividade e inversibilidade de elementos não nulos. Para exemplificar este problema, basta tomar o caso do conjunto M_n (conjunto de todas as matrizes quadradas nxn definidas sobre o corpo dos complexos); Em geral, neste Sistema temos que $AB \neq BA$, um elemento não nulo pode não possuir inverso multiplicativo e além disto, pode ocorrer que existam A, B elementos não nulos de M_n tais que $A\,B = 0$ mesmo que $B\,A \neq 0$.

Muitos problemas interessantes recaem em equações do tipo $Ax' + Bx = f$, com $A,B \in M_n$, portanto é necessário que sua solução possa ser encontrada, mesmo que A^{-1} não exista. Para tanto, iremos desenvolver um estudo sobre a inversa de Drazin, que possibilitará resolver muitos problemas no caso de matrizes singulares.

I.2 - PROPRIEDADES E DEFINIÇÕES:

A seguir, introduziremos o conceito de inversa de Drazin (3), propriedades relativas a unicidade e relações com a π - regularidade de Azumaya (2).

DEFINICAO I.2.1

Dado um anel associativo R e $x \in R$ então, x possui inversa de Drazin em R, se existe $c \in R$, tal que:

i) $cx = xc$

ii) $x^m = x^{m+1}c$; algum $m \in \mathbb{N}^*$

iii) $c = c^2x$

TEOREMA I.2.1

Seja R um anel associativo. Se $x \in R$, então x possui no máximo uma inversa de Drazin, e além disto, se esta inversa de Drazin existe, ela comuta com todos os elementos que comutam com x.

PROVA:

Sejam R anel associativo e $x \in R$. Vamos supor que c_1, c_2 sejam duas inversas de Drazin de x.

Assim temos:

Existem $m \in \mathbb{N}^*$, $n \in \mathbb{N}^*$ tais que:

$$c_1x = xc_1 \quad ; \quad x^m = x^{m+1}c_1 \quad ; \quad c_1 = c_1^2x$$

$$c_2x = xc_2 \quad ; \quad x^n = x^{n+1}c_2 \quad ; \quad c_2 = c_2^2x$$

Vamos supor que $m > n$ assim $\exists\ r \in \mathbb{N}^*$ tal que $m = r + n$.

E assim:

$$c_1 x^{m+1} = x^{m+1} c_1 = x^m = x^{r+n} = x^r \cdot x^n =$$

$$= x^r \, x^{n+1} c_2 = x^{r+n+1} c_2 = x^{m+1} c_2$$

Isto é:

A) $c_1 \, x^{m+1} = x^m = x^{m+1} c_2$

Por outro lado:

B) $$c_1 = c_1^{\,2} x = x c_1^{\,2}$$
$$c_2 = c_2^{\,2} x = x c_2^{\,2}$$

Vamos agora mostrar que $c_i = c_i^{\,n+1} \, x^n$, $n \in \mathbb{N}$. usando indução temos:

para $k = 1$

$$c_i = c_i^{\,2} x \quad \text{por B}$$

Vamos supor válido para $n \leq k$, $n \in \mathbb{N}$

Vamos provar que vale para $n = k + 1$

$$c_i^{\,(k+1)+1} \, x^{(k+1)} = c_i^{\,k} \, c_i^{\,2} x \, x^k = c_i^{\,k} \, c_i \, x^k = c_i^{\,k+1} \, x^k = c_i$$

pela hipótese de indução; e em particular obtemos:

C) $c_1 = c_1^{\,m+1} \, x^m \quad ; \quad c_2 = x^m \, c_2^{\,m+1}$

Assim, por A e C

$$c_1 = c_1^{\,m+1} \, x^m = c_1^{\,m+1} \quad (c_2 \, x^{m+1}) = (c_1^{\,m+1} \, x^m) \times c_2 =$$

$$= c_1 x c_2 = c_1 x \, (x^m c_2^{\,m+1}) = (c_1 \, x^{m+1}) \, c_2^{\,m+1} = x^m \, c_2^{\,m+1} = c_2$$

Assim provamos que $x \in R$ possui no máximo uma inversa de Drazin. Vamos supor agora que:

$x \in R \; ; \; \exists c \in R$, c inversa de Drazin de x

Seja y e R tq. ; xy = yx

Assim:

$$c\,x^m\,y = cyx^m = c\,y\,(x^{m+1}c) = c\,x^{m+1}\,yc = x^m\,y\,c$$

de onde por indução obtemos:

$c^{m+1}\,x^m\,y = x^m\,y\,c^{m+1}$ e portanto:

$$cy = c^{m+1}\,x^m\,y = x^m\,y\,c^{m+1} = yx^m\,c^{m+1} =$$
$$= y\,c^{m+1}\,x^m = yc$$

C.Q.D.

Este teorema nos diz que a inversa de Drazin, se existe é única e portanto podemos notá-la por x^d. Além disto quando x é inversível temos que $x^{-1} = x^d$, pois x^{-1} satisfaz i, ii, iii exigidos pela definição 1.

COROLÁRIO 1.2.1.1

Se $x_1, x_2, \ldots x_j$ são elementos de um anel associativo R, tais que $x_1^d, x_2^d, \ldots, x_j^d$ existem e com $x_s \cdot x_t = 0$ (s, t = 1,2,...j e s ≠ t), então:

$x_1 + x_2 + \ldots + x_j$ possui inversa de Drazin, com:
$(x_1 + x_2 + \ldots x_j)^d = x_1^d + x_2^d + \ldots + x_j^d$

PROVA:

Sem perda de generalidade, suponhamos j = 2.

Seja $x_1 = u$ e $x_2 = v$, com $u.v = 0 = v.u$

Isto é u e v comutam; Assim pelo teorema 1 temos que u, u^d, v, v^d comutam.

i) $(u^d + v^d)(u + v) = u^d u + u^d v + v^d u + v^d v$

$= u\,u^d + vu^d + uv^d + vv^d$

$= (u + v)(u^d + v^d)$

ii) $(u^d + v^d)^2 (u + v) = ((u^d)^2 + u^d v^d + v^d u^d + (v^d)^2)(u+v)$

$= (u^d)^2 u + (v^d)^2 v = u + v$

iii) Escolhendo m suficientemente grande temos que:

$$u^m = u^{m+1}\,u^d \quad e \quad v^m = v^{m+1}\,v^d$$

Logo:

$$(u + v)^{m+1}\,(u^d + v^d) = u^{m+1}\,u^d + v^{m+1}\,v^d = u^m + v^m = (u+v)^m$$

Assim vemos que $(u^d + v^d)$ satisfaz as propriedades da definição 1 para o elemento $u + v \in R$; assim pela unicidade da inversa de Drazin, quando existe temos que:

$$(u + v)^d = (u^d + v^d)$$

C.Q.D.

DEFINIÇÃO I.2.2

Chamamos de "índice de x" e notamos por $ind(x)$ ao menor inteiro positivo tal que $x^m = x^{m+1}\,x^d$

OBS: Convenciona-se que quando a inversa de Drazin de um elemento $x \in R$ não existe, então $ind(x) = \infty$

TEOREMA I.2.2

Seja $x \in R$, anel associativo tal que x^d exista, seja $k \in \mathbb{N}^*$ então x^k possui inversa de Drazin $(x^k)^d = (x^d)^k$ e $ind(x^k) = q \in \mathbb{N}^*$, tal que $0 \leq kq - ind(x) < k$.

PROVA:

Por i) da definição 1 e indução temos que:

$$x^k (x^d)^k = (x^d)^k x^k$$

Também por indução, por ii) e iii) da definição 1 respectivamente temos que:

$$x^{ind(x)} = x^{ind(x)+j} (x^d)^j \text{ e que}$$

$$x^d = (x^d)^{j+1} x^j, \text{ para } j = 1,2,...$$

Logo, como $kq \geq ind(x)$ temos

$$\begin{aligned}(x^d)^k &= x^{kq - ind(x)} x^{ind(x)} \\ &= x^{kq - ind(x)} x^{ind(x)+k} (x^d)^k = \\ &= (x^k)^{q+1} (x^d)^k\end{aligned}$$

e

$$(x^d)^k = (x^d)^{k+1} x^k = ((x^d)^k)^2 x^k$$

Assim $(x^d)^k$ satisfaz as condições para $(x^k)^d$ e $ind(x) \leq q$.

Finalmente, se $ind(x^k) < q$ teríamos:

$(x^k)^{q-1} = x^k (x^d)^k$ e como $x^d = x^{k-1} (x^d)^k$

e portanto

$$\begin{aligned}x^{k(q-1)} &= x^{kq + (k-1) - (k-1)} (x^d)^k = \\ &= x^{k(q-1)+1} (x^{k-1} (x^d)^k) = x^{k(q-1)+1} x^d\end{aligned}$$

isto é, pela definição de ind(x) teríamos que:

$$k\,(q-1) \geq \text{ind}(x)$$

o que contradiria nossa definição de q.

C.Q.D.

TEOREMA I.2.3

Dado um elemento x de um anel associativo, então se x possui inversa de Drazin x^d, temos que x^d também possui inversa de Drazin $(x^d)^d$, e $\text{ind}(x^d) = 1$, logo $(x^d)^d = x^2 x^d$.

PROVA:

Seja $x \in R$ anel, tq x^d exista.

Seja $f = x^2 x^d$

Vamos mostrar que $f = (x^d)^d$.

i) $x^d f = x^d x^2 x^d = x^d x x x^d = x^2 x^d x^d = f x^d$

ii) $f = x^2 x^d = x^2 (x^d)^2 x = x^2 x^d x x^d = f x (x^d)^2 x$

$= f x^2 x^d x^d = f^2 x^d$

iii) $(x^d)^2 f = (x^d)^2 x^2 x^d = (x^d)^2 x x x^d =$

$= x^d x x^d = (x^d)^2 x = x^d$

logo:

$$(x^d)^m = (x^d)^{m-1} x^d = (x^d)^{m-1} (x^d)^2 f =$$

$$= (x^d)^{m+1} f \qquad \text{para } m \geq 1$$

logo temos pelas definições 1 e 2 que:

$f = (x^d)^d$ e $\text{ind}(x^d) = 1$

C.Q.D.

COROLÁRIO I.2.3.1

Dado um elemento x de um anel associativo R, então $(x^d)^d = x$ se e somente se x possui inversa de Drazin e ind(x) = 1, neste caso, para $y \in R$; $xy = yx$ se e somente se $x^d y = yx^d$

PROVA:

Se $(x^d)^d = x$ pelo teorema anterior temos $ind((x^d)^d) = 1$ e portanto ind(x) = 1.

Vamos supor que x^d existe e que ind(x) = 1 dai como:

$x = x^2 x^d$, pelo teorema anterior temos

$(x^d)^d = f = x^2 x^d = x$

C.Q.D.

COROLÁRIO I.2.3.2

Dado um elemento $x \in R$ anel associativo tal que x^d exista, então $((x^k)^d)^d = x^k$, para $k \in \mathbb{N}$ e $k \geq ind(x)$.

PROVA:

Seja $x \in R$ tal que x^d exista.

Pelo teorema 1.2.2 temos que existe $(x^k)^d = (x^d)^k$, assim pelo teorema 1.2.3 $ind((x^k)^d) = 1$ e portanto pelo corolário 2.2.3.1 temos que $((x^k)^d)^d = x^k$.

C.Q.D.

COROLÁRIO I.2.3.3

Dado $x \in R$ anel associativo, tal que x^d exista então $((x^d)^d)^d = x^d$

PROVA:

Pelo teorema 1.2.3, como x^d existe, temos que $(x^d)^d$ existe e $ind(x^d) = 1$ assim pelo corolário 1.2.3.1 $((x^d)^d)^d = x^d$

C.Q.D.

Agora faremos um breve estudo sobre π - regularidade seguindo Azumaya (2) e assim mostraremos que a π - regularidade à direita implica na existência da inversa de Drazin.

DEFINIÇÃO I.2.3

Seja R um anel associativo, dizemos que $x \in R$, é fortemente π - regular em R se existem $a \in R$, $b \in R$ e $p \in \mathbb{N}^*$, $q \in \mathbb{N}^*$ tais que:

1) $x^P = x^{P+1} \cdot a$

2) $x^q = bx^{q+1}$

TEOREMA I.2.4

Dado um elemento $x \in R$ anel associativo, então x^d existe se e somente se x é fortemente π - regular.

PROVA:

Vamos supor que x^d existe; assim para qualquer $m \geq ind(x)$ temos:

$$x^m = x^{m+1} x^d \quad e \quad x^d x = x x^d$$

logo:

Existem $a = b = x$ e $p = q = m$ tais que

$$x^P = x^{P+1} \cdot q \quad e \quad x^q = b.x^{q+1}$$

Vamos supor agora que x é fortemente π - regular, assim existem $a, b \in R$ e $p, q \in \mathbb{N}^*$ tais que:

$$x^P = x^{P+1} \cdot a \quad e \quad x^q = bx^{q+1}$$

seja $m = máx\ (p, q)$ e $c = x^m a^{m+1}$

daí:

$$x^{m+1} a = x^m = bx^{m+1}$$

e

$$x^m.a = b.x^{m+1}.a = bx^m$$

assim por indução temos que

$$x^m a^k = b^k a^m \quad \text{para} \quad k = 1,2,...$$

escolhendo $c = x^m a^{m+1} = b^{m+1} x^m$ temos as propriedades:

i) $xc = x x^m a^{m+1} = x^{m+1} a a^m = x^m a^m = b^m x^m =$

$= b^{m+1} x^{m+1} = b^{m+1} x^m x = c x$

ii) Por indução temos que

$$x^{m+k}\ a^{k} = x^{m}$$

iii) Por i e ii acima:

$$c^{2}m = cxc = cx^{m+1}\ a^{m+1} = x^{m+1}\ c\ a^{m+1} =$$

$$= x^{m}\ a^{m+1} = c$$

Assim pela definição 1.2.1 e pelo teorema 1.2.1 temos que $c = x^{d}$

C.Q.D.

Pela prova do teorema anterior temos que ind (x) $\leq$ max (p, q), além disto também é fácil mostrar que ind(x) $\leq$ min (p, q), pois se $p < q$ temos que:

$$x^{P} = x^{P} + (q-p)\ a^{q-p} = x^{q}\ a^{q-p}$$

assim,

$$b\ x^{P+1} = b\ x\ x^{q}\ a^{q-P} = b\ x^{q+1}\ a^{q-1} =$$

$$= x^{q}\ a^{q-p} = x^{P}$$

Para maiores informações sobre π - regularidade, ver Azumaya (2).

COROLÁRIO 1.2.4.1

Seja R uma álgebra de dimensão finita. Então para um dado $x \in R$, existe x^{d} e x^{d} pertence a uma subalgebra gerada por x.

PROVA:

Seja $k = \dim(R)$, desta forma temos que

$x, x^2, x^3, \ldots, x^k, x^{k+1}$ são linearmente dependentes, dai, para $j \leq k+1$, x^j pode ser escrito como uma combinação linear do x^{j+1}, $x^{j+2}, \ldots,$ isto é:

$$x^j = \sum_{i=j+1}^{k+1} a_i x^i = \sum_{i=0}^{k-j} (a_{j+i+1} x^i) x^{j+1}$$

Assim x é fortemente π - regular com $a = b$ na definição de fortemente π - regular como um polinômio em x e assim pelo teorema 1.2.4 x^d existe.

C.Q.D.

Mais geralmente, este resultado vale para todos os anéis algébricos, nos quais por definição a cada elemento x corresponde um inteiro $j(x)$ tal que $x^{j(x)}$ é combinação linear de $x^{j(x)+1}$ e potências maiores.

Da definição e da unicidade temos que tomar a inversa de Drazin, quando existir, de um elemento comuta com todo homomorfismo e anti-homomorfismo contidos no anel. Em particular, numa álgebra matricial sobre o corpo dos complexos, a inversa de Drazin de um conjugado (ou transposto) de uma matriz dada é o complexo conjugado (ou transposto) da inversa de Drazin. Assim, a inversa de Drazin de uma matriz x dada, é real (simétrica hermiteana, etc...) quando x o for. Pode-se também mostrar usando iii) e o coro

lário 1.2.4.1 que a propriedade de ter todos os autovalores reais e não negativos é preservada.

I.3 CONDIÇÕES SUFICIENTES PARA A PSEUDO-INVERSIBILIDADE EM ANÉIS.

Seguindo Azumaya (2) podemos definir:

DEFINIÇÃO I.3.1

Seja R um anel associativo. Dizemos que $x \in R$ é π - regular à direita se existem p inteiro positivo e $a \in R$ tais que $x^P = x^{P+1}a$.

DEFINIÇÃO I.3.2

Chamamos de índice de x à direita em R anel associativo e notamos por r(x) ao menor inteiro p tal que $x^P = x^{P+1}.a$, para $a \in R$; Dizemos que $r(x) = \infty$ se x não é π - regular à direita.

Da mesma forma podemos definir:

DEFINIÇÃO I.3.3

Seja R um anel associativo, dizemos que $x \in R$ é π - regular à esquerda se existem q inteiro positivo e $b \in R$ tais que: $x^q = bx^{q+1}$.

DEFINIÇÃO I.3.4

Seja R um anel associativo, chamamos de índice à esquerda em R e notamos por $l(x)$ ao menor inteiro q tal que $x^q = bx^{q+1}$, para $b \in R$; Dizemos que $l(x) = \infty$ quando x não é π - regular à esquerda.

Obviamente, pelo teorema 4 temos que $ind(x)$ é finito se e somente se $r(x)$ e $l(x)$ são finitos e seguindo a demonstração deste mesmo teorema temos que se $ind(x) < \infty$ então $ind(x) = l(x) = r(x)$. Observamos também que apesar não existir inversa de Drazin de um elemento $x \in R$, pode acontecer de $l(x) < \infty$ e $r(x) < \infty$.

DEFINIÇÃO I.3.5

Seja T um subconjunto de um anel associativo R, assim definimos:

$$i(T) = \sup ind(x), \quad x \in T$$

$$r(T) = \sup r(x), \quad x \in T$$

$$l(T) = \sup l(x), \quad x \in T$$

Onde o supremo tem conversão natural para valores infinitos; isto é, $i(T) = \infty$ sempre que $ind(x) < \infty$, $\forall x \in T$, mas estes valores são ilimitados, ou quando $i(x) = \infty$ para algum $x \in T$, observações similares valem para $r(T)$ e $l(T)$.

Notemos também que $r(T) \leq i(T)$ e também que as definições de $ind(x)$, $l(x)$ e $r(x)$ são consistentes com o

conceito de índice de um dado elemento nilpotente de um anel, isto é, cada elemento x nilpotente, possui inversa de Drazin $x^d = 0$ e portanto $ind(x) = r(x) = l(x) < \infty$ e satisfaz:

$$x^{ind(x)} = 0 \quad com \quad x^{ind(x)-1} \neq 0$$

(caso contrário, como $x^{ind(x)} = x^{ind(x)+k} \cdot (x^d)^k$ (*) para algum k grande se $x^{i(x)-1} = 0$ teríamos que (*) vale para ind(x)-1 o que seria uma contradição).

Seja $N(R) = \{x \in R / x$ é nilpotente$\}$, assim observamos que:

$i(N) = r(N) = l(N)$ possivelmente infinitos, agora se $i(N) < \infty$ teríamos expressa a condição dos elementos nilpotentes terem índice limitado.

TEOREMA 1.3.1

Seja R um anel associativo, cujos elementos nilpotentes tem índice limitado ($i(N) < \infty$). Então cada elemento x π - regular à direita de R possui inversa de Drazin, com $ind(x) = r(x) = l(x) \leq i(N)$.

PROVA:

Seja $x \in R$ π - regular a direita.

Dai existem p inteiro positivo e $q \in R$ tais que $x^P = x^{P+1}.a$

Pelo teorema 1.2.4 basta-nos mostrar que existem q inteiro positivo e $b \in R$ tais que $x^q = b.x^{q+1}$

Por indução temos; $x^P = x^{P+k} \cdot a^k$, $k = 1,2...$ e assim,

$$x^{P+k}\ (x^P - a^k.\ x^{P+k}) = (x^P - x^{P+k}.a^k)\ x^{P+k} = 0$$

para $k = 1,2,\ldots$

e também, cada um dos 2^t monômios da expressão $(x^P - a^k\ x^{P+k})^t$, possuem x^{P+k} como fator pela direita, e assim tomando-se $p.t > p+k$ temos que para cada k; $(x^P - a^k\ .\ x^{P+k})^{t+1} = 0$ para t suficientemente grande.

Como $i(N) < \infty$ temos que:

$(x^P - a^k\ x^{P+k})^{i(N)} = 0$ e assim

$$x^{i(N)P} \in Rx^{P+k},\quad k = 1,2,\ldots$$

Agora escolhendo $k = (i(N) - 1)\ p+1$ chegamos ao desejado, isto é:

$b \in R$ tal que $x^q = b\ x^{q+1}$ onde $q = i(N)\ p$ e assim de i) e ii) da definição 1.2.1 temos que $(x - x^2\ x^d)^m = 0$ para algum m, de onde concluimos que

$(x - x^2\ x^d)^{i(N)} = 0$ e assim por i)

$x^{i(N)} = x^{i(N)+1}\ .\ y$, onde y é um polinômio em x e x^d, adequado com coeficientes inteiros e sem termos constantes e logo, por i) e pela prova do teorema 4 concluimos que $ind(x) \leq i(N)$.

C.Q.D.

OBS.: Na demonstração acima foi explicitada a representação $x^d = x^P.\ a^{P+1}$.

COROLÁRIO 1.3.1.1

Seja R um anel associativo cujos elementos nilpotentes tem índice limitado. Então, se cada elemento de R é π - regular à direita, R deve ser limitadamente π - regular à direita, isto é r(R) é finito e r(R) = i(R) = i(N) $< \infty$.

PROVA:

Do teorema 1.3.1 segue que

$i(R) \leq i(N)$, assim

$$r(R) \leq i(R) = i(N) \leq r(R)$$

C.Q.D.

Nota: Azumaya (2) mostra que a hipótese do corolário 1.3.1.1 de π - regularidade à direita pode ser substituída por π - regularidade.

CAPITULO II

II - A INVERSA MATRICIAL DE DRAZIN

2.1 INTRODUÇÃO

Neste capítulo será explorado o conceito de inversa de Drazin para o caso particular da Álgebra das matrizes quadradas n x n definidas sobre o corpo dos complexos M_n. O fato de M_n possuir divisores do zero, ou seja de não possuir inversa multiplicativa para todos os seus elementos distintos de zero, faz da inversa de Drazin uma fonte de estudo bastante interessante. Em particular, ela é de grande utilidade na resolução de equações diferenciais (ou em diferenças) matriciais com coeficiêntes sigulares.

Também será visto que a inversa matricial de Drazin de uma matriz quadrada A, pode ser expressa como um polinômio em A, cujos coeficientes podem ser calculados em termos dos autovalores de A, ou através da forma canônica de Jordan, pela qual podemos encontrar uma matriz não singular T, tal que para qualquer $A \in M_n$;

$$A = T\begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1} \qquad (1)$$

onde C é inversível e $C \in M_s$ e N é nilpotente e $N \in M_t$ onde $s = \dim(R(A^k))$, $t = \dim(N(A^k))$ e $n = s+t$

Além disto será mostrado que

$$A^D = T\begin{bmatrix} C^{-1} & 0 \\ 0 & 0 \end{bmatrix} T^{-1} \qquad (2)$$

é a inversa de Drazin de A. Observa-se também que se A é inversível o bloco N ausentar-se-á de (1) e portanto $A^D = A^{-1}$

e se A é nilpotente o bloco C ausentar-se-á de (1) e portanto $A^D=0$.

2.2 DEFINIÇÕES E PROPRIEDADES ALGÉBRICAS

Se A é uma matriz complexa n x n, é conhecido que existe um inteiro não negativo m tal que $C^n=R(A^m)+N(A^m)$, ou equivalentemente, posto (A^{m+1}) = posto (A^m), onde R e N denotam respectivamente imagem e núcleo. O menor inteiro com esta propriedade é chamado de índice da matriz A e será notado por K= ind(A). Quando K= 0 temos que A é não singular.

Como já é conhecido pelo capítulo anterior que a inversa de Drazin quando existe é única, podemos definir:

DEFINIÇÃO 2.2.1

Seja $A \in M_n$ com K= ind(A). Uma matriz A^D com as propriedades:

i) $A^D A A^D = A^D$

ii) $A A^D = A^D A$

iii) $A^{K+1} A^D = A^K$

Será dita a inversa de Drazin de A.

A existência da inversa matricial de Drazin é conseqüência de uma das variações mais simples do teorema de Jordan.

TEOREMA 2.2.1

Sejam $A \in M_n$ e $ind(A) = k \geq 0$, então existe uma matriz T não singular tal que:

$$A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$$

onde C é inversível e N nilpotente de índice K.

PROVA:

Seja A uma transformação linear induzida sobre C^n e $K = ind(A)$

se $r = posto\ (A^K)$ então $dim(N(A^K)) = n - r$

sejam

$V_1, V_2, \ldots, V_r$ uma base para $R(A^K)$

$V_{r+1}, V_{r+2}, \ldots, V_n$ uma base para $N(A^K)$

como

$C^n = R(A^K) + N(A^k)$

$V_1, V_2, \ldots, V_n$ é uma base para C^n.

Como $R(A^K)$ e $N(A^K)$ são subespaços invariantes de A e $A^K(N(A^K)) = 0$, tomando

$T = [V_1, V_2, \ldots, V_n]$ temos o teorema.

C.Q.D.

Utilizando a definição de inversa de Drazin e a forma canônica para A será encontrada agora, a forma

da inversa de Drazin A^D.

$$\text{Seja } A = T \begin{bmatrix} C & O \\ O & N \end{bmatrix} T^{-1}$$

com $T \in M_n$ não singular

$A \in M_n$

C matriz quadrada não singular.

N matriz nilpotente de ordem K.

$$\text{Seja } A^D = T \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} T^{-1}$$

onde A_{ij} (i= 1,2; j= 1,2) são matrizes quadradas onde C e A_{11} tem as mesmas dimensões. Para que A^D seja a inversa de Drazin da matriz A, devemos ter que

$$A^{k+1} A^D = A^K, \text{ logo:}$$

$$T \begin{bmatrix} C^{k+1} & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} T^{-1} = T \begin{bmatrix} C^K & 0 \\ 0 & 0 \end{bmatrix} T^{-1}$$

e assim, concluimos que

$$A_{11} = C^{-1} \quad \text{e} \quad A_{12} = 0$$

usando a comutatividade entre A e A^D temos que

$$A^D \cdot A^{k+1} = A^K, \text{ isto é } A_{21} = 0$$

Finalmente, como $A^D A A^D = A^D$, temos

$$T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} \begin{bmatrix} C^{-1} & 0 \\ 0 & A_{22} \end{bmatrix} T^{-1} = T \begin{bmatrix} C^{-1} & 0 \\ 0 & A_{22} \end{bmatrix} T^{-1}$$

logo:

(3) $N.(A_{22})^2 = A_{22}$ multiplicando por N^{k-1}:

$$N^k (A_{22})^2 = N^{k-1} A$$

(4) $0 = N^{k-1} A_{22}$ isto é $0 = N^{k-1}(A_{22})^2$

da mesma forma, multiplicando (3) por N^{k-2}

$$N^{k-1}(A_{22})^2 = N^{k-2} A_{22}$$

por 4

$$N^{k-2} A_{22} = 0$$

usando o mesmo raciocínio sucessivamente, temos:

$$A_{22} = N(A_{22})^2 = 0 \quad \text{isto é} \quad A_{22} = 0$$

e portanto

$$A^D = T \begin{bmatrix} C^1 & 0 \\ 0 & 0 \end{bmatrix} T^{-1}$$

que satisfaz a definição 2.2.1. Como M_n é um anel associativo, decorre do teorema do capítulo I e da construção acima que A^D existe e é única. Além disto A^D coincide com A^{-1} quando ind(A) = 0.

Temos assim as propriedades:

i) $A^{P+1} A^D = A^P$ se $p \geq \text{ind}(A)$. p inteiro não negat.

ii) Se A é não singular $A^D = A^{-1}$

iii) $R(A^D) = R(A^K)$

iv) $N(A^D) = N(A^K)$

v) $A \cdot A^D = A^D \cdot A = P_{R(A^K)} \cdot N(A^K)$

vi) $(I - A A^D) = (I - A^D A) = P_{N(A^K)} \cdot R(A^K)$

onde K = ind (A)

TEOREMA 2.2.2

Sejam $A \in M_n$ tal que ind(A)= K, p inteiro não negativo e X elemento de M_n tal que XAX= X, AX= XA e A^{p+1} X= X, então $p \geq K$ e $X= A^D$.

PROVA:

Se A^{p+1} X= A^p então $R(A^{p+1}) \subseteq R(A^p)$
seja $r \in R(A^p)$ isto é; existe y tal que A^p Y= r
ou A^{p+1} XY= r, isto é $r \in R(A^{p+1})$
logo A^{p+1} X= A^p e $R(A^p)= R(A^{p+1})$ e assim só podemos ter que $p \geq k$.

Agora, seja p= k + i com $i \geq 0$
$A^K= A^{P-i} = A^{-i} A^P = A^{-i} A^{p+1}$ X= A^{P-i+1} X= A^{K+1} X e assim X satisfaz a definição de A^D, logo pela existência e unicidade de A^D já provadas tem que $X= A^D$.

C.Q.D.

DEFINIÇÃO 2.2.2

Seja $A \in M_n$, chamamos de "CENTRO DE A" e notamos por C_A, ao produto

$$C_A= A A^D A= A^2 A^D= A^D A^2$$

DEFINIÇÃO 2.2.3

Seja $A \in M_n$, chamamos de "PARTE NILPOTENTE DE A" e notamos por N_A, à expressão:

$$N_A = A - C_A = (I - A^D A)A$$

DEFINIÇÃO 2.2.4

A decomposição $A = C_A + N_A$ é dita decomposição "CENTRO NILPOTENTE DE A".

Agora em termos da representação canônica de A, serão encontradas as formas de C_A e N_A como já foi feito para A^D. Isto é, sabemos que existem T,C matrizes inversíveis e N matriz nilpotente tais que:

$$A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1} \quad e \quad A^D = T \begin{bmatrix} C^{-1} & 0 \\ 0 & 0 \end{bmatrix} T^{-1}$$

assim,

$$C_A = A^2 A^D = T \begin{bmatrix} C & 0 \\ 0 & 0 \end{bmatrix} T^{-1}$$

e

$$N_A = A - C_A = T \begin{bmatrix} 0 & 0 \\ 0 & N \end{bmatrix} T^{-1}, \quad N_A \text{ nilpotente de índice } K = \text{ind}(A)$$

TEOREMA 2.2.3

Seja $A \in M_n$, A possui decomposição única na forma $A = X + Y$ onde $XY = YX = 0$ $\text{ind}(X) \leq 1$ e Y nilpotente de índice $K = \text{ind}(A)$. Mais ainda, neste caso $X = C_A$ e $Y = N_A$.

PROVA:

$$\text{Seja} \quad A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$$

sejam X, Y tais que $A = X + Y$, $XY = YX = 0$, $ind(X) \leq 1$ e Y nilpotente com índice $K = ind(A)$.

- se $ind(X) = 0$ então X é inversível, logo $Y = 0$ e A é inversível.

- se $ind(X) = 1$:

vamos escrever X e Y em sua forma canônica

$$X = P \begin{bmatrix} C_1 & 0 \\ 0 & C_1 \end{bmatrix} P^{-1} \quad \text{e} \quad Y = P \begin{bmatrix} C_2 & 0 \\ 0 & N_2 \end{bmatrix} P^{-1}$$

como $ind(X) = 1 \rightarrow N_1 = 0$

como Y é nilpotente $C_2 = 0$

Assim temos que $XY = YX = 0$

e $A = X + Y \rightarrow C_1 = C$ e $N_2 = N$

logo

$$X = C_A \quad \text{e} \quad Y = N_A$$

C.Q.D.

COROLÁRIO 2.2.3.1

Seja $A \in M_n$, p inteiro positivo, assim:

$(C_A)^P = C_A$; $(N_A)^P = N_A$; $A^D = C_A + N_A$

se $p \geq ind(A)$ então $A^D = C_A$

LEMA 2.2.1

Seja $A \in M_n$ valem as afirmações

i) $N_A . C_A = C_A . N_A = 0$

ii) $N_A . A^D = A^D N_A$

iii) $ind(A^D) = ind(C_A) = 1$ se $ind(A) \geq 1$
e 0 se $ind(A) = 0$

iv) $C_A \; A \; A^D = A \; A^D \; C_A = C_A$

v) $(A^D)^D = C_A$

vi) $A = C_A$ se $ind(A) \leq 1$

vii) $((A^D)^D)^D = A^D$

viii) $A^D = (C_A)^D$; $C_A \; C_A^D \; C_A = C_A$

ix) $(A^D)^T = (A^T)^D$

x) $(I - A \; A^D)^D = I - A \; A^D$

xi) $A^D (I - A \; A^D) = (I - A \; A^D) \; A^D = 0$

xii) $(a \; A)^D = a^{-1} \; A^D$ se a^{-1} existe

xiii) $(I - A \; A^D)^r = I - A \; A^D$ para $r = 1,2,3,...$

OBS.: Para demonstrar qualquer das propriedades acima basta fazer as contas usando a forma canônica, e em xiii) usando indução.

2.3 PROPRIEDADES ESPECTRAIS DA INVERSA DE DRAZIN

Neste item, a notação $\partial(A)$ será usada como sendo o espectro da matriz A, isto é:

$\partial(A) = \{ w / w$ é autovalor de $A\}$

Da álgebra Linear, sabemos que se A é uma matriz não singular valem as propriedades:

1) $w \in \partial(A)$ se e somente se $w^{-1} \in \partial(A)$.

2) X é autovetor associado à w de A se e somente se X é autovetor associado à w^{-1} de A^{-1}.

3) Se $A \in M_n$ e X é um vetor não nulo, tal que existe p inteiro positivo e $w \in \partial(A)$ escalar, para o qual $(A - wI)^P X = 0$ e $(A - wI)^{P-1} X \neq 0$, então X é dito autovalor generalizado de A de grau p.

4) X é autovalor generalizado de grau p de A associado à $w \in \partial(A)$ se e somente se X^{-1} é autovalor generalizado de grau p de A^{-1} associado a $w^{-1} \in \partial(A^{-1})$.

Nesta seção, serão vistas algumas situações semelhantes a estas para a inversa de Drazin A^D.

TEOREMA 2.3.1

Sejam $A \in M_n$, $k = ind(A)$, $w \neq 0$

i) $w \in \partial(A)$ se e somente se $w^{-1} \in \partial(A^D)$

ii) X é autovetor generalizado de A de grau p associado à $w \in \partial(A)$ se e somente se X é autovetor generalizado de A^D de grau p associado a $w^{-1} \in \partial(A^D)$

iii) X é autovetor generalizado de A associado à $w = 0$ se e somente se $X \in N(A^K) = N(A^D)$

PROVA:

Se ind(A)= 0 então A é inversível, logo vale o teorema.

Se ind(A) $\geq$ 0

Seja $A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$ e $X = T \begin{bmatrix} U_1 \\ U_2 \end{bmatrix}$

com T,C inversíveis, N nilpotente, X autovetor generalizado de A de grau p associado a $w \neq 0$

Assim

$$(A - wI)^p X = 0 \quad e \quad (A - wI)^{p-1} X \neq 0$$

isto é

$$\left[T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1} - T \begin{bmatrix} wI & 0 \\ 0 & wI \end{bmatrix} T^{-1} \right]^p T \begin{bmatrix} U_1 \\ U_2 \end{bmatrix} = 0$$

$$\left[T \begin{bmatrix} C - wI & 0 \\ 0 & N - wI \end{bmatrix} T^{-1} \right]^p T \begin{bmatrix} U_1 \\ U_2 \end{bmatrix} = 0$$

$$\begin{bmatrix} (C - wI)^p U_1 \\ (N - wI)^p U_2 \end{bmatrix} = 0$$

e isto ocorre se e somente se U_1 é autovetor generalizado de grau p para C e $U_2 = 0$.

Como C é inversível e

$A^D = T \begin{bmatrix} C & 0 \\ 0 & 0 \end{bmatrix} T^{-1}$, temos o teorema

C.Q.D.

COROLÁRIO 2.3.1.1

Seja $A \in M_n$ com $K = ind(A)$, se X é autovetor generalizado de A correspondente a $w \neq 0$, então $X \in R(A^K)$

PROVA:

Para $X \in R(A^K)$ deve existir Y Tq:

$$A^K Y = X$$

pelo teorema anterior temos que $X = T \begin{bmatrix} U_1 \\ 0 \end{bmatrix}$

logo, existe $Y = T \begin{bmatrix} C^{-K} U_1 \\ 0 \end{bmatrix}$ tal que

$$T \begin{bmatrix} C^K & 0 \\ 0 & 0 \end{bmatrix} T^{-1} T \begin{bmatrix} C^{-K} & U_1 \\ & 0 \end{bmatrix} = T \begin{bmatrix} U_1 \\ 0 \end{bmatrix} = X$$

C.Q.D.

2.4 REPRESENTAÇÃO DE A^D COMO UM POLINÔMIO

Sabe-se, da teoria das matrizes que se A é não singular então A^{-1} pode ser expresso como um polinômio em A. Agora será visto que A^D possui uma propriedade semelhante.

TEOREMA 2.4.1

Se $A \in M_n$, então existe um polinômio $p(x)$ tal que $A^D = p(A)$

PROVA:

Seja $A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$, T, C inversíveis e N nilpotente de índice K

C é não singular, logo existe q(x) polinômio tal que $C^{-1} = q(C)$

Seja $p(x) = x^k (q(x))^{k+1}$, assim:

$$p(A) = A^K (q(A))^{K+1} = T \begin{bmatrix} C^k & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} q(C) & 0 \\ 0 & q(N) \end{bmatrix}^{k+1} T$$

$$p(A) = T \begin{bmatrix} C^k (q(C))^{k+1} & 0 \\ 0 & 0 \end{bmatrix} T^{-1} = T \begin{bmatrix} C^{-1} & 0 \\ 0 & 0 \end{bmatrix} T^{-1} = A^D$$

C.Q.D.

Observa-se que o polinômio construido acima é, em geral, de grau mais elevado que o necessário. Será construído agora um polinômio de grau menor, que da mesma forma expressa A^D em termos de A.

TEOREMA 2.4.2

Seja $A \in M_n$, sejam $w_0, w_1, \ldots, w_t$ os autovalores distintos de A com $w_0 = 0$. Seja m_i a multiplicidade algébrica do autovalor w_i (i= 1,2,..., t) e $m = n - m_0 = m_1 + m_2 + \ldots m_t$.

Seja p(x) um polinômio de grau n - 1 tal que

$p(x) = x^m (r_0 + r_1 x + \ldots + r_{m-1} x^{m-1})$, cujos coeficientes r_i são as únicas soluções do sistema m x m de equações lineares.

(OBS.: $(.)^{(i)}$ notará a iézima derivado com respeito a x.)

$$\frac{1}{w_i} = p(w_i) \qquad i = 1,2,\ldots, t$$

$$\frac{-1}{(w_i)^2} = p'(w_i)$$

$$\vdots$$

$$\frac{(-1)^{m_i-1} (m_i-1)!}{(w_i)^{m_i}} = p^{(m_i-1)}(w_i)$$

desta forma $p(A) = A^D$

PROVA:

Seja $A = T \begin{bmatrix} J & 0 \\ 0 & N \end{bmatrix} T^{-1}$ escrita em forma de Jordan

com J, N matrizes banda diagonais.

Assim $J = \text{diag.}\ (B_1, \ldots, B_r)$

$N = \text{diag.}\ (N_1, \ldots, N_g)$

onde cada B_j é uma forma de Jordan correspondente aos autovalores não nulos, com $w_e \neq 0$, isto é:

$$B_j = \begin{bmatrix} w_e & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & w_e & 1 & 0 & & 0 & 0 \\ \cdot & & & & & \cdot & \cdot \\ \cdot & & & & & \cdot & \cdot \\ \cdot & & & & & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \dots & w_e & 1 \\ 0 & 0 & 0 & \dots\dots & & 0 & w_e \end{bmatrix} \quad (1) \quad s \times s$$

com $s \leq m_e$

E cada N_j uma matriz banda de Jordan correspondente a um auto-valor nulo, isto é cada N_j tem a forma de (1) com $w_e = 0$. Desta forma J é não singular e $N \in M_{m_0}$ é nilpotente de índice $K = ind(A) < m_0$

$$A^D = T \begin{bmatrix} J^{-1} & 0 \\ 0 & 0 \end{bmatrix} T^{-1}$$

e agora,

$$p(A) = T \begin{bmatrix} p(J) & 0 \\ 0 & p(N) \end{bmatrix} T^{-1} = T \begin{bmatrix} p(J) & 0 \\ 0 & 0 \end{bmatrix} T^{-1}$$

pois $N^{m_0} = 0$ implica que $p(N) = 0$

como

$$p(J) = \text{diag}\,(p(B_1), \dots\ p(B_r))$$

basta mostrar que $p(B_j) = B_j^{-1}$ para cada J.

De (1) temos que:

$$p(B_j) = \begin{bmatrix} p(w_e) & \frac{p'(w_e)}{2!} & \cdots\cdots & \frac{p^{(s-1)}(w_e)}{(s-1)!} \\ 0 & p(w_e) & \cdots\cdots & \vdots \\ \vdots & & \cdots\cdots & \frac{p'(w_e)}{1!} \\ 0 & 0 & \cdots\cdots & p(w_e) \end{bmatrix}_{s \times s} =$$

$$= \begin{bmatrix} \frac{1}{w_e} & \frac{-1}{w_e^2} & \frac{1}{w_e^3} & \cdots\cdots & \frac{(-1)^{s-1}}{(w_e)^s} \\ 0 & \frac{1}{w_e} & \frac{-1}{w_e^2} & \cdots\cdots & \vdots \\ \vdots & & & & \frac{-1}{w_e^2} \\ 0 & \cdots\cdots & \cdots\cdots & 0 & \frac{1}{w_e} \end{bmatrix} = (B_j)^{-1}$$

assim $p(A) = A^D$

C.Q.D.

O teorema acima pode ser usado com eficiência no cálculo de A^D se m é grande em relação a n.

Exemplo 1:

$$\begin{bmatrix} 2 & 4 & 6 & 5 \\ 1 & 4 & 5 & 4 \\ 0 & -1 & -1 & 0 \\ -1 & -2 & -3 & -3 \end{bmatrix}$$

$\partial(A) = \{0,0,1,1\}$ isto é $m_0 = 2 \quad m_1 = 2$

onde

$$p(x) = x^m (a_0 + a_1 x + \ldots + a_{m-1} x^{m-1}) \quad \text{e}$$

$$p(a_i) = \frac{1}{a_i} \qquad p'(a_i) = \frac{-1}{(a_i)^2} \quad , \text{ isto é:}$$

$$p(1) = 1 = a_0 + a_1$$

$$p'(1) = -1 = 2a_0 + 3a_1$$

isto é $a_0 = 4$ e $a_1 = -3$

e

$$A^D = A^2 (a_0 I + a_1 A) = A^2(4I + 3A) = \begin{bmatrix} 3 & -1 & 2 & 2 \\ 2 & 1 & 3 & 3 \\ -1 & 0 & -1 & -1 \\ -1 & 0 & -1 & -1 \end{bmatrix}$$

Sabe-se que para cada matriz $A \in M_n$ existem dois polinômios de especial importância, o característico e o minimal. Seja m(x) o polinômio minimal de A, isto é:

$$m(x) = x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0$$

Se $a_0 = 0$ então A é singular, logo $\det(A) = 0$

se e somente se $a_0 = 0$ em $m(x)$, assim, se $a_0 \neq 0$

$$A^{-1} = \frac{-1}{a_0} (A^{d-1} + a_{d-1} A^{d-2} + \ldots + a_2 A + a_1 I)$$

Agora se $\det(A) = 0$, isto é $a_0 = 0$ temos:

DEFINIÇÃO 2.4.1

Chama-se índice do autovalor nulo ao menor número i tal que:

$$0 = a_0 = \ldots = a_{i-1} \quad e \quad a_i \neq 0$$

TEOREMA 2.4.3

Se $A \in M_n$ e $m(x) = x^s + a_{s-1} x^{s-1} \ldots + a_i x^i$, com $a_i \neq 0$ é o polinômio minimal de A, então $i = ind(A)$.

PROVA:

$$\text{Seja } A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$$

com T, C inversíveis e N nilpotente de índice K $m(A) = 0$, logo:

$$0 = T \begin{bmatrix} C^s & 0 \\ 0 & N^s \end{bmatrix} T^{-1} + \ldots + a_i T \begin{bmatrix} C^i & 0 \\ 0 & N^i \end{bmatrix} T^{-1}$$

isto é

$$0 = N^s + \ldots + a_i N^i = N^i (N^{s-1} + a_{s-1} N^{s-1-i} \ldots + a_1 I)$$

como $(N^{s-1} + a_{s-1} N^{s-1-i} + \ldots + a_1 I)$ é inversível só podemos ter que $N^i = 0$ isto é $i \geq K$. Se $i > K$ então

$$A^D A^i = A^{i-1}$$

seja $m(x) = A^i \; q(A)$ assim $A^d m(x) = A^D \; A^i \; q(A)$ como $m(x) = 0$ então

$0 = A^{i-1} \; q(A)$ logo existe $r(x) = x^{i-1} \; q(x)$ tal que $r(A) = 0$ e grau$(r(x))$ < grau$(m(x))$ o que é uma contradição, logo $K = i$.

C.Q.D.

COROLÁRIO 2.4.3.1

Seja $A \in M_n$, $K = ind(A)$ e m_0 a multiplicidade algébrica do autovalor nulo.

Neste caso $m_0 \geq K$

PROVA:

Seja $m(x) = x^k (x^{s-k} + a_{s-1} \; x^{s-1-k} + \ldots + a_{k+1} x + a_k)$ o polinômio minimal descrito no teorema anterior com $a_k = 0$. Como $m(x)$ divide $p(x)$ só podemos ter que $m_0 \geq k$.

C.Q.D.

Pode-se notar que calcular A^D através do teorema 2.4.2 é uma tarefa difícil, pois é necessário encontrar todos os autovalores de A e suas multiplicidades, porém muitas vezes poder-se-á calcular os coeficientes do polinômio característico de A mais facilmente sem utilizar seus autovalores.

TEOREMA 2.4.4

Seja $A \in M_n$ e $K = \text{ind}(A)$, escrevendo uma equação característica como

$$0 = x^{m_0}(x^{n-m_0} + \beta_{n-1} x^{n-1-m_0} + \ldots + \beta_{m_0+1} x + \beta_{m_0}) = x^{m_0} q(x)$$

com $\beta_{m_0} \neq 0$ e

$$r(x) = \frac{-1}{\beta_{m_0}} (x^{n-m_0-1} + \beta_{n-1} x^{n-m_0-2} + \ldots + \beta_{m_0+1}),$$

se $m_0 < n$; e $r(x) = 0$ se $m_0 = n$, então

$$A^D = A^e (r(A))^{e+1} \quad \text{para cada inteiro } e \geq k.$$

PROVA:

Se $m_0 = n$ então A é nilpotente, logo $A^D = 0$

Se $m_0 < n$

$0 = A^{m_0} q(A)$ multiplicando ambos os lados por $(A^D)^{m_0-1}$

temos:

$$0 = (A^D)^{m_0-1} A^{m_0} q(A) = (A^D)^{m_0-2} A^{m_0-1} q(A) =$$

$$= \ldots = A^D q(A)$$

assim

$$A A^D r(A) = AA^D \left(\frac{-1}{\beta_{m_0}} (A^{n-m_0-1} + \ldots + \beta_{m_0+1}) \right) =$$

$$= A^D \left(\frac{-1}{\beta_{m_0}} (A^{n-m_0} + \ldots + \beta_{m_0+1} A + \beta_{m_0}) + I \right) =$$

$$= A^D \left(\frac{-1}{\beta_{m_0}} q(A) + I \right) = A^D$$

isto é $A^D = A A^D r(A)$ e portanto:

$$(A^D)^{e+1} = A A^D (r(A))^{e+1}, \text{ dai,}$$

$$A^e (A^D)^{e+1} = A^{e+1} A^D (r(A))^{e+1}$$

C.Q.D.

Sabe-se que o índice de uma matriz jamais poderá exceder sua dimensão nem o número m_0 do corolário 2.4.3.1, logo teremos assim:

COROLÁRIO 2.4.4.1

Seja $A \in M_n$; $A^D = A^n(r(A))^{n+1} = A^{m_0}(r(A))^{m_0+1}$ onde $r(x)$ é o polinômio descrito no teorema 2.4.4.

Para $A \in M_n$ os coeficientes da equação característica $x^n + \beta_{n-1} x^{n-1} + \ldots + \beta_1 x + \beta_0 = 0$ de A podem ser calculados recursivamente como:

(2) $\beta_{n-j} = \frac{-1}{j} T_r(A S_{j-1})$ onde:

(3) $S_0 = I \quad S_j = A S_{j-1} + \beta_{n-j} I$

pois $S_j = A^j + \beta_{n+1} A^{j-1} + \ldots + \beta_{n-j} I$

Este algorítmo poderá ser usado para obter a matriz $r(A)$, como está mostrado no teorema abaixo.

TEOREMA 2.4.5

Seja $A \in M_n$ e $r(x)$ como no teorema 2.4.4.

Se $n = m_0$ então $A^D = 0$, se $n > m_0$ então $r(A) = -\frac{1}{\beta_{m_0}} S_{n-m_0-1}$, onde β_{m_0} e $S_{m_0+1\ n-m_0-1}$ são calculados como em (2) e (3). Então

$$A^D = -\left[\frac{1}{\beta_{m_0}}\right]^{l+1} A^l S_{n-m_0-1}^{l+1} \text{ para cada } l \geq \text{ind}(A)$$

2.5 A^D COMO UM LIMITE

Nesta seção será mostrado como a inversa de Drazin e o índice da matriz quadrada podem ser caracterizados em termos de um limite.

DEFINIÇÃO 2.5.1

Sejam: $A \in M_n$; $C_A = A\,A^D\,A$; $N_A = A - C_A = (I - AA^D)\,A$ então definimos poro inteiros $m \geq -1$

$$C_A^{(m)} = A^{m+1}\,A^D = \begin{cases} A^D & \text{se } m = -1 \\ A\,A^D & \text{se } m = 0 \\ C_A^{\,m} & \text{se } m \geq 1 \end{cases}$$

$$N_A^{(m)} = \begin{cases} 0 & \text{se } m = -1 \\ I - A\,A^D & \text{se } m = 0 \\ N_A^{\,m} & \text{se } m \geq 1 \end{cases}$$

TEOREMA 2.5.1

Seja $A \in M_n$ e $\text{ind}(A) = K$, para $l \geq k$ inteiro

$$A^D = \lim_{z \to 0} (A^{l+1} + zI)^{-1} A^l$$

Para cada $l \in \mathbb{N}$

$$A^D = \lim_{z \to 0} (A^{l+1} + zI)^{-1} C_A^{(l)}$$

PROVA:

Se $k = 0$ então $\det(A) \neq 0$ logo vale o resultado.

Se $k > 0$, e para qualquer $l \geq k$

$$(A^{l+1} + zI)^{-1} A^l = P \begin{bmatrix} C^{l+1} + zI & 0 \\ 0 & N^{l+1} + zI \end{bmatrix}^{-1} \begin{bmatrix} C^l & 0 \\ 0 & N^l \end{bmatrix} P^{-1}$$

$$= P \begin{bmatrix} (C^{l+1} + zI)^{-1} C^l & 0 \\ 0 & 0 \end{bmatrix} P^{-1}$$

como C é inversível

$$\lim_{z \to 0} (A^{l+1} + zI)^{-1} A^l = P \begin{bmatrix} C^{-1} & 0 \\ 0 & 0 \end{bmatrix} P^{-1} = A^D$$

Para l inteiro positivo, temos:

$$(A^{l+1} + zI)^{-1} C_A^l = P \begin{bmatrix} C^{l+1} + zI & 0 \\ 0 & N^{l+1} + zI \end{bmatrix} \begin{bmatrix} C^l & 0 \\ 0 & 0 \end{bmatrix} P^{-1}$$

$$= P \begin{bmatrix} (C^{l+1} + zI)^{-1} C^l & 0 \\ 0 & 0 \end{bmatrix} P^{-1}$$

logo como C é inversível

$$\lim_{z \to 0} (A^{l+1} + zI) C_A^l = A^D$$

C.Q.D.

COLORÁRIO 2.5.1.1.

Seja $A \in M_n$ $A^D = \lim_{z \to 0} (A^{n+1} + zI)^{-1} A^n$

PROVA:

Como $n \geq ind(A)$ pelo teorema 2.5.1, vale o corolário.

C.Q.D.

LEMA 2.5.2

Se $A \in M_n$ é uma matriz singular, então para um inteiro positivo p, temos que:

$ind(A^p) = 1$ se e somente se $p \geq ind(A)$. Equivalentemente temos que o menor inteiro positivo l para o qual $ind(A^l) = 1$ é o índice de A.

PROVA:

Seja $A \in M_n$, escrita em sua forma canônica, isto é $A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$ com T, C inversíveis e N nilpotente de índice $K = ind(A)$. Vamos supor $p < ind(A)$

Se $N = 0$ então $ind(A) = 1$ isto é $p = 0$

Contradição

Se $N \neq 0$

$$A^P = T \begin{bmatrix} C^P & 0 \\ 0 & N^P \end{bmatrix} T^{-1} \quad \text{e } N^P \neq 0 \quad \text{pois } p < ind(A)$$

logo $ind\ A^P \neq 1$

isto é $ind(A^D) = 1$ então $p \geq ind(A)$

Suposição $p \geq \text{ind}(A)$ e $A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$

$$A^D = T \begin{bmatrix} C^p & 0 \\ 0 & N^p \end{bmatrix} T^{-1} = T \begin{bmatrix} C^p & 0 \\ 0 & 0 \end{bmatrix} T^{-1}$$

logo $\text{ind}(A^p) = 1$

C.Q.D.

LEMA 2.5.3

Se $N \in M_n$ é nilpotente e $\text{ind}(N) = K$, e m, p são inteiros não negativos, então:

$$\lim_{z \to 0} z^m (N + zI)^{-1} N^p$$

existe se e somente se $m + p \geq K$.

Quando este limite existe temos:

$$\lim_{z \to 0} z^m (N + zI)^{-1} N^p = \begin{cases} 0 & \text{se } m = 0 \\ (-1)^{m-1} N^{m+p-1} & \text{se } m > 0 \end{cases}$$

PROVA:

Se $N = 0$ então $K = 1$ e

$$\lim_{z \to 0} z^{m-1} 0^p = \begin{cases} \lim_{z \to 0} z^{m-1} I & \text{se } p = 0 \text{ e } m \geq 1 \\ 0 & \text{se } p \geq 1 \end{cases}$$

isto é $\lim_{z \to 0} z^{m-1} 0^p$ existe para $K = 1$ se e somente se

$m + p \geq k$

Se $N \neq 0$ então $K > 1$ e $(N + zI)^{-1} = \sum_{i=0}^{k-1} (-1)^i \frac{N^i}{z^{i+1}}$

Assim:

$$z^m(N + zI)^{-1} N^p = z^{m-1} N^p - z^{m-2} N^{p+1} + \ldots +$$

$$+ (-1)^{m-2} z N^{m+p-2} + (-1)^{m-1} N^{m+p-1} +$$

$$+ \frac{(-1)^m N^{m+p}}{z} + \ldots + \frac{(-1)^{k-1} N^{p+k-1}}{z^{k-m}}$$

Se $m + p \geq k$ então o limite existe pelo descrito acima. Se o limite existe então pelos cálculos acima devemos ter que $N^{m+p} = 0$

logo $m + p \geq k$

C.Q.D.

TEOREMA 2.5.4

Sejam $A \in M_n$ e $ind(A) = K$, m,p inteiros, são negativos, o limite:

(4) $\lim_{z \to 0} z^m(A + zI)^{-1} A^p$ existe se e somente se

$m + p \geq k$ e neste caso o valor do limite é dado por

(5) $$\lim_{z \to 0} z^m(A + zI)^{-1} A^p = \begin{cases} A^D A^p & \text{se } m = 0 \\ (-1)^{m-1} (I - AA^D) A^{m+p-1} & \text{se } m > 0 \end{cases}$$

PROVA:

Se $k = 0$ é imediato

Se $k \geq 1$

Seja $A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$ com P,C inversíveis e N nilpotente de índice k

então:

$$(6) \quad z^m(A + zI)^{-1} A^p = T \begin{bmatrix} z^m(C+zI)^{-1} C^p & 0 \\ 0 & z^m(N+zI)^{-1} N^p \end{bmatrix} T^{-1}$$

como C é não singular,

$$(7) \quad \lim_{z \to 0} z^m(C+zI)^{-1} = \begin{cases} 0 & \text{se } m > 0 \\ C^{p-1} & \text{se } m = 0 \end{cases}$$

assim o limite desejado existe se e somente se

$\lim_{z \to 0} z^m(N+zI)^{-1} N^p$ existe

pelo lema anterior temos que este limite existe se e somente se $m + p \geq k$ e a expressão 5 é obtida de 6,7 e do lema anterior.

C.Q.D.

COROLÁRIO 2.5.4.1

Seja $A \in M_n$, equivalem-se:

i) $ind(A) = K$

ii) K é o menor inteiro não negativo tal que

$$\lim_{z\to 0} (A + zI)^{-1}A^K \text{ existe}$$

iii) k é o menor inteiro não negativo tal que

$$\lim_{z\to 0} z^k(A + ZI)^{-1} \text{ existe}$$

iv) se ind(A)= k então $\lim_{z\to 0} (A+zI)^{-1}A^k=(AA^D)A^{k-1}=$

$C_A^{(k-1)}$

v) Quando k > 0 $\lim_{z\to 0} z^k(A+zI)^{-1}= (-1)^{k-1}(I-AA^D)A^{k-1}=$

$N_A^{(k-1)}$

COROLÁRIO 2.5.4.2

Sejam $A \in M_n$ e l inteiro tal que $l \geq ind(A)>0$, então $\lim_{z\to 0} (A + zI)^{-1} (A^l + z^l I)^{-1} = A^{l-1}$

TEOREMA 2.5.5

Seja $A \in M_n$; O menor inteiro não negativo tal que

(8) $\lim_{z\to 0} (A^{l+1} + zI)^{-1} A^l$ existe é o índice A.

PROVA:

Se ind(A)= 0 a existência de (8) é clara.

Se ind(A)= $k \geq 1$

Seja $A=T\begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$ com T,C inversíveis e N nilpotente de índice K.

$$(A^{l+1}+zI)^{-1}\ A^{l} = T\begin{bmatrix}(C^{l+1}+zI)^{-1}C^{l} & 0\\ 0 & (N^{l+1}+zI)^{-1}N^{l}\end{bmatrix}T^{-1}$$

como C é inversível $\lim_{z\to 0}(C^{l+1}+zI)^{-1}C^{l}$ existe,

agora

$$(N^{l+1}+zI)^{-1}\ N^{l} = \left[I+\frac{N^{l+1}}{z}\right]^{-1}\ \frac{N^{l}}{z} =$$

$$\left[\sum_{m=0}^{n}(-1)^{m}\left|\frac{N}{z}\right|^{m\,m(l+1)}\right]\ \frac{N^{l}}{z}$$

que possui limite se e somente se $N^{l}=0$,

isto é $l \geq \text{ind}(A)$

C.Q.D.

2.6 A INVERSA DE DRAZIN COMO UM GRADIENTE

Recentemente Gabriel e Hartwig (8) caracterizaram a inversa de Drazin de uma matriz quadrada A como o gradiente matricial do algorítmo de uma função exponencial, explorando para tanto, uma expressão dos coeficientes da matriz adjunta adj(wI - A). Os resultados mais simples serão enunciados a seguir.

Sabe-se que para uma matriz inversível A a fórmula de Cayley é:

$$A^{-1} = \frac{\text{adj}(A)}{|A|}$$

pode ser escrita na forma conveniente:

$$(A^{-1})^T = \frac{1}{|A|}\,(\mathrm{adj}(A))^T = \nabla_A \ln|A| \qquad (1)$$

onde

$$\nabla_X f(x) = \left(\frac{\partial f}{\partial x_{ij}}\right)_{nxn}, \quad X = [X_{ij}]\ nxn$$

$$f(X) = f(x_{11}, x_{12}, \ldots, x_{nn})$$

De fato, se A possui determinante $|A|$ e cofatores A_{ij}, então.

$$\mathrm{adj}(A)^T = \nabla_A |A|$$

onde os componentes a_{ij} da matriz A são consideradas como variáveis independentes, logo

$$\nabla_A \ln|A| = \frac{1}{|A|}\ \nabla_A|A| = \frac{\mathrm{adj}(A)^T}{|A|}$$

A generalização de (1) para a inversa de Drazin é da forma

$$(A^D)^T = \nabla_A \ln |W(A)|$$

para uma função apropriada W(x). Esta estabelecido em (8) que a matriz potencial W(x) pode ser expressa na forma:

$$W(x) = \frac{1}{x_k}\begin{bmatrix} x_k^2 & x_k x_{k-1} & \cdots & x_k x_0 \\ x_{k+1} & x_k & \ddots & \\ \vdots & \vdots & & 0 \\ x_{2k} & x_{2k-1} & \cdots & x_k \end{bmatrix}_{(k+1)\ x\ (k+1)}$$

onde os x_k são coeficientes de polinômio característico de $wI - x$, isto é,

$$|wI - x| = w^k [x_k + x_{k+1} w + \ldots + w^{n-k}] = w^k \Delta(w)$$

com $x_k \neq 0$ para $k \geq 0$

Também é conveniente salientar que os autores constroem outros $N(x)$, de função potenciais para os "coeficientes adjuntos" X_j da matriz

$$adj(wI - X) = X_0 + X_1 w + \ldots + I w^{n-1}$$

2.7 DOIS ALGORÍTMOS PARA O CÁLCULO DE A^D

ALGORÍTMO 2.7.1

Computação de A^D onde $A \in M_n$ e $ind(A) = K$

I) Seja p inteiro tal que $p \geq k$

(Podemos tornar p= n se nenhum valor menor puder ser determinado)

Se $A^p = 0$ então A é nilpotente logo $A^D = 0$.

Vamos supor que $A^p \neq 0$

II) Reduz-se A^p por linhas à sua forma hermiteana escalonada $H_A P$. (Ver observação 1). A seqüência da redução não precisa ser armazenada.

III) Notando a posição na diagonal principal dos elementos não nulos em $H_A P$ seleciona-se as colunas distintas de A^P que chama-se de V_1, $V_2 \ldots V_r$ (Esta é uma base para $R(A^k)$).

IV) Forma-se a matriz $I - H_A P$ e armazena-se suas colunas não nulas. Chamaremos estes elementos de V_{r+1}, $V_{r+2} \ldots, V_n$. (Esta é uma base para $N(A^K)$).

V) Constroi-se a matriz não singular

$P = [V_1 \ldots V_r \quad V_{r+1} \ldots V_n]$

VI) Computa-se P^{-1}

VII) Forma-se o produto P^{-1} AP, que será da forma

$$P^{-1} A P = \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix}, \quad \begin{array}{l} C \text{ não singular} \\ N \text{ nilpotente} \end{array}$$

VIII) Computa-se C^{-1}

IX) Computa-se A^D, como $A^D = P \begin{bmatrix} C^{-1} & 0 \\ 0 & 0 \end{bmatrix} P^{-1}$

Exemplo 2.7.1

$$\text{Seja } A = \begin{bmatrix} 2 & 0 & 0 \\ -1 & 1 & 1 \\ -1 & -1 & -1 \end{bmatrix}$$

Vamos encontrar A^D pelo algorítmo acima.

I) Como não é conhecido ind(A) seja p= 3

$$A^3 = \begin{bmatrix} 8 & 0 & 0 \\ -8 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$A^3 \neq 0$ logo passo II

II) $$H_A{}^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

III) elementos não nulos da diagonal $a_{11} = 1$, logo a 1ª coluna de A^3 é tomado como a base de $R(A^K)$ isto é:

$$V_1 = \begin{bmatrix} 8 \\ -8 \\ 0 \end{bmatrix}$$

IV) $$I - H_A P = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

suas 2ª e 3ª colunas não são nulas, logo:

$$V_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \qquad V_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$ são base para $N(A^k)$

V) Assim $$P = \begin{bmatrix} -8 & 0 & 0 \\ -8 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

VI) $$P^{-1} = \begin{bmatrix} 1/8 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

VII) $$P^{-1} A P = \left[\begin{array}{c|cc} 2 & 0 & 0 \\ \hline 0 & 1 & 1 \\ 0 & -1 & -1 \end{array}\right]$$

VIII) $C = 2$ assim $C^{-1} = 1/2$

IX) $A^D = P \begin{bmatrix} 1/2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} P^{-1} = \begin{bmatrix} 1/2 & 0 & 0 \\ -1/2 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$.

ALGORITMO 2.7.2

Computação de A^D, $A \in M_n$

I) Faça $S_0 = I$ recursivamente compute

$$S_j = A S_{j-1} + b_{n-j} I; \quad b_{n-j} = -\frac{1}{j} Tr (A S_{j-1}),$$

até algum $S_t = 0$ com $S_{t-1} \neq 0$.

II) Seja u um número tal que $b_{n-u} \neq 0$ e $b_{n-u-1} = b_{n-u-2} = \ldots = b_{n-t-1} = 0$ (note que $n-u = m_0$ a multiplicidade algébrica do autovalor zero).

III) Seja $\ell = n-u$ e compute $S^{\ell+1}_{n-m_0-1} = S^{\ell+1}_{u+1}$

IV) Compute A^D como:

$$A^D = \frac{1}{b_\ell^{\ell+1}} A^\ell S^{\ell+1}_{u+1}$$

Note que nem todo S_j computado deve ser armazenado. Se $b_{n-j} \neq 0$, então S_{j-2} pode ser esquecido. Além disto S_{j-1} precisa ser armazenado até o próximo b não zero aparecer. Note também que este algoritmo produz o valor da multiplicidade algébrica do auto valor zero de A.

EXEMPLO 2.7.2

Seja

$$A = \begin{bmatrix} -10 & -8 & 6 & -3 \\ 12 & -10 & 8 & -4 \\ 1 & -1 & +1 & 0 \\ -2 & 2 & -2 & 2 \end{bmatrix}$$

Vamos usar o algorítmo acima para computar A^D.

I) $S_0 = I \qquad b_3 = -Tr\ (AS_0) = -Tr\ (A) = -3$

$$S_1 = A\,S_0 - 3I = \begin{bmatrix} 7 & -8 & 6 & -3 \\ 12 & -13 & 8 & -4 \\ 1 & -1 & -2 & 0 \\ -2 & 2 & -2 & -1 \end{bmatrix}$$

$$A\,S_1 = \begin{bmatrix} -14 & 12 & -10 & 5 \\ -20 & 18 & -16 & 8 \\ -4 & 4 & -4 & 1 \\ 4 & -4 & 4 & -4 \end{bmatrix}, \quad b_2 = \frac{1}{2}\,Tr(AS_1) = 2$$

$$S_2 = A\,S_1 + 2I = \begin{bmatrix} -12 & 12 & -10 & 5 \\ -20 & 20 & -16 & 8 \\ -4 & 4 & -2 & 1 \\ 4 & -4 & 4 & -2 \end{bmatrix}$$

$$A\,S_2 = \begin{bmatrix} -4 & -4 & 4 & -2 \\ 8 & -8 & 8 & -4 \\ 4 & -4 & 4 & -2 \\ 0 & 0 & 0 & 0 \end{bmatrix}; b_1 = \frac{-1}{3}\,\mathrm{Tr}(A\,S_2) = 0$$

$$S_3 = A\,S_2$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

e $\quad S_4 = A\,S_3 = 0$

Assim $t = 4$ no exemplo, é a multiplicidade algébrica do auto valor zero é $m_0 = 2$

II) Seja $u = 2$

III) Seja $\ell = 2$

IV) Compute $A^D = \frac{1}{b_2^3}\,A^2\,S_1^3 = \frac{-1}{8}\,A^2\,S_1^3$

como segue. Como $S_2 = A\,S_1 + b_2\,I$ temos que $A\,S_2\,S_1^2 = A^2\,S_1^3 + b_2\,A\,S_1^2$.

$$A^2\,S_1^3 = [(A\,S_2)\,S_1 - b_2\,(A\,S_1)]\,S_1 .$$

$A\,S_2$ e $A\,S_1$ já foram computados somente duas multiplicações matriciais serão necessárias.

Agora:

$$(A\ S_2)\ S_1 = \begin{bmatrix} -12 & 12 & -12 & 6 \\ -24 & 24 & -24 & 12 \\ -12 & 12 & -12 & 6 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$[(AS_2)S_1 - 2(AS_1)] = \begin{bmatrix} 16 & -12 & 8 & -4 \\ 16 & -12 & 8 & -4 \\ -4 & 4 & -4 & \\ -8 & 8 & -8 & 8 \end{bmatrix}$$

$$[(A\ S_2)S_1 - 2\ (AS_1)]S_1 = \begin{bmatrix} -16 & 12 & -8 & 4 \\ -16 & 12 & -8 & 4 \\ 8 & -8 & 8 & -8 \\ 16 & -16 & 16 & -16 \end{bmatrix}$$

Logo:

$$A^D = -\frac{1}{8}\ A^2\ S_1^{\,3} = \begin{bmatrix} 2 & -3/2 & 1 & -1/2 \\ 2 & -3/2 & 1 & -1/2 \\ -1 & 1 & -1 & 1 \\ -2 & 2 & -2 & 2 \end{bmatrix}$$

CAPITULO III

III - A INVERSA MATRICIAL DE DRAZIN EM CORPOS E ANÉIS FINITOS:

3.1 INTRODUÇÃO

Neste capítulo, iremos estudar a inversa de Drazin de matrizes quadradas definidas sobre Z_t. Os casos mais importantes para as aplicações dadas no capítulo 5 são Z_{26}, Z_2 e Z_{13}.

Como já sabemos dos capítulos anteriores a inversa de Drazin de uma matriz quadrada A é a única matriz quadrada, notada por A^D que satisfaz simultaneamente as três equações:

i) $A^{K+1} A^D = A^k$, para algum $k > 0$

ii) $A^D A A^D = A^D$

iii) $A A^D = A^D A$

Além disto, também já foi mostrado no capítulo 2 que a inversa de Drazin, A^D, de uma matriz quadrada sobre $\mathbb{C}$, pode ser expressa como:

$$A^D = A^k \ [q(A)]^{k+1},$$

onde f(x) é um polinômio tal que $C^{-1} = q(C)$ e

$$A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$$, com T e C inversíveis e N nilpotente.

No caso de corpos e anéis finitos, será demonstrado o mesmo resultado por caminho diferente.

3.2 DEFINIÇÕES:

DEFINIÇÃO 3.2.1

Y é dita uma $(1^k, 5)$ inversa de A se $A^k\ Y\ A = A^k$ e $AY = YA$.

LEMA 3.2.1

Se Y é uma $(1^l, 5)$ inversa da matriz quadrada A, então $X = A^l\ Y^{l+1}$ é uma inversa de Drazin para A.

PROVA:

Seja Y uma $(1^l, 5)$ inversa de A.

Assim:

$A^{l+1}\ Y = A^l$ e $AY = YA$

logo, se $X = A^l\ Y^{l+1}$ temos,

i) $AX = A(A^l\ Y^{l+1}) = (A^l\ Y^{l+1})\ A = XA$

ii) $A^l\ X\ A = A^{2l+1}\ X^{l+1} = A^{2l}\ Y^l = A^{2l-1}\ Y^{l-1} = \ldots$

$\ldots = A^{l+1}\ Y = A^l$

iii) $X\ A\ X = A^{2l+1}\ Y^{2l+2} = Y^{2l}\ Y^{2l+1} = \ldots = A^l\ Y^{l+1} = X$

C.Q.D.

Sabemos que $|\lambda\ I - A| = 0$ é a equação característica para A matriz quadrada nxn, logo:

$$\Delta(\lambda) = |\lambda\ I - A| = \lambda^n + a_1\ \lambda^{n-1} + \ldots + a_{n-r}\ \lambda^r + a_{n-r-1}\ \lambda^{r-1} + \ldots + a_{n-1}\ \lambda + a_n = 0$$

onde $a_i = (-1)^i \sigma_i$ e σ_i é a soma dos menores

principais de ordem i, assim, temos que:

Existe $r \geq 0$ tal que $a_n - r \neq 0$, $(a_{n-r})^{-1}$ existe e $a_{n-r+1} = a_{n-r+2} = \ldots = a_n = 0$

logo:

1) Se $r = 0 \rightarrow A^D = A^{-1}$ pois $a_n = (-1)^n |A|$ e $(a_n)^{-1}$ existe.

2) Se $r = n \rightarrow A^D = 0$ pois, como $a_0 = 1$ $\Lambda(\lambda) = 0$, logo $A^n = 0$ e portanto A é nilpotente.

3) Se $0 < r < n$ temos que:

$$\lambda^n + a_1 \lambda^{n-1} + a_2 \lambda^{n-2} + \ldots + a_{n-r} \lambda^r = 0$$

$$(a_{n-r})^{-1} [\lambda^n + a_1 \lambda^{n-1} + \ldots + a_{n-(r+1)} \lambda^{r+1}] + \lambda^r = 0$$

$$\lambda^r = \lambda^{r+1} [-(a_{n-r})^{-1} (\lambda^{n-r-1} + a_1 \lambda^{n-r-2} + \ldots + a_{n-r-1})]$$ daí fazendo

$q(\lambda) = -(a_{n-r})^{-1} (\lambda^{n-r-1} + \ldots + a_{n-r-1})$ temos que:

$$\lambda^r = \lambda^{r+1} q(\lambda)$$

Além disto $q(A)$ é uma $(1^r, 5)$ inversa de A, pois:

i) $A^{r+1} q(A) = A^r$

ii) $A \cdot q(A) = q(A) \cdot A$

logo pelo lema 3.2.1, só podemos ter que:

$X = A^r (q(A))^{r+1}$ e uma inversa de Drazin de A, e assim, pela unicidade da inversa de Drazin temos que:

$$A^D = A^r (q(A))^{r+1}$$

Observamos que na fórmula acima, as potências maiores que n-1 podem ser substituídas utilizando o fato que:

$$A^n + a_1 \quad A^{n-1} + \ldots + a_{n-r} A^r = 0$$

Exemplo 1: Vamos encontrar a inversa de Drazin da Matriz A definida sobre o anel Z_{26}.

$$A = \begin{bmatrix} 9 & 8 & 15 & 19 \\ 8 & 7 & 0 & 11 \\ 15 & 0 & 8 & 1 \\ 19 & 11 & 1 & 14 \end{bmatrix}$$

Primeiramente vamos calcular os menores principais de A:

$$\sigma_1 = 9+7+8+14 = 12 \pmod{26}$$

$$\sigma_2 = \begin{bmatrix} 9 & 8 \\ 8 & 7 \end{bmatrix} + \begin{bmatrix} 9 & 15 \\ 15 & 8 \end{bmatrix} + \begin{bmatrix} 9 & 19 \\ 19 & 14 \end{bmatrix} + \begin{bmatrix} 7 & 0 \\ 0 & 8 \end{bmatrix} + \begin{bmatrix} 7 & 11 \\ 11 & 14 \end{bmatrix} + \begin{bmatrix} 8 & 1 \\ 1 & 14 \end{bmatrix} \equiv + 15 \pmod{26}$$

$$\sigma_3 = \begin{bmatrix} 9 & 8 & 15 \\ 8 & 7 & 0 \\ 15 & 0 & 8 \end{bmatrix} + \begin{bmatrix} 9 & 8 & 19 \\ 8 & 7 & 11 \\ 19 & 11 & 14 \end{bmatrix} + \begin{bmatrix} 9 & 15 & 19 \\ 15 & 8 & 1 \\ 19 & 1 & 14 \end{bmatrix} + \begin{bmatrix} 7 & 0 & 11 \\ 0 & 8 & 1 \\ 11 & 1 & 14 \end{bmatrix} =$$

$$3 + 0 + 3 + 17 \equiv 23 \pmod{26}$$

$$\sigma_4 = |A| = 0$$

assim

$$a_1 = -\sigma_1 = -12 \equiv 14 \pmod{26}$$

$$a_2 = \sigma_2 \equiv 15 \pmod{26}$$

$$a_3 = -\sigma_3 = -23 \equiv 3 \pmod{26}$$

$$a_4 = \sigma_4 = 0$$

e portanto:

$$A^4 + 14\,A^3 + 15\,A^2 + 3\,A = 0$$

$$3^{-1}A\ (A^3 + 14\,A^2 - 15\,A) + A = 0$$

$$-9\,A^2\ (A^2 + 14\,A + 15\,I) = A$$

$$17\,A^2\ (A^2 + 14\,A + 15\,I) = A$$

$$A^2\ (17\,A^2 + 4\,A + 21\,I) = A$$

e portanto temos por i) que:

$$q(A) = 17A^2 + 4\,A + 21\,I \quad \text{para } r = 1$$

Assim,

$$A^D = A\,q(A)^2 = A\,(17\,A^2 + 4\,A + 21\,I)^2 =$$

$$= 3A^5 + 6A^4 + 2A^3 + 15A^2 + 25A)$$

$$= 3(25A^3 + 25A^2 + 16A) + 6(12A^3 + 11A^2 + 23A)$$

$$+ 2A^3 + 12A^2 + 25A = 19A^3 + 2A^2 + 3A$$

assim

$$A^D = \begin{bmatrix} 19 & 6 & 19 & 9 \\ 6 & 18 & 17 & 8 \\ 12 & 17 & 17 & 23 \\ 9 & 8 & 23 & 19 \end{bmatrix}$$

Para simplificar os cálculos, no fim deste capítulo, uma tabela que lista as inversas de Drazin das matrizes quadradas não inversíveis e não nilpotentes de ordem menor ou igual à 5 em termos de seus coeficientes da equação ca

racterística.

Observações:

1) Quando a_n^{-1} existe então A^{-1} existe e $A^{-1} = A^D$

Exemplo:

Se $\Delta(A) = A^2 + 2A + 3I \rightarrow a_n = 3$ e $a_n^{-1} = 9$

$$A^{-1}(A + 2I + 3A^{-1}) = 0$$

como $A^{-1} \neq 0$ só podemos ter que:

$$A + 2I + 3A^{-1} = 0$$

$$9A + 18I + A^{-1} = 0$$

$$A^{-1} = 17A + 8I$$

2) Se uma matriz quadrada A, satisfaz uma equação $M(A) = 0$ de grau menor que n, então A^D pode ser calculado, usando $M(A) = 0$.

3.3 A^D NUM ANEL GERAL Z_T.

Para encontrarmos a inversa de Drazin num anel Z_t qualquer, iremos necessitar do Teorema do resto Chinês, aqui enunciado, o qual está demonstrado em Tim Anderson [5].

TEOREMA 3.3.1 (TEOREMA DO RESTO CHINÊS)

Sejam $m_1, m_2, \ldots m_w$ inteiros 2 a 2 primos entre si. Assim o sistema de congruências $x \equiv C_1 \pmod{m_1}; \ldots ; x \equiv c_w \pmod{m_w}$ possui solução x dada por:

$$x = (M_1 x_1 C_1 + M_2 x_2 C_2 + \ldots + M_w x_w C_w) \pmod{M}$$

onde $M_i = \frac{M}{m_i}$, $M = m_1 . m_2, \ldots, m_w$ e x_i é a solução da congruência $M_i x_i \equiv 1 \pmod{m_i}$.

Vamos agora encontrar a inversa de Drazin de uma matriz quadrada A definido sobre Z_t. Para isto, vamos primeiramente considerar o caso particular, onde $t = p_1 . p_2, \ldots, p_w$ com $p_i \neq p_j$ para $i \neq j$. Sabemos que

$$\Delta(\lambda) = \lambda^n + a_1 \lambda^{n-1} + \ldots + a_{n-r} \lambda^r + a_{n-r+1} \lambda^{r-1} + \ldots + a_{n-1} \lambda a_n$$

com $\Delta(A) = 0$.

Frequentemente, teremos que o último coeficiente não nulo deste polinômio é não inversível em Z_t e nestes casos iremos considerar as congruências simultâneas

$$\Delta(A) \equiv 0 \pmod{p_1}$$
$$\Delta(A) \equiv 0 \pmod{p_2}$$
$$\vdots$$
$$\Delta(A) \equiv 0 \pmod{p_w}$$

obtendo-se assim $A^D \equiv A^D \pmod{p_i}$, e desta forma aplicando o teorema do resto Chinês chegamos a $A^D \pmod{t}$.

EXEMPLO 3.3.1

Vamos encontrar A^D, sabendo que $\Delta(A) = A^3 + 3A^2 + 14A$ é sua equação característica e $t = 26 = 13.2$

MDC $(14,26) \neq 1$ logo não existe $(14)^{-1}$ (mod 26)

Assim, vamos considerar as congruências simultâneas.

$$A^3 + 3A^2 + A = 0 \quad (\text{mod } 26)$$
$$A^3 + 3A^2 = 0 \quad (\text{mod } 2)$$

pela tabela 1 do apêndice encontramos:

$$A^D = 3A^2 + 8A \quad (\text{mod } 13)$$
$$A^D = A^2 \quad (\text{mod } 2)$$

Agora, aplicando o teorema do resto chinês, usando os coeficientes do A^2 como x e os de A como y temos:

$$x \equiv 1 \pmod 2 \quad \text{e} \quad x \equiv 3 \pmod{13}$$
$$y \equiv 0 \pmod 2 \quad \text{e} \quad y \equiv 8 \pmod{13}$$

fazendo $m_1 = 2$ e $m_2 = 13$ MDC $(2,13) = 1$ e $M = m_1 . m_2 = 26$

temos $M_1 = \frac{M}{m_1} = 13$ $\qquad M_2 = \frac{M}{m_2} = 2$

$$M_1 x_1 \equiv 2 \pmod 2 \rightarrow 13x_1 \equiv 1 \pmod 2$$
$$\rightarrow x_1 \equiv 1 \pmod 2$$
$$M_2 x_2 \quad 1 \pmod{13} \rightarrow 2x_2 \equiv 1 \pmod{13}$$
$$\rightarrow x_2 \equiv 7 \pmod{13}$$

$$M_1 y_1 \equiv 1 \pmod 2 \rightarrow y_1 \equiv 1 \pmod 2$$
$$M_2 y_2 \equiv 1 \pmod{13} \qquad y_2 \equiv 7 \pmod{13}$$

e portanto

$$x \equiv M_1 C_1 x_1 + M_2 C_2 x_2 = 13.1.1.+2.3.7 = 55$$

$$x \equiv 3 \pmod{26}$$

e

$$y \equiv M_1 C_3 y_1 + M_2 C_4 y_2 = 2.7.8 = 112$$

$$y \equiv 8 \pmod{26}$$

e assim temos que

$$A^D = 3A^2 + 8A \pmod{26}$$

Nota: Para $t = 26$ obtem-se a regra prática:
Se $x \equiv C_1 \pmod 2$ e $x \equiv C_2 \pmod{13}$
então a^1 solução é dada ^{2}por:
$x \equiv (C_2 + 13) \pmod{26}$ se $C_1 + C_2$ é ímpar.
$x \equiv C_2 \pmod{26}$ se $C_1 + C_2$ é par.

Vamos agora considerar o caso geral isto é:

$t = p_1^{h_1} . p_2^{h_2} . \ldots . p_w^{h_w}$, onde pelo menos um dos h_i é maior ou igual a 2 e com $p_i \neq p_j$ para $i \neq j$.

Como no caso anterior consideraremos as congruências simultâneas.

$$\Delta(A) \equiv 0 \pmod{p_1^{h_1}}, \ldots, \Delta(A) \equiv 0 \pmod{p_w^{h_w}}$$

e deste modo obteremos:

$$A^D \equiv A_i^D \pmod{p_i^{h_i}}, \quad (1 = 1, \ldots w)$$

Agora, usando-se o lema combinam-se estas congruências para encontrarmos A^D em Z_t. Obviamente nosso problema aparecerá ao calcularmos A^D se A está em Z_p^h com $h \geq 2$, para resolve-lo, iremos considerar sua equação característica.

$$A^n + a_{n-1} A^{n-1} + \ldots + a_k A^k + a_{k-1} A^{k-1} + \ldots + a_1 A + a_0 I \equiv 0 \pmod{p^h}$$ com p primo e $h \geq 2$.

1) Se $a_0, a_1 \ldots a_{n-1}$ são múltiplos de p então:

$$A^n = p\,(\alpha_0 A^{n-1} + \ldots + \alpha_{n-1} I) \pmod{p^h}$$

elevando tudo à h temos:

$A^{nh} \equiv 0 \pmod{p^h}$, isto é A é nilpotente e portanto $A^D \equiv 0 \pmod{p^h}$

2) Se existe $i \in \mathbb{N}$ tal que a_i não é múltiplo de p, isto é existe k tal que $(a_k)^{-1}$ existe e $a_{k-1}, a_{k-2}, \ldots a_0$ são múltiplos de p. Assim:

$$A^n + a_{n-1} A^{n-1} + \ldots a_k A^k = p\,(\beta_0 A^{k-1} + \ldots + \beta_k I)$$

e portanto

$$(A^n + a_{n-1} A^{n-1} + \ldots + a_k A^k)^h \equiv 0 \pmod{p^h}$$

$$a_k^h A^{kh} (I + \gamma_0 A + \gamma_1 A_2 + \ldots + \gamma_{n-k-1} A^{n-k})^h \equiv 0 \pmod{p^h}$$

$$A^{kh} (I - AQ(A)) \equiv 0 \pmod{p^h}$$

onde

$$Q(A) = -(\gamma_0 + \gamma_1 A + \ldots + \gamma_{n-k-1} A^{n-k-1})$$

e assim

$$A^{kh} - A^{kh+1} Q(A) \equiv 0 \pmod{p^h}$$

isto é

$$A^{kh} = A^{kh+1} Q(A)$$

além disto

$AQ(A) = Q(A)A$, e portanto $Q(A)$ é uma $(1^k, 5)$inversa de A e assim pelo lema 3.2.1 temos que:

$$A^D = A^{kh} (Q(A))^{kh+1} \pmod{p^h}$$

EXEMPLO 3.3.2

Seja o anel Z_{72} e $A^2 - A + 6I \equiv (\text{mod } 72)$

Assim $A^D = ?$

$72 = 8.9 = 2^3.3^2$, isto é $p_1 = 2 \quad h_1 = 3$

$p_2 = 3 \quad h_2 = 2$

$A^2 + 7A + 6I \equiv 0 \pmod 8$, e 7 não é multiplo de 2 logo, iremos aplicar o caso 2.

$$A^2 + 7A = 2I \pmod 8$$

$$(A^2 + 7A)^3 \equiv 0 \pmod 8$$

$$(A(A+7I))^3 \equiv 0 \pmod 8$$

$$A^3 (A+7I)^3 \equiv 0 \pmod 8$$

desenvolvendo

$$A^3 (A^3 + 5A^2 + 3A + 7I) \equiv 0 \pmod 8$$

$$A^3 (I + 7^{-1} A^3 + 7^{-1} . 5 . A^2 + 7^{-1}.3.A) \equiv 0 \pmod 8$$

$$A^3 (I - A (A^2 + 5A + 3I) \equiv 0 \pmod 8$$

$$A^3 = A^4 (A^2 + 5A + 3I)$$

assim

$Q(A) = A^2 + 5A + 3I$ mas, $A^2 = A + 2I$, logo:

$Q(A) = 6A + 5I$ e portanto,

$$A^D = A^3 (6A + 5I)^4$$

$A^D = A^3$ pois $Q^2 = 4A^2 + 4A + I$ e assim $Q^4 = I$

$$A^D = A^3 = A^2 + 2A = 3A + 2I \pmod 8$$

$$A^2 - A + 6I \equiv 0 \pmod 9$$

$$A^2 + 8A + 6I \equiv 0 \pmod 9$$

8 não é múltiplo de 9 logo aplicaremos o caso 2.

$$A^2 + 8A \equiv 3I \pmod 9$$

$$(A^2 + 8A)^2 \equiv 0 \pmod 9$$

$$A^2 (A + 8I)^2 \equiv 0 \pmod 9$$

$$A^2 (A^2 + 7A + I) \equiv 0 \pmod 9$$

$$A^2 (I + A(A + 7 I)) \equiv 0 \pmod 9$$

$$A^2 (I - A (8A + 2I)) \equiv 0 \pmod 9$$

$$A^2 \equiv A^3 (8A + 2I) \pmod 9$$

assim

$$Q(A) = 8A + 2I$$

$$A^D = A^2 (8A + 2I)^3$$

$$A^D = A^2 (8A^3 + 6A^2 + 6A + 8I)$$

mas $A^2 = A + 3I$, logo

$$A^D = A^2 (8(A^2 + 3A) + 6A^2 + 6A + 8I)$$

$$A^D = A^2 (5A^2 + 3A + 8I)$$

$$A^D = A^2 (5 (A + 3I) + 3A + 8I)$$

$$A^D = 8A^3 + 5A^2$$

$$A^D = 8(A^2 + 3A) + 5A^2$$

$$A^D = 4A^2 + 6A$$

$$A^D \equiv A + 3I \pmod 9$$

Isto é:

$$A^D \equiv 3A + 2I \pmod 8$$

$$A^D \equiv A + 3I \pmod 9$$

Agora, usando o teorema do resto chinês da mesma forma que no exemplo 3.3.1 obteremos

$$A^D \equiv 19A + 66I \pmod{72}$$

3.4. APÊNDICE

TABELA DAS INVERSAS DE DRAZIN DE MATRIZES QUADRADAS SINGULARES E NÃO NILPOTENTES ATÉ ORDEM 5 EM TERMOS DOS COEFICIENTES DA EQUAÇÃO CARACTERÍSTICA.

ORDEM 2

2.1 $A^2 + aA = 0$ $\qquad A^D = a^{-2} A$

ORDEM 3

3.1 $A^3 + aA^2 = 0$ $\qquad A^D = a^{-3} A^3$

3.2 $A^3 + aA^2 + bA = 0$ $\qquad A^D = b^{-2} [a A^2 + (a^2-b) A]$

ORDEM 4

4.1 $A^4 + a A^3 = 0$ $\qquad A^D = a^{-4} A^3$

4.2 $A^4 + a A^3 + b A^2 = 0$ $\qquad A^D = [(a^2 - b) A^3 + (a^3 - 2ab) A^2]$

4.3 $A^4+a A^3+b A^2+cA = 0$ $\qquad A^D = c^{-2} [b A^3+(ab-c) A^2+(b^2-ac) A]$

ORDEM 5

5.1 $A^5 + a A^4 = 0$ $\qquad A^D = - a^{-5} A^4$

5.2 $A^5 + a A^4 + b A^3 = 0$ $\qquad A^D = b^{-4} [(a^3-2ab) A^4+(a^4-3a^2b+b^2)A^3]$

5.3 $A^5 + a A^4 + b A^3 + cA^2 = 0$ $\qquad A^D = c^{-3} [(ac-b)^2 A^4 + (a^2c-ab^2+bc)A^3 + (2abc-b^3-c^2)A^2]$

5.4 $A^5 + a A^4 + b A^3 + cA^2 + dA = 0$ $\qquad A^D = d^{-2} [(c A^4 + (ac-d) A^3 + (bc-ad)A^2 + (c^2-bd) A]$

TABELA DAS INVERSAS EM Z_{26} E Z_{13}

em Z_{26}:

x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

em Z_{13}:

x	1	2	3	4	5	6	7	8	9	10	11	12
x^{-1}	1	7	9	10	11	8	2	5	3	4	6	12

CAPITULO IV

IV - EQUAÇOES DIFERENCIAIS MATRICIAIS ORDINARIAS

4.1 INTRODUÇÃO

A solução da equação diferencial matricial.

1) $Ax' + Bx = f(t), \quad x(0) = x_0$

é obtida através de fórmula de variação dos parâmetros quando A é uma matriz não singular; mais precisamente:

2) $x = x_h + x_p$

onde

3) $x_h = e^{-A^{-1}Bt} \; x(0)$

é a solução da equação homogênea associada, e

4) $x_p = \int_0^t e^{-A^{-1}B(t-s)} f(s)ds$

é uma solução particular de 4) que satisfaz $x_p(0)=0$.

Se A é uma matriz singular, as fórmulas 3) e 4) não podem ser utilizadas. Mais que isto, o problema inicial 1) pode ser inconsistente (sem soluções), ou consistente (com soluções), mas sem unicidade.

Como exemplo podemos citar:

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

O problema de valor inicial $Ax' + Bx = 0$, $x(0) = [1,1]^T$ claramente não tem solução.

Agora, se $A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

com $x(0) = [1,1,1]^T$ não é difícil verificar que o problema de valor inicial $Ax' + Bx = 0$, $x(0) = c$ possui infinitas soluções. Note que nos dois exemplos acima até temos que $AB = BA$.

O nosso estudo restringir-se-á ao caso em que se 1) possuir soluções elas são únicas, propriedade esta que será referida como **solúvel** ou **tratável.** Estabeleceremos uma condição equivalente de solubilidade, para dali determinar a validade das fórmulas 3) e 4) com modificações apropriadas. Isto será feito com o auxílio da inversa de Drazin. Este estudo dividir-se-á em duas etapas, a primeira onde consideramos o caso onde os coeficientes matriciais A e B comutam e a segunda, o caso geral.

4.2 A EQUAÇÃO $Ax' + Bx = F(T)$ QUANDO $AB = BA$

Consideramos a equação homogênea matricial.

1) $$Ax' + Bx = 0 \quad , \quad AB = BA$$

e a decomposição centro nilpotente de A (dada no capítulo 2)

2) $$A = C_A + N_A = T \begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} T^{-1}$$

onde

$$C_A = AA^DA \quad e \quad N_A = A(I - A^DA)$$

são tais que $C_A N_A = N_A C_A = 0$, e o N_A é nilpotente de índice $k = ind(A)$. Em 2), C é inversível e N é nilpotente de ordem k.

Agora, considerando

3) $\quad x_1 = A^D Ax \quad e \quad x_2 = (I - A^D A)x$

e multiplicando 1) por A^D e $(I - A^D)$ respectivamente, obtemos o "desacoplamento":

4) $\quad x'_1 + A^D B x_1 = -A^D B x_2$

5) $\quad N_A x'_2 + B x_2 = 0$

devido a:

$$x = x_1 + x_2$$

$$N_A x_1 = N_A A^D Ax = A(I - A^D A)A^D Ax = 0,$$

e as matrizes envolvidas comutarem,

É claro que a existência ou unicidade da solução do problema inicial,

6) $\quad Ax' + Bx = 0, \quad x(0) = x_0, \quad AB = BA$

dependerá essencialmente da análise da equação 5), pois para cada solução x_2 de 5), quando existir, obtemos facilmente a solução x_1 de 4). Em particular, como $x_2 = 0$ é solução, obtemos que

7) $\quad x(t) = e^{-A^D B t} AA^D q$

é a solução de 1) para cada vetor q. Além disto, 6) é consistente sempre que $x_0 = A^D Aq$ para algum vetor q.

Observamos que a solução 7) é analítica em t e que a procura de soluções analíticas

$$x(t) = \sum_{m=0}^{\infty} C_m \frac{t^m}{m!}$$

para a equação 1), equivale a solução de equações em diferenças.

8) $$AC_{m+1} + BC_m = 0$$

utilizando o desacoplamento anterior, ou seja

$$u_m = A^D AC_m \quad e \quad v_m = (I - A^D A)c_m$$

obtemos o sistema equivalente a 8)

8') $$u_{m+1} + A^D B u_m = -A^D B v_m$$

8'') $$N_A v_{m+1} + B v_m = 0$$

Como $u_m = 0$ satisfaz 8''), decorre que

9) $$u_m = (-A^D B)^m u_0$$

onde

9') $$u_0 = A^D A q$$

para algum vetor q. Assim:

$$x(t) = \sum_{m=0}^{\infty} u_m \frac{t^m}{m!} = \sum_{m=0}^{\infty} (-A^D B)^m \frac{t^m}{m!} A^D A q =$$

$$= e^{-A^D B t} A^D A q,$$

coincide com 7).

O seguinte lema será frequentemente utilizado.

LEMA 4.2.1

Sejam A e B matrizes que comutam e que $N(A) \cap N(B) = \{0\}$. Considerando A em sua forma centro-nilpotente, então

10) $$B = T \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix} T^{-1}$$

onde B_2 é inversível e de dimensão igual a parte nilpotente de A, isto é N. Além disto

11) $$(I - A^D A)\, B^D B = I - A^D A$$

PROVA

Escrevamos $$B = T \begin{bmatrix} B_1 & G_1 \\ G_2 & B_2 \end{bmatrix} T^{-1}$$

com B_1 e B_2 de mesma dimensão de C e N respectivamente. Como A e B comutam, temos que $A^j B = BA^j$ para cada inteiro $j \geq 0$. Portanto $C^j B_1 = B_1 C^j$, $C^j G_1 = G_1 N^j$, $N^j G_2 = G_2 C^j$, $N^j B_2 = B_2 N^j$.

Fazendo j igual ao índice de A e utilizando o fato que C é inversível, decorre que $G_1 = G_2 = 0$.

Se B_2 não fosse inversível, teríamos que $B_2 v = 0$ para algum v não nulo. Sendo N nilpotente, existe um inteiro m não negativo tal que $N^m v = 0$, $N^{m-1} v \neq 0$ e $B_2 (N^{m-1}) v \neq N^{m-1} (B_2 v) = 0$. Por outro lado, $x = T \begin{bmatrix} 0 \\ N^{m-1} v \end{bmatrix}$ seria não nulo, com $Ax = Bx = 0$. Por hipótese isto não pode ocorrer, logo B_2 é inversível.

Temos ainda que:

$$(T^{-1}BT)^D = T^{-1}B^DT = \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix}^D = \begin{bmatrix} B_1^D & 0 \\ 0 & B_2^D \end{bmatrix}$$

logo

$$(I-A^DA)B^DB = T \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} T^{-1}T \begin{bmatrix} B_1^D & 0 \\ 0 & B_2^D \end{bmatrix} T^{-1}T \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix} T^{-1}$$

$$= T \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} T^{-1} = (I-A^DA).$$

C.Q.D.

TEOREMA 4.2.1

Suponha que AB=BA e que $N(A) \cap N(B) = \{ 0 \}$, então:

1) Qualquer solução da equação $Ax' + Bx = 0$, é da forma:

12) $$x(t) = e^{-A^D Bt} A^D Aq$$

2) Qualquer solução da equação $AC_{m+1} + BC_m = 0$ é a forma:

13) $$C_m = (-A^DB)^m C_0 \ , \quad C_0 = A^D Aq, \text{ para algum vetor } q.$$

PROVA:

É suficiente estabelecer que as equações 5) e 8'') possuem somente a solução nula. Para tanto vamos multiplicar 5) por N_A^{k-1}, onde k é o índice da matriz A. Decorre daí que $BN_A^{k-1}x_2 = 0$.

Fazendo $x_2 = T \begin{bmatrix} u \\ v \end{bmatrix}$,

obtemos:

$$0 = BN_A^{k-1} x_2 = T \begin{bmatrix} 0 & 0 \\ 0 & B_2N^{k-1} \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix} = T \begin{bmatrix} 0 \\ B_2N^{k-1} v \end{bmatrix}$$

Sendo B_2 inversível, decorre que $N^{k-1}v = 0$ e portanto $N_A^{k-1}x_2 = 0$.

Agora multiplicando 5) por N_A^{k-2}, e como $N_A^{k-1}x_2' = 0$, obtemos que $BN_A^{k-2}x_2 = 0$. Utilizando o argumento anterior, segue-se que $N_A^{k-2}v = 0$ e que $N_A^{k-2}x_2 = 0$. Seguindo do mesmo modo, chegamos à $v = 0$ e $Bx_2 = 0$. Portanto, temos $x_2 = T \begin{bmatrix} u \\ 0 \end{bmatrix}$ com $B_1u = 0$

Porém, $(I - AA^d)x_2 = x_2$ implica que

$$0 = T \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} u \\ 0 \end{bmatrix} = T \begin{bmatrix} u \\ 0 \end{bmatrix}$$

isto é, $u = 0$ pois T é não singular, consequentemente, devemos ter $x_2 = 0$.

A mesma demonstração é feita para a segunda parte do teorema (equação em diferenças).

C.Q.D.

Campbell em seu trabalho observa que na demonstração do teorema anterior, são usadas muitas propriedades de Drazin, logo uma inversa distinta da de Drazin geralmente não poderá ser usada.

Nos exemplos dados anteriormente para a equação $Ax' + Bx = 0$ tínhamos como coeficientes:

a) $$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Assim $N(A) \cap N(B) = \{0\}$ e como A é nilpotente temos $A^D = 0$, logo a equação dada possui somente a solução trivial.

b) $$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Assim $N(A) \cap N(B) \neq \{0\}$

Notamos que $e^{-A^D Bt A^D A}$ é nulo, mas a equação possui soluções não triviais.

Comparando agora a inversa de Drazin com uma (1,2) inversa para A, isto é, é uma pseudoinversa X para a matriz dada, tal que satisfaça as equações $AXA = A$ e $XAX = X$, podemos ver que $X = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$ é uma [1,2] inversa para A do exemplo a), e que $e^{-XBt}XAq = e^{-Xt}XAq$ é distinta de zero para qualquer q distinto de zero e portanto é uma solução não trivial de $Ax' + Bx = 0$, o que contradiria o teorema anterior, assim concluimos que não é possível resolver este problema com uma (1,2) inversa.

Vamos agora considerar a equação não homogênea

14) $Ax' + Bx = f(t)$, $AB = BA$

Utilizando a decomposição 2) em 14), decorre que

15) $x_1' + A^D B x_1 = A^D f$

16) $N_A x_2' + B x_2 = (I - AA^D) f$

uma solução de 15) é imediata:

17) $x_1(t) = \int_a^t e^{-A^D B(t-s)} A^D f(s) ds$

Afirmamos que:

18) $x_2(t) = (I - AA^D) \sum_{j=0}^{k-1} (-AB^D)^j B^D f^{(j)}(t)$

é a solução de 16) para f k-vezes diferenciável, e $N(A) \cap N(B) = \{0\}$. Façamos $T^{-1}x_2 = [u \quad v]^T$. Multiplicando 8) por N_A^{k-1} e utilizando o lema 4.2.1, obtemos:

$BN_A^{k-1}x_2 = N_A^{k-1}(I - AA^D)f$, isto é:

$$\begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & N^{k-1} \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & N^{k-1} \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \end{bmatrix} \begin{bmatrix} 0 \\ B_2^{k-1} \end{bmatrix} =$$

$$= \begin{bmatrix} 0 \\ N^{k-1} \quad f_2 \end{bmatrix}$$

portanto, $N^{k-1} v = B_2^{-1} N^{k-1} f_2$

ou equivalentemente, $N_A^{k-1}x_2 = N_A^{k-1}B^D f$

Multiplicando 8) por N_A^{k-2} e utilizando o fato que $N_A^{k-1}x_2' = N_A^{k-1}B^D f'$, decorre $BN_A^{k-2}x_2 = N_A^{k-2} \cdot (I - AA^D)f - N_A^{k-1}B^D f'$ e portanto temos:

$$N_A^{k-2}v = B_2^{-1} N^{k-2} f_2 - B_2^{-2} N^{k-1} f_2,$$

ou simplesmente

$$N_A^{k-2} x_2 = N_A^{k-2} B^D f - N_A^{k-1} (B^D)^2 f',$$

Em geral

$$N_A^{k-j} v = \sum_{i=0}^{j-1} (-1)^i N^{k+i-j} B^{-(i+1)} f_2^{(i)}, \text{ ou ainda } N_A^{k-j} x_2 = \sum_{i=0}^{j-1} (-1)^i N_A^{k+i-j} (B^D)^{i+1} f^{(i)} =$$

$$= N_A^{k-j} \sum_{i=0}^{j-1} (-N_A B^D)^i B^D f^{(i)}$$

fazendo $k = j$ obtemos

$$x_2 = \sum_{i=0}^{k-1} (I - AA^D)^i (-AB^D)^i B^D f^{(i)} =$$

$$= (I - AA^D) \sum_{i=0}^{k-1} (-AB^D)^i B^D f^{(i)}$$

devido à, $(I - AA^D) = \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} = (I - AA^D)^i$

Com esta demonstração acima, acabamos de mostrar o:

TEOREMA 4.2.2

Se $AB = BA$, $N(A) \cap N(B) = \{0\}$, $k = ind(A)$ e se f é k-vezes continuamente diferenciável então $Ax' + Bx = f$ é consistente e uma solução particular é dada por:

$$x = A^D e^{-A^D Bt} \int_a^t e^{A^D Bs} f(s) +$$

$$+ (I - AA^D) \sum_{n=0}^{k-1} (-AB^D)^n B^D f^{(n)} \text{ com a arbitrário.}$$

TEOREMA 4.2.3

Se $AB = BA$ e $N(A) \cap N(B) = \{0\}$, então a solução geral da equação $Ax' + Bx = f(t)$, com $f(t)$ k-vezes diferenciável, é dada por:

11) $x = e^{-A^D Bt} A^D Aq + \int_a^t e^{-A^D B(t-s)} A^D f(s)\, ds +$

$$+ (I - AA^D) \sum_{i=0}^{k-1} (-AB^D)^i B^D f^{(i)}$$

onde k é o índice da matriz A, e q é um vetor.

OBS.: A prova deste teorema é uma consequência direta do teorema 4.2.2 e 4.2.1 .

LEMA 4.2.2

Se existe c tal que (cA + B) é inversível, então comutam $\hat{A}_c = (cA + B)^{-1} A$ e $\hat{B}_c = (cA + B)^{-1} B$

PROVA:

Vamos supor que existe c tal que $(cA + B)^{-1}$ existe assim:

$I = (cA + B)^{-1} (cA + B) = c(cA + B)^{-1} A + (cA + B)^{-1} B$, isto é:

$I = c\hat{A}_c + \hat{B}_c$

agora multiplicando esta equação por $\hat{A}_c$ pela esquerda e depois pela direita obtemos que:

$\hat{A}_c = c\hat{A}_c\hat{A}_c + \hat{A}_c c\hat{B}_c$ e

$\hat{A}_c = c\hat{A}_c\hat{A}_c\, c + \hat{B}_c\hat{A}_c$

e assim temos que

$\hat{A}_c\, \hat{B}_c = \hat{B}_c\, \hat{A}_c$

C.Q.D.

DEFINIÇÃO 4.2.1

A equação $Ax' + Bx = 0$ será dita regular quando o polinômio $p(w) = \det(wA + B)$ não se anula identicamente, isto é $(cA + B)^{-1}$ existe para algum escalar c.

TEOREMA 4.2.4

A equação $Ax' + Bx = 0$ tem solução única para condições iniciais consistentes se e somente se ela é regular.

PROVA:

Vamos supor que existe c tal que $(cA + B)$ é inversível, assim $N(A) = N((cA + B)^{-1} A)$ e $N(B) = N((cA + B)^{-1}B)$.

Seja $v \in N(A) \cap N(B)$.

Assim $Av = 0$ e $Bv = 0$ logo $(cA + B)v = 0$ e como $(cA + B)$ é inversível temos que $v = 0$, isto é $N(\hat{A}_c) \cap N(\hat{B}_c) = \{0\}$

logo, pelo teorema 4.2.1 temos que $(cA + B)^{-1} Ax' + (cA+B)^{-1} Bx = 0$ tem solução única para condições iniciais consistentes.

Agora supondo que $Ax' + Bx = 0$ possui solução única para condições iniciais consistentes e que $(cA + B)$ não é inversível para nenhum c temos:

Existe $w_c \neq 0$ vetor tal que $(cA + B)\, w_c = 0$, fazendo $x_c = e^{tc} w_c$ temos:

$Ax_c' = ce^{tc} Aw_c = -e^{tc} Bw_c = -Bx$ e assim x_c é uma solução de $Ax' + Bx = 0$.

Somente n dos w_c podem ser LI, assim tomemos um subconjunto $w_{c_i=i,t}$ $c_i \neq 0$ e portanto são vetores LD, assim

$$\sum_{i=1}^{l} m_i w_{c_i} = 0$$

vamos definir

$$x = \sum_{i=1}^{l} m_i \; e^{tc_i} \; w_{c_i}$$

logo, x e zero satisfazem a equação dada em $x(0) = 0$ o que contraria a hipótese de solução única para condições iniciais consistentes.

C.Q.D.

LEMA 4.2.3

Se A e B são matrizes quadradas de dimensão n tais que $(cA + B)^{-1}$ existe para algum c, então independem do c escolhido,

$\hat{A}^D_c \hat{A}_c$; $\hat{A}^D_c \hat{B}_c$; $\hat{A}^D_c (cA+B)^{-1}$; $\hat{B}^D_c (cA+B)^{-1}$; $\hat{A}_c \hat{B}^D_c$ e $\text{ind}(\hat{A}_c)$

PROVA:

Se $b \neq c$ tal que $(bA + B)^{-1}$ exista

1) $\hat{A}_b (bA+B)^{-1} = ((bA+B)^{-1} (cA+B) (cA+B)^{-1} A)^D (bA+B^{-1}) =$

$= ((cA+B)^{-1} (bA+B))^{-1} \hat{A}_c)^D (bA+B)^{-1} =$

$= A^D_c [(cA+B)^{-1} (bA+B)] (bA+B)^{-1} = \hat{A}^D_c (cA+B)^{-1}$

2) multiplicando 1) por A pela direita temos

$$\hat{A}^D_c \hat{A}_c = \hat{A}_b{}^D \hat{A}_b$$

3) multiplicando 1) por B pela direita temos

$$\hat{A}^D_c \hat{B}_c = \hat{A}^D_b \hat{B}_b$$

4) Prova de forma semelhante a 1) que

$$\hat{B}_c^{\,d}\,(cA + B)^{-1} = \hat{B}_b\,(bA + B)^{-1}$$

5) De 4), multiplicando por A pela direita e usando o lema anterior temos que $\hat{B}_c^{\,D}\,\hat{A}_c = \hat{B}_b^{\,D}\,\hat{A}_b$ isto é $\hat{A}_c\,\hat{B}_c^{\,D}$

6) $\text{ind}(\hat{A}^c)$ é o menor inteiro k tal que posto $(\hat{A}_c^{\,k})$ = posto $\hat{A}_c^{\,k+1}$

assim

posto $(\hat{A}_b^{\,k})$ = posto $[(b\hat{A}_c + \hat{A}_c)^{-1}\hat{A}_c]^k$ = posto $[(b\hat{A}_c+\hat{B}_c)^{-k}\hat{A}_c^{\,k}]$ = posto $(\hat{A}_c^{\,k})$

C.Q.D.

Dada uma equação diferencial matricial singular regular

$$Ax' + Bx = f,$$

consideramos a equação associada

$$\hat{A}x' + \hat{B}x = \hat{f},$$

onde

$$\hat{A} = (cA+B)^{-1}\,A;\ \hat{B} = (cA+B)^{-1}\,B;\ \hat{f} = (cA+B)^{-1}\,f$$

são tais que $\hat{A}\hat{B} = \hat{B}\hat{A}$

TEOREMA 4.2.5

Supondo que: 1) $Ax' + Bx = 0$ tem solução única para condições iniciais consistentes ou equivalentemente, existe c tal que $(cA+B)$ é inversível e 2) $\hat{A}$, $\hat{B}$, $\hat{f}$ estão definidas como acima 3) $k = ind(\hat{A})$,

Então:

$Ax' + Bx = f$, $x(0) = x_0$ tem solução se e somente se

19) $x_0 = \hat{A}\hat{A}^D q + (I-\hat{A}\hat{A}^D) \sum_{n=0}^{k-1} (-1)^n (\hat{A}\hat{B}^D)^n \hat{B}^D \hat{f}^{(n)}(0)$, para algum q

uma solução particular de $Ax' + Bx = f$ é:

20) $x = \hat{A}^D e^{-A^D Bt} \int_a^t e^{\hat{A}^D Bs} \hat{f}(s)ds + (I-\hat{A}\hat{A}^D) \sum_{n=0}^{k-1} (-\hat{A}\hat{B}^D)^n \hat{B}^D \hat{f}^{(n)}$

onde a é arbitrário.

A solução geral de $Ax' + Bx = f$ é:

21) $x = e^{-\hat{A}^D \hat{B}t} \hat{A}\hat{A}^D q + \hat{A}^D e^{-\hat{A}^D \hat{B}t} \int_a^t e^{\hat{A}^D \hat{B}s} \hat{f}(s)ds +$

$+ (I - \hat{A}\hat{A}^D) \sum_{n=0}^{k-1} (-\hat{A}\hat{B}^D)^n \hat{B}^D \hat{f}^{(n)}$

com $q \in C^n$. Além disto, a solução satisfazendo $x(0) = x_0$ é encontrada fazendo $q = x_0$ e $a = 0$ em 21.

EXEMPLO 4.2.1

Consideremos a equação diferencial homogênea $Ax' + Bx = 0$

onde

$$A = \begin{bmatrix} 1 & 0 & -2 \\ -1 & 0 & 2 \\ 2 & 3 & 2 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 & 2 \\ -27 & -22 & -17 \\ 18 & 14 & 10 \end{bmatrix}$$

Vemos que A e B são ambas singulares e não comutam, mas A + B é uma matriz inversível, logo multiplicando a equação por $(A + B)^{-1}$ chegamos à $\hat{A}x' + \hat{B}x = 0$ onde

$$\hat{A} = (A+B)^{-1}A = \frac{1}{3}\begin{bmatrix} -3 & -5 & -4 \\ 6 & 5 & -2 \\ -3 & 2 & 10 \end{bmatrix} \quad \text{e}$$

$$\hat{B} = I - \hat{A} = \frac{1}{3}\begin{bmatrix} 6 & 6 & 4 \\ -6 & -2 & 2 \\ 3 & -2 & 7 \end{bmatrix}$$

Os auto valores de $\hat{A}$ são 0, 1, 3 assim A^D pode ser computada pelo teorema 2.4.2 como:

$$\hat{A}^D = \begin{bmatrix} -27 & -41 & -28 \\ 54 & 77 & 46 \\ -27 & -34 & -14 \end{bmatrix}$$

Logo para condições iniciais consistentes temos que:

$$(I-\hat{A}\hat{A}^d)x(0) = \frac{1}{9}\begin{bmatrix} 18 & 14 & 10 \\ -18 & -14 & -10 \\ 9 & 7 & 5 \end{bmatrix}\begin{bmatrix} x_1(0) \\ x_2(0) \\ x_3(0) \end{bmatrix} = 0$$

Existe somente uma equação independente envolvida:

$$9x_1(0) + 7x_2(0) + 5x_3(0) = 0$$

Como os autovalores de $(-\hat{A}^D B)$ são 0, 0, 2/3, não é difícil computar a matriz exponencial como:

$$x(t) = e^{-A^D\hat{B}t}x(0) = \frac{1}{18}\begin{bmatrix} 18 & 1-e^{2t/3} & 2(1-e^{2t/3}) & x_1(0) \\ 0 & 26-8^{2t/3} & 16(1-e^{2t/3}) & x_2(0) \\ 0 & 13(e^{2t}-1) & 26\,e^{2t/3}-8 & x_3(0) \end{bmatrix}$$

Neste sistema podemos usar a equação para eliminar um dos x_i.

TEOREMA 4.2.6

Se a equação homogênea $Ax_{n+1} = Bx_n$ é tratável, então a solução geral é dada por:

$$22) \qquad x_n \begin{cases} \hat{A}\hat{A}^D q & \text{se } n = 0 \\ (\hat{A}^D\hat{B})^n q & \text{se } n = 1,2,3,\ldots \end{cases} \qquad q \text{ vetor de } C^m$$

onde $\hat{A} = (wA-B)^{-1}A$ e $\hat{B} = (wA-B)^{-1}B$ e w um número complexo tal que $(wA-B)^{-1}$ existe. Mais ainda, c e C^m é vetor consistente inicial para 22 e somente se $c \in R(\hat{A}^k)$, onde $k = \text{ind}(\hat{A})$. Neste caso a única solução, sujeita à $x_0 = c$, é dada por $x_n = (\hat{A}^D\hat{B})^n c$, $n=0,1,2,3,\ldots$. A equação não homogênea $Ax_{n+1} = Bx_n + f_n$ também é tratável. Sua solução geral é para $n \geq 1$.

$$23) \quad x_n = (\hat{A}^D\hat{B})^n \hat{A}\hat{A}^D q + \hat{A}^D \sum_{i=0}^{n-1} (\hat{A}^D\hat{B})^{n-i-1} \hat{f}_i - (I-\hat{A}\hat{A}^D) \sum_{i=0}^{k-1} (\hat{A}\hat{B}^D)^i \hat{B}^D \hat{f}_{n+i}$$

onde

$$\hat{A} = (wA - B)^{-1}A, \quad \hat{B}(wA - B)^{-1}B, \quad \hat{f}_i = (wA - B)^{-1}f$$

$k = \text{ind}(\hat{A})$ e $q \in \mathbb{C}^m$.

A solução x_n é independente de w.

Seja $\hat{w} = -(I - \hat{A}\hat{A}^D) \sum_{i=0}^{k-1} (\hat{A}\hat{B}^D)^i \hat{B}^D \hat{f}_i$. O vetor c é um vetor consistente inicial se e somente c está no domínio $\{w + R(\hat{A}^k)\}$.

PROVA:

Como $Ax_{n+1} = Bx_n$ é tratável, multiplicando por $(wA-B)^{-1}$ obtemos a equação equivalente:

$\hat{A}x_{n+1} = \hat{B}x_n$, isto é

$$\begin{bmatrix} C & 0 \\ 0 & N \end{bmatrix} \begin{bmatrix} x^{(1)}_{n+1} \\ x^{(2)}_{n+1} \end{bmatrix} = \begin{bmatrix} I + wC & 0 \\ 0 & I+wN \end{bmatrix} \begin{bmatrix} x^{(1)}_{n} \\ x^{(2)}_{n} \end{bmatrix}$$

Assim $x_n^{(2)} = (I - wN)^{-k} N^k = 0$

$$x_n^{(1)} = C^{-1} (I - wC)^n x_0^{(1)} ,$$

e a solução da equação homogênea segue.

O resto da prova segue diretamente do teorema 4.2.5 .

C.Q.D.

CAPITULO V

V - APLICAÇÕES DA INVERSA DE DRAZIN NO SISTEMA CRIPTOGRÁFICO DE HILL

5.1 INTRODUÇÃO

Neste capítulo apresentaremos algumas aplicações da inversa de Drazin em problemas de criptogragia, mais precisamente no sistema desenvolvido por Hill [7] [8]. O conceito básico na crixptografia é o de "codificação", o qual entenderemos como uma transformação injetiva entre dois conjuntos numéricos discretos. Sua transformação inversa é referida como "decodificação".

Por exemplo, se considerarmos as letras do alfabeto em correspondência biunívoca com Z_{26}, então a transformação linear $E(x) = ax + b$, onde a é primo com 26 e b é um número arbitrário de Z_{26}, define uma codificação de Z_{26}, nele mesmo. Neste caso, $D(y) = (y-b).a^{-1}$ é a função decodificação. Se supuzermos que a correspondência usada é $a \to 1$; $b \to$; .... $z \to 26$ teremos que a palavra "massa" corresponde à (13, 1, 19, 19, 1). Usando em $E(x)$ $a = 3$ e $b = 1$ temos que a codificação pela transformação $E(x)$ em Z_{26} é (14, 4, 5, 5, 4), a qual usando novamente a correspondência alfa numérica corresponde as letras N, D, E, E, D. Tendo a disposição a função "decodificação" $D(y) = (y-1).9$, é a mensagem recebida NDEED obtem-se que a mensagem enviada é MASSA.

Este dispositivo, todavia é muito fraco para manter segredo da mensagem enviada, pois mesmo não possuindo

a função decodificação seria possível por tentativas e pela freqüência alfabética na língua portuguesa, isto é, no português duas letras iguais juntas provavelmente serão ss ou rr e portanto a letra E → s ou E → r em ambos os casos D é uma vogal, sendo assim um texto extenso seria facilmente decodificado. [13]

Para evitar este problema Hill em 1929 introduziu a codificação matricial que consiste na transmissão de bloco de letras em lugar de letras simples (mono alfabético), de modo a tornar muito oneroso os cálculos da freqüência alfabética. Assim, vamos considerar uma função codificação E(x) de $(Z_{26})^m$ em si mesmo, onde m denota o comprimento do bloco. Em particular, Hill considera

$$E(x) = Kx$$

onde k é uma matriz mxm, cujo determinante é primo com 26 e portanto não singular e x um vetor mx1. Porém, com o advento do computador, mesmo estes cálculos tornam-se viáveis e assim Levine em 1958 propos k como sendo a matriz

$$k = A + Bt$$

onde A, B são matrizes mxm fixas e t é um parâmetro em Z_{26} que varia a cada bloco. Além do esforço computacional no processo de decodificação, surgem problemas com erros de transmissão, os quais no caso matricial propagam-se tornando indecifrável a mensagem. Por tanto, é de interesse determinar a possibilidade de construir um código sem este defeito. Gabriel [11] demonstra esta possibilidade e seus resultados foram generalizados e simplificados por Hartwing [12,13] utilizando a inversa de Drazin, este mé-

todo será o objetivo deste capítulo.

5.2 A INVERSA DE DRAZIN NO SISTEMA CRIPTOGRÁFICO DE HILL (W-KEY)

Na seção anterior, foi mencionada a possibilidade de um sistema de codificação no qual a chave para o próximo passo seria uma função codificada a cada passo e não dependente de uma codificação prévia. Um método assim foi aperfeiçoado usando inversa de Drazin em conjugação ao sistema criptográfico de Hill. Em [10] mostra-se como construir matrizes com as propriedades acima mancionadas. Aqui iremos discutir 2 destes métodos com exemplos.

1º CASO, W-KEY

As matrizes chaves de Drazin usam conjuntos de parâmetros:

1) Uma sequência de números inteiros $\{n_1, n_2, \ldots\}$ $1 \leq n_i \leq m$ onde m grafos estão sendo codificados.

2) Duas sequências de elementos inversíveis de Z_t $\{\alpha_1, \alpha_2, \ldots\}$; $\{\beta_1, \beta_2, \ldots\}$.

Os métodos para geração destes parâmetros serão descritos posteriormente.

No sistema de Hill, como usual, o texto é escrito na forma de uma matriz retangular com m linhas e n colunas. A sequência n_i é usada para "quebrar" o texto em blocos com n_i colunas adicionadas de colunas suficientes de zeros para formar matrizes quadradas, as quais chamaremos de P_1, P_2, ... Cada bloco P_i será codificado como uma unidade.

Definimos a W-key como:

$$k(P_i) = \alpha_i (P_i^D)^2 + \beta_i (I - P_i P_i^D)$$

Nesta fórmula α_i e β_i são selecionados das sequências $\{ \alpha_i \}$,$\{ \beta_i \}$ respectivamente e P_i representa um bloco e P^D sua inversa de Drazin.

P_i então será codificado para C_i, definido por:

$$C_i = k(P_i)\ P_i$$

(3) A matriz $k(P_i)$ é inversível com inversa $k'(C_i)$ onde

$$k'(C_i) = \alpha_i (C_i^D)^2 + \beta_i^{-1} (I - C_i C_i^D)$$

Assim cada bloco P_i do texto original será dado por:

$$P_i = k'(C_i) . C_i$$

Logo, as fórmulas codificação e decodificação 2 e 4 podem ser simplificadas para:

$$C_i = \alpha_i P_i^D + \beta_i (I - P_i P_i^D) P_i \qquad (5)$$

$$P_i = \alpha_i C_i^D + \beta_i^{-1} (I - C_i C_i^D) C_i \qquad (6)$$

Onde 5 e 6 constituem a W-key.

Antes de dar um exemplo, vamos provar as afirmações 3,5,6.

1) $k(P_i)$ é inversível: (Obs.: Vamos omitir o sub índice i).

PROVA:

Basta mostrar que $k(P) \cdot k^D(P) = I$.

Seja $A = \alpha(P^D)^2$ e $B = \beta(I - PP^D)$

Assim temos:

$$A.B = \alpha\,\beta(P^D)^2\,(I - PP^D) = \alpha\,\beta P^D(P^D - P^D PP^D) =$$

$$= \alpha\,\beta P^D\,(P^D - P^D) = 0$$

e da mesma forma

$$B.A = 0$$

logo, como $(A + B)^D = A^D + B^D$ se $A.B = B.A = 0$ temos:

$$k^D(P) = (A + B)^D = A^D + B^D = (\alpha\,(P^D)^2)^D + (\beta(I - PP^D))^D =$$

$$= \alpha^{-1}\,((P^D)^D)^2 + \beta^{-1}\,(I - PP^D)^D =$$

$$= \alpha^{-1}\,(P^2\,P^D)^2 + \beta^{-1}\,(I - PP^D) =$$

$$= \alpha^{-1}\,P^4\,(P^D)^2 + \beta^{-1}\,(I - PP^D) =$$

$$= \alpha^{-1}\,P^3\,P^D + \beta^{-1}\,(I - PP^D)$$

Logo:

$$k(P) \cdot k^D(P) = [\,\alpha\,(P^D)^2 + \beta\,(I - PP^D)]\,[\,\alpha^{-1}P^3P^D + \beta^{-1}\,(I - PP^D)] =$$

$$= P^3(P^D)^3 + (I - PP^D)^2 + \alpha\,\beta^{-1}(P^D)^2\,(I - PP^D) + \alpha^{-1}\beta\,(I-PP^D)P^3P^D =$$

$$= P^2(P^DPP^D)P^D + I - PP^D + \alpha\,\beta^{-1}[(P^D)^2 - P^DP^DPP^D] + \alpha^{-1}\beta(P^3P^D - P^3P^DPP^D) =$$

$$= P \cdot P \cdot P^D\,P^D + I - PP^D + 0 + 0 = I$$

C.Q.D.

2) $k'(C) = k^{-1}(P)$

PROVA:

$$C^D = (k(P)P)^D = [(\alpha (P^D)^2 + \beta(I - PP^D))P]^D =$$

$$= (\alpha P^D + \beta (I - PP^D)P)^D = (\alpha P^D)^D +$$

$$+ [\beta(I - PP^D)P]^D =$$

$$= \alpha^{-1} P^2 P^D \text{ , pois:}$$

$$[\beta(I - PP^D)P] [\alpha P^D] = [\alpha P^D] [\beta(I - PP^D)P] =$$

$$= (\beta(I - PP^D)P [\alpha P^D] = \alpha\beta [PP^D - PP^D PP^D] = 0$$

Além disto,

$$C.C^D = [\alpha P^D + \beta(I - PP^D)P] [\alpha^{-1} P^2 P^D] =$$

$$= P^D P^2 P^D + \beta \alpha^{-1} (I - PP^D) PP^D = PP^D$$

Logo:

$$k'(C) = (\alpha^{-1} P^2 P^D)^2 + \beta^{-1} (I - PP^D) =$$

$$= \alpha^{-1} (P^4 (P^D)^2) + \beta^{-1} (I - PP^D) =$$

$$= \alpha^{-1} P^3 P^D + \beta^{-1} (I - PP^D) = k^D(P) = k^{-1}(P)$$

C.Q.D.

3) $C = \alpha P^D + \beta (I - PP^D)P$

PROVA:

$$C = k(P)P = [\alpha\ (P^D)^2 + \beta\ (I - PP^D)]P =$$

$$= \alpha\ P^D + \beta\ (I - PP^D)P$$

C.Q.D.

$$P = \alpha C^D + \beta^{-1}\ (I - CC^D)C$$

PROVA:

$$P = k'\ (C).C = [\alpha(C^D)^2 + \beta^{-1}\ (I - CC^D)]C$$

$$= \alpha C^D + \beta^{-1}\ (I - CC^D)C$$

C.Q.D.

EXEMPLO 1:

Vamos codificar o texto "MÉTODO DE HILL" usando W-key com, $m = 5$ $n_1 = 1$, $n_2 = 2$, $n_3 = 2$ $\alpha_1 = 7$, $\beta_1 = 9$, $\alpha_2 = 15$, $\beta_2 = 23$, $\alpha_3 = 3$, $\beta_3 = 11$ e usando a correspondência alfabética:

A = 7	B = 12	C = 20	D = 0
E = 1	F = 14	G = 13	H = 4
I = 6	J = 21	K = 19	L = 11
M = 3	N = 16	O = 5	P = 15
Q = 10	R = 23	S = 22	T = 2

U = 18 V = 24 W = 8 X = 9

Y = 17 Z = 25

1) A primeira coisa a ser feita é formar o retângulo com o texto a ser codificado, com m = 5, completando os espaços exedentes com uma letra qualquer

M	E	T	O	D
O	D	E	H	I
L	L	D	D	D

2) Usando a tabela alfa-numérica dada, temos:

3	1	2	5	0
5	0	1	4	6
11	11	0	0	0

3) Usando $n_1 = 1$, $n_2 = n_3 = 2$ e completando as colunas que sobram com zeros, encontrando assim as matrizes P_1, P_2, P_3.

$$\underset{P_1}{\begin{bmatrix} 3 & 0 & 0 \\ 5 & 0 & 0 \\ 11 & 0 & 0 \end{bmatrix}} \quad \underset{P_2}{\begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 11 & 0 & 0 \end{bmatrix}} \quad \underset{P_3}{\begin{bmatrix} 5 & 0 & 0 \\ 4 & 6 & 0 \\ 0 & 0 & 0 \end{bmatrix}}$$

1) Codificando P_1

$$P_1 = \begin{bmatrix} 3 & 0 & 0 \\ 5 & 0 & 0 \\ 11 & 0 & 0 \end{bmatrix}$$

$\sigma_1 = 3 \rightarrow a_1 = -3 \equiv 23 \pmod{26}$

$\sigma_2 = 0$

$\sigma_3 = 0$

Assim, temos que

$$(P_1)^3 + 23(P_1)^2 \equiv 0 \pmod{26}$$

como existe $(23)^{-1}$ pela tabela do apêndice do capítulo 3 temos:

$$(P_1)^D \equiv -25(P_1)^2 \equiv (P_1)^2 \pmod{26}$$

$$(P_1)^D = (P_1)^2 = \begin{bmatrix} 9 & 0 & 0 \\ 15 & 0 & 0 \\ 11 & 0 & 0 \end{bmatrix}$$

como $(I - P_1 P_1^D) P_1 = 0$ temos:

$$C_1 = 7(P_1)^D = \begin{bmatrix} 11 & 0 & 0 \\ 1 & 0 & 0 \\ 23 & 0 & 0 \end{bmatrix}$$

agora, desprezando as duas últimas colunas da matriz C_1 e usando a tabela alfa numérica dada, temos as letras

L

E

R

2) Codificando P_2

$$P_2 = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 11 & 0 & 0 \end{bmatrix}$$

$\sigma_1 = 1 + 1 = 2 \rightarrow a_1 = -2 \equiv 24 \pmod{26}$

$\sigma_2 = 1 \rightarrow a_2 = 1$

$\sigma_3 = 0$

Assim temos que:

$$(P_2)^3 + 24\ (P_2)^2 + P_2 \equiv 0 \pmod{26}$$

como existe $(1)^{-1}$ pela tabela do apêndice do capítulo 3 temos:

$$(P_2)^D = 1\ [24\ (P_2)^2 + (24^2 - 1)\ P_2]$$

$$(P_2)^D = 24\begin{bmatrix} 1 & 4 & 0 \\ 0 & 1 & 0 \\ 11 & 22 & 0 \end{bmatrix} + 3\begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 11 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 24 & 0 \\ 0 & 1 & 0 \\ 11 & 8 & 0 \end{bmatrix}$$

como

$$(I - P_2\ P_2^D) = 0 \quad \text{temos:}$$

$$C_2 = 15\begin{bmatrix} 1 & 24 & 0 \\ 0 & 1 & 0 \\ 11 & 8 & 0 \end{bmatrix} = \begin{bmatrix} 15 & 22 & 0 \\ 0 & 15 & 0 \\ 9 & 16 & 0 \end{bmatrix}$$

agora, desprezando a última coluna da matriz C_2 e usando a tabela alfa numérica dada, temos as letras

P S

D P

X N

3) Codificando P_3

$$P_3 = \begin{bmatrix} 5 & 0 & 0 \\ 4 & 6 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$\sigma_1 = 5 + 6 = 11 \rightarrow a_1 = -11 \equiv 15 \pmod{26}$

$\sigma_2 = 4 \pmod{26} \rightarrow a_2 \equiv 4 \pmod{26}$

$\sigma_3 = 0$

daí:

$$(P_3)^3 + 15(P_3)^2 + 4\ P_3 = 0$$

como MDC (4,26) $\neq$ 1 vamos usar o teorema do resto chinês para encontrar $(P_3)^D$.

$$(P_3)^3 + 2(P_3)^2 + 4\ P_3 \equiv 0 \pmod{13}$$

$$(P_3)^3 + (P_3)^2 \equiv 0 \pmod{2}$$

pela tabela do apêndice do capítulo 3:

$$(P_3)^D \equiv 5\ (P_3)^2 \pmod{13}$$

$$(P_3)^D \equiv (P_3)^2 \pmod{2}$$

pelo teorema do resto chinês:

$$(P_3)^D \equiv 5(P_3)^2 \pmod{26}$$

$$(P_3)^D = \begin{bmatrix} 21 & 0 & 0 \\ 12 & 24 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

como $(I - P_3\ P_3^D)\ P_3 = 0$, temos:

$$C_3 = 3 \begin{bmatrix} 21 & 0 & 0 \\ 12 & 24 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 11 & 0 & 0 \\ 10 & 20 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

o que corresponde as letras

L	D
Q	C
D	D

logo, por 1), 2), 3) temos a mensagem codificada:

L	P	S	L	D
E	D	P	Q	C
R	X	N	D	D

isto é,

L E R L D F D P Q C V X N D D

será a mensagem transmitida.

EXEMPLO 2:

Vamos decodificar a mensagem " L E R L D F D P Q C V X N D D" usando n_1, n_2, n_3, m, β_1, β_2, β_3, α_1, α_2, α_3 idênticos ao exemplo 1.

A primeira coisa a ser feita é arranjar a mensagem em blocos, obtendo C_1, C_2, C_3 com o uso da tabela alfa numérica.

L	P	S	L	D
E	D	P	Q	C
R	X	N	D	D

assim temos:

$$\begin{bmatrix} 11 & 0 & 0 \\ 1 & 0 & 0 \\ 23 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 5 & 22 & 0 \\ 0 & 15 & 0 \\ 21 & 16 & 0 \end{bmatrix} \quad \begin{bmatrix} 11 & 0 & 0 \\ 10 & 20 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

C_1 C_2 C_3

1) Decodificando C_1.

$$C_1 = \begin{bmatrix} 11 & 0 & 0 \\ 1 & 0 & 0 \\ 23 & 0 & 0 \end{bmatrix} \qquad \begin{aligned} \sigma_1 &= 11 \rightarrow a_1 = 15 \\ \sigma_2 &= \sigma_3 = 0 \end{aligned}$$

Assim:

$$(C_1)^3 + 15(C_1)^2 \equiv 0 \pmod{26}$$

pela tabela do apêndice do capítulo 3:

$$(C_1)^D = 21(C_1)^2 = \begin{bmatrix} 19 & 0 & 0 \\ 23 & 0 & 0 \\ 9 & 0 & 0 \end{bmatrix}$$

como $(I - C_1 C_1^D) C_1 = 0$

$$P_1 = 7 \begin{bmatrix} 19 & 0 & 0 \\ 23 & 0 & 0 \\ 9 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 \\ 5 & 0 & 0 \\ 11 & 0 & 0 \end{bmatrix}$$

o que corresponde ás letras

M

O

L

2) Decodificando C_2

$$C_2 = \begin{bmatrix} 15 & 22 & 0 \\ 0 & 15 & 0 \\ 9 & 16 & 0 \end{bmatrix} \qquad \begin{aligned} \sigma_1 &= 4 \rightarrow a_1 = 22 \\ \sigma_2 &= 17 = a_2 \\ \sigma_3 &= 0 \end{aligned}$$

Assim,

$$(C_2)^3 + 22\,(C_2)^2 + 17\,(C_2) \equiv 0 \pmod{26}$$

pela tabela do apêndice do capítulo 3:

$$(C_2)^D = (17)^{-2}\,[22(C_2)^2 + (22^2 - 17)C_2] = \begin{bmatrix} 7 & 14 & 0 \\ 0 & 7 & 0 \\ 25 & 0 & 0 \end{bmatrix}$$

como $(I - C_1\,C_1^D)\,C_1 = 0$

$$P_1 = 15 \begin{bmatrix} 7 & 14 & 0 \\ 0 & 7 & 0 \\ 25 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 11 & 0 & 0 \end{bmatrix}$$

o que corresponde às letras

E	T
D	E
L	D

3) Decodificando C_3

$$C_3 = \begin{bmatrix} 11 & 0 & 0 \\ 10 & 20 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$\sigma_1 = 5 \rightarrow a_1 = 21$

$\sigma_2 = 12$

$\sigma_3 = 0$

Assim

$$(C_3)^3 + 21(C_3)^2 + 12\,C_3 \equiv 0 \pmod{26}$$

como MDC (12, 26) $\neq 1$

$$(C_3)^3 + 8(C_3)^2 + 12\,C_3 \equiv 0 \pmod{13}$$

$$(C_3)^3 + (C_3)^2 \equiv 0 \pmod{2}$$

pela tabela do apêndice do capítulo 3:

$$(C_3)^D \equiv 8(C_3)^2 \pmod{13}$$

$$(C_3)^D \equiv (C_3)^2 \pmod{2}$$

Assim, pelo teorema do resto chinês,

$$(C_3)^D \equiv 21\ C_3^2 \pmod{26}$$

$$(C_3)^D = \begin{bmatrix} 19 & 0 & 0 \\ 10 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

como $(I - C_3\ C_3^D)\ C_3 = 0$

$$P_3 = 3(C_3)^D = \begin{bmatrix} 5 & 0 & 0 \\ 4 & 6 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

o que corresponde às letras:

O	D
H	I
D	D

Logo, por 1), 2), 3) temos o bloco

M	E	T	O	D
O	D	E	H	I
L	L	Ø	Ø	Ø

isto é

METODO DE HILL

É importante detectar possíveis falhas do sistema dado, o sistema W-Key depende essencialmente de 3 pontos:

1) A escolha da correspondência alfabética
2) A escolha dos parâmetros n_1, α_i, β_i
3) A escolha de m.

Supondo 1 e 3 conhecidos e supondo também que $1 \leq n_1 \leq m$, α_i e β_i desconhecidos, vemos em Z_{26} α_i e β_i podem ter escolhas a cada passo da codificação. Se n_i, α_i e β_i são 1 ou algum outro valor conhecido, não existe problema algum para encontrar o texto P. Assim, é muito importante a variação destes parâmetros.

Devemos notar também que se num dado passo $CC^D = I$, ou $(I - CC^D)C = 0$ então o texto P será dado por $P = \alpha C^D$ com α limitado a 12 escolhas, se $n_i = m$, isto sugere que o texto cifrado seja escrito em conjuntos de m colunas consecutivas 1, 2, ... m; 2, 3, ... m + 1; 3, 4, ... m + 2; ... formando assim matrizes inversíveis que podem ser testadas para o plano texto com 12 tentativas dadas por $P = \alpha C^{-1}$ se $n_i < m$ escreveremos o texto cifrado em h colunas

1, 2, ... h; 2, 3, ... h + 1; ...

estes conjuntos de h colunas para os quais $(I - CC^D)\ C = 0$ podem ser testados usando as 12 escolhas para α em $P = \alpha C^D$.

Iremos agora obter uma forma alternativa de

$$C = \alpha P^D + \beta (I - PP^D)P$$

$$P = \alpha C^D + \beta^{-1} (I - C C^D)C$$

Da formação dos blocos P_i pela adição de colunas nulos, como já foi visto na seção anterior quando $n_i < m$, temos que o bloco P_i pode ser escrito na forma:

$$P = \left[\begin{array}{c|c} A & 0 \\ \hline B & 0 \end{array}\right]$$

onde A é uma matriz quadrada $n_i \times n_i$ e P é uma matriz quadrada m x m. Assim, pelo capítulo 2 temos que:

$$P^D = \left[\begin{array}{c|c} A^D & 0 \\ \hline B(A^D)^2 & 0 \end{array}\right]$$

Daí;

$$PP^D = \begin{bmatrix} AA^D & 0 \\ BA^D & 0 \end{bmatrix}$$

$$P^2\,P^D = \begin{bmatrix} A^2\,A^D & 0 \\ BAA^D & 0 \end{bmatrix}$$

$$(I - PP^D)P = P - P^2\,P^D = \begin{bmatrix} A(I - AA^D) & 0 \\ B(I - BB^D) & 0 \end{bmatrix}$$

Assim:

$$C = \alpha \begin{bmatrix} A^D & 0 \\ B(A^D)^2 & 0 \end{bmatrix} + \beta \begin{bmatrix} A(I - AA^D) & 0 \\ B(I - BB^D) & 0 \end{bmatrix}$$

Da mesma forma temos:

$$C = \begin{bmatrix} A' & 0 \\ B' & 0 \end{bmatrix}$$

Onde A' é uma matriz quadrada $n_i \times n_i$ e C é uma matriz quadrada n x n

$$C^D = \begin{bmatrix} (A')^D & 0 \\ B'(A')^D & 0 \end{bmatrix}$$

$$P = \alpha \begin{bmatrix} (A')^D & 0 \\ (B(A')^D & 0 \end{bmatrix} + \beta^{-1} \begin{bmatrix} A'(I - A'A'^D) & 0 \\ B'(I - B'B'^D) & 0 \end{bmatrix}$$

Vamos agora considerar os casos:

1) Se A' é inversível $\rightarrow A' A'^D = I \rightarrow P = \alpha C^D$

n e $C = \alpha P^D$

2) Se A' é nilpotente $\rightarrow (A')^h = 0$ algum $h \rightarrow A'^D = 0$

$\rightarrow P = \beta^{-1} C$ e $C = \beta P$

3) Se $n_i = 1 \rightarrow A = [a_1]$; $A' [a_1']$

$P = \text{col}\ (a_1, a_2, \ldots a_n)$

$C = \text{col}\ (a_1, a_2, \ldots a_n')$

Neste caso $C = U P$ e $P = U^{-1} C$

o que é fácil demonstrar

OBS.: Quando $n_i = 1$

x	1	3	7	9	11	15	17	19	21	23	25	13	0	2	4	6	8	10	12
x^D	1	9	15	3	19	7	23	11	5	17	25	23	0	20	10	24	18	4	12

14	16	18	20	22	24
14	22	8	2	16	6

4) Se $n_i = 2(Z_{26})$

a) Se $A'^2 + \sigma A' + 2\tau I = 0 \pmod{26}$

com,

$(\sigma, 26) = 1, \quad 2\sigma \neq 0 \quad C = \begin{bmatrix} A' & 0 \\ B' & 0 \end{bmatrix}$

então $P = \alpha C^D + 13 \begin{bmatrix} 0 & 0 \\ B'(A'+I) & 0 \end{bmatrix}$

b) Se $A'^2 + \sigma A' + 2\tau I = 0$

σ par e $\sigma = 0$, $2\tau \neq 0$ então $P = \alpha C^D + 13C$

RESUMO:

Na codificação de uma W-key em Z_{26} temos:

$P = UC \quad (C = U^{-1}P)$ quando:

1) $n_i = m$ e C é inversível
2) $n_i < m$ e $C = C^2 C^D$
3) $(A')^h = 0$ algum h
4) $n_i = 1$

Supondo o alfabeto e o valor de m conhecidos, um método para atacar as W-key é:

1) Se $n_i = m$

Começando com as colunas

1, 2, ... m ; 2, 3, ... m + 1 ...

determinar se C^{-1} existe ($I - CC^{D} = 0$) se sim, $P = UC$ e como U^{-1} existe testa-se as 12 escolhas possíveis para U, olhando para o plano texto horizontal e verticalmente

2) Se $n_i = h < m$

testa-se $(I - CC^{D})C$

Se for zero, $P = UC$ e usam-se as colunas

1, 2, ... h ; 2, 3, ... h + 1 ; ...

testa-se vertical e horizontalmente

3) teste se $(A')^{r} = 0$ para algum r

assim $P = UC$

4) P/ $n_i = 2$ use as fórmulas dadas acima.

5) $n_i = 1$ $P = UC$ para cada coluna cifrada

Em todos os casos existem 12 escolhas para U, o que é bem melhor que o caso geral, no qual existem $144 = 12^2$ escolhas para α e β.

5.3 O MÉTODO V-KEY

No método V-key são adicionadas características não existentes no W-key que irá acrescentar a este método grande dose de segurança.

Além das sequências (n_i), (α_i), (β_i) de parâmetros o método V-key possui uma sequência de matrizes simétricas $(B_1, B_2, \ldots)$, $(B_i = B^T)$, cujas dimensões dependem da sequência (n_i).

Como no caso anterior o texto será escrito na forma de uma matriz retangular de m linhas e a sequência (n_i) determinará como as colunas serão quebradas, para formar os blocos de tamanho $m \times n_i$. Os blocos serão chamados de P_i e a matriz B_i associada ao bloco P_i terá a dimensão $n_i \times n_i$.

Uma matriz quadrada V_i (m x m) será definida por:

1) $$V_i = P_i B_i P_i^T = V_i^T$$

e a matriz chave $k_i(V_i)$ m x m correspondente ao bloco P_i será definida por:

2) $$k_i(V_i) = \alpha_i V_i^D + \beta_i (I - V_i V_i^D)$$ V-key

o código correspondente ao texto P_i será

3) $$C_i = k_i(V_i) P_i$$

Para decodificação do bloco C_i, a matriz Y_i (m x m) será definida por:

4) $$Y_i = C_i B_i C_i^T$$

que será usada para definir a matriz chave de decodificação

5) $$k_i'(Y_i) = \alpha_i Y_i^D + \beta_i^{-1}(I - Y_i Y_i^D)$$

onde

$$P_i = k_i'(Y_i)\, C_i$$

Vamos mostrar agora que $k_i(V_i)$ é inversível e que

$$k'(Y) = k^{-1}(V)$$

Para tanto

1) $k(V).k^D(V) = I$

$$k(V) = \alpha V^D + \beta(I - VV^D)$$

$$k^D(V) = (\alpha V^D + \beta(I - VV^D))^D = (\alpha V^D)^D + \beta(I - VV^D)^D$$

pois $V^D(I - VV^D) = 0$

$$= \alpha^{-1} V^2 V^D + \beta^{-1}(I - VV^D)$$

logo:

$$k(V).K^D(V) = [\alpha V^D + \beta(I - VV^D)]\,[\alpha^{-1} V^2 V^D + \beta^{-1}(I - VV^D)]^2$$

$$= V^2 (V^D)^2 + \alpha\beta^{-1}(I - VV^D) + \beta\alpha^{-1} V^2 V^D (I - VV^D) + (I - VV^D)^2 =$$

$$= VV^D + 0 + 0 + I - VV^D = I$$

Além disto; $VV^D = YY^D$, pois:

$$Y = [k(V)P]\, B\, [K(V)P)]^T = k(V)P\, B\, P^T\, (k(V))^T =$$

$$= k(V)V\, (k(V))^T$$

como B é simétrica:

$$V^T = (P\, B\, P^T)^T = P\, B^T\, P^T = PBP^T = V$$

V também é

Considerando agora que

k(V) é simétrica, isto é

$$(k(V))^T = [\alpha V^D + \beta(I - VV^D)]^T = \alpha V^D + \beta[I - (V^D)^T V^T]$$

$$= \alpha V^D + \beta(I - V^D V) = k(V)$$

temos que:

$$Y = K(V)V\ K(V) = [\alpha V^D + \beta(I-VV^D)]V[\alpha V^D+\beta\ (I-VV^D)]$$

$$= \alpha^2(V^D)^2\ V + \alpha\beta V^D V(I-VV^D) + \beta\alpha(I-VV^D)VV^D+\beta^2(I-VV^D)V(I-VV^D)$$

$$= \alpha^2\ V^D + \beta^2\ (I - VV^D)V$$

e assim

$$Y^D = [\alpha^2\ V^D + \beta^2\ (I - VV)^D V]^D = \alpha^{-2}\ V^2\ V^D$$

pois $V^D\ (I - VV^D)V = 0$

e portanto:

$$YY^D = [\alpha^2\ V^D + \beta^2\ (I - VV^D)V]\ [\alpha^{-2}\ V^2\ V^D] = VV^D$$

Assim,

$$K'(Y) = \alpha Y^D + \beta^{-1}\ (I - YY^D) = \alpha\ (\alpha^{-2}\ V^2\ V^D)+\beta^{-1}(I-VV^D) =$$

$$= \alpha^{-1}\ V^2\ V^D + \beta^{-1}\ (I - VV^D) = K^D(V) = K^{-1}(V)$$

C.Q.D.

Agora daremos um exemplo do método, codificando o mesmo texto anterior

METODO DE HILL

EXEMPLO 3

Vamos codificar o texto "MÉTODO DE HILL" usando V-Key com

$m = 3$ $\quad (\alpha_1, \beta_1) = (7, 9)$

$n_1 = 1$ $\quad (\alpha_2, \beta_2) = (15, 23)$

$n_2 = 2$ $\quad (\alpha_3, \beta_3) = (3, 11)$

$n_3 = 2$

usando a correspondência alfabética

A = 6	B = 12	C = 11	D = 0	E = 1	F = 14
G = 13	H = 4	I = 7	J = 21	K = 19	L = 20
M = 3	N = 16	O = 5	P = 15	Q = 10	R = 23
S = 22	T = 2	U = 18	V = 24	W = 8	X = 9
Y = 17	Z = 25				

M	E	T	O	D
O	D	E	H	I
L	L	D	D	D

convertendo a valores numéricos

$n_1 = 1$	$n_2 = 2$		$n_3 = 2$	
3	1	2	5	0
5	0	1	4	7
20	20	0	0	0
P_1	P_2		P_3	

como sequência B_i vamos usar as matrizes simétricas

$$B_1 = [6] \qquad B_2 = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \qquad B_3 = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

Neste exemplo os parâmetros foram escolhidos arbitrariamente.

1) Cálculo de C_1

$$V_1 = \begin{bmatrix} 3 \\ 5 \\ 20 \end{bmatrix} [6] [3\ 5\ 20] = \begin{bmatrix} 2 & 12 & 22 \\ 12 & 20 & 2 \\ 22 & 2 & 8 \end{bmatrix}$$

Para obter a equação característica de V_1 calculamos:

$$\sigma_1 = 4 \rightarrow a_1 = -4 \equiv 22 \pmod{26}$$

$$\sigma_2 = \sigma_3 = 0$$

logo

$$V_1^3 + 22V_1^2 = 0 \qquad \text{mas} \quad \text{MDC}(22, 26) \neq 1$$

logo:

$$V_1^3 + 9V_1^2 \equiv 0 \pmod{13}$$

$$V_1^3 \equiv 0 \pmod{2}$$

pela tabela do apêndice do capítulo 3:

$$(V_1)^D \equiv -9^{-3} (V_1)^2 \pmod{13}$$

$$(V_1)^D \equiv 0 \pmod{2}$$

isto é

$$(V_1)^D \equiv 12 (V_1)^2 \pmod{13}$$

$$(V_1)^D \equiv 0 \pmod{2}$$

Assim pelo teorema do resto chinês temos:

$$V_1^D \equiv 12(V_1)^2 \pmod{26}$$

$$(V_1)^D = \begin{bmatrix} 18 & 4 & 16 \\ 4 & 24 & 18 \\ 16 & 18 & 20 \end{bmatrix}, \quad V_1(V_1)^D = \begin{bmatrix} 20 & 16 & 12 \\ 16 & 18 & 20 \\ 12 & 20 & 2 \end{bmatrix},$$

$$I - V_1(V_1)^D = \begin{bmatrix} 7 & 10 & 14 \\ 10 & 9 & 6 \\ 14 & 6 & 25 \end{bmatrix}$$

logo, como $(\alpha_1, \beta_1) = (7, 9)$

$$k_1(V_1) = 7\,V_1^D + 9(I - V_1(V_1)^D) = \begin{bmatrix} 7 & 14 & 4 \\ 14 & 15 & 24 \\ 4 & 24 & 1 \end{bmatrix}$$

e portanto

$$C_1 = k_1(V_1)P_1 = \begin{bmatrix} 7 & 14 & 4 \\ 14 & 15 & 24 \\ 4 & 24 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 5 \\ 20 \end{bmatrix} = \begin{bmatrix} 15 \\ 25 \\ 22 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} P \\ Z \\ S \end{bmatrix}$$

2) Cálculo de C_2

$$V_2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 20 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 20 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 14 & 5 & 2 \\ 5 & 2 & 20 \\ 2 & 20 & 20 \end{bmatrix}$$

$\sigma_1 = 10 \rightarrow a_1 = 16$

$\sigma_2 = 23$

$\sigma_3 = 0$

$23^{-1} = 17$

Daí:

$$V_2^3 + 16V_2^2 + 23V_2 \equiv 0 \pmod{26}$$

$(23, 26) = 1$ logo pela tabela do capítulo 3 temos:

$$V_2^D = (23)^{-2} [16 V_2^2 + (16^2 - 23) V_2]$$

$$V_2^D = 3 [16 V_2^2 + (22 - 23) V_2]$$

$$V_2^D = 22V_2^2 + 23V_2$$

$$V_2^D = \begin{bmatrix} 10 & 14 & 4 \\ 14 & 0 & 20 \\ 4 & 20 & 8 \end{bmatrix} + \begin{bmatrix} 10 & 11 & 20 \\ 11 & 20 & 18 \\ 20 & 18 & 18 \end{bmatrix} =$$

$$= \begin{bmatrix} 20 & 25 & 24 \\ 25 & 20 & 12 \\ 24 & 12 & 0 \end{bmatrix}$$

$$V_2 . V_2^D = \begin{bmatrix} 11 & 6 & 6 \\ 6 & 15 & 14 \\ 6 & 14 & 2 \end{bmatrix} \quad I - V_2 V_2^D = \begin{bmatrix} 16 & 20 & 20 \\ 20 & 12 & 12 \\ 20 & 12 & 25 \end{bmatrix}$$

como $(\alpha_2, \beta_2) = (15, 23)$

$$k_2(V_2) = 15 V_2^D + 23(I - V_2 V_2^D) = \begin{bmatrix} 18 & 3 & 14 \\ 3 & 4 & 14 \\ 14 & 14 & 3 \end{bmatrix}$$

logo:

$$C_2 = k_2(V_2) P_2 = \begin{bmatrix} 18 & 3 & 14 \\ 3 & 4 & 14 \\ 14 & 14 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 20 & 0 \end{bmatrix} = \begin{bmatrix} 12 & 13 \\ 23 & 10 \\ 22 & 16 \end{bmatrix} \rightarrow$$

$$\rightarrow \begin{bmatrix} B & G \\ R & Q \\ S & N \end{bmatrix}$$

3) Cálculo de C_3

$$V_3 = P_3 \, B_3 \, P_3^T$$

$$V_3 = \begin{bmatrix} 5 & 0 \\ 4 & 7 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 5 & 4 & 0 \\ 0 & 7 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} 24 & 23 & 0 \\ 23 & 4 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Sua equação característica é:

$$(V_3)^3 + 24(V_3)^2 + 9\,(V_3) \equiv \pmod{26}$$

como $(9\,,\,26) = 1$ diretamente pela tabela do capítulo 6 teremos:

$$V_3^D = 8(V_3)^2 + 7V_3 = \begin{bmatrix} 0 & 4 & 0 \\ 4 & 18 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 12 & 5 & 0 \\ 5 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 12 & 9 & 0 \\ 9 & 20 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$V_3 \cdot V_3^D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad I - V_3 \, V_3^D = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

como $(\alpha_3, \beta_3) = (3, 11)$ temos:

$$K_3(V_3) = 3V_3^D + 11(I - V_3V_3^D) = \begin{bmatrix} 10 & 1 & 0 \\ 1 & 8 & 0 \\ 0 & 0 & 11 \end{bmatrix}$$

logo:

$$C_3 = k_3(V_3)P_3 = \begin{bmatrix} 2 & 7 \\ 11 & 4 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} T & I \\ C & H \\ D & D \end{bmatrix}$$

e assim a mensagem recebida seria

P	B	G	T	I
Z	R	Q	C	H
S	S	N	D	D

"P B G T I Z R Q C H S S N D D"

EXEMPLO 4:

Vamos decodificar

"P B G T I Z R Q C H S S N D D"

usando os mesmos dados dos exemplo 3.

1º) Separa-se o texto em bloco

P	' B	G	' T	I
Z	' R	Q	' C	H
S	, S	N	, D	D

Assim: $C_1 = \begin{bmatrix} 15 \\ 25 \\ 22 \end{bmatrix}$ $C_2 = \begin{bmatrix} 12 & 13 \\ 23 & 10 \\ 22 & 10 \end{bmatrix}$ $C_3 = \begin{bmatrix} 10 & 1 \\ 1 & 8 \\ 0 & 0 \end{bmatrix}$

Agora dedodificando C_1, C_2, C_3, isto é encontrando P_1, P_2, P_3:

1) Calculando P_1

$$Y_1 = C_1 B_1 C_1^T = \begin{bmatrix} 15 \\ 25 \\ 22 \end{bmatrix} [6] [15 \quad 25 \quad 22] = \begin{bmatrix} 24 & 14 & 4 \\ 14 & 6 & 24 \\ 4 & 24 & 18 \end{bmatrix}$$

cuja equação característica é:

$$(Y_1)^3 + 4(Y_1)^2 \equiv 0 \pmod{26}$$

Assim

$$(Y_1)^3 + 4(Y_1)^2 \equiv 0 \pmod{13}$$

$$(Y_1)^3 \equiv 0 \pmod{2}$$

pela tabela do apêndice do capítulo 3 temos:

$$(Y_1)^D \equiv Y_1^2 \pmod{13}$$

$$(Y_1)^D \equiv 0 \pmod{2}$$

Assim, pelo teorema do resto chinês:

$$(Y_1)^D \equiv 14 \quad (Y_1)^2 \pmod{26}$$

isto é

$$(Y_1)^D = \begin{bmatrix} 8 & 22 & 10 \\ 22 & 2 & 8 \\ 10 & 8 & 6 \end{bmatrix}$$ e assim; como $\alpha = 7$ e $\beta^{-1} = 3$

$$k_1'(Y_1) = 7Y_1^D + 3(I - Y_1 Y_1^D) = \begin{bmatrix} 25 & 2 & 8 \\ 2 & 15 & 22 \\ 8 & 22 & 13 \end{bmatrix}$$

e

$$P_1 = k_1'(Y_1)C_1 = \begin{bmatrix} 3 \\ 5 \\ 20 \end{bmatrix} \iff \begin{matrix} M \\ O \\ L \end{matrix}$$

2) Calculando P_2

$$Y_2 = C_2 B_2 C_2^T = \begin{bmatrix} 12 & 13 \\ 23 & 10 \\ 22 & 16 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 12 & 23 & 22 \\ 13 & 10 & 16 \end{bmatrix} =$$

$$\begin{bmatrix} 2 & 9 & 18 \\ 9 & 2 & 22 \\ 18 & 22 & 0 \end{bmatrix}$$

$$\sigma_1 = 2 + 2 = 4 \rightarrow a_1 = 22$$

$$\sigma_2 = \begin{bmatrix} 2 & 9 \\ 9 & 2 \end{bmatrix} + \begin{bmatrix} 2 & 18 \\ 18 & 0 \end{bmatrix} + \begin{bmatrix} 2 & 22 \\ 22 & 0 \end{bmatrix} = 4-3-12-16 = 25$$

logo, a Equação característica correspondente é:

$$(Y_2)^3 + 22\, Y_2^2 + 25 Y_2 \equiv 0 \pmod{26}$$

pela tabela do capítulo 3 temos:

$$(Y_2)^D = 25^{-2} [22\, Y_2^2 + (22^2 - 25) Y_2] =$$

$$= 1^2 (22\, Y_2^2 + 17 Y_2)$$

$$(Y_2)^D = 22\, Y_2^2 + 17\, Y_2 = 22 \begin{bmatrix} 19 & 16 & 0 \\ 16 & 23 & 24 \\ 0 & 24 & 2 \end{bmatrix} + 17 \begin{bmatrix} 2 & 9 & 18 \\ 9 & 2 & 22 \\ 18 & 22 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 14 & 0 \\ 14 & 12 & 8 \\ 0 & 8 & 18 \end{bmatrix} + \begin{bmatrix} 8 & 23 & 20 \\ 23 & 8 & 10 \\ 20 & 10 & 0 \end{bmatrix} = \begin{bmatrix} 10 & 11 & 20 \\ 11 & 20 & 18 \\ 20 & 18 & 18 \end{bmatrix}$$

como $(\alpha, \beta^{-1}) = (15, 17)$ temos:

$$k_2'(Y_2) = 15(Y_2)^D + 17(I-Y_2Y_2^D) = 15\begin{bmatrix}10 & 11 & 20\\ 11 & 20 & 18\\ 20 & 18 & 18\end{bmatrix} + 17\begin{bmatrix}16 & 20 & 20\\ 20 & 12 & 12\\ 20 & 12 & 25\end{bmatrix}$$

$$= \begin{bmatrix}20 & 9 & 14\\ 9 & 14 & 10\\ 14 & 10 & 10\end{bmatrix} + \begin{bmatrix}12 & 2 & 2\\ 2 & 22 & 22\\ 2 & 22 & 9\end{bmatrix} = \begin{bmatrix}6 & 11 & 16\\ 11 & 10 & 6\\ 16 & 6 & 19\end{bmatrix}$$

$$P_2 = k_2'(Y_2)\,C_2 = \begin{bmatrix}6 & 11 & 16\\ 11 & 10 & 6\\ 16 & 6 & 19\end{bmatrix}\begin{bmatrix}12 & 13\\ 23 & 10\\ 22 & 16\end{bmatrix} =$$

$$\begin{bmatrix}1 & 2\\ 0 & 1\\ 20 & 0\end{bmatrix} \Longleftrightarrow \begin{matrix}E & T\\ D & E\\ L & D\end{matrix}$$

Calculando P_3

$$Y_3 = C_3B_3C_3^T = \begin{bmatrix}2 & 7\\ 11 & 4\\ 0 & 0\end{bmatrix}\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}\begin{bmatrix}2 & 7 & 0\\ 11 & 4 & 0\end{bmatrix} = \begin{bmatrix}4 & 3 & 0\\ 3 & 24 & 0\\ 0 & 0 & 0\end{bmatrix}$$

cuja equação característica é:

$$(Y_3)^3 + 24\,Y_3^2 + 9\,Y_3 \equiv 0 \pmod{26}$$

como $(26, 1) = 1$ diretamente da tabela do capítulo 3:

$$(Y_3)^D = (9)^{-2}\,[24(Y_3)^2 + (24^2 - 9)Y_3]$$

$$Y_3^D = 8Y_3^2 + 7Y_3 = \begin{bmatrix}18 & 22 & 0\\ 22 & 0 & 0\\ 0 & 0 & 0\end{bmatrix} + \begin{bmatrix}2 & 21 & 0\\ 21 & 12 & 0\\ 0 & 0 & 0\end{bmatrix} = \begin{bmatrix}20 & 17 & 0\\ 17 & 12 & 0\\ 0 & 0 & 0\end{bmatrix}$$

$$Y_3 . Y_3^{D} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad (I - Y_3 Y_3^{D}) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

como $(\alpha_3, \beta_3^{-1}) = (3, 19)$

$$k_3'(Y_3) = 3Y_3^{D} + 19(I - Y_3 Y_3^{D}) = \begin{bmatrix} 8 & 25 & 0 \\ 25 & 10 & 0 \\ 0 & 0 & 19 \end{bmatrix}$$

$$P_3 = k_3'(Y_3)\, C_3 = \begin{bmatrix} 8 & 25 & 0 \\ 25 & 10 & 0 \\ 0 & 0 & 19 \end{bmatrix} \begin{bmatrix} 2 & 7 \\ 11 & 4 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 0 \\ 4 & 7 \\ 0 & 0 \end{bmatrix} \Longleftrightarrow \begin{matrix} O & D \\ H & I \\ D & D \end{matrix}$$

Assim escrevendo

$$P_1\ P_2\ P_3 = \begin{matrix} M & E & T & O & D \\ O & D & E & H & I \\ L & L & D & D & D \end{matrix}$$

temos a mensagem decodificada

"METODO DE HILL"

5.4 GERAÇÃO DE SEQUÊNCIAS E PARÂMETROS

Nesta seção serão sugeridos métodos para gerar várias sequências de parâmetros

1) A sequência $(n_1) = (n_1, n_2, \ldots)$

usa-se uma fórmula de recorrência, por exemplo se m = 4 e

$$x_{n+2} = x_{n+1} + x_n \pmod{53}$$

$x_1 = 5$

$x_2 = 17$

teríamos; a sequência:

(5, 17, 22, 39, 8, 47, 2, 49, 51, 47, 45...) a qual reduzido a uma sequência módulo 4, na qual usamos a classe do 4 ao invés da classe do zero, teríamos a sequência (n_i)

$$(n_i) = (1, 1, 2, 3, 4, 2, 1, 3, 3, 1, \ldots)$$

2) As sequências (α_i) e (β_i)

Usamos também fórmulas de recorrência, mas tomando módulo 12 e após a tabela de correspondência

(mod 12)	0	1	2	3	4	5	6	7	8	9	10	11
α ou β	1	3	5	7	9	11	15	17	19	21	23	25

Por exemplo, tomando a mesma fórmula de recorrências anterior com $x_1 = x_2 = 5$ obtemos a sequência módulo 12

5, 5, 10, 3, 8, 11, 2, 1, 3, ...

e agora pela tabela anterior, temos

(11, 11, 23, 7, 19, 25, 5, 3, 7, ...)

que é aceitável como sequência (α_i) ou (β_i), e depois variando as condições iniciais, obtem-se sequências distintas para α_i e β_i.

3) A sequência matricial B_i

Selecionam-se duas matrizes inversíveis triangulares inferiores (mxm) e definidas em Z_{26}, as quais chamaremos de A_1, A_2.

Definem-se as matrizes:

$$A_3 = A_2 \cdot A_1$$

$$A_4 = A_3 \cdot A_2, \ldots$$

que são também inversíveis e triangulares inferiores.

Define-se

$$B_i' = A_i \, A_i^T$$

Para um dado n_i, usa-se o canto superior esquerdo.

EXEMPLO

$$\text{Sejam } A_1 = \begin{bmatrix} 3 & 0 & 0 \\ 4 & 5 & 0 \\ 17 & 6 & 19 \end{bmatrix} \quad A_2 = \begin{bmatrix} 7 & 0 & 0 \\ 19 & 1 & 0 \\ 4 & 12 & 17 \end{bmatrix}$$

assim,

$$A_3 = A_2 . A_1 = \begin{bmatrix} 21 & 0 & 0 \\ 9 & 5 & 0 \\ 11 & 6 & 11 \end{bmatrix}$$

$$A_4 = A_3 . A_2 = \begin{bmatrix} 17 & 0 & 0 \\ 2 & 5 & 0 \\ 1 & 8 & 5 \end{bmatrix}, \text{ etc } \ldots$$

Agora se $n_1 = 2 \quad n_2 = 1 \quad n_3 = 3 \quad n_4 = 2 \ldots$ teríamos:

$$B_1' = A_1 \cdot A_1^T = \begin{bmatrix} 9 & 12 & 25 \\ 12 & 15 & 20 \\ 25 & 20 & 10 \end{bmatrix}$$

e como $n_1 = 2 \quad B_1 = \begin{bmatrix} 9 & 12 \\ 12 & 15 \end{bmatrix}$

$$B_2' = A_2 A_2^T = \begin{bmatrix} 23 & 3 & 2 \\ 3 & 24 & 10 \\ 2 & 10 & 7 \end{bmatrix}$$

e como $n_2 = 1 \quad B_2 = [23]$

$$B_3' = A_3 A_3^T = \begin{bmatrix} 25 & 7 & 23 \\ 7 & 2 & 25 \\ 23 & 25 & 18 \end{bmatrix}$$

e como $n_3 = 3 \qquad B_3 = \begin{bmatrix} 25 & 7 & 23 \\ 7 & 2 & 25 \\ 23 & 25 & 18 \end{bmatrix}$

$$B_4' = A_4 . A_4^T = \begin{bmatrix} 3 & 8 & 17 \\ 8 & 3 & 16 \\ 17 & 16 & 12 \end{bmatrix}$$

e como $n_4 = 2 \qquad B_4 = \begin{bmatrix} 3 & 8 \\ 8 & 3 \end{bmatrix}$

e assim por diante.

OBS.: Se um texto de comprimento L for codificado, usando m-grafos, isto requererá um arranjo retangular de m linhas.
$L = nN + N'$ com $(0 < N' < m)$
Se $N' > 0$, juntam-se zeros suficentes ao texto para ser possível construir um retângulo de n colunas, onde o novo comprimento do texto L será dado pela fórmula anterior onde
$n=N$ se $N' = 0$ e $n=N+1$ se $N' > 0$.
Também será feita uma adaptação nas n_i sequências, se tivermos que:
$n_1 + n_2 + \ldots + n_h < n$
e
$n_1 + n_2 + \ldots n_{h+1} > n$
neste caso n_{h+1} será substituído por:
$n_{h+1} = n - (n_1 + n_2 + \ldots n_h)$

Claramente notamos que os métodos V-Key e W-Key vistos neste capítulo não são métodos manuais, mas computacionais, mesmo que sejam usados para "mensagens curtas, além disto a W-Key é certamente mais fraca que a V-Key.

REFERÊNCIAS:

(1) Álgebra de dimensão finita.
Bernardo Felzenszwalb, 12º colóquio Brasileiro de Matemática, Poços de Caldas 16-28 julho 1979.

(2) G. Azumaya, Strangly π - regular rings J. Fac. Sci. Hokkaido University vol. 13 1954. pp. 34-39

(3) M.P. Drazin, Pseudo - inverses in associative rings and Semi groups.
American Mathematical Montly 65(1958), 506-514.

(4) A.Ben Israel and T.N.E. Greville, Generalized Inverses, theory and applications, Wiley, New York, 1974.

(5) Tim Anderson, Modern Algebra, Charles E. Merril Publ. Co., Columbus Omio (1974)

(6) Campbell S.L. And Meyer C.D. Jr. Generalized inverses of linear transformation Pitman publishing limited London - (1979)

(7) Campbell S.L. And Meyer C.D. Jr. Application of the Drazin inverse to linear sistems of differential equations withs singular constant coeficients Siam J. Appl. Math. 31, 411-425, 1976

(8) The Drazin inverse as a gradient.
R. Gabriel, R. Hartwing.

(9) Campbell S.L. Linear sistems of differential equations with singular coefficients. Siam J. Math. Anal. 8, 1057-1066 (1977)

(10) Levine, Jack and Hartwing Robert E. Applications of the Drazin inverse to the Hill cryptolographic system

(11) R. Gabriel, Pseudo-Inverses,
Mit schulüssel und ein system der algebraishen kryptographie, Rev. Roumaine de Math. Pures Et appl. XXII 8 (1977), 1077-1099.

(12) Lester S. Hill, Cripto Graphy in a algebraic alphabet, Amer. Math. Monthly 36(1929), 306-312

(13) Lester S. Hill, Concerning certain linear transformation apparatus of cryptography, Amer. Math. Monthly 38(1931), 135-154

(14) Jack Levine, Some Elementary cryptanalysis of algebric cryptography, Amer. Math. Monthly 68(1961), 411-418

(15) Jack Levine, Variable Matrix substitution in algebric cryptography, American, Math. Monthly 65(1958), 170-179.