Roney Rachide Nunes

Sistemas Dinâmicos Discretos Lineares

Universidade Federal de Minas Gerais
2010

Roney Rachide Nunes

Sistemas Dinâmicos Discretos Lineares

Dissertação de mestrado apresentada como requisito da obtenção do título de Mestre pelo Departamento de Matemática do Instituto de Ciências Exatas, Universidade Federal de Minas Gerais.

Orientador: Israel Vainsencher

Universidade Federal de Minas Gerais
2010

Agradecimentos

Agradeço aos meus pais que sempre me apoiaram em cada etapa da minha vida, me ajudando e me incentivando em tudo.

Ao meu orientador Israel Vainsencher, principalmente pela paciência e constante incentivo.

Aos meus colegas e professores, especialmente à minha amiga Elisa.

Aos meus amigos de Divinópolis e Viçosa que sempre estão do meu lado em todos os momentos.

A todos, que esqueci de mencionar, mas que de alguma forma contribuiram com esta trajetória, obrigado!

Resumo

Neste trabalho, concentraremos nossa atenção no estudo dos sistemas dinâmicos finitos: sistemas dinâmicos determinísticos, vistos em tempo discreto, e com um número finito de possíveis estados.

O propósito deste trabalho é tratar o caso de um sistema dinâmico finito linear (SDFL). O mesmo se apresenta como uma história de sucesso, em que o caso geral pode ser reduzido a essencialmente dois casos básicos: bijetivo e nilpotente. Tal redução ocorre por meio de ferramentas de álgebra linear, principalmente a forma normal de Smith e o teorema chinês do resto. Recorremos ainda a resultados referentes a polinômios com coeficientes em um corpo finito, que simplificam o estudo de um SDFL bijetivo.

Abstract

This work studies finite dynamical systems. These are deterministic dynamical systems, with discrete time and a finite number of possible states.

We focus on linear finite dynamical system (LFDS). This is a rather successful case. It can be reduced to essentially two basic subcases: bijective and nilpotent. The reduction uses tools from linear algebra, mainly the Smith normal form and the Chinese Remainder Theorem. We also employ some results on polynomials over finite fields in order to deal with bijective LFDS.

Sumário

Introdução

Em geral, o termo *sistemas dinâmicos* vem associado a equações diferenciais, sejam elas ordinárias ou parciais. Trata-se da determinação de leis que relacionam o estado atual e futuro de processos evolutivos em áreas aplicadas tais como biologia, física, economia ou engenharia, dentre outras. Como exemplos de sistemas dinâmicos, temos as equações de ondas, os modelos de crescimento populacional e as equações do calor.

Neste trabalho, concentraremos nossa atenção no estudo dos sistemas dinâmicos finitos: sistemas dinâmicos determinísticos, vistos em tempo discreto, e com um número finito de possíveis estados. Formalmente, um sistema dinâmico finito (SDF) é um par (X, f) onde X é um conjunto finito (de estados) e f uma aplicação de X em X (lei de evolução).

Podemos restringir a situação em que o $X = \mathbb{F}_q^n$, onde $\mathbb{F}_q$ é o corpo finito com $q = p^t$ elementos. Assim, a função f é dada por meio de funções coordenadas $(f_1, \cdots, f_n)$, cada $f_i : \mathbb{F}_q^n \to \mathbb{F}_q$. Neste caso, principal vantagem encontrada é que toda função de $\mathbb{F}_q^n \to \mathbb{F}_q$ é polinomial.

Exemplos de aplicações destes sistemas incluem as redes booleanas, e mais recentemente, autômatos celulares e regulação gênica na área de biologia, como os abordados em [7].

Uma questão complexa no estudo de SDF é a obtenção do grafo associado ao sistema. Em geral, não temos disponível nenhum resultado que auxilie na obtenção deste. Nos sistemas dinâmicos finitos monomiais (cada função componente é um monômio), por exemplo, temos apenas resultados que permitem identificar a existência de pontos fixos (ver [3], [4]).

O propósito deste trabalho é tratar o caso de um sistema dinâmico finito linear (SDFL). O mesmo se apresenta como uma história de sucesso, em que o caso geral pode ser reduzido, por meio de ferramentas de álgebra linear, a essencialmente dois casos básicos: bijetivo e nilpotente.

No capítulo (1), fazemos uma breve revisão de alguns resultados básicos na teoria de corpos finitos. A partir disso, voltamos nossa atenção para a determinação da ordem de um polinômio com coeficientes em $\mathbb{F}_q$ e ferramentas que simplifiquem seu cálculo. Tais resultados serão essenciais no capítulo (3), no estudo de um SDFL bijetivo.

O capítulo (2) traz os resultados de álgebra linear essenciais na decomposição de um SDFL. O principal deles, a forma normal de Smith - peça chave no processo apresentado - combinada com o teorema chinês do resto, é o que possibilita a redução do sistema original.

Finalmente, no capítulo (3), aplicamos os resultados estudados nos capítulos anteriores para a obtenção do grafo de um SDFL.

No apêndice, são apresentadas duas implementações computacionais em Singular. A

primeira visa determinar a ordem de um polinômio com coeficientes em um corpo finito. A segunda, identificar a estrutura de grafo do SDFL por meio dos resultados apresentados no capítulo (3).

A referência base deste trabalho é o artigo *Linear Finite dynamical systems*, de Hernandez-Toledo [12].

Capítulo 1

Corpos Finitos

Neste capítulo, cujo cerne é a teoria dos corpos finitos, procuraremos demonstrar um de seus principais teoremas, que garante a sua existência e classificação. A notação $\mathbb{F}_q$ é usada para indicar um corpo finito com q elementos, ou ordem q. Em seguida, serão abordados alguns resultados referentes a polinômios irredutíveis com coeficientes em um corpo finito, em especial como determinar a ordem destes e suas potências.

1.1 Existência e classificação dos corpos finitos

Seja $\mathbb{F}_q$ um corpo finito. Nesta seção, estamos interessados em dois resultados principais: o primeiro, um teorema que garante que q é, necessariamente, potência de um número primo p. Em seguida, mostrar que dados um primo p e um inteiro n, existe um único corpo (a menos de isomorfismo) com p^n elementos.

Nosso resultado inicial relaciona a característica de um corpo finito com seu número de elementos:

Lema 1.1. *Seja $\mathbb{F}_q$ um corpo finito com $\operatorname{car}(\mathbb{F}_q) = p$, onde p é um número primo. Então, $\mathbb{F}_q$ contém um subcorpo $\mathbb{F}_p$ isomorfo a $\mathbb{Z}_p$. Em particular, $q = p^n$ para algum número natural n.*

Prova:
Consideremos a aplicação

$$\begin{array}{rccc} \phi: & \mathbb{Z}_p & \longrightarrow & \mathbb{F}_q \\ & [n] & \longmapsto & n1 \end{array}.$$

Iniciaremos mostrando que ϕ está bem definida. Para tal, sejam m, n inteiros tais que $[m] = [n]$, ou seja, existe um inteiro t tal que $m = n + tp$. Com isso,

$$m1 = (n + tp)1 = n1 + (tp)1 = n1 + t(p1) = n1 + t0 = n1.$$

Portanto, a aplicação independe do representante da classe de equivalência tomada, e assim ϕ está bem definida.

ϕ é um homomorfismo, já que

$$\phi([m]+[n]) = \phi([m+n]) = (m+n)1 = m1 + n1 = \phi([m]) + \phi([n])$$

$$\phi([m][n]) = \phi([mn]) = (mn)1 = m(n1) = (m1)(n1) = \phi([m])\phi([n]).$$

Para mostrar que $\mathbb{F}_q$ tem um subcorpo isomorfo a $\mathbb{Z}_p$, é suficiente mostrar que ϕ é injetora e $\phi(\mathbb{Z}_p)$ é subcorpo de $\mathbb{F}_q$, pois desta forma $\widetilde{\phi} : \mathbb{Z}_p \to \phi(Z_p)$ é um isomorfismo de corpos.

Sejam $[m], [n] \in \mathbb{Z}_p$ tais que $\phi([m]) = \phi([n])$. Então, $\phi([m]-[n]) = 0$, daí $(m-n)1 = 0$, portanto $[m-n] = [0]$, já que $\mathbb{F}_q$ não tem divisores de 0. Assim, $[m] = [n]$ e ϕ é injetora. Resta mostrar que $\phi(\mathbb{Z}_p)$ é subcorpo de $\mathbb{F}_q$, ou seja, dados elementos $\alpha, \beta \in \phi(Z_p),\ \beta \neq 0$, verificar que $\alpha - \beta \in \phi(Z_p)$ e $\alpha\beta^{-1} \in \phi(Z_p)$. Sejam $[m], [n] \in Z_p$ tais que $\phi([m]) = \alpha$ e $\phi([n]) = \beta$. Então,

$$\alpha - \beta = \phi([m]) - \phi([n]) = \phi([m-n]) \in \phi(Z_p)$$

$$\alpha\beta^{-1} = \phi([m])\phi([n])^{-1} = \phi([m])\phi([n^{-1}]) = \phi([m][n^{-1}]) = \phi([mn^{-1}]) \in \phi(Z_p).$$

Portanto, $\phi(Z_p)$ é um subcorpo de $\mathbb{F}_q$, isomorfo a Z_p. Assim, $\mathbb{F}_q$ é extensão do corpo $\phi(Z_p)$, e dessa forma, pode ser visto como espaço vetorial sobre o mesmo. Como $\mathbb{F}_q$ é finito, sua dimensão sobre $\phi(Z_p)$ é finita. Se $\gamma_1, \cdots, \gamma_n$ é uma base de $\mathbb{F}_q$ sobre $\phi(Z_p)$, todo elemento de $\mathbb{F}_q$ pode ser escrito de modo único na forma

$$\sum_{i=1}^{n} \lambda_i \gamma_i, \quad \lambda_i \in \phi(Z_p),\ i = 1, \cdots, n.$$

Temos, com isso, $q = p^n$.

□

Embora o resultado acima seja demonstrado apenas para o caso em que a característica do corpo é um número primo, o próximo resultado nos garante que se aplica a qualquer corpo finito.

Lema 1.2. *Se $\mathbb{F}_q$ é um corpo finito, então* $\operatorname{car}(\mathbb{F}_q)$ *é um número primo (ver [2, pág. 62]).*

Combinando os lemas (1.1) e (1.2), obtemos o seguinte teorema:

Teorema 1.3. *Todo corpo finito $\mathbb{F}_q$ tem p^n elementos, para algum primo p e algum número natural n.*

Verificamos, então, que dado um corpo finito arbitrário, este tem um número de ele-

mentos que é potência de um primo. Resta saber quanto a recíproca. Dados um primo p e um inteiro n, existe um corpo com p^n elementos? Em caso afirmativo, como encontrá-lo? O próximo teorema responde ambas as perguntas. Para sua demonstração, necessitaremos de alguns resultados preliminares.

Lema 1.4. *Seja $\mathbb{F}_q$ um corpo finito de característica p. Para quaisquer $a, b \in \mathbb{F}_q$, temos*

$$(a \pm b)^q = a^q \pm b^q.$$

(ver [2, pág. 63]).

Corolário 1.5. *Seja $\mathbb{F}_q$ um corpo finito de característica p, $q = p^r$ para algum inteiro positivo r. Sejam $a_1, \cdots, a_n \in \mathbb{F}_q$. Então*

$$(a_1 + \cdots + a_n)^q = a_1^q + \cdots + a_n^q.$$

Prova:
Basta usar indução sobre n. O resultado decorre diretamente do lema (1.4).

□

Lema 1.6. *Seja $\mathbb{F}_q$ um corpo finito com q elementos e f um polinômio com coeficientes em $\mathbb{F}_q$. Existe uma extensão Ł de $\mathbb{F}_q$ que é um corpo de decomposição de f. Além disso, quaisquer dois corpos de decomposição de f sobre $\mathbb{F}_q$ são isomorfos (ver [14, pág. 35]).*

Lema 1.7. *Sejam $\mathbb{F}_q$ um corpo finito com q elementos, $\alpha \in \mathbb{F}_q^*$ e $r \in \mathbb{N}$, então*

$$\operatorname{ord}(\alpha^r) = \frac{\operatorname{ord}(\alpha)}{\operatorname{mdc}(\operatorname{ord}(\alpha), r)}.$$

(ver [2, pág. 67]).

Lema 1.8. *Sejam $\mathbb{F}_q$ um corpo finito com q elementos e $\alpha, \beta \in \mathbb{F}_q$ elementos cujas ordens satisfazem a relação* $\operatorname{mdc}(\operatorname{ord}(\alpha), \operatorname{ord}(\beta)) = 1$. *Então* $\operatorname{ord}(\alpha\beta) = \operatorname{ord}(\alpha)\operatorname{ord}(\beta)$ *(ver [2, pág. 67]).*

Temos agora as ferramentas necessárias para a demonstração do teorema a seguir.

Teorema 1.9. *Seja p um primo e $q = p^n$, com $n \geq 1$.*

(a) Existe um corpo de ordem q.

(b) Quaisquer dois corpos de ordem q são isomorfos.

(c) *Seja $\mathbb{F}_q$ um corpo de ordem q. Os elementos de $\mathbb{F}_q$ são raízes do polinômio $x^q - x$. Este polinômio tem raízes distintas e se fatora como produto de fatores lineares sobre $\mathbb{F}_q$.*

(d) *O grupo multiplicativo $\mathbb{F}_q^*$ é cíclico de ordem $q - 1$.*

Prova:

(a) Seja $q = p^n$, e seja $\mathbb{K}$ o corpo de decomposição do polinômio $x^q - x$ sobre $\mathbb{F}_p$ (tal corpo existe pelo lema (1.6)).

Todas as raízes do polinômio $x^q - x$ são distintas, já que

$$\text{mdc}(x^q - x, (x^q - x)') = \text{mdc}(x^q - x, qx^{q-1} - 1) = \text{mdc}(x^q - x, -1) = 1,$$

uma vez que $\text{mdc}\,(f, f') = 1$, se e só se f não possui raizes múltiplas.

Considere o conjunto $\mathcal{S} = \{a \in \mathbb{F};\ a^q = a\}$. Note que este conjunto contém q elementos, já que é formado pelas raízes do polinômio $x^q - x$, que são todas distintas.

Mostremos que $\mathcal{S}$ é um subcorpo de $\mathbb{K}$.

(i) $0,\ 1\ \in \mathcal{S}$

(ii) Sejam a, b elementos de $\mathcal{S}$. Pelo lema (1.4),

$$(a - b)^q = a^q + (-b)^q = a^q - b^q = a - b.$$

Portanto $a - b \in \mathcal{S}$.

(iii) Se $b \neq 0$,

$$(ab^{-1})^q = a^q(b^{-1})^q = a^q(b^q)^{-1} = ab^{-1}.$$

Portanto $ab^{-1} \in \mathcal{S}$.

Com isso, $\mathcal{S}$ é um subcorpo de $\mathbb{K}$, que contém todas as raízes de $x^q - x$, ou seja $x^q - x$ fatora-se completamente em $\mathcal{S}$. Portanto, $\mathcal{S} = \mathbb{K}$ e $\mathbb{K}$ é um corpo finito com q elementos, $\mathbb{K} = \mathbb{F}_q$.

O item (c) decorre da demonstração do item (a).

(b) Dados dois corpos $\mathbb{F}_q$ e $\mathbb{F}'_q$ com q elementos, ambos tem característica p e contém $\mathbb{F}_p$ como subcorpo primo, e, consequentemente são extensões deste. Como já foi demonstrado anteriormente, ambos são corpos de decomposição do polinômio $x^q - x$ sobre $\mathbb{F}_p$. O resultado decorre do lema (1.6).

A demonstração de (d) é decorrente dos lemas (1.7) e (1.8). Temos

$$\mathbb{F}_q^* = \mathbb{F}_q - \{0\}.$$

Todo elemento x de $\mathbb{F}_q^*$ satisfaz $x^{q-1} = 1$. Com isso, $\text{ord}\,(x) \leq q-1$ (ordem visto como elemento do grupo multiplicativo). Para mostrar que $\mathbb{F}_q^*$ é cíclico, basta exibir um elemento de ordem $q-1$.

Seja a o elemento de $\mathbb{F}_q^*$ de ordem máxima, $\text{ord}\,(a) = m$.

Mostremos que, para qualquer $b \in \mathbb{F}_q^*$, verifica-se a relação $\text{ord}\,(b)|\text{ord}\,(a)$. Para tal, escrevamos $\text{ord}\,(b) = ds$, onde $d = \text{mdc}\,(\text{ord}\,(b), m)$. Consequentemente, temos $\text{mdc}\,(s, m) = 1$. Para concluir o resultado, basta mostrar que $s = 1$. Para tal, suponhamos $s > 1$. Recorrendo ao lema (1.7) temos

$$\text{ord}\,(b^d) = \frac{\text{ord}\,(b)}{\text{mdc}\,(\text{ord}\,(b), d)} = \frac{ds}{d} = s > 1.$$

Por outro lado, pelo lema (1.8), $\text{ord}\,(ab^d) = ms$. Combinando os resultados, temos $\text{ord}\,(ab^d) > m$, o que contradiz a maximalidade da ordem de a.

Assim, todo elemento de $\mathbb{F}_q^*$ satisfaz $x^m - 1 = 0$. Com isso, $q - 1 = |\mathbb{F}_q^*| \leq m$.

Como $m \leq q-1$, pois todos os elementos de $\mathbb{F}_q^*$ tem ordem $\leq q-1$, segue que $m = q-1$, e

$$\mathbb{F}_q^* = \{a^0, a^1, a^2, \cdots, a^{q-2}\}.$$

Um elemento gerador de $\mathbb{F}_q^*$ é dito *elemento primitivo* de $\mathbb{F}_q$.

□

A parte (a) do teorema é um resultado que nos diz sob quais condições temos um corpo finito. A forma de encontrar tal corpo é dada pelo item (c). Quanto ao item (b), este garante a unicidade dos corpos finitos, a menos de isomorfismo. Assim, temos um teorema de existência e "unicidade". Quanto ao item (d), este nos garante a existência do elemento primitivo, importante na demonstração de muitos resultados na teoria de corpos finitos, alguns dos quais serão apresentados na próxima seção.

Agora, estudaremos alguns resultados referentes a polinômios com coeficientes em um corpo finito.

1.2 Polinômios com coeficientes em um corpo finito

Nesta seção, estamos interessados no estudo dos polinômios com coeficientes em um corpo finito e algumas propriedades relacionadas a estes e suas raízes.

Nosso objetivo inicial é identificar todas as raízes de um polinômio irredutível sobre um

corpo finito, exigindo para tal que seja conhecida apenas uma delas. Para demonstrarmos tal teorema, necessitamos do seguinte lema:

Lema 1.10. *Seja $\mathbb{F}_q$ um corpo finito com q elementos e $f \in \mathbb{F}_q[x]$. Se $\gamma \in \mathbb{F}$ é uma raiz de f, então γ^q também é raiz de f.*

Prova:

Escrevendo $f(x) = \sum_{i=0}^{m} a_i x^i$, com $a_i \in \mathbb{F}_q$, $0 \leq i \leq m$, vamos utilizar o corolário (1.5) e o teorema (1.9) para obter o resultado desejado.

Calculando $f(\gamma^q)$, temos

$$\begin{aligned} f(\gamma^q) &= a_m\gamma^{qm} + a_{m-1}\gamma^{q(m-1)} + \cdots + a_q\gamma^q + a_0 \\ &= a_m^q\gamma^{qm} + a_{m-1}^q\gamma^{q(m-1)} + \cdots + a_1^q\gamma^q + a_0^q \\ &= (a_m\gamma^m + a_{m-1}\gamma^{(m-1)} + \cdots + a_1\gamma + a_0)^q \\ &= f(\gamma)^q \\ &= 0 \end{aligned}$$

□

Observe que o resultado é válido para um polinômio qualquer em $\mathbb{F}_q[x]$, não necessariamente irredutível, embora nosso foco esteja voltado para aqueles que são irredutíveis.

Teorema 1.11. *Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m. Então, f tem uma raiz $\alpha \in \mathbb{F}_{q^m}$. Ainda, todas as raízes de f estão em $\mathbb{F}_{q^m}$, são todas distintas e da forma α^{q^i}, $i = 0, 1, \cdots m-1$.*

Prova:

Seja $\mathbb{K}$ o corpo de decomposição de f sobre $\mathbb{F}_q$ e α uma raiz de f em $\mathbb{K}$. Temos $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \text{grau}(f) = m$. Como corpos finitos de dada ordem são únicos a menos de isomorfismo, temos $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Mostramos, com isso, que $\alpha \in \mathbb{F}_{q^m}$.

Pelo lema (1.10), $\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}$ são raízes de f e são elementos de $\mathbb{F}_{q^m}$. Resta mostrar que estas são todas as raízes de f, ou seja, que são todas distintas. Provemos por contradição.

Suponhamos que duas das raízes encontradas acima sejam iguais, isto é, $\alpha^{q^r} = \alpha^{q^s}$, com $0 \leq r < s \leq m-1$. Elevando ambos os membros da igualdade a q^{m-s}, obtemos

$$\alpha^{q^{m-s+r}} = \alpha^{q^m} = \alpha.$$

Com isso, α está no corpo de decomposição do polinômio $x^{q^{m-s+r}} - x$, que é isomorfo a $\mathbb{F}_{q^{m-s+r}}$. Assim,

$$[\mathbb{F}_{q^{m-s+r}} : \mathbb{F}_q] = [\mathbb{F}_{q^{m-s+r}} : \mathbb{F}_{q^m}][\mathbb{F}_{q^m} : \mathbb{F}_q]$$

ou seja,

$$m - s + r = [\mathbb{F}_{q^{m-s+r}} : \mathbb{F}_{q^m}]m.$$

Contudo, $m - s + r < m$, donde temos um absurdo. Portanto, $\alpha^{q^i}, 0 \leq i \leq m-1$ são duas a duas distintas, e como f tem grau m, estas são todas as suas raízes.

□

Decorre do teorema acima que:

Corolário 1.12. *Sejam f e g polinômios irredutíveis de grau m em $\mathbb{F}_q[x]$. Então*

a) f e g tem corpos de decomposição isomorfos.

b) É suficiente conhecermos uma raiz de f para obtermos seu corpo de decomposição, o qual será isomorfo a $\mathbb{F}_{q^m}$, e, portanto, denotado como tal.

Queremos, agora, saber como se relacionam a ordem de um elemento arbitrário $\alpha \in \mathbb{F}_q$ e a ordem de algumas de suas potências particulares, mais precisamente, as da forma $\alpha^{q^i}, i \in \mathbb{N}$.

Teorema 1.13. *Seja $\alpha \in \mathbb{F}_{q^m}, \alpha \neq 0$. Então $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$ têm a mesma ordem em $\mathbb{F}^*_{q^m}$.*

Prova:
Pelo lema (1.7) a ordem de α^{q^i} no grupo multiplicativo $\mathbb{F}^*_{q^m}$ é dada por

$$\text{ord}\,(\alpha^{q^i}) = \frac{\text{ord}\,(\alpha)}{\text{mdc}\,(q^i, \text{ord}\,(\alpha))}, \quad 0 \leq i \leq m-1.$$

Como $\alpha \in \mathbb{F}^*_{q^m}$ e a ordem de $\mathbb{F}^*_{q^m}$ é $q^m - 1$, concluímos que $\text{ord}\,(\alpha) | q^m - 1$. Portanto, $\text{mdc}\,(q^i, \text{ord}\,(\alpha)) = 1$, e segue o resultado.

□

A partir do teorema (1.13), verificamos que se f é um polinômio irredutível sobre $\mathbb{F}_q$, então todas as suas raízes têm a mesma ordem. Consequentemente, se α é um elemento primitivo de $\mathbb{F}^*_{q^m}$, então $\alpha^{q^i}, i \in \mathbb{N}$, também o é.

1.2.1 Ordem de um polinômio sobre $\mathbb{F}_q$

Dado um corpo finito $\mathbb{F}_q$, sabemos que a ordem de um elemento não nulo $\alpha \in \mathbb{F}_q$ é sua ordem no grupo multiplicativo $\mathbb{F}_q^*$. Desejamos, agora, estender o conceito de ordem para um polinômio arbitrário $f \in \mathbb{F}_q[x]$. Direcionando para tal definição, apresentamos o seguinte lema:

Lema 1.14. *Seja $f \in \mathbb{F}_q[x]$ um polinômio de grau $m \geq 1$ com $f(0) \neq 0$. Então, existe um inteiro positivo $t \leq q^m - 1$ tal que $f(x)|(x^t - 1)$.*

Prova:

O anel $\mathbb{F}_q[x]/(f)$ contem q^m elementos, dos quais $q^m - 1$ são não nulos. Considere os q^m elementos $x^i + (f), i = 0, 1, \cdots, q^m - 1$, os quais são todos não nulos, uma vez que f não divide x^i. Assim, existem inteiros r, s com $0 \leq r < s \leq q^m - 1$ tais que $x^r + (f) = x^s + (f)$.

$$f \text{ divide } x^s - x^r = x^r(x^{s-r} - 1).$$

Como x e f são relativamente primos (pois $f(0) \neq 0$), f divide $x^{s-r} - 1$. Portanto, existe um inteiro $t = s - r$ tal que f divide $x^t - 1$, e $0 < t \leq q^m - 1$.

□

A partir do resultado acima, definimos a ordem de polinômio em $\mathbb{F}_q[x]$:

Definição 1.15. Seja $f \in \mathbb{F}_q[x]$ um polinômio não nulo, tal que $f(0) \neq 0$. Então, o menor inteiro positivo t tal que f divide $x^t - 1$ é chamado de *ordem de f*, denotado por $\text{ord}\,(f)$. Se $f(0) = 0$, escrevemos $f(x) = x^r g(x)$, $t \in \mathbb{N}$ e $g(x) \in \mathbb{F}_q[x]$ tal que $g(0) \neq 0$, e definimos $\text{ord}\,(f) = \text{ord}\,(g)$.

Em particular, se $f(x) = c$, onde c é uma constante, temos $\text{ord}\,(f) = 1$.

Temos um interesse particular na ordem de polinômios irredutíveis, pois estes serão importantes na construção dos grafos de sistemas dinâmicos finitos lineares, apresentado no capítulo (3), em particular no teorema (3.23).

No caso em que f é um polinômio irredutível sobre $\mathbb{F}_q$, o teorema seguinte mostra que sua ordem coincide com a ordem de suas raízes.

Teorema 1.16. *Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m, com $f(0) \neq 0$. Então, a ordem de f é igual à ordem de qualquer uma de suas raízes no grupo multiplicativo $\mathbb{F}_{q^m}^*$.*

Prova:

Seja α uma raiz de f. Pelo corolário (1.12), temos $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Pelo teorema (1.13),

sabemos que todas as raízes de f estão em $\mathbb{F}_{q^m}$ e tem a mesma ordem. Portanto, é suficiente mostrar que $\text{ord}(\alpha) = \text{ord}(f)$.

Sejam $e = \text{ord}(f)$ e $t = \text{ord}(\alpha)$. Da primeira igualdade, resulta $f|x^e - 1$. Daí $\alpha^e - 1 = 0$, de onde obtemos $\alpha^e = 1$. Da definição de ordem de um elemento de um grupo, $t \leq e$. Como $t = \text{ord}(\alpha)$, $\alpha^t = 1$, então $\alpha^t - 1 = 0$. Como f é irredutível e tem α como raiz, obtemos $f|x^t - 1$, mas e é o menor inteiro com essa propriedade, portanto $e \leq t$.

Segue que $e = t$. Portanto f tem a mesma ordem de qualquer uma de suas raízes.

□

Com o teorema acima, podemos estabelecer uma relação entre a ordem de um polinômio irredutível sobre $\mathbb{F}_{q^m}$ e a ordem do próprio corpo.

Corolário 1.17. *Seja f um polinômio de grau m em $\mathbb{F}_q[x]$ irredutível sobre $\mathbb{F}_q$. Então,* $\text{ord}(f)$ *divide* $q^m - 1$.

Prova:

Se $f(x) = \lambda x$, temos $\text{ord}(f) = 1$, e o resultado é imediato.

Do contrário, seja α uma raiz de f em $\mathbb{F}_{q^m}$. Neste caso, $\alpha \neq 0$ já que $f(0) \neq 0$. Portanto, $\alpha \in \mathbb{F}_{q^m}^*$, e $\text{ord}(\alpha)$ divide a ordem de $\mathbb{F}_{q^m}^*$, que é $q^m - 1$. Assim, recorrendo ao teorema (1.16), concluímos que $\text{ord}(f)$ divide $q^m - 1$.

□

Os próximos resultados conduzem ao principal resultado da seção: o teorema (1.20), que relaciona a ordem de um polinômio irredutível e de suas potências, facilitando assim o cálculo da ordem destas.

Teorema 1.18. *Seja f um polinômio em $\mathbb{F}_q[x]$ com $f(0) \neq 0$. Dado um inteiro positivo c, f divide $x^c - 1$ se e somente se* $\text{ord}(f)$ *divide c.*

Prova:

Seja $e = \text{ord}(f)$.

($\Longrightarrow$) Suponhamos que f divida $x^c - 1$. Da definição de ordem de um polinômio, temos $e \leq c$. Pelo algoritmo da divisão, podemos escrever $c = me + n$, com $m, n \in \mathbb{N}$ e $0 \leq n < e$. Assim,

$$x^c - 1 = x^{me+n} - 1 = x^{me+n} - 1 + x^n - x^n = (x^{me} - 1)x^n + (x^n - 1)$$

Como f divide $x^c - 1$ e $(x^{me} - 1)x^n$, a igualdade acima nos diz que f divide $x^n - 1$. Mas $n < e$, portanto pela definição da ordem de um polinômio temos $n = 0$ e $c = me$.

($\Longleftarrow$) Se e divide c, $x^e - 1$ divide $x^c - 1$. Da definição de ordem, f divide $x^e - 1$. Portanto, f divide $x^c - 1$.

□

Como consequência do teorema (1.18), temos

Corolário 1.19. *Sejam f e g polinômios em $\mathbb{F}_q[x]$ tais que f divide g. Então* $\mathrm{ord}\,(f)$ *divide* $\mathrm{ord}\,(g)$.

É nosso intuito encontrar meios mais práticos e computacionalmente mais rápidos para determinar a ordem de um polinômio. Afinal, a ordem de um polinômio de grau m em $\mathbb{F}_q[x]$ está limitada por $q^m - 1$, e pode ser um número não tão simples de ser calculado. O próximo teorema visa simplificar o cálculo da ordem de polinômios, em um caso particular: quando este é potência de um irredutível. Os resultados até o momento visam a sua demonstração. Sua importância está na aplicação do teorema (3.23) no capítulo (3), simplificando os cálculos necessários para a obtenção do resultado final.

Teorema 1.20. *Seja g um polinômio em $\mathbb{F}_q[x]$ irredutível sobre $\mathbb{F}_q$, com $g(0) \neq 0$,* $\mathrm{ord}\,(g) = e$ *e $f = g^b$, b um inteiro positivo. Seja t o menor inteiro com a propriedade $p^t \geq b$, onde p é a característica de $\mathbb{F}_q$. Então* $\mathrm{ord}\,(f) = ep^t$.

Prova:
Seja $c = \mathrm{ord}\,(f)$.
Como g divide f, pelo corolário (1.19) e divide c. Portanto $c = ek,\ k \in \mathbb{N}$.
Por outro lado:

$$\left.\begin{array}{r} g \text{ divide } x^e - 1 \Rightarrow f \text{ divide } (x^e-1)^b \\ (x^e-1)^{p^s} = x^{ep^s} - 1 \end{array}\right\} \implies \begin{array}{l} f \text{ divide } x^{ep^s} - 1 \\ \text{sempre que } p^s \geq b. \end{array}$$

Em particular, para t o menor inteiro tal que $p^t \geq b$, a relação acima é válida. Pelo corolário (1.19), c divide ep^t, isto é, $ep^t = cl$, $l \in \mathbb{N}$. Combinando com a relação obtida anteriormente, temos

$$ep^t = cl = ekl \Rightarrow kl = p^t.$$

Como p é primo, obtemos que $c = ep^u$, com $0 \leq u \leq t$. Resta determinar o valor de u. Isso será feito pela comparação do número de raízes e suas respectivas multiplicidades, entre os polinômios f e $x^{ep^u} - 1$.

Pelo corolário (1.17), e divide $q^m - 1$, logo p não divide e. Com isso, concluímos que o polinômio $x^e - 1$ não possui raízes múltiplas, visto que $x^e - 1$ e sua derivada são primos entre si. Assim, o polinômio $x^{ep^u} - 1 = (x^e - 1)^{p^u}$ tem e raízes distintas de multiplicidade p^u.

Quanto ao polinômio $f = g^b$, este possui m raízes, de multiplicidade b. Como g é irredutível, todas as suas raízes são distintas, daí f tem m raízes distintas, cada uma delas com multiplicidade b.

Como f divide $x^{ep^u} - 1$, toda raiz de f é raiz de $x^{ep^u} - 1$. Daí $b \leq p^u$. Como $0 \leq u \leq t$, obtemos $u = t$. Portanto $\text{ord}\,(f) = ep^t$ e t o menor inteiro tal que $p^t \geq b$, como queríamos demonstrar.

□

Para facilitar o cálculo da ordem do polinômio irredutível g, utilizamos o corolário (1.17), que reduzirá as possibilidades da órbita de g, que até então estavam limitadas por $q^m - 1$.

Capítulo 2

Forma Normal de Smith

O objetivo deste capítulo é apresentar um algoritmo que possibilite determinar a forma racional de uma matriz quadrada A sobre um corpo arbitrário $\mathbb{F}$ (não necessariamente finito). Para tal, vamos recorrer a forma normal de Smith, apresentada no teorema (2.17) deste capítulo, válida sobre domínios euclidianos quaisquer, em particular em $\mathbb{F}[x]$. Do algoritmo apresentado neste teorema, resultarão os fatores invariantes da matriz A e, consequentemente, sua forma racional. Os resultados apresentados neste capítulo são válidos tanto para corpos finitos como para infinitos.

2.1 Diagonalização de matrizes em um domínio euclidiano

Dada uma matriz quadrada A com coeficientes em um corpo $\mathbb{F}$, a obtenção da forma normal de Smith é decorrente de um processo de diagonalização da matriz $x \cdot I - A$ com coeficientes em $\mathbb{F}[x]$. Assim, nossos primeiros resultados serão com o intuito de determinar meios de diagonalizá-la.

Definição 2.1. Um *domínio euclidiano* $(R, +, \cdot, \phi)$ é um domínio de integridade $(R, +, \cdot)$ com uma função

$$\phi : R \setminus \{0\} \to \mathbb{N}$$

que goza da seguinte propriedade:

(divisão euclidiana) $\forall\, a, b \in R$, $b \neq 0$, existem $t, r \in R$ tais que

$$a = bt + r, \;\; \text{com} \;\; \phi(r) < \phi(b) \;\; \text{ou} \;\; r = 0;$$

Exemplo 2.2. São exemplos de domínios euclidianos:

a) $\mathbb{Z}$ com a função $\phi(z) = |z|$;

b) $\mathbb{Z}[i]$ com a função $\phi(a+bi) = a^2 + b^2$;

c) $\mathbb{K}[x]$ para um corpo arbitrário $\mathbb{K}$, com a função $\phi(f) =$ grau de f;

d) $\mathbb{K}[[x]]$, o anel das séries de potência formais sobre $\mathbb{K}$. Definimos $\phi(f)$ como a menor potência de x que aparece em f.

Exemplo 2.3. Um exemplo de domínio não-euclidiano:

$\mathbb{Z}[x]$ não é um domínio euclidiano. Se fosse euclidiano, o mdc de 5 e x seria 1, pois os dois são irredutíveis em $\mathbb{Z}[x]$ e não são associados. Em um anel euclidiano, o mdc de dois elementos é sempre uma combinação linear destes. Assim, se $\mathbb{Z}[x]$ fosse euclidiano, teríamos $f(x), g(x) \in \mathbb{Z}[x]$ tais que $5f(x) + xg(x) = 1$. Como essa é uma igualdade entre funções, podemos substituir x por 0 e a igualdade continua válida, donde obtemos $1 = 5f(0)$. Isso porém é impossível, pois 5 não é invertível em $Z[x]$.

Definiremos agora algumas operações que serão efetuadas a partir da matriz $x \cdot I - A$, para que possamos obter uma matriz diagonal como citado no iniício desta seção. Observe que elas são válidas para matrizes com entradas em um anel arbitrário, não necessariamente um domínio euclidiano.

Definição 2.4. Seja (R, ϕ) um domínio euclidiano e seja $M = (a_{ij})$ uma matriz $m \times n$ com entradas em R. Chamamos *operações elementares sobre as linhas (colunas) de* M as seguintes operações:

1. troca da $i-$ésima linha (coluna) de M por sua $j-$ésima linha (coluna), denotado $L_i \longleftrightarrow L_j$ $(C_i \longleftrightarrow C_j)$.

2. multiplicação da $i-$ésima linha (coluna) de M por uma unidade $u \in R$, denotado $L_i \longleftarrow uL_i$ $(C_i \longleftarrow uC_i)$.

3. substituição da $i-$ésima linha (coluna) de M por sua soma com α vezes sua $j-$ésima linha (coluna), $\alpha \in R$, denotado $L_i \longleftarrow L_i + \alpha L_j$ $(C_i \longleftarrow C_i + \alpha C_j)$.

Note que a primeira operação elementar apresentada poderia ser omitida, uma vez que é consequência da seguinte sequência de operações:

$$L_j \longleftarrow L_i + L_j; \quad L_i \longleftarrow L_i - L_j; \quad L_i \longleftarrow -L_i; \quad L_j \longleftarrow L_j - L_i:$$

$$\begin{matrix} L_i \\ L_j \end{matrix} \longrightarrow \begin{matrix} L_i \\ L_i + L_j \end{matrix} \longrightarrow \begin{matrix} -L_j \\ L_i + L_j \end{matrix} \longrightarrow \begin{matrix} L_j \\ L_i + L_j \end{matrix} \longrightarrow \begin{matrix} L_j \\ L_i \end{matrix}.$$

Embora a primeira operação seja consequência das outras duas, omiti-la aumentaria o número de operações elementares a serem efetuadas, uma vez que para efetuarmos uma simples troca de linha seriam necessárias quatro outras operações elementares.

A divisão euclidiana, combinada com operações elementares sobre as linhas e colunas de uma matriz com entradas em R, será a chave para o processo de diagonalização.

Definição 2.5. Duas matrizes M e N são chamadas *matrizes equivalentes*, denotado por $M \approx N$, se a matriz N pode ser obtida a partir da matriz M por uma sequência finita de operações elementares realizadas em linhas e/ou colunas.

Definição 2.6. Uma matriz é dita *elementar* se pode ser obtida da matriz identidade a partir de uma única operação elementar.

Seja M uma matriz $m \times n$ com entradas $a_{ij} \in R$. Cada operação elementar realizada sobre as colunas de M corresponde a multiplicação à direita por uma matriz elementar $n \times n$, enquanto operações elementares sobre as linhas correspondem a multiplicação à esquerda por uma determinada matriz elementar $m \times m$. No primeiro caso, a matriz elementar é obtida realizando nas linhas da matriz identidade $n \times n$ a operação que se deseja realizar nas colunas da matriz. No segundo, efetuamos na identidade $m \times m$ a mesma operação que desejamos na matriz. Com isso, se $M \approx N$, existem matrizes invertíveis P e Q, $m \times m$ e $n \times n$ respectivamente, tais que

$$M = PNQ.$$

Com a igualdade acima, verificamos que a relação $\approx$ é uma relação de equivalência.

Definição 2.7. Duas matrizes quadradas M e N são *semelhantes* se existir uma matriz invertível P tal que

$$M = P^{-1}NP.$$

Note que matrizes semelhantes são um caso particular de matrizes equivalentes.

O seguinte teorema é o mais importante resultado deste capítulo. Dos resultados que dele decorrem, podemos obter a forma normal de Smith de uma matriz quadrada arbitrária. Em sua demonstração, utilizaremos o conceito de matrizes equivalentes, bem como a divisão euclidiana. Ao longo desta demonstração utilizaremos que $\approx$ é uma relação de equivalência, sem menção a isso.

Teorema 2.8. *Sejam $m \geq 1$ e $n \geq 1$ dois inteiros. Sejam (R, ϕ) um domínio euclidiano e $M = (a_{ij})$ uma matriz $m \times n$ com entradas em R. Então, através de uma sequência finita de operações elementares sobre suas linhas e colunas, a matriz M pode ser transformada em uma matriz diagonal da forma*

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

onde D é uma matriz diagonal $r \times r$, $0 \leq r \leq \min\{m, n\}$, $d_{ii} \in R\backslash\{0\}$ e os elementos de sua diagonal satisfazem $d_{11}|d_{22}|\cdots|d_{rr}$.

Prova:

Caso M seja a matriz nula, nada precisa ser feito. Assim, consideremos $M = (a_{ij})$ uma matriz não nula. Definimos

$$\phi(M) = \min\{\phi(a_{ij});\ a_{ij} \neq 0\}$$

e

$$t = \min\{\phi(N);\ N \approx M\}.$$

Seja $N_1 = (b_{ij})$ uma matriz tal que $\phi(N_1) = t$. Podemos supor, sem perda de generalidade, que a entrada de N_1 com menor $\phi-$valor seja b_{11} já que do contrário basta trocarmos convenientemente as linhas e colunas (o que corresponde a efetuarmos operações elementares sobre linhas e colunas). Se considerarmos I o ideal gerado pelas entradas da matriz M, o elemento b_{11} será seu gerador com menor $\phi-$valor.

Mostremos agora que existe uma matriz $N_2 = (c_{ij})$ tal que $N_2 \approx N_1$, $c_{11} = b_{11}$ e $c_{1j} = 0$ para $j > 1$:

$$N_2 = \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix}$$

Na matriz N_1, se algum $b_{1j} \neq 0$, da divisão euclidiana de b_{1j} por b_{11}, temos

$$b_{1j} = q_j b_{11} + r_j, \ \text{ com } \ r_j = 0 \ \text{ ou } \ \phi(r_j) < \phi(b_{11}).$$

Podemos, então, efetuar em N_1 a operação elementar

$$C_j \longleftarrow C_j - q_j C_1.$$

A nova matriz $\widetilde{N}_1$ obtida tem a entrada $1j$ igual a r_j. Assim, r_j deve ser obrigatoriamente nulo. Do contrário, teríamos

$$t \leq \phi(\widetilde{N}_1) \leq \phi(r_j) < \phi(b_{11}) = t.$$

Se a única entrada não nula na primeira linha de $\widetilde{N}_1$ for a entrada 11, tomemos $\widetilde{N}_1 = N_2$. Do contrário, repetimos o processo com $\widetilde{N}_1$. Em no máximo $n - 1$ passos, temos uma matriz cuja única entrada não nula na primeira linha é a entrada 11, que é igual a b_{11}. Obtemos, assim, a matriz N_2.

O mesmo pode ser feito na primeira coluna, e assim obtemos uma matriz $(d_{ij}) = N_3 \approx M$, da forma

$$N_3 = \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & d_{22} & \cdots & d_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & d_{m2} & \cdots & d_{mn} \end{pmatrix} = \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}$$

onde A é uma matriz $(m-1) \times (n-1)$.

Mostremos, agora, que b_{11} divide cada uma das entradas de A.

Suponha que exista uma entrada d_{ij} tal que b_{11} não divida d_{ij}. Da divisão euclidiana de d_{ij} por b_{11}, temos

$$d_{ij} = qb_{11} + r, \;\; r \neq 0 \;\text{ e }\; \phi(r) < \phi(b_{11}).$$

Efetuamos em N_3 a seguinte operação elementar:

$$L_1 \longleftarrow L_1 + L_i$$

e na nova matriz obtida efetuamos

$$C_j \longleftarrow C_j - qC_1.$$

A matriz final obtida tem entrada $1j$ igual a r. Assim, calculando ϕ nesta matriz, o valor encontrado é inferior a $\phi(r)$, mas $\phi(r) < \phi(b_{11}) = t$, o que contradiz a minimalidade de t. Chegamos a um absurdo, por supor que exista uma entrada de A que não é divisível por b_{11}. Concluímos, com isso, que b_{11} divide todas as entradas de N_3.

Para concluir nosso resultado, usamos indução sobre o tamanho da matriz. Como A é uma matriz $(m-1) \times (n-1)$, existe uma matriz diagonal $B \approx A$ da forma

$$B = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}, \;\; D = \begin{pmatrix} d_2 & 0 & \cdots & 0 \\ 0 & d_3 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r \end{pmatrix}$$

com $d_2, \cdots, d_r \in R\backslash\{0\}$ e d_j divide d_{j+1}, $j = 2, \ldots, r-1$.

Assim,

$$N_3 = \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix} \approx \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}.$$

Resta agora mostrar que b_{11} divide d_2. Como b_{11} divide cada uma das entradas de A, e as entradas de B foram obtidas por meio de somas de múltiplos das entradas de A, concluímos a afirmação desejada. Basta, então, tomarmos $d_1 = b_{11}$.

□

O inteiro d_1 é o mdc $\{a_{ij},\ i = 1, \cdots, m,\ j = 1, \cdots, n\}$, uma vez que este é o gerador do ideal formado pelas entradas da matriz M. Por indução, podemos determinar $d_2, \cdots, d_r$ também utilizando o mdc: $\prod_{r=1}^{l} d_r$ é o mdc dos menores $l \times l$ de M.

O inteiro r é chamado *posto de* M, e é único. Quanto aos elementos $d_1, \cdots, d_r \in R$, estes são únicos a menos de multiplicação por um elemento invertível de R: suponha que $M \approx N$ e $M \approx \widetilde{N}$,

$$N = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} \text{ e } \widetilde{N} = \begin{pmatrix} \widetilde{D} & 0 \\ 0 & 0 \end{pmatrix}.$$

$$D = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_{r_1} \end{pmatrix} \text{ e } \widetilde{D} = \begin{pmatrix} \widetilde{d_1} & 0 & \cdots & 0 \\ 0 & \widetilde{d_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \widetilde{d_{r_2}} \end{pmatrix}$$

Como $N \approx \widetilde{N}$, $D \approx \widetilde{D}$, temos $r_1 = r_2 = r$, visto que cada $d_i, \widetilde{d_i}$ é não nulo. Mostremos, agora, que d_1 e $\widetilde{d_1}$ são associados em D, isto é, que $d_1 = u\widetilde{d_1}$, onde u é um elemento invertível de D. Da relação de divisibilidade, d_1 divide cada entrada da matriz D, e, consequentemente, cada entrada de qualquer matriz equivalente a D. Portanto, divide cada entrada de $\widetilde{D}$. Assim, d_1 divide $\widetilde{d_1}$. Pelo mesmo motivo, temos que $\widetilde{d_1}$ divide d_1. Portanto, são associados.

Para verificar que d_2 e $\widetilde{d_2}$ são associados em D. Novamente pela relação de divisibilidade, temos que $d_1 d_2$ divide cada menor 2×2 da matriz D, e, consequentemente, de qualquer matriz que seja equivalente a D. Portanto, $d_1 d_2$ divide cada menor 2×2 de $\widetilde{D}$, em particular $d_1 d_2$ divide $\widetilde{d_1}\widetilde{d_2}$. Analogamente, $\widetilde{d_1}\widetilde{d_2}$ divide $d_1 d_2$. Como d_1 e $\widetilde{d_1}$ são associados, concluímos que d_2 e $\widetilde{d_2}$ também o são. Repetindo o processo para os menores $i \times i$, concluímos que d_i e $\widetilde{d_i}$ são associados, $i = 3, \cdots, r$, verificando assim a unicidade a menos de associado, da matriz obtida no teorema (2.8).

Dados dois elementos a, b em um domínio euclidiano, o seguinte resultado nos dá um algoritmo para determinar o valor de mdc (a, b):

Observação 2.9. Seja R um domínio euclidiano e $a, b \in R$. Consideremos a sequência de divisões sucessivas:

$$
\begin{aligned}
a &= bq_1 + r_1,\ \phi(r_1) < \phi(b) \\
b &= r_1q_2 + r_2,\ \phi(r_2) < \phi(r_1) \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n,\ \phi(r_n) < \phi(r_{n-1}) \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}
$$

onde r_n é o último resto não nulo na sequência de divisões. Então, $\text{mdc}\,(a,b) = r_n$. Da unicidade do algoritmo da divisão decorre que r_n é determinado de modo único pela sequência de divisões.

Para encontrarmos os mdc 's desejados, utilizamos que

$$\text{mdc}\,(a_1, a_2, \cdots, a_n) = \text{mdc}\,(a_1, \text{mdc}\,(a_2, \cdots, a_n)).$$

Utilizemos o resultado apresentado para trabalharmos com aplicações lineares entre módulos.

2.2 Aplicações lineares entre módulos

Sejam R um anel e M, N $R-$módulo livres finitamente gerados. Estamos interessados em aplicações $R-$lineares $T : N \to M$. Ao escolhermos uma base ordenada $\beta = \{v_1, \cdots, v_n\}$ para N e uma base ordenada $\beta' = \{w_1, \cdots, w_m\}$ de M, podemos escrever para cada $j \in \{1, \cdots, n\}$,

$$T(v_j) = \sum_{i=1}^{m} a_{ij}w_i,\ \ a_{ij} \in R.$$

Obtemos, com isso, uma matriz $A = (a_{ij})$ com entradas em R, que representa a aplicação linear T em relação a β e β'. A matriz, claramente, depende da escolha das bases de M e N.

Em ambas as bases, podemos efetuar uma sequência de operações elementares, de forma a obtermos novas bases de M e N.

Definição 2.10. Chamamos operações elementares as seguintes operações:

i) permutação dos elementos: $v_i \longleftrightarrow v_j$ ou $w_i \longleftrightarrow w_j$;

ii) somar um múltiplo de um elemento a outro: $v_i \longleftarrow v_i + \alpha v_j$ ou $w_i \longleftarrow w_i + \alpha w_j$, $\alpha \in A$;

iii) multiplicar um elemento por uma unidade de A: $v_i \longleftarrow uv_i$ ou $w_i \longleftarrow uw_i$.

Vejamos os efeitos na matriz A consequentes das operações elementares realizadas:

1. trocando os elementos w_i e w_j em β', tal mudança nos dá uma nova base ordenada de M. A nova matriz é obtida pela troca da $i-$ésima coluna da matriz A por sua $j-$ésima coluna, já que

$$\begin{aligned} T(v_k) &= a_{1k}w_1 + \cdots + a_{ik}w_i + \cdots + a_{jk}w_j + \cdots + a_{mk}w_m \\ &= a_{1k}w_1 + \cdots + a_{jk}w_j + \cdots + a_{ik}w_i + \cdots + a_{mk}w_n, \quad k = 1, \cdots, n \end{aligned}$$

2. multiplicando w_i por uma unidade $u \in A$, a matriz na nova base é obtida multiplicando-se a $i-$ésima coluna da matriz anterior por u^{-1}, já que

$$\begin{aligned} T(v_k) &= a_{1k}w_1 + \cdots + a_{ik}w_i + \cdots + a_{mk}w_m \\ &= a_{1k}w_1 + \cdots + (u^{-1}a_{ik})uw_i + \cdots + a_{mk}w_m \quad k = 1, \cdots, n \end{aligned}$$

3. ao substituir um elemento w_j pelo elemento $w_j - \alpha w_i$, $\alpha \in A$, a matriz em relação a nova base é obtida substituindo a $i-$ésima coluna da matriz na base anterior por sua soma com α vezes sua $j-$ésima coluna, pois

$$\begin{aligned} T(v_k) &= a_{1k}w_1 + \cdots + a_{ik}w_i + \cdots + a_{jk}w_j + \cdots + a_{mk}w_m \\ &= a_{1k}w_1 + \cdots + (a_{ik} + \alpha a_{jk})w_i + \cdots + a_{jk}(w_j - \alpha w_i) + \cdots + a_{mk}w_m \\ & \quad k = 1, \cdots, n \end{aligned}$$

Analogamente, mudanças na base de N acarretam mudanças na matriz A. Para que estas sejam identificadas, basta olhar para a matriz A^T, e proceder como acima em suas colunas, posteriormente voltamos mais uma vez à transposta, e teremos mudanças correspondentes realizadas sobre as linhas de A:

1. ao trocarmos de posição os geradores v_i e v_j, tal mudança acarreta na troca da $i-$ésima linha pela $j-$ésima coluna na matriz A.

2. multiplicando v_i por uma unidade $u \in A$, a nova matriz é obtida multiplicando a $i-$ésima linha de A por u^{-1}.

3. substituindo v_j por $v_j - \alpha v_i$, obtemos a matriz correspondente substituindo a $j-$ésima linha de A pela soma de sua $j-$ésima linha com $-\alpha$ vezes a $i-$ésima linha.

Evidenciamos, com isso, como operações elementares efetuadas nas bases de M e N afetam as linhas e colunas da matriz que representa T.

No caso em que R é um domínio euclidiano, temos o seguinte resultado, que decorre do teorema (2.8):

Corolário 2.11. *Seja R um domínio euclidiano. Sejam M, N módulos livres sobre R finitamente gerados e $T : N \to M$ um homomorfismo de módulos. Então, existe uma base $\beta = \{v_1, \cdots, v_n\}$ de N e uma base $\beta_1 = \{w_1, \cdots, w_m\}$ de M tais que a matriz que representa T em relação a estas bases está na forma*

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

onde D é uma matriz diagonal $r \times r$, $0 \leq r \leq \min\{m, n\}$, $d_{ii} \in R\backslash\{0\}$ e cada elemento da diagonal divide o seguinte.

Prova:

Sejam γ e γ' bases ordenadas de N e M, respectivamente, e A a matriz que representa T em relação a essas bases. A matriz A é uma matriz com entradas em R. Portanto, pelo teorema (2.8), pode por meio de uma sequência de operações elementares ser posta na forma

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

onde D é uma matriz diagonal $r \times r$, $0 \leq r \leq \min\{m, n\}$, $d_{ii} \in R\backslash\{0\}$ e cada elemento da diagonal divide o seguinte.

Para encontrarmos as bases correspondentes, basta que para cada operação elementar efetuada na matriz A, na respectiva ordem, seja efetuada a correspondente transformação elementar nas bases γ e γ', obtendo assim as bases β e β' desejadas. □

Definição 2.12. Sejam M um $R-$módulo livre e N um submódulo de M. Uma base $\{x_1, \cdots, x_n\}$ de M é uma *base adaptada* a N se existem elementos $d_1, \cdots, d_r \in R\backslash\{0\}$ tais que $\{d_1x_1, \cdots, d_rx_r\}$ é uma base de N e d_i divide d_{i+1}, $i = 1, \cdots, r-1$. Os elementos $d_1, \cdots, d_r$ são os chamados *fatores invariantes de M em N*.

Vejamos, agora, como os resultados apresentados até o momento nos permitem encontrar uma base adaptada para um submódulo de um dado módulo M.

Teorema 2.13. *Seja R um domínio euclidiano. Sejam M um $R-$módulo livre de posto m e N um $R-$submódulo de M. Então, existe uma base $\beta' = \{w_1, \cdots, w_m\}$ de M e elementos $d_1, \cdots, d_r \in R\backslash\{0\}$ tais que d_j divide d_{j+1}, $j = 1, \ldots, r-1$ e $\{d_1w_1, \cdots, d_rw_r\}$ é uma base de N. Ainda, dada uma base $x_1, \cdots, x_m$ de M e dado um conjunto ordenado de geradores $y_j = \sum_{i=1}^{m} a_{ij}x_i$, $j \in \{1, \cdots, n\}$, do submódulo N, uma base de N pode ser efetivamente encontrada.*

Prova:

Como M é um $R-$módulo livre de posto m, o submódulo N é finitamente gerado. Sejam γ um conjunto ordenado gerador de N, e γ' uma base de M. Consideremos $i : N \to M$ a inclusão de N em M e A a matriz correspondente em relação a γ e γ'. Pelo teorema (2.8), podemos por meio de operações elementares em linhas e colunas, obter uma matriz diagonal

$$B = \begin{pmatrix} d_1 & & & \vdots & \\ & \ddots & & \vdots & 0 \\ & & d_r & \vdots & \\ \cdots & \cdots & \cdots & & \cdots \\ & 0 & & \vdots & 0 \end{pmatrix}$$

onde d_j divide d_{j+1}, $j = 1, \cdots, r-1$. A matriz B é a matriz correspondente à aplicação i em relação a um conjunto de geradores β de N e uma determinada base $\beta' = \{w_1, \cdots, w_m\}$ de M. Assim, $\beta = \{d_1 w_1, \cdots, d_r w_r\}$. Para concluir que β é uma base de N, resta mostrarmos que os elementos são linearmente independentes.

Sejam $a_1, \cdots, a_r \in R$ tais que

$$\sum_{i=1}^{r} a_i(d_i w_i) = 0,$$

ou seja,

$$\sum_{i=1}^{r} (a_i d_i) w_i = 0.$$

Como β' é base de M, $w_1, \cdots, w_r$ são linearmente independentes. Portanto, obtemos $a_i d_i = 0$, para $i = 1, \cdots, r$. Como cada d_i é não nulo e D é um domínio, obtemos $a_j = 0$, $j = 1, \cdots, r$. Portanto, β é base de N.

Para a segunda parte do teorema, basta lembrarmos que cada operação elementar efetuada em A ao utilizarmos o teorema (2.8) acarreta uma mudança no conjunto ordenado de geradores de N e na base de M. Tais mudanças podem ser efetivamente calculadas, uma vez que são conhecidos o conjunto gerador de N e a base de M, e as operações que devem ser realizadas. O novo conjunto obtido nos dá a base desejada, pela primeira parte do teorema.

□

2.3 A forma racional

Sejam $\mathbb{F}$ um corpo arbitrário (não necessariamente finito) e $R = \mathbb{F}[x]$ o anel de polinômios na variável x com coeficientes em $\mathbb{F}$. Seja M um $R-$módulo. Suponha

$\phi : R^m \to M$ um homomorfismo sobrejetor de $R-$módulos. Como $\operatorname{Nuc}\phi$ é um submódulo de R^m, é finitamente gerado e livre. Sejam $x_1, \cdots, x_m$ uma base de R^m e $y_1, \cdots, y_n$ uma base de $\operatorname{Nuc}\phi$.

Escrevamos

$$y_k = a_{1k}x_1 + a_{2k}x_2 + \cdots + a_{mk}x_m, \quad k = 1, 2, \cdots, n$$

com coeficientes $a_{ij} \in R$. A matriz A é chamada *matriz de relações*.

Se $\operatorname{Nuc}\phi = \{0\}$, então toda matriz de relações é nula, e $M \cong R^m$. Caso $\operatorname{Nuc}\phi \neq \{0\}$, independente da base de R^m e do conjunto gerador de $\operatorname{Nuc}\phi$, a matriz de relações nunca será nula. Neste caso, aplicamos o teorema (2.13).

Por meio de operações elementares sobre as linhas e colunas da matriz de relações A podemos obter uma matriz da forma

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

em que D é uma matriz diagonal com entradas não nulas $a_1, a_2, \cdots, a_k,\ k \leq n$, satisfazendo $a_1 \mid a_2 \mid \cdots \mid a_k$. Concluímos, com isso, que

$$M \cong \frac{R}{(a_1)} \oplus \frac{R}{(a_2)} \oplus \cdots \oplus \frac{R}{(a_k)} \oplus R^{n-k}.$$

A decomposição de M como soma direta como acima se dá de forma única, o que decorre do seguinte teorema::

Teorema 2.14. *Seja R um domínio de ideais principais, e seja M um $R-$módulo não nulo.*

a) M é soma direta de módulos cíclicos,

$M \cong \frac{R}{(a_1)} \oplus \frac{R}{(a_2)} \oplus \cdots \oplus \frac{R}{(a_m)} \oplus R^k$, com a_i não nulos e não invertíveis em R para todo i e $a_1|a_2|\cdots|a_m$.

b) A decomposição na parte (a) é única, isto é, se M também pode ser escrito da forma

$M \cong \frac{R}{(b_1)} \oplus \frac{R}{(b_2)} \oplus \cdots \oplus \frac{R}{(b_s)} \oplus R^l$, com b_i não nulos e não invertíveis em R para todo i e $b_1|b_2|\cdots|b_s$, então $m = s$ e $(a_i) = (b_i)$, para todo i.

A construção feita anteriormente demonstra o item (a) caso $R = \mathbb{F}[x]$. A demonstração do teorema pode ser encontrada em [8, pág. 380].

Eventualmente teremos $a_1 = \cdots = a_r = 1,\ r \leq k$, e os somandos diretos correspondentes são iguais a 0. Removendo tais fatores, que não contribuem para a identificação do módulo M, obtemos os *fatores invariantes* do módulo M: os elementos a_i não constantes.

Cada um dos somandos diretos remanescentes é um $R-$módulo cíclico, que tem como gerador a imagem dos novos elementos da base de R^n.

A nova base de R^n obtida é reflexo das operações elementares efetuadas sobre as colunas da matriz de relações.

Estes resultados serão utilizados na obtenção da forma racional associada a uma transformação linear $T : E \to E$, onde E é um espaço vetorial de dimensão finita.

2.3.1 Forma racional de uma transformação linear

Seja V um espaço vetorial de dimensão finita sobre $\mathbb{F}$ e T uma transformação linear sobre V. Consideraremos V_T como um $\mathbb{F}[x]-$módulo, em que um elemento $p(x) \in \mathbb{F}[x]$ age em V da seguinte forma: se $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, então

$$pv = a_n T^n(v) + a_{n-1}T^{n-1}(v) + \cdots + a_1 T(v) + a_0 v.$$

Como V tem dimensão finita sobre $\mathbb{F}$, segue que V_T é um $\mathbb{F}[x]-$módulo finitamente gerado. Então os resultados anteriores são válidos.

Mostraremos que existe uma base de V_T em relação à qual a matriz da transformação linear T está em uma forma que será chamada *forma racional*. Usaremos a decomposição em fatores invariantes de V_T para obter essa forma.

Definição 2.15. Seja V um espaço vetorial de dimensão finita e $T : V \to V$ uma transformação linear. Se A é a matriz que representa T em relação a uma base de V, o polinômio $\det(x \cdot I - A) \in \mathbb{F}[x]$ é chamado *polinômio característico de* T, que denotaremos $p_T(x)$.

O polinômio característico de T é um polinômio mônico, cujo grau é exatamente $\dim V$.

Considere o conjunto

$$\text{Ann}(V) = \{f(x) \in \mathbb{F}[x] / f(T) = 0\}.$$

$\text{Ann}(V)$ é um ideal de $\mathbb{F}[x]$. Como $\mathbb{F}[x]$ é um domínio de ideais principais, já que $\mathbb{F}$ é um corpo, admite um único polinômio mônico como gerador.

Definição 2.16. O polinômio mônico em $\mathbb{F}[x]$ que gera $\text{Ann}(V)$ é chamado *polinômio minimal* de T, denotado $m_T(x)$.

O polinômio característico de T, em particular, é um polinômio em $\text{Ann}(V)$, portanto, é múltiplo do polinômio minimal. Com isso, temos que o grau do polinômio minimal é no máximo n.

Pelos resultados da seção anterior, existem polinômios $a_1, \cdots, a_k$ tais que $a_1 \mid a_2 \mid \cdots \mid a_k$, e

$$V \cong \frac{\mathbb{F}[x]}{(a_1)} \oplus \frac{\mathbb{F}[x]}{(a_2)} \oplus \cdots \oplus \frac{\mathbb{F}[x]}{(a_k)} \oplus R^{n-k}.$$

Definimos como fatores invariantes de uma matriz A como os fatores invariantes associados a matriz $x \cdot I - A$, com entradas em $\mathbb{F}[x]$.

Teorema 2.17. (Forma Normal de Smith) *Seja A uma matriz $n \times n$ sobre um corpo $\mathbb{F}$. Por meio de operações elementares, podemos transformar a matriz $x \cdot I - A$ com entradas em $\mathbb{F}[x]$ em uma matriz da forma*

$$\begin{pmatrix} Id & 0 \\ 0 & D \end{pmatrix}$$

em que Id é uma matriz identidade $(n-m) \times (n-m)$ e D é uma matriz diagonal $m \times m$ da forma

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_m \end{pmatrix}$$

em que $a_1, \cdots, a_m$ são polinômios mônicos não constantes em $\mathbb{F}[x]$ satisfazendo $a_1 \mid a_2 \mid \cdots \mid a_m$. Os elementos $a_1, \cdots, a_m$ são os fatores invariantes de A.

Prova: A demonstração decorre imediatamente da construção apresentada na seção anterior. Como $\det(x \cdot I - A)$ é um polinômio mônico não nulo, as linhas da matriz são linearmente independentes, o que nos garante que, por meio de operações elementares, podemos deixá-la na forma diagonal sem que nenhuma linha se anule.

Após obtermos a forma diagonal, se algum elemento d_{ii} é constante e diferente de 1, multiplicamos a linha i por d_{ii}^{-1}. O mesmo vale se algum polinômio não for mônico, e multiplicamos a linha pelo inverso do coeficiente de seu termo líder. Isso é possível, uma vez que $\mathbb{F}$ é um corpo.

□

Seja $\{v_1, \cdots, v_n\}$ uma base de V_T como espaço vetorial, e A a matriz que representa T em relação a esta base.

Consideremos o homomorfismo

$$\phi : \mathbb{F}[x]^n \to V_T$$

$$\phi(p_1, p_2, \cdots, p_n) = \sum_{i=1}^{n} p_i v_i.$$

ϕ é sobrejetivo, uma vez que dado $v \in V_T$, este se escreve de modo único da forma $v = \sum a_i v_i$. Assim, $v = \phi(a_1, a_2, \cdots, a_n)$.

Desejamos, agora, mostrar que $\text{Nuc}\,(\phi) = \{(x \cdot I - A)v,\ v \in V_T\}$.

Comecemos mostrando que $\{(x \cdot I - A)v,\ v \in V_T\} \subset \text{Nuc}\,(\phi)$. Para isso, basta mostrar que $(x \cdot I - A)e_i = 0$, onde $\{e_1, \cdots, e_n\}$ é a base canônica de $\mathbb{F}[x]^n$.

$$\begin{aligned}
\phi((x \cdot I - A)e_i) &= \phi(xe_i - Ae_j) \\
&= x\phi(e_i) - \phi(\textstyle\sum_{i=1}^{n} a_{jk}e_k) \\
&= xv_i - \textstyle\sum_{i=1}^{n} a_{jk}\phi(e_k) \\
&= T(v_i) - \textstyle\sum_{i=1}^{n} a_{jk}v_k \\
&= 0
\end{aligned}$$

Para a inclusão contrária, consideremos N gerado pelas colunas de $x \cdot I - A$, e o homorfismo

$$\phi' : \mathbb{F}[x]^n/N \to V_T$$

$$phi'(u + N) = \phi(u).$$

Como ϕ é sobrejetora, ϕ' também o é. Por outro lado, a dimensão dos espaços subjacentes (dimensão vista como espaço vetorial) são iguais. Assim, ϕ' é um isomorfismo. Portanto, decorre que

$$\mathbb{F}[x]/N \cong V_T,$$

e pelo teorema do homorfismo, que $\text{Nuc}\,(\phi) = \{(x \cdot I - A)v,\ v \in V_T\}$.

Assim, em consequência do teorema (2.17), V_T pode ser escrito da seguinte forma:

$$V \cong \frac{\mathbb{F}[x]}{(a_1)} \oplus \frac{\mathbb{F}[x]}{(a_2)} \oplus \cdots \oplus \frac{\mathbb{F}[x]}{(a_m)}.$$

Por meio desta decomposição, poderemos definir a forma racional da transformação T.

O primeiro passo é compreender o que se passa em cada somando direto. Para isso, consideremos o anel quociente $\mathbb{F}[x]/(f(x))$, onde $f(x) = x^t + b_{t-1}x^{t-1} + \cdots b_1 x + b_0 \in \mathbb{F}[x]$. Pelo algoritmo da divisão, temos que dado $g(x) \in \mathbb{F}[x]$, este pode ser escrito de forma única como $g(x) = q(x)f(x) + r(x)$, $q(x), r(x) \in \mathbb{F}[x]$, $r \equiv 0$ ou $\text{grau}\, r < t$. Assim, no anel quociente, $g(x)$ e $r(x)$ representam o mesmo elemento, uma vez que $f(x)q(x) = 0$ em $\mathbb{F}[x]/(f(x))$. Com isso, o quociente é gerado como $\mathbb{F}-$espaço vetorial pelos elementos $\overline{1}, \overline{x}, \overline{x}^2, \cdots, \overline{x}^{n-1}$, com $\overline{x}^k = x^k \mod f(x)$. Como tais elementos são linearmente independentes, formam uma base do $\mathbb{F}-$espaço vetorial $\mathbb{F}[x]/(f(x))$. Com respeito a tal base, a transformação linear (multiplicação por x) age da seguinte maneira:

$$x : \begin{cases} 1 & \mapsto & \overline{x} \\ \overline{x} & \mapsto & \overline{x}^2 \\ \overline{x}^2 & \mapsto & \overline{x}^3 \\ \vdots & & \\ \overline{x}^{t-2} & \mapsto & \overline{x}^{t-1} \\ \overline{x}^{t-1} & \mapsto & \overline{x}^t = -b_0 - b_1\overline{x} - \cdots - b_{t-1}\overline{x}^{t-1} \end{cases}$$

Nessa base, a matriz da transformação é dada por

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & 0 & -b_1 \\ 0 & 1 & \cdots & 0 & 0 & -b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -b_{t-2} \\ 0 & 0 & \cdots & 0 & 1 & -b_{t-1} \end{pmatrix}.$$

A matriz acima é chamada *matriz companheira* do polinômio mônico $f(x)$, que será denotada $C_{f(x)}$. Segue o seguinte resultado:

Proposição 2.18. *Sejam $f(x) \in \mathbb{F}[x]$ e $C_{f(x)}$ sua matriz companheira. Então, polinômios característico e minimal de $C_{f(x)}$ coincidem, e são iguais a $f(x)$. Se T é uma transformação linear, seu polinômio característico é dado pelo produto dos fatores invariantes, enquanto seu polinômio minimal é fator invariante de maior grau.*

Voltando a decomposição de V_T como soma direta, tomamos β_i a base do $\mathbb{F}-$submódulo de V associado a $\mathbb{F}[x]/(a_i(x))$. Relativa à base $\beta = \bigcup \beta_i$, a transformação linear T tem matriz dada pela soma direta das matrizes companheiras dos fatores invariantes:

$$\begin{pmatrix} C_{a_1(x)} & & & & \\ & C_{a_2(x)} & & & \\ & & \ddots & & \\ & & & C_{a_{m-1}(x)} & \\ & & & & C_{a_m(x)} \end{pmatrix}$$

Uma matriz é dita na *forma racional* se é soma direta de matrizes companheiras de polinômios mônicos $a_1(x), \cdots, a_m(x)$, os quais são os fatores invariantes da matriz. Tais polinômios são não constantes e satisfazem $a_1 \mid a_2 \mid \cdots \mid a_m$. A forma racional de uma transformação linear T é a matriz de T que está na forma racional.

Mostramos, com isso, que qualquer transformação linear T tem uma forma raciona e que a mesma é determinada a partir de seus fatores invariantes. Como vimos anteriormente, os fatores invariantes de uma matriz são únicos. Consequentemente, a forma

racional também será. Decorre então o seguinte teorema:

Teorema 2.19. (Forma Racional de uma Transformação Linear) *Seja V um espaço vetorial de dimensão finita sobre um corpo $\mathbb{F}$ e T uma transformação linear de V em V. Então, existe uma base de V em relação à qual a matriz de T está na forma racional. A forma racional de T é única.*

O seguinte teorema nos permite classificar as transformações lineares a menos de forma racional:

Teorema 2.20. *Sejam S e T transformações lineares de V em V. Então, as três afirmações são equivalentes:*

1. *S e T são transformações lineares semelhantes;*
2. *os $\mathbb{F}[x]-$módulos V_T e V_S são isomorfos.*
3. *S e T tem a mesma forma racional.*

Vamos, agora, estender o conceito de forma racional a matrizes quadradas. A versão matricial do teorema (2.19):

Teorema 2.21. (Forma Racional para Matrizes) *Seja A uma $n \times n$ matriz sobre um corpo $\mathbb{F}$. Então, a matriz A é semelhante a uma única matriz na forma racional, ou seja, existe uma matriz invertível P sobre $\mathbb{F}$ tal que $P^{-1}AP$ é uma matriz formada por blocos diagonais que são matrizes companheiras de polinômios mônicos $a_1(x), \cdots, a_m(x)$ não constantes e tais que $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$.*

Decorre do teorema acima que duas matrizes semelhantes possuem a mesma forma racional. Sendo assim, podemos estabelecer no conjunto das matrizes $n \times n$ uma relação de equivalência, em que $A \sim B$ se A e B tem a mesma forma racional. Deste modo, o teorema nos permite classificar as matrizes (ou transformações lineares) por meio desta relação de equivalência.

Vejamos agora como identificar a base de V para a qual a matriz que representa T está na forma racional.

Dado um espaço vetorial de dimensão finita V com base $\{e_1, \cdots, e_n\}$ e uma transformação T de V em V com matriz A em relação a essa base, seguimos o seguinte roteiro:

1º) Primeiramente obtemos a forma normal de Smith da matriz A, como no teorema (2.17). Para tal, usamos operações elementares nas linhas e colunas da matriz $x \cdot I - A$.

   ✓ troca de colunas ($C_i \longleftrightarrow C_j$) ou de linhas ($L_i \longleftrightarrow L_j$).

✓ somar a uma coluna um múltiplo em $\mathbb{F}[x]$ de outra coluna ($C_i \longleftarrow C_i + p(x)C_j$) ou a uma linha um múltiplo em $\mathbb{F}[x]$ de outra linha ($L_i \longleftarrow L_i + p(x)L_j$).

✓ multiplicar uma coluna por uma unidade de $\mathbb{F}[x]$ ($C_i \longleftarrow uC_i$) ou uma linha por uma unidade de $\mathbb{F}[x]$ ($L_i \longleftarrow uL_i$).

Sejam $d_1, \cdots, d_m$ os graus dos fatores invariantes não-constantes $a_1(x), \cdots, a_m(x)$ que aparecem na diagonal da matriz, respectivamente.

2º) Inicie com a matriz identidade $n \times n$. Para cada operação efetuada nas linhas na etapa anterior, respeitando a mesma ordem, devemos fazer uma operação correspondente nas colunas de I, procedendo da seguinte forma:

✓ Para a troca de linhas $L_i \longleftrightarrow L_j$, realizamos a operação $C_i \longleftrightarrow C_j$.

✓ Para a operação $L_i \longleftarrow L_i + p(x)L_j$, $p(x) \in \mathbb{F}[x]$, efetuamos a operação $C_j \longleftarrow C_j - p(A)C_i$.

✓ Para a operação $L_i \longleftarrow uL_i$ faça $C_i \longleftarrow u^{-1}C_i$.

3º) Obtemos na primeira etapa uma matriz como no teorema (2.17), e na segunda uma matriz em que as $n-m$ primeiras colunas são nulas. As m colunas restantes formam a base do $\mathbb{F}[x]-$módulo associados aos fators invariantes da matriz. Para a $i-$ésima coluna não nula, devemos multiplicá-la por $I, A, A^2, \cdots, A^{d_i-1}$, o que nos dá a base ordenada como espaço vetorial para o módulo associado a $\mathbb{F}[x]/(a_i)$. Procedendo desta forma com todas as colunas não nulas, obtemos uma base ordenada para a V, em relação à qual a matriz de T está na forma racional.

Assim, quanto menos operações forem efetuadas sobre linhas para se obter os fatores invariantes da transformação, mais fácil será obter a base correspondente à forma racional.

Exemplo 2.22. Apliquemos a construção apresentada para obter a forma racional da matriz associada abaixo, com entradas em $\mathbb{F}_3$:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & -1 & 1 \\ -1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} x & 0 & 0 & 0 & -1 & 0 \\ 0 & x+1 & 0 & 0 & -1 & 0 \\ 0 & 0 & x & -1 & 1 & -1 \\ 1 & -1 & -1 & x & 0 & -1 \\ 0 & -1 & -1 & -1 & x-1 & -1 \\ 0 & 0 & 0 & 0 & 0 & x \end{bmatrix} \xrightarrow[L_4 \longleftrightarrow L_1]{} \begin{bmatrix} 1 & -1 & -1 & x & 0 & -1 \\ 0 & x+1 & 0 & 0 & -1 & 0 \\ 0 & 0 & x & -1 & 1 & -1 \\ x & 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & -1 & -1 & x-1 & -1 \\ 0 & 0 & 0 & 0 & 0 & x \end{bmatrix}$$

$$\xrightarrow[L_4 \longleftarrow L_4 - xL_1]{} \begin{bmatrix} 1 & -1 & -1 & x & 0 & -1 \\ 0 & x+1 & 0 & 0 & -1 & 0 \\ 0 & 0 & x & -1 & 1 & -1 \\ 0 & x & x & -x^2 & -1 & x \\ 0 & -1 & -1 & -1 & x-1 & -1 \\ 0 & 0 & 0 & 0 & 0 & x \end{bmatrix} \xrightarrow[\begin{array}{c} C_2 \longleftarrow C_2 + C_1 \\ C_3 \longleftarrow C_3 + C_1 \\ C_4 \longleftarrow C_4 - xC_1 \\ C_6 \longleftarrow C_6 + C_1 \end{array}]{}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & x+1 & 0 & 0 & -1 & 0 \\ 0 & 0 & x & -1 & 1 & -1 \\ 0 & x & x & -x^2 & -1 & x \\ 0 & -1 & -1 & -1 & x-1 & -1 \\ 0 & 0 & 0 & 0 & 0 & x \end{bmatrix} \xrightarrow[\begin{array}{c} C_2 \longleftrightarrow C_5 \\ C_2 \longleftarrow -C_2 \end{array}]{} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & x+1 & 0 \\ 0 & -1 & x & -1 & 0 & -1 \\ 0 & 1 & x & -x^2 & x & x \\ 0 & 1-x & -1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & x \end{bmatrix}$$

$$\xrightarrow[C_5 \longleftarrow C_5 - (x+1)C_2]{} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & x & -1 & x+1 & -1 \\ 0 & 1 & x & -x^2 & -1 & x \\ 0 & 1-x & -1 & -1 & x^2-2 & -1 \\ 0 & 0 & 0 & 0 & 0 & x \end{bmatrix} \xrightarrow[\begin{array}{c} L_3 \longleftarrow L_3 + L_2 \\ L_4 \longleftarrow L_4 - L_2 \\ L_5 \longleftarrow L_5 - (1-x)L_2 \end{array}]{}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & x & -1 & x+1 & -1 \\ 0 & 0 & x & -x^2 & -1 & x \\ 0 & 0 & -1 & -1 & x^2-2 & -1 \\ 0 & 0 & 0 & 0 & 0 & x \end{bmatrix} \xrightarrow[\begin{array}{c} C_4 \longleftrightarrow C_3 \\ C_3 \longleftarrow -C_3 \end{array}]{} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & x & x+1 & -1 \\ 0 & 0 & x^2 & x & -1 & x \\ 0 & 0 & 1 & -1 & x^2-2 & -1 \\ 0 & 0 & 0 & 0 & 0 & x \end{bmatrix}$$

$$\xrightarrow[\substack{L_4 \longleftarrow L_4 - x^2 L_3 \\ L_5 \longleftarrow L_5 - L_3}]{} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & x & x+1 & -1 \\ 0 & 0 & 0 & -x^3+x & -x^3-x^2-1 & x^2+x \\ 0 & 0 & 0 & -1-x & x^2-x & 0 \\ 0 & 0 & 0 & 0 & 0 & x \end{bmatrix}$$

$$\xrightarrow[\substack{C_4 \longleftarrow C_4 - xC_3 \\ C_5 \longleftarrow C_5 - (x_1)C_3 \\ C_6 \longleftarrow C_6 + C_3}]{} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -x^3+x & -x^3-x^2-1 & x^2+x \\ 0 & 0 & 0 & -1-x & x^2-x & 0 \\ 0 & 0 & 0 & 0 & 0 & x \end{bmatrix} \xrightarrow{C_5 \longleftarrow C_5 + C_6}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -x^3+x & -x^3+x-1 & x^2+x \\ 0 & 0 & 0 & -1-x & x^2-x & 0 \\ 0 & 0 & 0 & 0 & x & x \end{bmatrix} \xrightarrow{C_4 \longleftarrow C_4 - C_5}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -x^3+x-1 & x^2+x \\ 0 & 0 & 0 & -x^2-1 & x^2-x & 0 \\ 0 & 0 & 0 & -x & x & x \end{bmatrix} \xrightarrow[L_6 \longleftarrow L_6 + xL_4]{L_5 \longleftarrow L_5 + (x^2+1)L_4}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -x^3+x-1 & x^2+x \\ 0 & 0 & 0 & 0 & -x^5-1 & x^4+x^3+x^2+x \\ 0 & 0 & 0 & 0 & -x^4+x^2 & x^3+x^2+x \end{bmatrix} \xrightarrow[C_6 \longleftarrow C_6 - (x^2+x)C_4]{C_5 \longleftarrow C_5 - (-x^3+x-1)C_4}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -x^5-1 & x^4+x^3+x^2+x \\ 0 & 0 & 0 & 0 & -x^4+x^2 & x^3+x^2+x \end{bmatrix} \xrightarrow{L_5 \longleftarrow L_5 - xL_6}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -x^3-1 & x \\ 0 & 0 & 0 & 0 & -x^4+x^2 & x^3+x^2+x \end{bmatrix} \xrightarrow[C_5 \longleftarrow -C_5]{C_5 \longleftarrow C_5 + x^2 C_6}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & x \\ 0 & 0 & 0 & 0 & -x^5-x^3-x^2 & x^3+x^2+x \end{bmatrix} \xrightarrow{C_6 \longleftarrow C_6 - x^2 C_5}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -x^5-x^3-x^2 & x^6+x^4+2x^3+x \end{bmatrix} \xrightarrow{L_6 \longleftarrow L_6 + (x^5+x^3+x^2)L_5}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & x^6+x^4+2x^3+x \end{bmatrix}$$

Assim, a forma racional será

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Vamos agora determinar a base do $\mathbb{F}[x]-$módulo associado ao fator invariante $x^6 + x^4 + 2x^3 + x$. Iniciamos com a matriz identidade 6×6, e realizamos a seguinte sequência de operações elementares:

1) $C_4 \longleftrightarrow C_1$
2) $C_1 \longleftarrow C_1 + AC_4$
3) $C_2 \longleftarrow C_2 - C_3$
4) $C_2 \longleftarrow C_2 + C_4$
5) $C_2 \longleftarrow C_2 + (Id - A)C_5$
6) $C_3 \longleftarrow C_3 + A^2C_4$
7) $C_3 \longleftarrow C_3 + C_5$
8) $C_4 \longleftarrow C_4 - (A^2 + Id)C_5$
9) $C_4 \longleftarrow C_4 - AC_6$
10) $C_6 \longleftarrow C_6 + AC_5$
11) $C_5 \longleftarrow C_5 - (A^5 + A^3 + A^2)C_6$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[C_4 \longleftrightarrow C_1]{} \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[\substack{C_1 \longleftarrow C_1 + AC_4 \\ C_2 \longleftarrow C_2 - C_3}]{}$$

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[C_2 \longleftarrow C_2 + C_4]{} \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[\substack{C_2 \longleftarrow C_2 + (Id - A)C_5 \\ C_3 \longleftarrow C_3 + A^2C_4}]{}$$

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[\substack{C_3 \longleftarrow C_3 + C_5 \\ C_4 \longleftarrow C_4 - (A^2 + Id)C_5}]{} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[C_4 \longleftarrow C_4 - AC_6]{}$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[\substack{C_6 \longleftarrow C_6 + AC_5 \\ C_5 \longleftarrow C_5 - (A^5 + A^3 + A^2)C_6}]{} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Assim, $(1,1,2,0,1,1)$ é a base para o $F[x]-$módulo associado ao fator invariante, e

$$(1,1,2,0,1,1),(1,0,0,0,2,0),(2,2,1,2,2,0),(2,0,0,1,1,0),(1,1,0,1,2,0),(2,1,2,0,1,0)$$

é base de V na qual a matriz que representa T está na forma racional.

2.4 Teorema chinês do resto

Para atingirmos nossos objetivos no capítulo (3), necessitaremos ir além da forma racional e dos fatores invariantes. Para tal, recorremos ao teorema chinês do resto. Sua demonstração é nosso próximo objetivo.

Definição 2.23. Dois ideais A e B de um anel R são ditos *comaximais* se $A+B=R$.

Teorema 2.24. ***(Teorema Chinês do Resto)***
Sejam $A_1,\cdots,A_n$ ideais em R. O mapa

$$\phi : R \to \frac{R}{A_1}\times\frac{R}{A_2}\times\cdots\times\frac{R}{A_n}$$
$$r \to (r+A_1, r+A_2,\cdots,r+A_n)$$

é um homomorfismo de anéis com núcleo $A_1\cap\cdots\cap A_n$. Se A_i e A_j são comaximais sempre que $i\neq j$, então o mapa é sobrejetivo e $A_1\cap\cdots\cap A_n = A_1\cdots A_n$, e

$$\frac{R}{A_1\cdots A_n} = \frac{R}{A_1\cap\cdots\cap A_n} \cong \frac{R}{A_1}\times\cdots\times\frac{R}{A_n}.$$

Prova: Usaremos indução sobre n para provar o resultado. Se $n=2$, consideremos o mapa

$$\phi : R \to \frac{R}{A}\times\frac{R}{B}$$

dado por $\phi(r)=(r+A, r+B)$. Cada componente de ϕ corresponde a projetarmos R em R/A e R/B, respectivamente. Assim, ϕ é um homomorfismo de anéis. Quanto ao núcleo de ϕ, este será composto pelos elementos $r\in R$ tais que $r+A=0$ e $r+B=0$, isto é, aqueles em $A\cap B$.

Uma vez que A e B são comaximais, existem elementos $a\in A, b\in B$, tais que $a+b=1$. Assim,

$$\phi(a) = (a+A, a+B) = (0,1);$$
$$\phi(b) = (b+A, b+B) = (1,0).$$

Seja $(r_1 + A, r_2 + B)$ um elemento de $R/A \times R/B$, e calculemos $\phi(r_2 a + r_1 b)$:

$$\begin{aligned}\phi(r_2 a + r_1 b) &= \phi(r_2)\phi(a) + \phi(r_1)\phi(b) = \\ &= (r_2 + A, r_2 + B)(0, 1) + (r_1 + A, r + 1 + B)(1, 0) \\ &= (0, r + 2 + B) + (r_1 + A, 0) \\ &= (r_1 + A, r_2 + B).\end{aligned}$$

Isso nos mostra que ϕ é sobrejetora.

Como A e B são ideais, temos AB contido em $A \cap B$. Resta mostrar a inclusão contrária. Seja $c \in A \cap B$.

$$c = c \cdot 1 = c \cdot (a + b) = c \cdot a + c \cdot b \in AB.$$

Verifica-se então o resultado para $n = 2$.

Caso $n > 2$, basta tomarmos $A = A_1$ e $B = A_2 \cdots A_n$, e usar a hipótese de indução. Potanto, temos o resultado verificado. □

Vamos agora aplicar o teorema (2.24) em cada quociente $R/(a_i)$.

Para tal, escrevemos os fatores invariantes de A da seguinte forma:

$$\begin{aligned} a_1 &= p_0^{\alpha_{10}} p_1^{\alpha_{11}} \cdots p_t^{\alpha_{1t}} \\ &\vdots \\ a_m &= p_0^{\alpha_{m0}} p_1^{\alpha_{m1}} \cdots p_t^{\alpha_{mt}}\end{aligned}$$

em que p_i são polinômios irredutíveis em $\mathbb{F}[x]$, mônicos e dois a dois distintos. Consideraremos $p_0 = x$. Da relação de divisibilidade entre os fatores invariantes, temos que $\alpha_{ij} \leq \alpha_{kj}$ se $i \leq k$. As potências de irredutíveis $p_i^{\alpha ij}$ são chamados *divisores elementares* de T. Caso p_j não apareça na fatoração a_i, basta tomarmos $\alpha_{ij} = 0$.

Como $p_i's$ são polinômios irredutíveis, temos que $A_{ij} = (p_j^{\alpha_{ij}})$ são comaximais. Portanto, verifica-se a hipótese do teorema (2.24). Assim, temos a seguinte decomposição em soma direta:

$$\frac{\mathbb{F}[x]}{(a_i(x))} \cong \frac{\mathbb{F}[x]}{(p_0^{\alpha_{i1}})} \oplus \frac{\mathbb{F}[x]}{(p_1^{\alpha_{i2}})} \oplus \cdots \oplus \frac{\mathbb{F}[x]}{(p_t^{\alpha_{it}})}.$$

Cada $p_j^{\alpha_{ij}}$ é chamado *divisor elementar de A*.

α_{ij} possa ser eventualmente nulo. Neste caso, o somando direto é nulo.

A vantagem em lidarmos com os divisores elementares e suas matrizes companheiras é que, nesse caso, além do polinômio característico e minimal coincidirem, como garante a proposição (2.18), ambos são potências de um polinômio irredutível em $\mathbb{F}[x]$. Essa é uma das hipóteses fundamentais do teorema (3.23), base para a caracterização para espaço de fase de um sistema dinâmico finito linear.

Para o resultado apresentado no próximo capítulo, buscaremos a partir de uma dada

matriz A determinar seus fatores invariantes e seus divisores elementares. Tais informações permitirão escrever a matriz inicial como soma direta de outras mais simples, e com estrutura previamente determinadas. Necessitaremos ainda dos resultados apresentados no capítulo anterior, referentes a ordem de um polinômio irredutível, para identificarmos a ordem dos divisores elementares de A e de seus divisores.

Capítulo 3

Sistemas dinâmicos finitos

O estudo de sistemas dinâmicos visa determinar e estudar leis que relacionem o estado atual e futuro de fenômenos de natureza biológica, física ou econômica, dentre outros. Temos um modelo matemático que reproduz o comportamento do sistema, tendo como objetivo principal a descrição de seu comportamento futuro a partir de um dado estado inicial e a determinação de suas possíveis trajetórias.

Nosso interesse está voltado para o estudo de Sistemas Dinâmicos Finitos (SDF): sistemas dinâmicos determinísticos, vistos em tempo discreto, e com um número finito de possíveis estados.

3.1 Definições e conceitos básicos

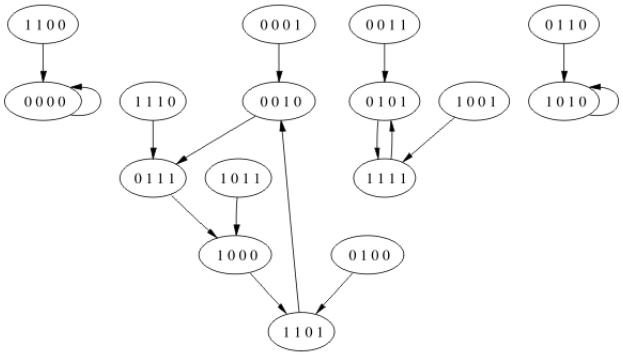
Um sistema dinâmico finito é um par (X, f), onde X é um conjunto finito e f uma função de X em X.

A cada SDF (X, f), associamos o espaço de fase de f, denotado $\mathcal{G}_f$: trata-se de um grafo direcionado cujos vértices são os elementos de X e a existência de uma seta partindo de x para y ocorre quando $f(x) = y$.

Exemplo 3.1. Considere $X = \mathbb{F}_2^4$ e $f : X \to X$ dada por

$$f(x, y, z, t) = (x + y, x + y + z, y + z, x + y + z).$$

O grafo de f é



Definimos a *órbita* de um elemento x como o conjunto $\mathcal{O}(x) = \{x, f(x), f^2(x), \cdots\}$.

$$x \longmapsto f(x) \longmapsto f^2(x) \longmapsto \cdots$$

Vemos que o grafo decompõe-se como a união de todas as órbitas dos elementos de X. Visto que X é finito, para cada $x \in X$ existem inteiros m, r tais que $f^{m+r}(x) = f^r(x)$. Vamos supor que m e r sejam mínimos com tal propriedade. Assim, temos algumas situações a considerar:

a) Caso $r = 0$, então $f^m(x) = x$. Neste caso, a órbita $\mathcal{O}(x)$ é dita um *ciclo*, e seu comprimento é m.

   No SDF apresentado no exemplo (3.1) vemos que são ciclos as órbitas de cada um dos seguintes elementos:

   $(0,0,0,0), (0,0,1,0), (0,1,1,1), (1,0,0,0), (1,1,0,1), (0,1,0,1), (1,1,1,1), (1,0,1,0)$.

b) Se $m = 1$ e $r = 0$, temos $f(x) = x$. Neste caso, $\mathcal{O}(x) = \{x\}$. x é chamado *ponto fixo de* f.

   No SDF apresentado no exemplo (3.1) $(0,0,0,0)$ e $(1,0,1,0)$ são pontos fixos.

c) Se $m > 0$ e $r > 0$, o conjunto $\{x, f(x), \cdots, f^{r-1}(x)\}$ é chamado *parte transiente* de $\mathcal{O}(x)$, enquanto $\{f^r(x), \cdots, f^{r+m-1}\}$ é chamado *ciclo terminal* de $\mathcal{O}(x)$.

   No SDF apresentado no exemplo (3.1), a órbita do elemento $(1,1,0,0)$ tem parte transiente formada por ele mesmo e ciclo terminal $(0,0,0,0)$.

   Os elementos $(0,0,0,1), (1,1,1,0), (1,0,1,1)$ e $(0,1,0,0)$ são, respectivamente, as partes transientes de suas órbitas, e apresentam ciclo terminal comum, formado pelos elementos $(0,0,1,0), (0,1,1,1,), (1,0,0,0)$ e $(1,1,0,1)$.

Podemos restringir a situação em que o $X = \mathbb{F}_q^n$, onde $\mathbb{F}_q$ é o corpo finito com $q = p^t$ elementos. Assim, a função f é dada por meio de funções coordenadas $(f_1, \cdots, f_n)$, cada $f_i : \mathbb{F}_q^n \to \mathbb{F}_q$. Neste caso, principal vantagem encontrada é que toda função $g : \mathbb{F}_q^n \to \mathbb{F}_q$ é polinomial: dada qualquer função $g : \mathbb{F}_q^n \to \mathbb{F}_q$, existe por interpolação um polinômio $h \in \mathbb{F}_q[x_1, \cdots, x_n]$ tal que $g(c_1, \cdots, c_n) = h(c_1, \cdots, c_n)$, $\forall (c_1, \cdots, c_n) \in \mathbb{F}_q^n$:

$$h(x_1, \cdots, x_n) = \sum_{(c_1,\cdots,c_n)\in\mathbb{F}_q^n} \big[g(c_1, \cdots, c_n) \prod_{i=1}^{n} (1 - (x_i - c_i)^{q-1})\big].$$

Dado um elemento arbitrário $x \in X$, sua órbita sempre será formada de uma parte transiente (que eventualmente pode ser vazia) e de um ciclo terminal (eventualmente formado por um único elemento).

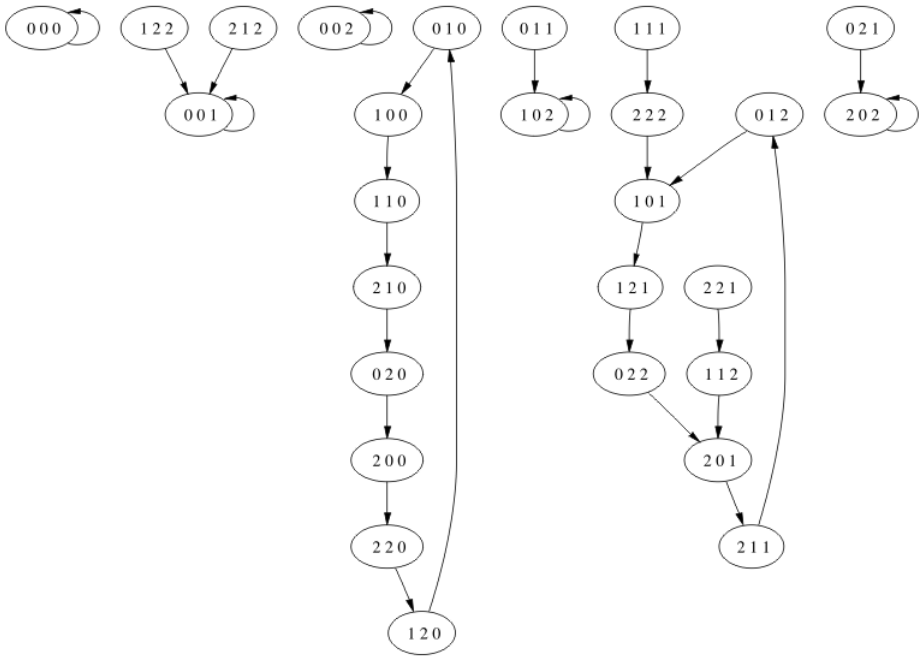
Se y é um elemento da órbita de x e $y \neq x$, dizemos que y é *sucessor* de x. Um elemento que não se encontra na órbita de nenhum outro é dito *fonte* do sistema.

Definimos em X a seguinte relação:

$$x \sim y \text{ se suas órbitas tem um elemento em comum.}$$

A relação $\sim$ é uma relação de equivalência. Suas classes de equivalência são chamadas *componentes conexas* do sistema, que correspondem às partes conexas do grafo associado.

Exemplo 3.2. Considere $X = \mathbb{F}_3^3$ e $f : X \to X$ dada por $f(x, y, z) = (x+y, x+xz, z+y^2z)$. O grafo de f possui 7 componentes conexas:



Temos as seguintes possibilidades para as componentes conexas de um sistema:

a) Se cada elemento da componente conexa é sucessor de algum outro, ou seja, nenhum deles é fonte, então a componente conexa será um ciclo. Neste caso, a componente conexa coincide com a órbita de cada um dos elementos que a compõe.

   No exemplo (3.2) vemos que são ciclos as órbitas dos seguintes elementos: $(0, 0, 0)$, $(0, 0, 2)$ e $(0, 1, 0)$. Seus comprimentos são 1, 1 e 8, respectivamente.

b) Se existe um elemento v na componente conexa tal que para qualquer outro elemento x nesta componente temos $f^m(x) = v$, onde m depende de x, e $f(v) = v$, então a componente conexa será uma *árvore*, de ponto terminal v. Se n o menor inteiro tal que $f^n(x) = v$ para todo x na componente conexa, chamamos n a *altura da árvore*. Uma árvore é uma componente conexa com um ponto fixo.

   Dentre as componentes conexas do grafo apresentado no exemplo (3.2), três delas são árvores: a primeira delas, formada pelos elementos $(1, 2, 2), (2, 1, 2)$ e $(0, 0, 1)$; a próxima, formada pelos elementos $(0, 1, 1)$ e $(1, 0, 2)$, e por último a formada pelos elementos $(0, 2, 1)$ e $(2, 0, 2)$, todas elas de altura 1.

c) A componente conexa não é um ciclo, nem uma árvore. Assim, como não é um ciclo, existem pontos fontes. Como não é uma árvore, não possui nenhum ponto fixo.

   No grafo do exemplo (3.2), a componente conexa em que está o elemento $(1, 1, 1)$ não é um ciclo, nem uma árvore.

Lema 3.3. *Toda componente conexa é formada por um ciclo terminal (formado por um único elemento, caso seja uma árvore) e acoplado a cada um dos elementos deste ciclo temos uma parte transiente (eventualmente vazia).*

Prova:

É suficiente mostrar que dados dois elementos quaisquer na componente conexa, eles possuem o mesmo ciclo terminal.

Caso os dois elementos tomados já estejam na mesma órbita, nada resta a fazer. Suponhamos agora que não estejam um na órbita do outro. Pela relação de equivalência, sabemos que ambos tem um elemento em comum em sua órbita, daí devem ter o mesmo ciclo terminal.

□

Com isso, cada componente conexa é uma árvore, um ciclo ou formada por um ciclo em que para cada um dos elementos existe uma árvore eventualmente vazia (parte transiente) que o tem como último elemento. Como cada espaço de fase é a união de suas componentes conexas, já sabemos a grosso modo o aspecto do grafo de um SDF.

Nas próximas seções, apresentaremos meios de identificar cada uma destas componentes conexas, para um caso particular de sistemas dinâmicos. Esta decomposição, combinada com algumas operações entre sistemas dinâmicos, dirão a estrutura do nosso grafo.

3.2 Operações entre sistemas dinâmicos finitos

Seja (X, f) um sistema dinâmico finito. Um subconjunto de Y de X é dito *parte invariante* de X quando $f(Y) \subset Y$. Os principais exemplos de parte invariante de X são suas componentes conexas, bem como as órbitas $\mathcal{O}(x), x \in X$. Como Y é $f-$invariante, podemos definir um sistema dinâmico finito $(Y, f\mid_Y)$.

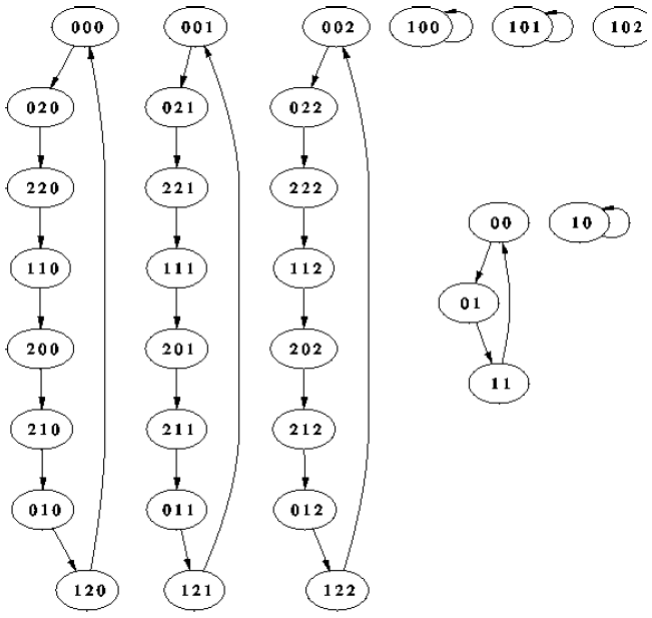
Temos um interesse especial em duas partes invariantes: as árvores e ciclos, que serão a base para os resultados apresentados nas próximas seções.

Iniciaremos com a definição de duas operações entre SDF's: soma e produto.

Definição 3.4. (Operações entre Sistemas Dinâmicos Finitos) Sejam (X, f) e (Y, g) SDF's.

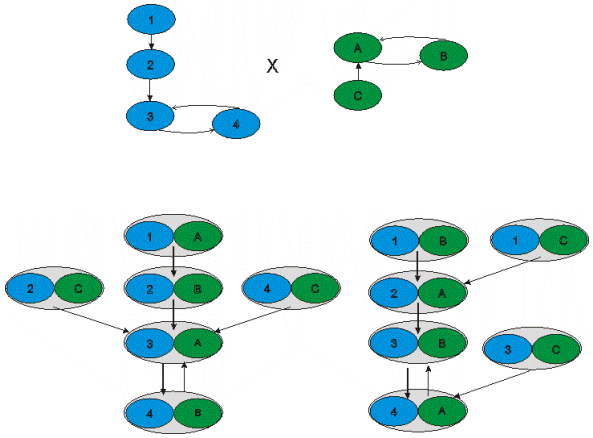
a) A *soma* de (X, f) com (Y, g) é definida como o SDF $(X \vee Y, f \vee g)$, onde $X \vee Y$ é a união disjunta de X e Y, e $(f \vee g)(z)$ é definido como $f(z)$ se $z \in X$ e $g(z)$ se $z \in Y$. O grafo da soma será denotado por $\mathcal{G}_f + \mathcal{G}_g$.

Exemplo 3.5. Considere $X = \mathbb{F}_2^2$ e $f(x, y) = (x + y, x - 1)$; $Y = \mathbb{F}_3^3$, $g(x, y, z) = (x + y, x - 1, z)$. Assim, está bem definida a operação de soma entre estes SDF. O grafo de $X \vee Y$ nada mais é que colocar lado a lado os grafos de X e Y:



b) O *produto* de (X, f) por (Y, g) é o SDF $(X \times Y, f \times g)$, onde $X \times Y$ é o produto cartesiano entre X e Y, e $(f \times g)(x, y) = (f(x), g(y))$. O grafo do produto é denotado por $\mathcal{G}_f\mathcal{G}_g$.

Exemplo 3.6. Vejamos como se dá o produto entre os dois SDF's abaixo:



Note que a multiplicação é distributiva com relação a soma: $\mathcal{G}_f(\mathcal{G}_g+\mathcal{G}_h) = \mathcal{G}_f\mathcal{G}_g+\mathcal{G}_f\mathcal{G}_h$.

Produto e soma de SDF's são associativos. A soma é comutativa, e, olhando apenas para a estrutura do grafo podemos ver o produto como comutativo.

A operação de soma age em dois grafos colocando-os lado a lado como um único grafo. Já o produto transforma os conjuntos iniciais em um novo conjunto dado pelo produto cartesiano destes, e a nova função age coordenada a coordenada: (f, g).

Uma vez definidas tais operações, vejamos alguns casos particulares de produto entre grafos. Mais precisamente, como ocorre o produto entre ciclos, o produto entre árvores o produto entre árvore e ciclo. Mais adiante, veremos a onde se aplicam ambas as operações.

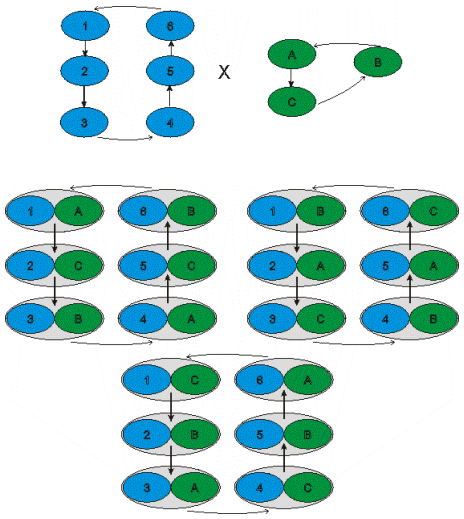
3.2.1 Produto entre ciclos

Proposição 3.7. (Produto de Ciclos) *Sejam C_r e C_s ciclos de comprimento r e s respectivamente, e sejam $m = \text{mmc}\,(r, s)$ e $n = \text{mdc}\,(r, s)$. O produto de C_r por C_s consiste de n ciclos disjuntos de comprimento m:*

$$C_rC_s = nC_m.$$

Prova: Seja $C_r = (X, f)$ e $C_s = (Y, g)$. Se $(f^t(x), g^t(y)) = (x, y)$, então t é um múltiplo comum de r e s. Portanto, todos os elementos de $X \times Y$ estão em um ciclo. Lembrando que o comprimento de um ciclo é o menor inteiro t tal que $f^t(v) = v$, e neste caso o inteiro com tal propriedade é $m = \text{mmc}\,(r, s)$, concluímos que todo elemento de $X \times Y$ está em um ciclo de comprimento m. Como o produto cartesiano tem exatamente rs elementos, e $rs = \text{mdc}\,(r, s)\text{mmc}\,(r, s) = mn$, temos exatos n ciclos de comprimento m. Obtemos, assim, o resultado desejado. □

Exemplo 3.8. Vejamos como se dá o produto entre os dois ciclos abaixo:



Exemplo 3.9. $C_{12} \cdot C_{27} = 3C_{108}$, pois $\text{mdc}\,(12, 27) = 3$ e $\text{mmc}\,(12, 27) = 108$.

3.2.2 Produto de SDF bijetivos

Veremos agora como multiplicar dois SDF's bijetivos. Para tal, vejamos antes como é a estrutura do grafo nesse caso.

Primeiramente, se C_r é um ciclo de comprimento r, então é bijetivo. Tal fato é verificado ao observarmos que cada elemento no ciclo tem exatamente um antecessor e, portanto, é injetivo. Como a aplicação se dá de um conjunto finito nele mesmo, temos uma bijeção.

Analogamente, seja (X, f) uma bijeção, e seja $x \in X$. A órbita de x, $O(x)$, é invariante por f. Quando restringimos f a $\mathcal{O}(x)$, obtemos um ciclo, já que cada elemento deve ter exatamente uma pré-imagem. Repetindo este procedimento para cada elemento de X, temos que todas as órbitas de elementos são ciclos. Portanto, a estrutura do grafo também é dada por um conjunto de ciclos: a soma destes.

Corolário 3.10. (Produto de SDF bijetivos) *O grafo de um SDF finito bijetivo consiste em uma soma de ciclos, e o produto de dois SDF bijetivos é resultado da soma de ciclos disjuntos, obtidos pela multiplicação dos ciclos de um deles pelos ciclos do outro.*

Prova:

Temos que $\mathcal{G}_f = C_{r_1} + \cdots + C_{r_l}$ e $\mathcal{G}_g = C_{s_1} + \cdots + C_{s_k}$. Basta utilizar a distributividade do produto em relação a soma, donde obtemos

$$\mathcal{G}_f \mathcal{G}_g = \sum_{i=1}^{l} \sum_{j=1}^{k} C_{r_i} C_{s_j}$$

e aplicar a proposição (3.7).

□

3.2.3 Produto entre árvores

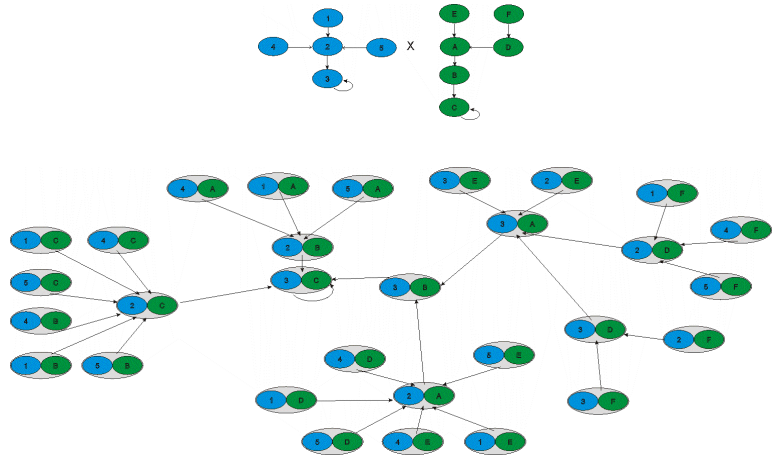
Vejamos, agora, como se dá o produto de duas árvores. Antes, precisamos introduzir o conceito de altura de um vértice da árvore. Se (X, f) é uma árvore com elemento terminal v, para cada elemento $x \in X$, definimos a *altura de* x, denotado $h(x)$, como o menor inteiro h tal que $f^h(x) = v$. Assim, a altura da árvore, denotada $h(X)$, é dada pelo máximo dentre a altura de seus elementos.

Proposição 3.11. (Produto de Árvores) *Sejam (X, f) e (Y, g) árvores de alturas m e n, respectivamente. Então, $(X \times Y, f \times g)$ é uma árvore de altura $h(X \times Y) = \max\{h(X), h(Y)\}$, que tem como elemento terminal o par formado pelos elementos terminais de X e Y. A altura de um elemento (x, y) é dada por $h(x, y) = \max\{h(x), h(y)\}$.*

Prova:

Sejam v_X e v_Y os pontos fixos de X e Y, respectivamente. Sejam $x \in X$, $y \in Y$ de alturas $h(x), h(y)$, respectivamente. Seja $h = \max\{h(x), h(y)\}$. Então, $(f \times g)^h(x, y) = (f^h(x), g^h(y)) = (v_X, v_Y)$. Ainda, h é o menor inteiro com tal propriedade. Isso mostra que $X \times Y$ é uma árvore, que a altura de (x, y) é dada por $\max\{h(x), h(y)\}$ e $X \times Y$ tem altura $\max\{h(X), h(Y)\}$. □

Exemplo 3.12. Calculemos o produto entre as duas árvores abaixo:



Resta, agora, saber quantos elementos de dada altura k existem no produto entre duas árvores. Este é o resultado da próxima proposição.

Proposição 3.13. *Sejam (X, f) e (Y, g) árvores de altura m e n respectivamente. Sejam a_i, b_i e c_i o número de elementos de altura i das árvores f, g e $f \times g$, respectivamente. Então,*

$$c_k = a_k \sum_{j=1}^{k-1} b_j + b_k \sum_{i=1}^{k-1} + a_k b_k$$

Prova:

Seja $(x, y) \in X \times Y$ um elemento de altura k. Pela proposição anterior, temos duas possibilidades: $h(x) = k$ ou $h(y) = k$. Se $h(x) = k$, então $h(y) \leq k$ (o que nos dá o primeiro somatório apresentado acima, e o último termo da soma). Analogamente, se $h(y) = k$, então $h(x) \leq k$. Um destes casos já foi considerado anteriormente ($h(x) = h(y) = k$) e os casos restantes nos dão o segundo somatório.

□

O próximo passo é identificar o que resulta do produto entre uma árvore e um ciclo.

3.2.4 Produto entre árvore e ciclo

Proposição 3.14. (Produto entre uma árvore e um ciclo). *Sejam (X, f) um ciclo de comprimento r e (Y, g) uma árvore de altura m. Então, $(X \times Y, f \times g)$ é um grafo conexo com ciclo terminal isomorfo a X e cada elemento do ciclo tem uma parte transiente que é isomorfa a Y.*

Prova:

Sejam v o ponto fixo de Y e x um elemento arbitrário de X. Temos $(f \times g)^s(x, v) = (f^s(x), g^s(v) = (f^s(x), v)$. Se $r = s$, $(f \times g)^s(x, v) = (x, v)$. Portanto, $X \times \{v\}$ é um ciclo de comprimento r. Para verificar que $X \times Y$ é conexo com ciclo terminal $X \times \{v\}$, basta observar que para cada elemento $y \in Y$, temos $(f \times g)^{h(y)}(x, y) = (f^{h(y)}(x), v)$. Para a parte restante da proposição, consideremos Y_{x_0} o conjunto formado pelos elementos (x, y) que tem como primeiro elemento de sua órbita no ciclo terminal o elemento (x_0, v). Outra forma de descrever Y_{x_0} é

$$Y_{x_0} = \{(f^{-h(y)}(x_0), y);\ y \in Y\}$$

onde $f^{-t} = (f^{-1})^t$. Definimos o SDF (Y_{x_0}, u) da seguinte forma: $u(x, y) = (f(x), g(y))$ se $y \neq v$ e $u(x_0, v) = (x_0, v)$. Definimos

$$\phi : Y \to Y_{x_0}, \quad \phi(y) = (f^{-h(y)}(x_0), y).$$

A função ϕ é injetora, uma vez que $\phi(y_1) = \phi(y_2)$ nos dá $(f^{-h(y_1)}(x_0), y_1) = (f^{-h(y_2)}(x_0), y_2)$ e portanto $y_1 = y_2$. A sobrejetividade de ϕ segue da caracterização dos elementos de Y_{x_0}: dado $(f^{-h(y)}(x_0), y)$ em Y_{x_0}, basta tomar $y \in Y$ e calcular $\phi(y)$. Portanto, ϕ é uma bijeção.

Mostremos que esta bijeção nos dá um isomorfismo entre os SDF (Y, g) e (Y_{x_0}, u). Se $y \neq v$, temos

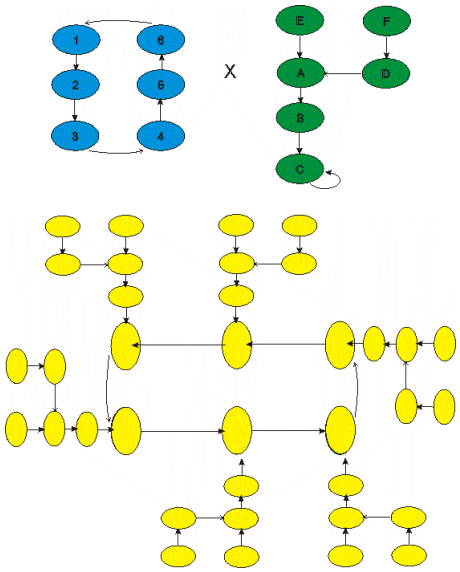
$$(u \circ \phi)(y) = u(f^{-h(y)}(x_0), y) = (f^{-h(y)+1}(x_0), g(y)) = \phi(g(y)) = (\phi \circ g)(y).$$

Usamos na terceira igualdade acima que $h(g(x)) = h(x) - 1$. Caso $y = v$, temos

$$(u \circ \phi)(v) = u(a, v) = (a, v) = \phi(v) = (\phi \circ g)(v).$$

Com isso, temos provada a proposição, pois acabamos de demonstrar que acoplado a cada vértice de $X \times \{v\}$ temos uma árvore, que é uma cópia da árvore Y.

Exemplo 3.15. Produto entre um ciclo de comprimento 6 e uma árvore de altura 4.



□

Aplicaremos os resultados apresentados nos capítulos anteriores, bem como as operações entre SDF's vistas nesta seção, com o intuito de descrever a estrutura do espaço de fase de um sistema dinâmico finito linear.

3.3 Sistemas dinâmicos finitos lineares

Um *Sistema Dinâmico Finito Linear* (SDFL) é um sistema dinâmico finito (E, T) em que E é um espaço vetorial de dimensão finita sobre $\mathbb{F}_q$ e $T : E \to E$ é uma aplicação linear.

Iniciaremos recorrendo ao fato de que dois espaços vetoriais de mesma dimensão (finita) sobre um dado corpo são isomorfos. Podemos então supor $E = \mathbb{F}_q^n$.

Temos por objetivo escrever T em uma base conveniente, a partir da qual determinaremos a estrutura de seu grafo sem a necessidade de calculá-lo efetivamente.

Iniciaremos nosso estudo dos sistemas dinâmicos finitos lineares por dois casos particulares: o caso em que (E, T) é nilpotente e seu índice de nilpotência coincide com a dimensão de E (chamado *nilpotente puro*), e em seguida, quando (E, T) é bijetivo com polinômios minimal e característico iguais, e da forma g^r, onde g é um polinômio irredutível sobre $\mathbb{F}_q$.

3.3.1 Grafo de um SDFL nilpotente puro

Iniciemos com (E, T) um SDFL nilpotente de índice de nilpotência s. Como $T^s(v) = 0, \forall v \in E$, concluímos que o grafo associado é uma árvore que tem como elemento terminal o vetor nulo. Assim, o grafo do SDFL nilpotente será uma árvore. Temos por objetivo determinar a estrutura de seu grafo: altura da árvore, quantos elementos de determinada altura e quantos pontos fontes.

Definição 3.16. (SDFL nilpotente puro) Um SDFL é dito *nilpotente puro* caso seja nilpotente, e o índice de nilpotência seja igual a dimensão de E.

Quando T é nilpotente puro existe uma base de E em relação à qual a matriz da transformação é nula, exceto na subdiagonal, na qual temos 1 em cada entrada.

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

Uma particularidade do SDFL nilpotente puro é que o núcleo da transformação linear tem dimensão exatamente 1. Este é o fato que mais nos interessa e que será peça chave para obter a estrutura de seu grafo. Abaixo segue o teorema.

Teorema 3.17. (Grafo de um SDFL nilpotente puro) *Seja $T : E \to E$ um SDFL nilpotente puro e seja n a dimensão de E sobre $\mathbb{F}_q$. Então, o grafo de T é uma árvore de altura n que tem como ponto terminal o vetor nulo. Cada vetor não-nulo do núcleo está em um galho de altura n. Todos os pontos de altura n são fontes, e todos os pontos de altura menor que n tem q pré-imagens. O número de eleemtnos de altura i é $h(i) = q^{i-1}(q-1)$.*

Prova:

Verificamos anteriormente que o grafo de um SDFL nilpotente é uma árvore que tem como ponto terminal o vetor nulo, em particular, se o SDFL é nilpotente puro. Portanto a estrutura do grafo como uma árvore já está garantida. Verifiquemos os outros resultados.

Como (E, T) é nilpotente puro, a dimensão do núcleo da transformação linear é 1. Recorrendo ao teorema do núcleo e da imagem para transformações lineares sobre espaços vetoriais de dimensão finita, obtemos que a dimensão da imagem é $n - 1$, e, portanto, q^{n-1} vetores possuem pré-imagem, e os $(q^n - q^{n-1})$ vetores restantes serão fontes. Fica a pergunta: qual a altura de cada um dos elementos que são fonte? Nosso objetivo é mostrar que é exatamente n.

Como o índice de nilpotência de T é n, temos $T^n(w) = 0, \forall w \in E$, e ainda que existe pelo menos um vetor $v \in E$ tal que $T^{n-1}(v) \neq 0$. Com isso, a altura da árvore é exatamente n, e cada elemento tem altura no máximo n, inclusive os elementos que são fonte.

Vamos agora contar o número de pré-imagens de cada elemento de E. Dado $u \in E$, caso este tenha alguma pré-imagem v então todos os elementos $v + w,\ w \in \mathrm{Nuc}\,(T)$ também são pré-imagem de u, e são suas únicas pré-imagens. Assim, ou um elemento não tem pré-imagem, ou tem exatamente q pré-imagens.

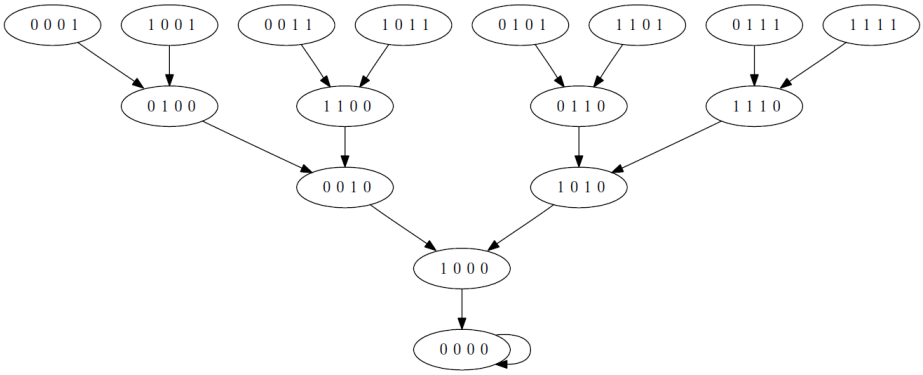
Para determinar a altura de cada fonte vamos contar todos os pontos que tenham altura menor ou igual a $n-1$. Denotemos por h_i o número de pontos que tenham altura i, lembrando que estes pontos podem, ou não, ter pré-imagens. Já vimos que o vetor nulo tem exatamente $q-1$ pré-imagens não-nulas ($\dim \mathrm{Nuc}\,(T) = 1$). Assim $h_1 = q-1$. Destes $q-1$ vetores, para cada elemento temos duas possibilidades: nenhuma pré-imagem ou exatamente q pré-imagens. Com isso, $h_2 \leq q(q-1)$. Por indução, concluímos que $h_i \leq q^{i-1}(q-1)$. Assim,

$$\begin{aligned} h_0 + h_1 + \cdots + h_{n-1} &\leq 1 + (q-1) + \cdots + q^{n-2}(q-1) \\ &= 1 + (q-1)(1 + q + \cdots + q^{n-2}) \\ &= 1 + (q-1)\frac{(q^{n-1}-1)}{q-1} = q^{n-1} \end{aligned}$$

Sabemos ainda que os elementos de altura n não possuem pré-imagem e que a dimensão da imagem é $n-1$. Portanto temos exatamente q^{n-1} elementos que não são fonte. Suponhamos, agora, que exista algum elemento de E que seja fonte e tenha altura menor que n. Assim, a desigualdade acima seria estrita, e teríamos menos que q^{n-1} elementos na imagem, o que é uma contradição. Com isso, verificamos que todas as fontes tem altura n, e que existem exatamente $q^{i-1}(q-1)$ elementos de altura i.

□

Exemplo 3.18. Considere o SDF $f : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ dado por $f(x_1, x_2, x_3, x_4) = (x_3, x_4, x_2, 0)$. Temos um SDF nilpotente puro, pois a transformação linear tem índice de nilpotência 4, que é a dimensão do espaço vetorial. Como garantido pelo teorema (3.17), cada elemento do grafo de altura 4 é fonte, todos os elementos que não são fonte são pré-imagem, e o número de elementos de altura i é $q^{i-1}(q-1)$.



3.3.2 Grafo de um SDFL bijetivo particular

Nosso próximo resultado descreve a estrutura de grafo de um SDFL bijetivo bem particular: em que o polinômio minimal e característico coincidem, e são potência de um polinômio irredutível sobre $\mathbb{F}_q$. Antes necessitamos apresentar algumas definições e resultados preliminares.

Definição 3.19. Seja E um espaço vetorial de dimensão finita e $T : E \to E$. Dado $v \in E$, definimos $m_{v,T}(x)$ como sendo o polinômio mônico de menor grau em $\mathbb{F}[x]$ tal que $m_{v,T}(T)(v) = 0$.

Proposição 3.20. *Seja $T : E \to E$ uma transformação linear, onde E é um espaço vetorial de dimensão finita sobre $\mathbb{K}$ e $m_T = f^m$, f irredutível sobre $\mathbb{F}$. Então, existe um vetor $v \in E$ tal que $m_T(x) = m_{v,T}(x)$ (ver [9, pág. 155]).*

Note que como E é finito, $v, T(v), \cdots, T^l(v), \cdots, l \in \mathbb{N}$ não podem ser todos distintos. Assim, existem $i, j \in \mathbb{N}$, $i < j$ tais que $T^i(v) = T^j(v)$. Consequentemente, $T^i(v - T^{j-i}(v)) = 0$. No caso em que T é uma bijeção, temos $T^{j-i}(v) = v$.

Definição 3.21. Definimos a ordem de um vetor $v \in E$ com respeito à uma transformação linear bijetiva $T : E \to E$ como o menor inteiro positivo r tal que $T^r(v) = v$, e será denotado por $\mathrm{ord}_T(v)$.

Vamos, agora, relacionar a ordem de um vetor $v \in E$ e a ordem de seu polinômio minimal com respeito à T.

Proposição 3.22. *Seja $T : E \to E$ uma transformação linear bijetiva, onde E é um espaço vetorial de dimensão finita sobre $\mathbb{F}$. Então,* $\mathrm{ord}_T(v) = \mathrm{ord}\,(m_{v,T})$.

Prova:

$s = \mathrm{ord}_T(v) \Leftrightarrow s$ é o menor inteiro tal que $T^s(v) = v \Leftrightarrow s$ é o menor inteiro tal que $(T^s - I)(v) = 0 \Leftrightarrow s$ é o menor inteiro positivo tal que $m_{v,T}$ divide $X^s - 1 \Leftrightarrow s = \mathrm{ord}\,(m_{v,T})$.

□

Teorema 3.23. ***(Elspas)*** *Seja $\mathbb{F}_q$ um corpo finito de característica p com q elementos. Seja E um espaço vetorial sobre $\mathbb{F}_q$ de dimensão n e seja $T : E \to E$ uma aplicação linear bijetiva. Suponha que o polinômio minimal, m_T e o polinômio característico de T sejam iguais. Se $m_T = f = g^s$, onde g é um polinômio irredutível de grau m, então a estrutura cíclica do grafo de T é dada por*

$$\mathcal{G}_T = 1 + \sum_{i=1}^{s} \frac{q^{mi} - q^{m(i-1)}}{r_i} C_{r_i},$$

onde 1 representa o ciclo correspondente ao vetor nulo, e C_{r_i} é um ciclo de comprimento $r_i = \operatorname{ord}(g^i)$.

Prova:

Lembremos que a dimensão de E coincide com o grau do polinômio característico, e, portanto, E tem dimensão ms, e possui q^{ms} elementos.

Faremos a demonstração por indução sobre s.

Para $s = 1$, temos $E = \operatorname{Nuc}(g(T))$, visto que $g(T)(v) = 0, \forall v \in E$. Seja $v \neq 0$. Como $m_{v,T}$ (o polinômio minimal de v com respeito a T) divide g e g é irredutível, temos $m_{v,T} = g$. Pela proposição (3.22), temos $\operatorname{ord}(g) = \operatorname{ord}_T(v) = r_1$. Assim, cada vetor não nulo pertence a um ciclo de comprimento r_1. Assim, temos exatamente $(q^m - 1)/r_1$ ciclos de comprimento r_1, e a estrutura do grafo é dada por

$$\mathcal{G}_T = 1 + \frac{q^m - 1}{r_1} C_{r_1}$$

Portanto, a fórmula é válida para $s = 1$.

Suponhamos agora que o resultado seja válido para $s = n$ e provemos que é valido para $s = n + 1$. Suponhamos $f = g^{n+1}$ e seja $K_i = \operatorname{Nuc}(g^i(T)), i = 1, \cdots, n + 1$. Note que $K_i \subset K_{i+1}$, e que a inclusão contrária não é válida. É claro que $K_n \nsubseteq k_{n+1}$, pois como o polinômio minimal é g^{n+1} existe $v \in E$, $v \neq 0$, tal que $g^n(T)(v) \neq 0$ e, é claro, $g^{n+1}(T)(v) = 0$. Daí, temos que $K_{n-1} \nsubseteq K_n$, já que $g^n(T)(g(T)(v)) = 0$ e $g^{n-1}(T)(g(T)(v)) \neq 0$. De modo geral, $K_{n-i} \nsubseteq K_{n-i+1}$, pois $g^{n-i+1}(g^i(T)(v)) = 0$ e $g^{n-i}(g^i(T)(v)) \neq 0$, $\forall i = 0, 1, \cdots, n - 1$.

Vejamos que K_i é invariante sobre T, para $i = 1, \cdots, n - 1$. Seja $i \in \{1, \cdots, n - 1\}$. Dado $v \in K_i$, temos $g^i(T)(T(v)) = T(g^i(v)) = T(0) = 0$. Logo, $T(v) \in K_i$. Então, podemos falar nos polinômios característico e minimal de T restrito a K_i.

É claro que para cada $i \in \{1, \cdots, n - 1\}$, o polinômio minimal de T restrito a K_i divide $g^i(x)$, logo é da forma $1 \leq l \leq i$. Como $g(x)$ é irredutível, temos que o polinômio característico da restrição de T a K_i também é da forma g^r, com $r \geq l$, uma vez que o

polinômio minimal divide o polinômio característico (Teorema de Cayley-Hamilton, [10, seção 7.2]). Em particular, se $i = n$ o polinômio característico da restrição de T a K_i é g^r, $r \geq n$, mas se $r = n + 1$ então K_n terá a mesma dimensão de $E = K_{n+1}$, o que é um absurdo. Logo, esse polinômio característico é g^n. Dam mesma forma, o polinômio característico de T restrito a K_{n-1} é da forma g^r, com $r \geq n-1$, mas se $r = n$ então $\dim K_{n-1} = \dim K_n$, o que é um absurdo. Continuando, vemos que o polinômio característico de T restrito a K_i é g^i, $i = 1, 2, \cdots, n+1$, portanto coincide com o polinômio característico.

Assim, por hipótese de indução, a estrutura cíclica dos vetores em K_n é conhecida. Seja v um elemento de $K_{n+1} \setminus K_n$. Então, $v \neq 0$ e $m_{v,T}$ divide g^{n+1} e não divide g^n, pois do contrário $g^n(T)(v) = 0$ e $v \in K_n$. Como $m_{v,T}$ divide m_T temos $m_{v,T} = g^{m+1}$. Assim, $\operatorname{ord}_T(v) = \operatorname{ord}(g^{n+1}) = r_{n+1}$ e os $q^{m(n+1)} - q^{mn}$ elementos de $K_{n+1} \setminus K_n$ estão divididos em $(q^{m(n+1)} - q^{mn})/r_{n+1}$ ciclos de comprimento r_{n+1}, e a estrutura cíciclica é dada por

$$\mathcal{G}_T = 1 + \frac{q^{m(n+1)} - q^{mn}}{r_{n+1}} C_{r_{n+1}} + \sum_{i=1}^{n} \frac{q^{mi} - q^{m(i-1)}}{r_i} C_{r_i}$$

□

Para encontrarmos a ordem dos polinômios g^i é suficiente que calculemos a ordem do polinômio g e, em seguida, podemos recorrer ao teorema (1.20).

A notação + usada no teorema (3.23) remete a operação de soma de grafos.

3.3.3 Dinâmica de um SDFL arbitrário

Mostraremos nesta seção que os teoremas (3.17) e (3.23) são suficientes para obtermos o gráfico de um SDFL qualquer. A base para a construção que será feita é dada pelo teorema da decomposição primária:

Teorema 3.24. (Teorema da Decomposição Primária) *Seja E um $\mathbb{F}$-espaço vetorial de dimensão finita, e $T : E \to E$ uma transformação linear. Seja p o polinômio minimal de T,*

$$p = p_0^{r_0} p_1^{r_1} \cdots p_k^{r_k}$$

onde cada p_i é um polinômio mônico irredutível sobre $\mathbb{F}_q$ e r_i um inteiro positivo. Seja $W_i = \operatorname{Nuc} p_i(T)^{r_i}, i = 1, \cdots, k$. Então,

(i) $V = W_0 \oplus \cdots \oplus W_k$;

(ii) cada W_i é $T-$invariante;

(iii) se T_i é a restrição de T a W_i, então o polinômio minimal de T_i é $p_i^{r_i}$.

(ver [10, pág. 220]).

O teorema acima nos mostra que é possível decompor o espaço vetorial E como soma direta de espaços vetoriais $T-$invariantes. Mostraremos que o grafo será obtido como o produto dos grafos associados a cada somando direto.

Proposição 3.25. *Seja p um polinômio que anula uma transformação linear $T : E \to E$ e suponha que p se fatore como $p = p_1 p_2$, com p_1 e p_2 primos entre si. Então, o espaço E pode ser escrito como uma soma direta*

$$E = E_1 \oplus E_2$$

com E_1 e E_2 subespaços $T-$invariantes, e cada p_i é um polinômio anulador da restrição de T a E_i.

Ainda, se $p = p_T$, cada p_i é o polinômio característico da restrição de T a E_i.

Seja (E, T) um SDFL e seja p seu polinômio característico. Podemos fatorar o polinômio p da seguinte forma:

$$p(x) = x^r q(x), \text{ com } q(0) \neq 0.$$

A decomposição feita se encaixa na decomposição apresentada na proposição (3.25). Assim, existem dois subespaços $T-$invariantes E_n e E_b, correspondentes respectivamente a x^r e q. O polinômio característico de T_n (T restrita a E_n) é x^r, e portanto T_n é uma aplicação nilpotente, que chamaremos parte nilpotente associada ao SDFL. Por outro lado, T_b (T restrita a E_b) tem polinômio característico q, e portanto T_b não tem 0 como autovalor, daí é um aplicação bijetiva, que será chamada parte bijetiva associada ao SDFL.

Nosso objetivo será construir o grafo associado às partes nilpotente e bijetiva, respectivamente, e a partir destes grafos, resgatamos o grafo de T por meio do produto entre os grafos, o que é possível pela seguinte proposição:

Proposição 3.26. *Seja (E, T) um SDFL e suponha que $E = E_1 \oplus E_2$, com E_1 e E_2 $T-$invariantes. Seja T_i a restrição de T a $E_i, i = 1, 2$. Então, (E_i, T_i) é um SDFL e*

$$(E, T) = (E_1, T_1) \times (E_2, T_2).$$

Prova:

Devemos provar apenas que $(E, T) = (E_1, T_1) \times (E_2, T_2)$, uma vez que a restrição de uma transformação linear a um subespaço invariante é uma transformação linear. Mostraremos que existe uma bijeção entre os vértices dos grafos (E, T) e $(E_1, T_1) \times (E_2, T_2)$, bem como das formas como estes estão conectados.

Seja $v \in E$. Como $E = E_1 \oplus E_2$, podemos escrever v de maneira única como $v = v_1 + v_2$, $v_i \in E_i$, $i = 1, 2$. Isso nos dá a correspondência bijetiva entre os vértices de ambos os grafos. Podemos, assim, associar E e $E_1 \times E_2$ de maneira natural, associando $v_1 + v_2$ a (v_1, v_2). Ainda, $T(v) = T(v_1) + T(v_2) = T_1(v_1) + T_2(v_2)$, a ligação entre os vértices ocorre, também, via bijeção, o que implica em $T = T_1 \times T_2$.

$$\begin{array}{c} (v_1, v_2) \\ \downarrow{\scriptstyle (T_1 \times T_2)} \\ (T_1(v_1), T_2(v_2)) \\ \downarrow{\scriptstyle (T_1 \times T_2)} \\ \vdots \end{array} \qquad \leftrightsquigarrow \qquad \begin{array}{c} v = v_1 + v_2 \\ \downarrow{\scriptstyle f} \\ f(v) = f_1(v_1) + f_2(v_2) \\ \downarrow{\scriptstyle f} \\ \vdots \end{array}$$

□

Podemos enunciar a proposição anterior de maneira equivalente, como

Proposição 3.27. *Seja $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ um SDFL representado matricialmente por*

$$A = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$$

onde B e C são matrizes quadradas. Então, o espaço de fase de A é isomorfo ao produto dos espaços de fase de B e C.

Com isso, podemos reduzir o estudo da dinâmica de (E, T) ao estudo de seus subespaços $T-$invariantes. Focaremos em dois subespaços invariantes particulares: os associados às partes bijetiva e nilpotente da transformação linear.

Já vimos anteriormente que o grafo associado à parte nilpotente consiste em uma árvore, tendo como ponto final o vetor nulo. Quanto à parte bijetiva, esta será composta por ciclos disjuntos.

A partir das proposições (3.25) e (3.26), podemos enunciar um dos principais teoremas que permitirão construir o grafo de um SDFL.

Teorema 3.28. *Seja (E, T) um SDFL. O grafo de E é dado pelo produto entre uma árvore (que corresponde a parte nilpotente de T) e uma soma de ciclos (correspondentes a parte bijetiva de T).*

Resta-nos, agora, encontrar meios para construir o grafo das partes nilpotente e bijetivas.

Para o caso nilpotente geral, recorremos ao seguinte teorema:

Teorema 3.29. *Seja $T : V \to V$ um operador linear nilpotente com índice de nilpotência $m \geq 1$, onde V é um espaço vetorial de dimensão finita sobre $\mathbb{F}$. Então, existem números*

positivos $t, m_1, \cdots, m_t$ *e vetores* $v_1, \cdots, v_t \in V$ *tais que*

(a) $m = m_1 \geq m_2 \geq \cdots \geq m_t$.

(b) o conjunto $\mathcal{B} = \{v_1, T(v_1), \cdots T^{m_1-1}(v_1), \cdots, v_t, T(v_t), \cdots, T^{m_t-1}(v_t)\}$ *é uma base de* V.

(c) $T^{m_i}(v_i) = 0$.

(ver [5, pág. 164]).

O teorema acima nos permite escrever a matriz $[T]_{\mathcal{B}}$ em blocos:

$$[T]_{\mathcal{B}} = \begin{pmatrix} J_{m_1}(0) & 0 & \cdots & 0 \\ 0 & J_{m_2}(0) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{m_t}(0) \end{pmatrix}$$

onde os 0's indicam matrizes nulas, e para cada $i = 1, \cdots, t$, $J_{m_i}(0)$ representa o bloco de Jordan $m_i \times m_i$ em 0, ou seja, a matriz

$$J_{m_i}(0) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

Para cada bloco de Jordan, temos um sistema nilpotente puro, cujo grafo pode ser obtido pelo teorema (3.17).

A decomposição em blocos está associada a uma decomposição em soma direta de subespaços, o que combinado com a proposição (3.25) nos dá o seguinte teorema:

Teorema 3.30. (Grafo de uma aplicação nilpotente) *O grafo de uma aplicação nilpotente é o produto de árvores de alturas correspondentes as dimensões dos blocos de Jordan associados a matriz obtida do teorema* (3.29).

A construção apresentada, porém, não nos permite dizer quem são os inteiros m_i. Tais inteiros, como veremos mais adiante, podem ser obtivos a partir dos fatores invariantes de T.

Devemos ainda encontrar meios para descrever a dinâmica de um SDFL bijetivo arbitrário.

Seja (E, T) um SDFL bijetivo. Como já mencionado anteriormente, o grafo associado é formado por um conjunto de ciclos disjuntos. O ciclo do qual o vetor nulo faz parte é formado apenas por ele (e denotado 1), visto que o único elemento que satisfaz $f(x) = 0$

é o próprio vetor nulo. Recorremos novamente a fatoração do polinômio característico de T. Como um polinômio em $\mathbb{F}[x]$ fatora-se produto de potências de polinômios irredutíveis e relativamente primos entre si, podemos escrever

$$p_T = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}.$$

Podemos, assim, obter uma base em relação à qual a matriz é formada de blocos diagonais, correspondentes a soma direta. Torna-se suficiente, então, encontrar a estrutura cíclica do grafo associado um destes subespaços $T-$invariantes, e recorrer a proposição (3.26).

Para isso, faremos uma nova decomposição em cada um dos blocos obtidos, em subblocos nos quais o polinômio minimal e característico coincidem, e serão da forma $p_i^{t_j}, t_j \leq r_i, i = 1, \cdots, s$. Isso é possível por meio da forma racional. Os grafos associados aos subblocos tem sua estrutura dada pelo teorema (3.23). Portanto, o seguinte teorema nos dá a estrutura do grafo de um SDFL bijetivo qualquer:

Teorema 3.31. (Grafo de um SDFL bijetivo) *Seja (E, T) um SDFL bijetivo. Suponha que o polinômio característico de T é p_T e este se fatora em potências de polinômios irredutíveis, da seguinte forma*

$$p_T = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}.$$

Então o grafo de T é o produto dos grafos associados a cada $p_i^{r_i}$ (recorrendo ao teorema (3.24)).

Observe que como T é bijetivo, $p_i(0) \neq 0, i = 1, \cdots, s$.

No ponto atual, ainda não podemos identificar a estrutura do grafo do nosso SDFL. Isso porque desconhecemos a estrutura dos grafos associados a cada $p_i^{r_i}$: o resultado do qual dispomos para grafos bijetivos exige que polinômio minimal e característico sejam iguais, e não estamos em tais condições. Contudo, é apenas uma questão de reordenar as informações obtidas, de forma a poder usar o teorema (3.23). Para tal, utilizemos então a forma racional da matriz e o teorema do resto chinês.

O que visamos é uma decomposição em que cada bloco esteja nas condições do teorema (3.23). Pela proposição (2.18), sabemos que se o bloco é a matriz companheira de algum polinômio irredutivel, então as condições estão satisfeitas, exceto pelo fato de que devem ser potência de um irredutível.

Recorremos à forma racional. Se A é a matriz que representa T em relação a uma base qualquer, sejam $a_1, \cdots, a_m$ tais que $a_1 \mid a_2 \mid \cdots \mid a_m$. Os elementos $a_1, \cdots, a_m$ são não constantes e mônicos.

Do capítulo anterior, temos que

$$E \cong \frac{\mathbb{F}_q[x]}{(a_1(x))} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{(a_m(x))}.$$

Fatorado como produto de polinômios irredutíveis, o polinômio característico p_T é escrito da forma

$$p(x) = x^s p_1(x)^{t_1} \cdots p_e(x)^{t_e}.$$

Assim, os fatores invariantes podem ser escritos como

$$\begin{aligned} a_1(x) &= x^{s_1} p_1(x)^{t_{11}} \cdots p_e(x)^{t_{1e}} \\ &\vdots \\ a_r(x) &= x^{s_r} p_1(x)^{t_{r1}} \cdots p_e(x)^{t_{re}} \end{aligned}$$

onde

$$0 \leq s_i \leq s_{i+1}, \;\; 0 \leq t_{ij} \leq t_{(i+1)j}$$

o que decorre da relação de divisibilidade dos fatores invariantes.

Os inteiros não nulos dentre $s_1, \cdots, s_r$ são aqueles que aparecem no teorema (3.29).

Recorrendo ao teorema chinês do resto, decompomos E como a soma direta

$$E \approx \underbrace{\frac{\mathbb{F}_q[x]}{(x^{s_1})} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{(x^{s_r})}}_{\text{parte nilpotente}} \oplus \underbrace{\frac{\mathbb{F}_q[x]}{(p_1^{t_{11}})} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{(p_1^{t_{r1}})} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{(p_e^{t_{1e}})} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{(p_e^{t_{re}})}}_{\text{parte bijetiva}}.$$

Temos, por fim, matrizes quadradas $B_1, \cdots, B_r$, $A_{11}, \ldots, A_{re}$ tais que o polinômio minimal e característico de B_i é x^{s_i} e o polinômio minimal e característico de A_{ij} é $p_i^{t_{ij}}$.

As matrizes B_i são exatamente aquelas descritas no teorema (3.29), então, agora, conhecemos efetivamente os valores de m_i.

A decomposição acima nos permite escrever uma matriz para T da seguinte forma:

$$J = \begin{bmatrix} B_1 & & & & & & \\ & \ddots & & & & & 0 \\ & & B_r & & & & \\ & & & A_{11} & & & \\ & & & & \ddots & & \\ & 0 & & & & & \\ & & & & & & A_{re} \end{bmatrix}$$

Aqui, temos que o SDFL associado a cada B_i é nilpotente puro, enquanto SDFL associado a cada A_{ij} satisfaz as hipóteses do teorema de Elspas. Assim, basta aplicarmos os teoremas (3.17) e (3.23) em cada um deles. Em seguida, efetuamos o produto entre as árvores, segundo descrito na proposição (3.11). Para os ciclos, efetuamos o produto

segundo a proposição (3.7). Para finalizar, multiplicamos a árvore obtida pela soma de ciclos, usando a distributividade, e a proposição (3.14).

Deste modo, temos a estrutura do grafo associado a um SDFL descrita por completo.

Exemplo 3.32. Consideremos em $\mathbb{F}_5^4$ o SDFL dado pela matriz 4×4

$$A = \begin{pmatrix} -2 & 2 & 1 & 0 \\ -1 & 0 & 1 & 2 \\ -2 & -1 & 0 & -1 \\ -2 & 2 & 1 & 0 \end{pmatrix}.$$

Vamos determinar a estrutura do grafo do SDFL recorrendo ao algoritmo apresentado no apêndice B, que reproduz os resultados apresentados no texto .

A tem como único fator invariante o polinômio

$$x^4 + 2x^3 + 2x^2 - x$$

e divisores elementares

$$x,\ x+2 \text{ e } \mathrm{x}^2 + 2.$$

A parte nilpotente associada ao grafo é correspondente ao fator invariante x e dada pelo vértice e quatro vetores de altura 1.

Identifiquemos agora a parte bijetiva associada ao grafo.

Iniciamos identificando a ordem dos divisores elementares.

$$x + 2 \text{ tem ordem } 4,$$
$$x^2 + 2 \text{ tem ordem } 8.$$

Aplicando o teorema de Elspas, obtemos:

Estrutura cíclica associada a $x + 2$:

$$C_1 + C_4.$$

Estrutura cíclica associada a $x^2 + 2$:

$$C_1 + 3C_8.$$

Efetuando o produto entre as estruturas cíclicas associadas a cada divisor elementar, obtemos

$$C_1 + C_4 + 15C_8.$$

O grafo do SDFL é dado pelo produto entre parte nilpotente e bijetiva, que pode ser calculado através da proposição (3.14).

Exemplo 3.33. Consideremos em $\mathbb{F}_7^{10}$ o SDFL dado pela matriz 10×10

$$A = \begin{pmatrix} 1 & 2 & 1 & 0 & -1 & -2 & -3 & 3 & 2 & -3 \\ -2 & -1 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & -2 \\ -3 & 3 & 2 & 3 & -3 & -2 & -1 & 0 & 1 & 2 \\ 1 & 0 & -1 & -2 & -3 & 3 & 2 & 3 & -3 & -1 \\ 0 & 1 & 2 & 1 & 0 & -1 & -2 & -3 & 3 & 2 \\ 3 & -3 & -2 & -1 & 0 & 1 & 2 & 0 & 2 & 1 \\ 0 & -2 & -3 & 3 & 2 & 3 & -3 & -2 & -1 & 0 \\ 1 & 2 & 1 & 0 & -1 & -2 & -3 & 3 & 2 & 3 \\ -3 & -1 & 0 & 1 & 0 & -1 & 0 & 1 & 2 & 0 \\ 1 & -1 & -2 & -1 & 0 & 1 & 2 & 1 & 0 & 0 \end{pmatrix}.$$

Façamos como no exemplo anterior.

A tem como único fator invariante o polinômio

$$x^{10} - 3x^9 - 2x^8 - 3x^7 + x^6 + 2x^5 - 2x^3 + 2x^2 - 3x + 1$$

e divisores elementares

$$x^5 + 2x^4 - 2x^3 - 3x^2 + x + 3,\ x^3 + x^2 - 2x + 3 \text{ e } \mathrm{x}^2 + \mathrm{x} - 3.$$

O grafo não possui parte nilpotente, uma vez que nenhuma potência de x é um divisor elementar.

Identifiquemos então a estrutura da parte bijetiva, que corresponderá a todo o grafo.

Iniciamos identificando a ordem dos divisores elementares.

$$x^5 + 2x^4 - 2x^3 - 3x^2 + x + 3 \text{ tem ordem } 8403,$$
$$x^3 + x^2 - 2x + 3 \text{ tem ordem } 171,$$
$$x^2 + x - 3 \text{ tem ordem } 24.$$

Aplicando o teorema de Elspas, obtemos:

Estrutura cíclica associada a $x^5 + 2x^4 - 2x^3 - 3x^2 + x + 3$:

$$C_1 + 2C_{8403}.$$

Estrutura cíclica associada a $x^3 + x^2 - 2x + 3$:

$$C_1 + 2C_{171}.$$

Estrutura cíclica associada a $x^2 + x - 3$:

$$C_1 + 2C_{24}.$$

Efetuando o produto entre as estruturas cíclicas associadas a cada divisor elementar, obtemos

$$C_1 + 2C_{24} + 2C_{171} + 12C_{1368} + 2C_{8304} + 12C_{67224} + 12C_{478971} + 72C_{3831768}$$

que é a estrutura do grafo associado ao grafo do nosso SDFL.

Exemplo 3.34. Consideremos em $\mathbb{F}_2^{25}$ o SDFL dado pela matriz 25×25

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

A tem como único fator invariante o polinômio

$$x^{25} + x^{23} + x^{22} + x^{20} + x^{16} + x^{15} + x^{13} + x^{12} + x^{11} + x^8 + x$$

e divisores elementares

$$x,\ x^{18}+x^{17}+x^{15}+x^{13}+x^{12}+x^{11}+x^9+x^7+x^5+x^4+x^3+x+1 \text{ e } \mathrm{x}^6+\mathrm{x}^5+\mathrm{x}^2+\mathrm{x}+1.$$

A parte nilpotente associada ao grafo é correspondente ao fator invariante x e dada pelo vértice e um vetor de altura 1.

Identifiquemos agora a parte bijetiva associada ao grafo.

Iniciamos identificando a ordem dos divisores elementares.

$$x^6+x^5+x^2+x+1 \text{ tem ordem } 63,$$
$$x^{18}+x^{17}+x^{15}+x^{13}+x^{12}+x^{11}+x^9+x^7+x^5+x^4+x^3+x+1 \text{ tem ordem } 13797.$$

Aplicando o teorema de Elspas, obtemos:

Estrutura cíclica associada a $x^6+x^5+x^2+x+1$:

$$C_1+C_{63}.$$

Estrutura cíclica associada a $x^{18}+x^{17}+x^{15}+x^{13}+x^{12}+x^{11}+x^9+x^7+x^5+x^4+x^3+x+1$:

$$C_1+19C_{13797}.$$

Efetuando o produto entre as estruturas cíclicas associadas a cada divisor elementar, obtemos

$$C_1+C_{63}+1216C_{13797}.$$

O grafo do SDFL é dado pelo produto entre parte nilpotente e bijetiva, que pode ser calculado através da proposição (3.14).

Exemplo 3.35. Consideremos em $\mathbb{F}_2^{15}$ o SDFL dado pela matriz 15×15

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

A tem como único fator invariante o polinômio

$$x^{15} + x^{12} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^2$$

e divisores elementares

$$x^2,\ x+1 \text{ e } \mathrm{x}^{12} + \mathrm{x}^{11} + \mathrm{x}^{10} + \mathrm{x}^7 + \mathrm{x}^6 + \mathrm{x}^4 + \mathrm{x}^2 + \mathrm{x} + 1.$$

A parte nilpotente associada ao grafo é correspondente ao fator invariante x^2 e dada pelo vértice, um vetor de altura 1 e dois vetores de altura 2.

Identifiquemos agora a parte bijetiva associada ao grafo.

Iniciamos identificando a ordem dos divisores elementares.

$$x + 1 \text{ tem ordem } 1,$$
$$x^{12} + x^{11} + x^{10} + x^7 + x^6 + x^4 + x^2 + x + 1 \text{ tem ordem } 315.$$

Aplicando o teorema de Elspas, obtemos:

Estrutura cíclica associada a $x + 1$:

$$2C_1$$

Estrutura cíclica associada a $x^{12} + x^{11} + x^{10} + x^7 + x^6 + x^4 + x^2 + x + 1$:

$$C_1 + 13C_{315}.$$

Efetuando o produto entre as estruturas cíclicas associadas a cada divisor elementar, obtemos

$$2C_1 + 26C_{315}.$$

O grafo do SDFL é dado pelo produto entre parte nilpotente e bijetiva, que pode ser calculado através da proposição (3.14).

Apêndice A

Cálculo da ordem de um polinômio em $\mathbb{F}_p$ no Singular

Abaixo, defina p (característica do corpo) e f (polinômio cuja ordem se deseja calcular). Tomamos aqui $p = 2$ e $f = x^7 + 3x^5 + x^4$.

```
int p = 2;
ring r = p,x,dp;
poly f = x7 + 3*x5 + x4;

int i = 1;
poly g = f;
while(gcd(g,x)<>1){g = g/x;}

int i = 1;
poly h = x^i - 1;
while(gcd(g,h)<>g){i++; h = x^i - 1;}

string ordem = "a ordem de f e";

ordem, i;
```

Apêndice B

Cálculo da estrutura do grafo de um SDFL no Singular

Abaixo, defina p (característica do corpo), n (dimensão do espaço vetorial, ou número de linhas da matriz associada) e a matriz m correspondente ao sistema dinâmico finito linear cujo grafo dejamos conhecer.

Tomamos aqui $p = 2$, $n = 10$ e $m = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.

```
proc min
 {def s=size(#);
 def m=#[1];for(int i=2;i<=s;i++){if(#[i]<m){m=#[i];}}
return(m);}
    //procedimento para determinar mínimo entre n elementos

proc max//intvec or list or whatever?
 {def s=size(#);
 def m=#[1];for(int i=2;i<=s;i++){if(#[i]>m){m=#[i];}}
return(m);}
    //procedimento para determinar máximo entre n elementos

//-------------------------------------------------------------------------
```

```
int p = 2;
    //característica do corpo
int q = p;
    // num d elementos no corpo
int n = 10;
    //tamanho da matriz; dimensão do espaço vetorial
ring r = p,x,dp;
    //definindo o anel...
LIB "jacobson.lib";
LIB "control.lib";
    //carregando biblioteca que permite usar a forma normal de smith

//-------------------------------------------------------------------------

    //m é a matriz associada ao sistema dinâmico finito linear
matrix m[n][n] =
0,0,0,0,1,1,0,0,0,1,
0,1,0,0,1,0,0,0,1,0,
0,1,1,0,1,0,0,1,0,0,
0,0,1,0,0,0,0,0,1,1,
0,0,0,0,1,1,1,0,0,0,
1,0,0,1,0,0,0,1,0,1,
1,0,0,1,0,1,0,1,0,1,
1,0,1,0,0,1,0,1,0,1,
1,0,1,1,1,0,1,0,1,0,
1,0,1,1,1,1,0,1,0,1;
matrix M =  -m + x;
poly f = det(M);

//-------------------------------------------------------------------------

//1º. Cálculo da ordem dos polinômios irredutíveis que dividem det(M).

int n1 = size(factorize(f)[1]);

list pol = factorize(f)[1];

list ordens;
```

```
    //lista onde serão armazenados polinômio/ordem.
    //ordens[i][2] é a ordem do polinômio ordem[i][1]

poly u;

ordens[1] = list(1,1);

int i = 2;

string calc = "calculando ordem...";

while(i<=n1){
u = pol[1][i];
if(u<>x){
int j = 1;
poly g = x - 1;
while(gcd(u,g)<>u){j++; g = x^j - 1;calc;}
ordens[i] = list(u,j);}
else{ordens[i] = list(u,0);}
i++;};

//--------------------------------------------------------------------------

matrix SM = divideUnits(smith(M));
    //forma de Smith da matriz M. Não necessariamente com
    //as primeiras entradas 1 e as ultimas polinômios.

//--------------------------------------------------------------------------

//2°. Vamos determinar a estrutura da parte nilpotente do SDF.

//2.1. Determinar a altura de sistemas nilpotentes puros da decomposição.

list arvores;
    // arvores[k][2] dá a altura do grafo nilpotente puro associado ao fator
    // invariante arvores[k][1]. Os fatores invariantes que não aparecem na
    // lista nos dão grafos bijetivos, portanto sem árvores na decomposição.

int i = 1;
```

```
while(i<=n)
{u = SM[i][i];
if(gcd(u,x)<>1&u<>1)
{int j = 1;
int k = 1;
while(gcd(u,x^j) == x^j){j++;};
arvores[k] = list (u,j-1);k++};
i++;};

//-------------------------------------------------------------------------


    // 2.2 Determinar a estrutura de cada árvore nil pura. Quantos elementos
    // de cada altura teremos em cada árvore.

list arvores2;
    // em arvores[i][j] temos quantos elementos de altura j estão na i-esima
    // árvore nilpotente pura.

int i = 1;

while (i<= size(arvores))
{int j = 1;
list auxiliar;
while(j<=arvores[i][2])
{auxiliar[j] = (q - 1)*q^(j - 1);
j++;k++;}
arvores2[i] = auxiliar;
i++;};

//-------------------------------------------------------------------------

//2.3 Efetuar o produto entre as árvores nilpotentes puras.

list nilpotente;
    // estrutura do grafo associado a parte nilpotente. nilpotente[i]
    // informa quantos elementos de altura i temos no produto.
```

```
list auxiliar;
auxiliar = arvores2[1];
int i = 2;
nilpotente = auxiliar;

while(i<=size(arvores2))
{int j = 1;
while(j<=max(size(arvores2[i]),size(auxiliar)))
{int a = 1;
 int b = 1;
int i1 = 1;

while(i1<min(j,size(auxiliar)))
{a = a + auxiliar[i1]; i1++;};

int i1 = 1;
    //usar i1 para falar quantos elementos de altura i1 temos na árvore auxiliar.
while(i1<min(j,size(arvores2[i])))
{b = b + arvores2[i][i1]; i1++;};

int n1 = 1; //total de elementos em auxiliar
int i2 = 1;

while(i2 <= size(auxiliar))
{n1 = n1 + auxiliar[i2]; i2++;}
int n2 = 1;
int i2 = 1;
while(i2<=size(arvores2[i]))
{n2 = n2 + arvores2[i][i2];i2++;}

//contar o número de elementos de cada altura, na árvore produto...

if(j<=size(arvores2[i])&j<=size(auxiliar)){
nilpotente[j] = auxiliar[j]*b + arvores2[i][j]*a + auxiliar[j]*arvores2[i][j];}
else{
if(j>size(arvores2[i])&j<=size(auxiliar)){nilpotente[j] = n2*auxiliar[j];}
else{nilpotente[j] = n1*arvores2[i][j];}
};j++;};
```

```
auxiliar = nilpotente;
i++;};

//--------------------------------------------------------------------------

// 3°. Estrutura de grafo da parte bijetiva.

// 3.1 - Identificar todos os divisores elementares de A.

list divisoreselementares;
    // divisoreselementares[i][1] é o polinômio irredutível, que aparece
    // com grau divisoreselementares[i][2] como divisor elementar.

list auxiliar;

int i = 1;
int k = 1;

while(i<=n)
{u = SM[i][i];
if(u<>1)
{auxiliar = factorize(u);
int j = 2;
while(j<=size(auxiliar[1]))
{if(auxiliar[1][j]<>x)
{divisoreselementares[k] = list(auxiliar[1][j],auxiliar[2][j]);
k++;};
j++;}
};
i++;}

//--------------------------------------------------------------------------

//3.2 - Buscar a ordem de divisoreselementares[i][1], na lista ordens.

list ciclosde;
list grau;

int i = 1;
```

```
while(i<=size(divisoreselementares))
{u = divisoreselementares[i][1];
int d = 1;
while(u<>ordens[d][1]){d++;};

//---------------------------------------------------------------------------

//3.3 - aplicar o teorema 1.20

int e = ordens[d][2];

int b = 1;
    // calcular a ordem de u^j, e saber quantos ciclos deste tamanho temos

list auxiliar;

while(b<=divisoreselementares[i][2])
{int t;
int a = p^t;
while(a<b){t++;a=p^t;}
auxiliar[b] = e*p^t; //e*p^t é a ordem de u^b;
b++;};
ciclosde[i] = auxiliar;
grau[i] = deg(u);
i++;}

//---------------------------------------------------------------------------

    //3.4 - aplicar o teorema 3.21 (elspas)

list auxelspas;
    // contar o número de ciclos para usar elspas

int i = 1;

while(i<=size(ciclosde))
{list auxiliar;
int j = 1;
```

```
while(j<=size(ciclosde[i]))
{auxiliar[j] = (q^(grau[i]*j) - q^(grau[i]*(j - 1)))/ciclosde[i][j];
j++;}
auxelspas[i] = auxiliar;
i++;};

//---------------------------------------------------------------------------

    // 3.5 - Acrescentar o ciclo correspondente ao vetor nulo as listas.

list basetamanho = ciclosde;

int i = 1;
while(i<=size(ciclosde))
{int j = size(ciclosde[i]);
basetamanho[i][j+1] = 1;
i++;}

list basenumero = auxelspas;

int i = 1;
while(i<=size(auxelspas))
{int j = size(auxelspas[i]);
basenumero[i][j+1] = 1;
i++;}

    //basetamanhos[i] e basenumero[i] informam tamanho e numero de ciclos
    //correspondentes a cada divisor elementar, resultado do teorema Elspas.

//---------------------------------------------------------------------------

//3.6 - Efetuar o produto entre os grafos bijetivos
    // associados a cada divisor elementar.

list tamanhoauxiliar1;
list numeroauxiliar1;

list tamanhoauxiliar2;
list numeroauxiliar2;
```

```
list tamanhociclos;
list numerociclos;

tamanhoauxiliar1 = basetamanho[1];
numeroauxiliar1 = basenumero[1];

tamanhociclos = tamanhoauxiliar1;
numerociclos = numeroauxiliar1;

int i = 2;

while(i<=size(basenumero))
{
int l = 1;

tamanhoauxiliar2 = basetamanho[i];
numeroauxiliar2 = basenumero[i];

int j = 1; ;
while(j<=size(tamanhoauxiliar1))
{int k = 1;
while(k<=size(tamanhoauxiliar2))
{tamanhociclos[l] = lcm(tamanhoauxiliar1[j],tamanhoauxiliar2[k]);
numerociclos[l] = numeroauxiliar1[j]*numeroauxiliar2[k]*
gcd(tamanhoauxiliar1[j],tamanhoauxiliar2[k]);
l++;
k++;};
j++;};

tamanhoauxiliar1 = tamanhociclos;
numeroauxiliar1 = numerociclos;

i++;};

//---------------------------------------------------------------------------

// 3.7 - Reescrevendo a resposta...
```

```
list auxiliar1;
list auxiliar2;

list bijetivo;
    //bijetivo[i][1] é o número de ciclos de tamanho bijetivo[i][2].

auxiliar1 = tamanhociclos;
auxiliar2 = numerociclos;

int a;
int b;
int i = 1;

int k = 1;

while(i<=size(auxiliar1))
{a= auxiliar1[i];
if(a<>0){
b = auxiliar2[i];
auxiliar1[i] = 0;

int j = 1;
while(j<=size(auxiliar1))
{if(auxiliar1[j]==a&a<>0)
{b = b + auxiliar2[j];
auxiliar1[j] = 0;};
j++;};
bijetivo[k] = list(b,a);
k++;};
i++;}
```

Obtemos "nilpotente", uma lista em em que a entrada nilpotente[i] nos diz quantos elementos de altura i temos na parte nilpotente, e "bijetivo", uma lista que informa a estrutura cíclica da parte bijetiva associada ao SDFL e a entrada bijetivo[i][1] nos diz quantos ciclos temos de tamanho bijetivo[i][2].

Referências Bibliográficas

[1] A. Garcia, Y. Lequain, *Elementos de Álgebra*. 3ª edição. Rio de Janeiro: IMPA. 2005.

[2] A. Hefez, M. L. Villela, *Códigos corretores de erros*. Rio de Janeiro: IMPA. 2002.

[3] D. Bollman, O. Colóon-Reyes, E. Orozco, *Determining When a Monomial Discrete Dynamical System is a Fixed Point System*, Pre-print.
http:// math.uprm.edu/ dbollman/FINALFINAL.pdf.

[4] D. Bollman, O. Colóon-Reyes, E. Orozco, *Fixed Points in Discrete Models for Regulatory Genetic Networks, EURASIP Journal of Bioinformatics and Systems Biology*, Volume 2007, Article ID 97356, 8 pages.

[5] D. S. Dummit, R. M. Foote, *Abstract Algebra*. Third edition. Hoboken, NJ: John Wiley & Sons Inc. 2004.

[6] E. Dimitorva, P. Vera-Licona, J. McGee, and R. Laubenbacher, *Discretization of time series data*, 2007. Submitted.
http://arxiv.org/ftp/q-bio/papers/0505/0505028.pdf.

[7] F. Celada, P. Seiden, *A computer model of cellular interactions in the immune system, Immunology Today*, 13 (1992), pp. 56-62.

[8] F. M. Goodman, *Algebra: Abstract and Concrete*, 2ª edition. Iowa City. 2006.
http://www.math.uiowa.edu/ goodman/algebrabook.dir/bookmt.pdf

[9] F. U. Coelho, M. L. Lourenço. *Um Curso de Álgebra Linear*. Editora da Universidade de São Paulo.

[10] K. Hoffman and R. Kunze, *Álgebra Linear*. Rio de Janeiro: LTC 2ª edição.

[11] R. Albert and H. Othmer, The topology of the regulatory interactions predicts the expression pattern of the segment polarity genes in Drosophila melanogaster, Journal of Theoretical Biology, 223 (2003), pp. 1-18.

[12] R. Hernandez-Toledo, *Linear finite dynamical systems*, Communications in Algebra, 33 (2005), pp. 2977-2989.

[13] S. Kauffman, Metabolic stability and epigenesis in randomly constructed genetic nets, Journal of Theoretical Biology, 22 (1969), pp. 437-467.

[14] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Revised Edition. Cambridge: Cambridge University Press. 1994.