Tópicos em Dinâmica Aritmética

VI Colóquio de Matemática da Região Centro-Oeste

Professor: Lucas Reis (UFMG)

Sobre as notas: Estas notas de aula visam apresentar uma versão expandida e detalhada do conteúdo que será abordado ao longo das três aulas do minicurso "Tópicos em Dinâmica Aritmética" no VI Colóquio de Matemática da Região Centro-Oeste.

1 Introdução e definições básicas

Começamos com uma definição fundamental.

Definição 1.1. *Um sistema dinâmico finito (SDF) é um par (X, f), onde X é um conjunto finito e $f : X \to X$ é uma função qualquer.*

Apesar da definição acima ser bem ampla, estaremos interessados em SDF's com estruturas algébricas. Por exemplo, podemos tomar $X = \mathbb{Z}_n$ como o anel de inteiros módulo n e f uma função polinomial qualquer. A seguir, temos algumas definições básicas associadas a um SDF.

Definição 1.2. *Seja $S = (X, f)$ um SDF e $a \in X$. Denotamos por $f^{(m)}$ a m-ésima iterada de f. Em outras palavras,*

$$f^{(m)}(a) = \underbrace{f(\cdots f}_{m \text{ vezes}}(a)\cdots).$$

Por convenção, temos $f^{(0)}(a) = a$.

1. *O elemento (ou ponto) $a \in X$ é* **puramente periódico** *se existe um inteiro $n \geq 1$ tal que $f^{(n)}(a) = a$. Neste caso, o menor inteiro positivo com tal propriedade é o* **período** *de a. Se $n = 1$, diremos que a é um* **ponto fixo** *de (X, f).*

2. *O pré-periodo de um elemento $a \in X$ é o menor inteiro não negativo m tal que $f^{(m)}(a)$ é puramente periódico.*

3. *A* **órbita** *de $a \in X$ é o conjunto $O_f(a) = \{a, f(a), f^{(2)}(a), \ldots\} \subseteq X$ e a* **órbita inversa** *de $a \in X$ é o conjunto*

$$O_f^{-\infty}(a) = \bigcup_{j \geq 1} \{b \in X \mid f^{(j)}(b) = a\} \subseteq X.$$

Observemos que, uma vez que X é finito, o pré-período de um elemento é sempre bem definido. Vamos a um exemplo.

Exemplo 1.3. *Considere o anel $X = \mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$ e $f : a \mapsto a^2 + 1$. Um cálculo direto nos dá o seguinte:*

(i) os pontos puramente periódicos são 2 e 5;

(ii) $O_f(3) = \{3, 10, 5, 2\}$ e o pré-período do ponto $3 \in \mathbb{Z}_{12}$ é igual a 2;

(iii) $O_f^{-\infty}(2) = O_f^{-\infty}(5) = \mathbb{Z}_{12}$.

1.1 Operações com SDF's, e algumas classes importantes

Podemos definir duas operações básicas entre dois SDF's.

Definição 1.4. *Dados (X, f) e (Y, g) dois SDF's, definimos*

1. *a soma (direta) como sendo o SDF $f \oplus g : X \cup Y \to X \cup Y$, onde*

$$(f \oplus g)(a) = \begin{cases} f(a) & \text{se } a \in X, \\ g(a) & \text{se } a \in Y. \end{cases}$$

2. *o produto (direto) como sendo o SDF $f \times g : X \times Y \to X \times Y$, onde $(f \times g)(a, b) = (f(a), g(b))$.*

Definimos ainda quando dois SDF's são conjugados.

Definição 1.5. *Dois SDF's (X, f) e (Y, g) são* **conjugados** *se existir uma bijeção $\pi : X \to Y$ tal que $f = \pi^{-1} \circ g \circ \pi$, isto é, $\pi \circ f = g \circ \pi$.*

Claramente, se dois SDF's são conjugados, os conjuntos X, Y possuem a mesma cardinalidade. Além disto, é simples de verificar que tal relação de conjugação, é uma *relação de equivalência.*

Exemplo 1.6. *Os SDF's* $(a \mapsto a^2 + 1, \mathbb{Z}_{12})$ *e* $(a \mapsto a^2 + 2a + 1, \mathbb{Z}_{12})$ *são conjugados: tome* $\pi : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ *com* $\pi(x) = x \pm 1$ *(dependendo de qual direção a conjugação está sendo considerada).*

Para o objetivo deste minicurso, será importante ainda definir duas classes de SDF's.

Definição 1.7. *Um SDF* (X, f) *é:*

1. **bijetivo** *se a função* $f : X \to X$ *é uma bijeção;*

2. **nilpotente** *se existir* $r \in X$ *tal que* $f(r) = r$ *(i.e.,* r *é um ponto fixo de* (X, f)*) e para todo* $a \in X$*, existe* $m \geq 1$ *tal que* $f^{(m)}(a) = r$*, ou seja,*

$$O_f^{-\infty}(r) = X.$$

   Neste caso, o ponto $r \in X$ *é o* **atrator** *de* (X, f)*.*

Exemplo 1.8. *Seja* $X = \mathbb{Z}_9$*,* $f : a \mapsto 5a$ *e* $g : a \mapsto 3a$*. Então* (X, f) *é bijetivo, e* (X, g) *é nilpotente com atrator* $0 \in \mathbb{Z}_9$*.*

Exemplo 1.9. *Seja* $c \in X$*,* $f : a \mapsto c$ *a função constante igual a* c*, então* (X, f) *é nilpotente com atrator* c*.*

2 O Grafo funcional de um SDF

Para cada SDF, podemos associar um grafo (direcionado), como segue.

Definição 2.1. *O* **grafo funcional** *de um SDF (X, f), denotado por $G(f/X)$, é o grafo direcionado com conjunto de vértices X e arestas direcionadas $a \longrightarrow f(a)$.*

Importante: Ao longo do texto, não faremos distinção do elemento $a \in X$ e o vértice de $G(f/X)$ associado a ele.

A seguir temos imagens dos grafos funcionais de alguns SDF's (obtidas usando o software SageMath).

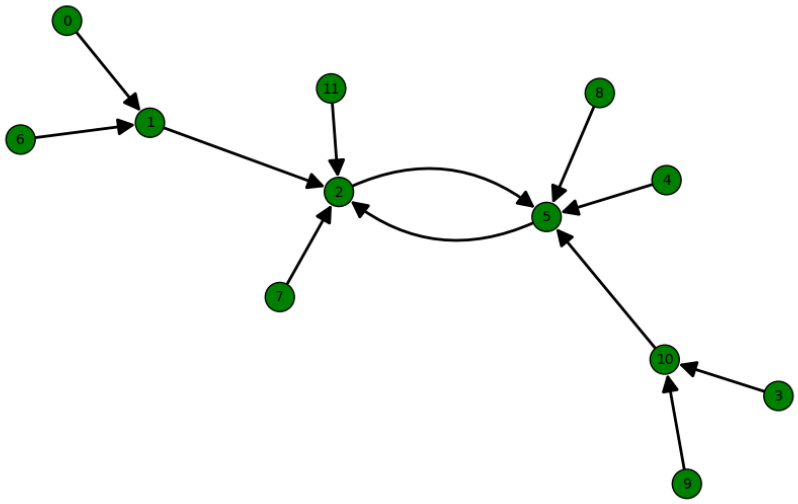

Figure 1: O grafo funcional $G(a \mapsto a^2 + 1/\mathbb{Z}_{12})$.

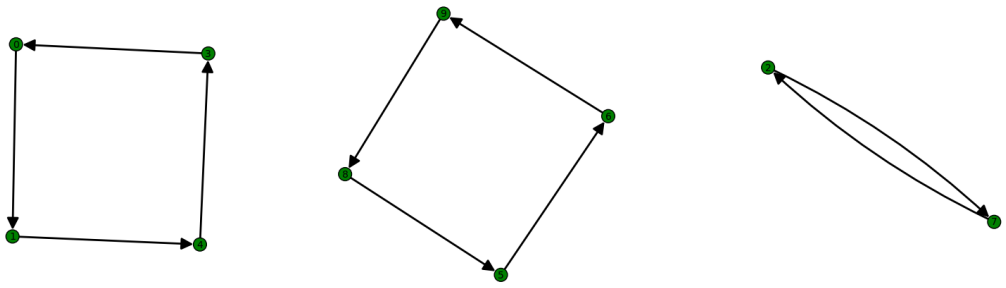

Figure 2: O grafo funcional $G(a \mapsto 3a + 1/\mathbb{Z}_{10})$.

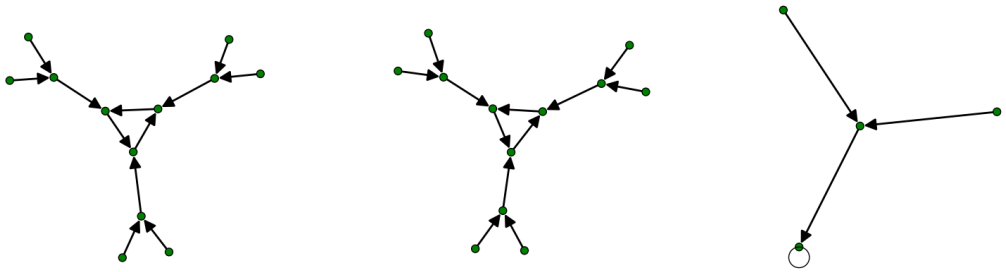

Figure 3: O grafo funcional $G(a \mapsto 2a/\mathbb{Z}_{28})$.

O grafo funcional $G(f/X)$ nos dá diversas informações sobre o sistema dinâmico (X, f):

1. a órbita $O_f(a)$ de um ponto $a \in X$ é descrita pelo maior caminho no grafo $G(f/X)$ partindo do vértice a (e seguindo as direções das arestas).

2. um ponto $a \in X$ é puramente periódico se, e somente se, existe um caminho que parte do vértice a e retorna para o mesmo (seguindo as direções das arestas).

3. o pré-periodo de um ponto $a \in X$ é exatamente o "comprimento" do caminho saindo de a para chegar em um ponto puramente periódico.

4. se o ponto $a \in X$ é puramente periódico, sua órbita inversa $O_f^{-\infty}(a)$ compreende exatamente os elementos que aparecem na componente conexa de $G(f/X)$ que contém a.

Importante: A estrutura geral das componentes (conexas) de um grafo funcional é a seguinte: temos um "grafo cíclico" (correspondendo aos pontos puramente periódicos), e em cada vértice de tal grafo temos uma árvore "pendurada".

2.1 Grafos direcionados e operações

Para um grafo direcionado G, escrevemos $G = G(V, E)$, onde V é o conjunto de vértices de G e E é o conjunto de arestas direcionadas de G. Vamos considerar aqui somente grafos **finitos**, onde de cada vértice "sai" exatamente **uma aresta direcionada**. Temos a noção clássica de isomorfismo de grafos.

Definição 2.2. *Dois grafos direcionados $G_1 = G_1(V_1, E_1)$ e $G_2 = G_2(V_2, E_2)$ são* **isomorfos** *se existe uma bijeção entre seus conjuntos de vértices que preserva adjacência, isto é, se existe bijeção $\pi : V_1 \to V_2$ tal que, para quaisquer $u, v \in V_1$ vale que $u \longrightarrow v \in E_1$ se, e somente se, $\pi(u) \longrightarrow \pi(v) \in E_2$.*

Temos duas classes importantes de grafos a serem definidas.

Definição 2.3.

1. *Um ciclo de comprimento n, denotato por $\mathrm{Cyc}(n)$, é um grafo com vértices $v_1, \ldots, v_n$ e arestas $v_i \longrightarrow v_{i+1}$ (índices tomados módulo n).*

2. *Uma árvore (direcionada) T é um grafo direcionado, conexo contendo somente um ciclo, cujo comprimento é exatamente 1. Neste caso, o elemento $v \in V$ pertecendo a tal ciclo é a* **raiz** *de T. Denotamos T^* o grafo obtido ao deletar tal ciclo e, por simplicidade, também chamaremos T^* de árvore.*

3. *Dada uma árvore direcionada T e um inteiro positivo m, denotamos por $\mathrm{Cyc}(m, T)$ o grafo obtido ao "pendurar" em cada vértice de $\mathrm{Cyc}(m)$, uma "cópia" de T^*. Em outras palavras, cada vértice de $\mathrm{Cyc}(m)$ será a raiz de uma árvore isomorfa a T^*.*

Podemos definir as seguintes operações em grafos direcionados.

Definição 2.4. *Dados dois grafos direcionados $G = G(V, E)$ e $H = H(U, E_0)$, definimos:*

1. *A* **soma direta** *$G \oplus H$ como sendo o grafo com vértices $V \cup U$ e arestas direcionadas $E \cup E_0$ (ou seja, só estamos considerando a "união" dos grafos). Para cada inteiro positivo n, definimos*

$$n \times G = \underbrace{G \oplus \cdots \oplus G}_{n \text{ vezes}}.$$

2. *O* **produto tensorial** $G \otimes H$ *como sendo o grafo com vértices* $V \times U$ *e arestas direcionadas* $(g,h) \longrightarrow (g_0,h_0)$*, onde* $g \longrightarrow g_0 \in E$ *e* $h \longrightarrow h_0 \in E_0$*.*

O seguinte lema nos dá algumas propriedades importantes das operações em grafos.

Lema 2.5. *Sejam* m,n *inteiros positivos,* G_1,G_2,G_3 *grafos direcionados e* T *uma árvore direcionada. A menos de isomorfismo, os seguintes valem:*

1. $G_1 \otimes G_2 = G_2 \otimes G_1$*;*
2. $G_1 \otimes (G_2 \oplus G_3) = (G_1 \otimes G_2) \oplus (G_1 \otimes G_3)$*;*
3. $\mathrm{Cyc}(m) \otimes \mathrm{Cyc}(n) = \mathrm{mdc}(m,n) \times \mathrm{Cyc}(\mathrm{mmc}(m,n))$;
4. $\mathrm{Cyc}(m) \otimes T = \mathrm{Cyc}(m,T)$.

2.2 SDF's e grafos funcionais

O seguinte teorema nos dá relações interessantes entre SDF's e seus grafos funcionais.

Teorema 2.6. *Sejam* (X,f) *e* (Y,g) *dois SDF's. Então os seguintes valem:*

1. $G(f \oplus g/X \cup Y) = G(f/X) \oplus G(g/Y)$*;*
2. $G(f \times g/X \times Y) = G(f/X) \otimes G(g/Y)$*;*
3. (X,f) *e* (Y,g) *são conjugados se, e somente se, os grafos funcionais* $G(f/X)$ *e* $G(g/Y)$ *são isomorfos.*

Demonstração. Os itens 1 e 2 seguem diretamente da definição de soma e produto (de SDF's e grafos direcionados). Para o item 3, observemos que as arestas de X (resp. de Y) são $a \longrightarrow f(a)$ com $a \in X$ (resp. $a \longrightarrow g(a)$ com $a \in Y$). Logo uma bijeção $\pi : X \to Y$ preserva adjacência entre os grafos $G(f/X)$ e $G(g/Y)$ se, e somente se, $\pi(f(a)) = g(\pi(a))$ para todo $a \in X$. Em outras palavras, $\pi \circ f = g \circ \pi$, ou seja, (X,f) e (Y,g) são conjugados. □

O seguinte lema nos dá informação sobre o grafo funcional de certos SDF. A prova fica como exercício.

Lema 2.7. *Seja (X, f) um SDF. Então os seguintes valem:*

1. *(X, f) é bijetivo se, e somente se, toda componente conexa de $G(f/X)$ é da forma* $\mathrm{Cyc}(m)$*;*

2. *(X, f) é nilpotente se, e somente se, $G(f/X)$ é uma árvore. Neste caso, a raiz da árvore corresponde ao atrator de (X, f).*

2.3 Uma classe especial de árvores direcionadas

Seja $\nu = (\nu_1, \ldots, \nu_k)$ uma sequência não crescente de inteiros positivos, i.e., $1 \leq \nu_{i+1} \leq \nu_i$. Para tal sequência ν, podemos associar a seguinte árvore $\mathcal{T}_\nu$:

1. começamos com $T_\nu^{(1)}$ a árvore com ν_1 vértices direcionados a um vértice (raiz);

2. para cada $2 \leq i \leq k$, seja $T_\nu^{(i)}$ a árvore obtida da seguinte maneira: tome ν_1 vértices direcionados a um vértice (raiz) e, para cada $j = 2, \ldots, i-1$, "penduramos" em $\nu_j - \nu_{j+1}$ destes vértices, árvores isomorfas a $T_\nu^{(j-1)}$, além de "pendurar" em ν_i dos vértices restantes, árvores isomorfas a $T_\nu^{(i-1)}$.

3. A árvore $\mathcal{T}_\nu$ é obtida a partir da árvore $T_\nu^{(k)}$, ao deletar um vértice direcionado a raiz que tenha pendurado uma árvore isomorfa a $T_\nu^{(k-1)}$, e adicionar um loop (ciclo de comprimento 1) a raiz.

Na Figura 4, temos uma representação desta construção indutiva quando $k = 4$ (omitindo as direções das arestas e o loop na raiz).

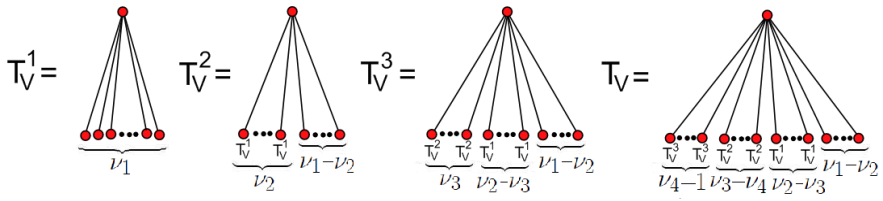

Figure 4: Construção recursiva de $\mathcal{T}_\nu$ quando $\nu = (\nu_1, \nu_2, \nu_3, \nu_4)$.

Na Figura 5 temos um exemplo numérico (omitindo as direções das arestas e o loop na raiz).

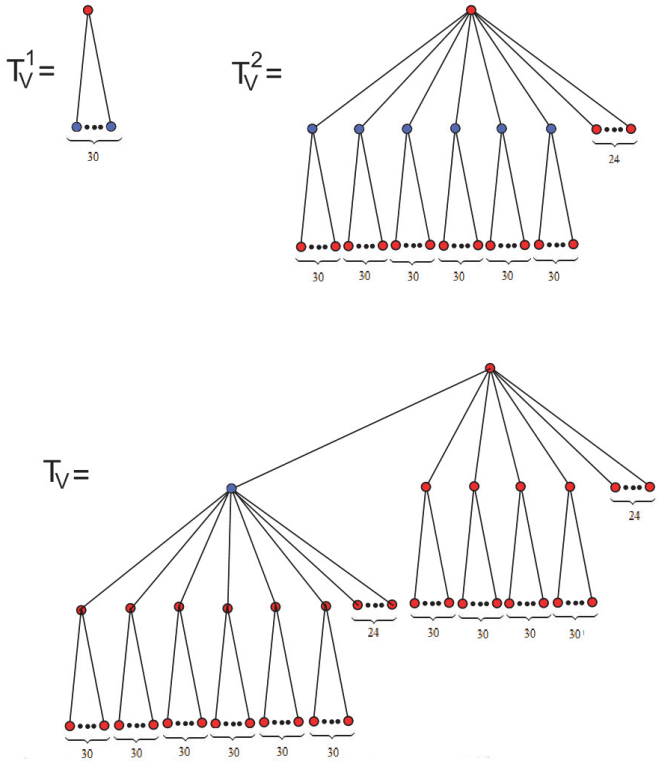

Figure 5: A árvore $\mathcal{T}_{(30,6,2)}$.

Importante: Quando todos os termos da sequência são iguais, vemos um comportamento "fractal" na árvore: se $d > 1$ e $\nu = (\underbrace{d, \ldots, d}_{n \text{ vezes}})$, então $\mathcal{T}_\nu$ é a árvore obtida pelas seguintes operações $O(i), 1 \leq i \leq n$:

1. $O(1)$ consiste em adicionar $d-1$ vértices á um vértice com loop (raiz);
2. para cada $2 \leq i \leq n$, $O(i)$ consiste em adicionar d vértices direcionados a cada um dos vértices novos criados no passo $O(i-1)$.

A Figura 6 exemplifica este processo para $d = 2$ e $n = 6$ (omitindo as direções das arestas e o loop).

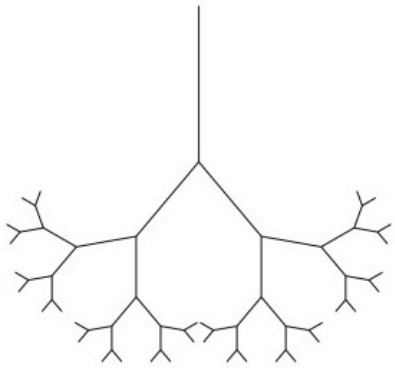

Figure 6: A árvore $\mathcal{T}_{(2,2,2,2,2,2)}$.

O lema a seguir nos dá algumas propriedades básicas das árvores $\mathcal{T}_\nu$.

Lema 2.8. *Seja $\nu = (\nu_1, \ldots, \nu_k)$ uma sequência não crescente de inteiros positivos com $\nu_k > 1$. Então os seguintes valem:*

1. *A árvore $\mathcal{T}_\nu$ possui $\nu_1 \cdots \nu_k$ vértices (e arestas), e possui profundidade k (i.e., o vértice mais distante da raiz corresponde a uma distância k).*
2. *Se ν^* é uma sequência qualquer obtida a partir de ν, acrescentando 1's nas últimas coordenadas, então $\mathcal{T}_\nu = \mathcal{T}_{\nu^*}$.*

Demonstração. O item 2 se verifica diretamente pela definição de $\mathcal{T}_\nu$. O item 1 se verifica por indução em k (utilizando fortemente a construção recursiva da árvore $\mathcal{T}_\nu$). □

O item 2 do lema anterior nos diz que, a partir de uma sequência ν, podemos definir várias sequências "equivalentes" (no sentido que elas geram as mesmas árvores). Em particular, podemos definir o seguinte produto.

Definição 2.9. *Sejam $\nu = (\nu_1, \ldots, \nu_k)$ e $\omega = (\omega_1, \ldots, \omega_m)$ duas sequências não crescentes de inteiros positivos tais que $m \geq k$. Definimos o* **produto estendido** *de ν e ω por*

$$\nu * \omega = (\nu_1 \cdot \omega_1, \ldots, \nu_k \cdot \omega_k, \omega_{k+1}, \ldots, \omega_m).$$

Em outras palavras, pegamos a sequência de menor comprimento, completamos com 1's e fazemos o produto coordenada a coordenada (agora bem definido).

Observamos que $\nu * \omega$ ainda define uma sequência não crescente de inteiros positivos. Em particular, podemos definir a árvore $\mathcal{T}_{\nu*\omega}$. O seguinte teorema nos dá uma importante informação sobre esta árvore em termos do produto tensorial.

Teorema 2.10. *Sejam ν, ω duas sequências não crescentes de inteiros positivos, então temos que*

$$\mathcal{T}_\nu \otimes \mathcal{T}_\omega = \mathcal{T}_{\nu*\omega}.$$

Em outras palavras, o produto tensorial das árvores associadas a ν e ω é igual a árvore associada ao produto estendido $\nu * \omega$.

A prova do teorema anterior, apesar de elementar (usamos o princípio de indução duas vezes), é um pouco técnica e evitaremos discutir aqui. Para mais detalhes, ver a Subseção 2.3 em [5].

3 SDF's lineares

Nesta seção discutiremos a descrição do grafo funcional associado a SDF's lineares, que basicamente é uma expansão do trabalho desenvolvido em [6] (com linguagem mais moderna e provas mais detalhadas).

Naturalmente, consideramos espaços vetoriais sobre um corpo finito.

Definição 3.1. *Seja q uma potência de primo e $\mathbb{F}_q$ o corpo finito com q elementos. Um* **sistema dinâmico finito linear (SDFL)** *é um par (V, T), onde V é um espaço vetorial de dimensão finita sobre $\mathbb{F}_q$ e $T : V \to V$ é uma transformação linear.*

A seguir, vamos resumir o procedimento para determinar os grafos $G(T/V)$: utilizando de resultados de Álgebra linear, iremos decompor (sucessivamente) o espaço V como soma direta de subespaços T-invariantes ($T(U) \subseteq U$), onde a restrição $T_0 = T|_U$ possui propriedades "boas", facilitando a descrição de $G(T_0/U)$. No final, utilizaremos o seguinte corolário imediato do Teorema 2.6.

Corolário 3.2. *Seja $V = V_1 \oplus \cdots \oplus V_m$, e seja T_i a restrição de T em V_i. Então*

$$G(T/V) = \bigotimes_{i=1}^{m} G(T_i/V_i).$$

Vamos começar com uma primeira redução nesta direção.

Lema 3.3. *Dado um SDFL (V, T), o conjunto*

$$U = \bigcup_{m \geq 0} \{u \in V \mid T^{(m)}(u) = 0\},$$

é um subespaço T-invariante e temos que $V = U \oplus W$ para algum subespaço T-invariante W tal que a restrição de T em W é uma bijeção. A decomposição $V = U \oplus W$ é a **T-decomposição** *de V.*

Demonstração. O fato de U ser um espaço vetorial T-invariante segue diretamente da definição de U. Observamos também que W é simplesmente o espaço completamento de U para V. Em particular, W é T-invariante e $W \cap U = \{0\}$. Para mostrar que a restrição de T em W é uma bijeção, basta mostrar que $\ker(T) \cap W = \{0\}$. Ora, o último decorre do fato de que $\ker T \subseteq U$ e $W \cap U = \{0\}$. □

Obtemos o seguinte resultado.

Lema 3.4. *Seja (V,T) um SDFL e seja $V = U \oplus W$ sua T-decomposição. Seja T_1, T_2 as restrições de T em U e W, respectivamente. Então os seguintes valem:*

(i) $\mathbb{T} = G(T_1/U)$ *é uma árvore;*

(ii) $G(T_2/W)$ *é da forma* $\bigoplus_{i=1}^{d} \mathrm{Cyc}(m_i)$*;*

(iii) para a árvore $\mathbb{T}$ *no item (i) e os mesmos inteiros* m_i *no item (ii), temos que*

$$G(T/V) = \bigoplus_{i=1}^{d} \mathrm{Cyc}(m_i, \mathbb{T}).$$

Demonstração. Pela definição de U, temos que (U, T_1) é nilpotente com atrator $0 \in U$ e (W, T_2) é bijetivo. Pelo Lema 2.7, obtemos os itens (i) e (ii). O item (iii) segue diretamente do Corolário 3.2 e o Lema 2.5. □

Em particular, o lema anterior nos diz que $G(T/V)$ possui simetria (as árvores "penduradas" são todas isomorfas entre si). O objetivo agora é descrever a árvore $\mathbb{T}$ e os inteiros m_i. Trataremos primeiro da árvore $\mathbb{T}$.

3.1 SDFL's nilpotentes

Observamos o seguinte: se $T : V \to V$ é nilpotente, i.e., se existe $n \geq 0$ tal que $T^{(n)}(v) = 0$ para todos $v \in V$, então existe uma base na qual a representação matricial de T se decompõe em blocos de Jordan (autovalor$= 0$). Vamos olhar primeiramente o caso em que tal matriz possui um único bloco de Jordan.

Lema 3.5. *Seja $\mathbb{F}_q$ o corpo finito com q elementos e seja $T : V \to V$ uma transformação linear nilpotente sobre V, um espaço vetorial de dimensão D. Se existe uma base na qual a representação matricial de T compreende um único bloco de Jordan, então*

$$G(T/V) = \mathcal{T}_{A_D},$$

onde $A_D = (\underbrace{q, \ldots, q}_{D \text{ vezes}})$ *e* $\mathcal{T}_{A_D}$ *é dada como na Subsec. 2.3.*

Demonstração. Diretamente verificamos que a equação $Tv = 0$ define um subespaço de dimensão 1 em V, logo tal equação possui q soluções. Em particular, para todo $u \in V$, a equação $Tv = u$ possui 0 ou q soluções. Por hipótese, D é o menor inteiro positivo tal que $T^{(D)}v = 0$ para todo $v \in V$. Logo $G(T/V)$ é uma árvore de "profundidade" D, onde em cada vértice é direcionado no máximo q arestas. Pelo Lema 2.8, $\mathcal{T}_{A_D}$ também é uma árvore de profundidade D, e observamos que para cada vértice de profundidade $0 < j < D$, temos q arestas direcionadas. Logo concluimos que $G(T/V)$ é um subgrafo de $\mathcal{T}_{A_D}$. Entretanto, ambos os grafos possuem q^n vértices e q^n arestas (este fato para $\mathcal{T}_{A_D}$ segue do Lema 2.8), e então devemos ter a igualdade $G(T/V) = \mathcal{T}_{A_D}$. □

Obtemos então o seguinte resultado.

Teorema 3.6. *Seja $\mathbb{F}_q$ o corpo finito com q elementos e seja $T : V \to V$ uma transformação linear nilpotente sobre V, um espaço vetorial de dimensão n. Se existe uma base na qual a representação matricial de T compreende blocos de Jordan de tamanhos $D_1 \leq \cdots \leq D_k$, então*

$$G(T/V) = \mathcal{T}_{n_{T,U}},$$

onde $n_{T,U} = (\underbrace{q^k, \ldots, q^k}_{D_1 \text{ vezes}}, \underbrace{q^{k-1}, \ldots, q^{k-1}}_{D_2 - D_1 \text{ vezes}}, \ldots, \underbrace{q^i, \ldots, q^i}_{D_{k-i+1} - D_{k-i} \text{ vezes}}, \ldots, \underbrace{q, \ldots, q}_{D_k - D_{k-1} \text{ vezes}})$ *e $\mathcal{T}_{n_{T,U}}$ é dada como na Subsec. 2.3.*

Demonstração. Para cada $1 \leq i \leq k$, seja V_i o subespaço de T-invariante correspondente ao bloco de Jordan de tamanho D_i. Logo $V = \bigoplus_{i=1}^{k} V_i$ e então, se T_i é a restrição de T em V_i, o Lema 3.5 nos dá $G(T_i/V_i) = \mathcal{T}_{A_{D_i}}$. Por outro lado, o Corolário 3.2 nos diz que

$$G(T/V) = \bigotimes_{i=1}^{k} G(T_i/V_i),$$

logo

$$G(T/V) = \bigotimes_{i=1}^{k} \mathcal{T}_{A_{D_i}} = \mathcal{T}_{\nu},$$

onde $\nu = A_{D_1} * \cdots * A_{D_k}$ e usamos o Teorema 2.10. Um cálculo direto nos dá que $\nu = n_{T,U}$. □

Exemplo 3.7. *Seja $V = \mathbb{F}_2^6$ e seja $T : V \to V$ a transformação linear cuja representação matricial (em alguma base) seja*

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

Temos $D_1 = 1, D_2 = 2, D_3 = 3$ e então

$$G(T/V) = \mathcal{T}_{(8,4,2)}.$$

Utilizando o software SageMath, conseguimos produzir o grafo $G(T/V)$.

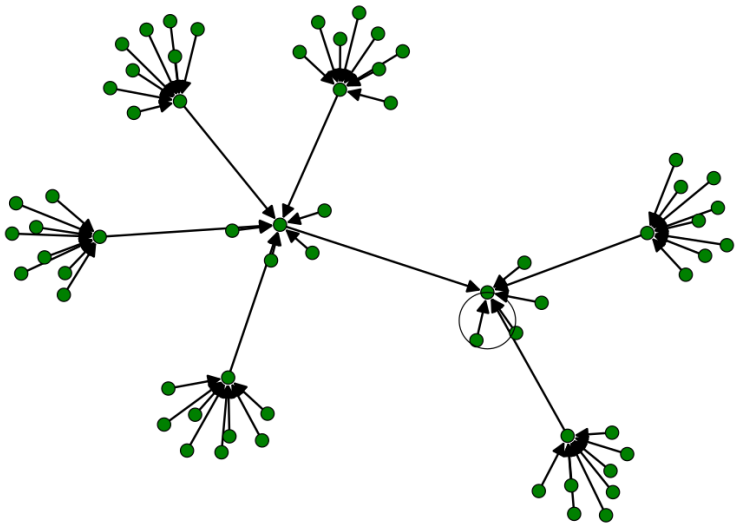

Figure 7: A árvore $\mathcal{T}_{(8,4,2)}$.

3.2 SDFL's bijetivos

Para a descrição de SDFL's bijetivos, precisaremos de mais algumas ferramentas de Álgebra Linear.

3.2.1 Subespaços invariantes minimais

Começamos com a seguinte definição.

Definição 3.8. *Dado (V,T), $v \in V$ e $f \in \mathbb{F}_q[x]$ com $f(x) = \sum_{i=0}^{d} a_i x^i$, definimos*

$$f(T) \cdot v = \sum_{i=0}^{d} a_i \cdot T^{(i)}(v),$$

e $I_{v,T} = \{g \in \mathbb{F}_q[x] \,|\, g(T) \cdot v = 0\}$.

Com a definição acima, vemos que V possui uma estrutura de $\mathbb{F}_q[x]$-módulo:

Lema 3.9. *Dados $(V,T), v \in V$ e $f, g \in \mathbb{F}_q[x]$, os seguintes valem:*

1. $(f+g)(T) \cdot v = f(T) \cdot v + g(T) \cdot v$;
2. $(f \times g)(T) \cdot v = f(T) \cdot (g(T) \cdot v)$.

Em particular, $I_{v,T}$ é um ideal (não nulo) de $\mathbb{F}_q[x]$.

Demonstração. As propriedades 1 e 2 podem ser verificadas diretamente, utilizando o fato de que T é linear. Em particular, segue da definição que $I_{v,t}$ é um ideal. Se $F(x)$ é o polinômio característico de $T : V \to V$, o **Teorema de Cayley-Hamilton** nos diz que $F(T) \cdot v = 0$ para todo $v \in V$. Logo $F(x) \in I_{v,T}$ para todo $v \in V$, i.e., $I_{v,T}$ é não nulo. □

Por um argumento de divisão euclidiana, $I_{v,T}$ é o conjunto dos múltiplos de um polinômio mônico $m_{v,T}(x)$, que é simplesmente o gerador deste ideal.

Definição 3.10. *O gerador (mônico) de $I_{v,T}$ é o* **polinômio minimal** *de T com respeito a $v \in V$. Denotaremos tal polinômio por $m_{v,T}(x)$. Dado $U \subseteq V$ subespaço vetorial, definimos $m_{U,T}(x)$ como sendo o gerador mônico do ideal*

$$I_{U,T} = \{g \in \mathbb{F}_q[x] \,|\, g(T) \cdot u = 0, \forall u \in U\}.$$

Observação 3.11. *O polinômio $m_{U,T}(x)$ é simplesmente o MMC dos polinômios $m_{u,T}(x)$ com $u \in U$. Além disto, temos que $g(T) \cdot u = 0$ se, e somente se, $m_{u,T}(x)$ divide $g(x)$.*

Exemplo 3.12. *Seja $V = \mathbb{F}_q^2$, $T : V \to V$ definida por $T(a,b) = (a, a+b)$. O polinômio característico de T é $(x-1)^2$. Temos $m_{0,T}(x) = 1$, $m_{v,T}(x) = x - 1$ para $v = (0,b)$ com $b \neq 0$ e $m_{v,T}(x) = (x-1)^2$ para os elementos restantes de V. Em particular, $m_{V,T}(x) = (x-1)^2$.*

No exemplo anterior, vimos uma transformação linear com a seguinte propriedade: o polinômio característico coincide com o minimal, e é igual a uma potência de um polinômio irredutível. O seguinte resultado de Álgebra Linear nos diz que sempre podemos decompor nosso espaço de maneira que a restrição de T em cada um dos subespaços possui tal propriedade.

Teorema 3.13 (Forma racional)**.** *Seja V um espaço vetorial de dimensão finita sobre um corpo $\mathbb{F}$ e $T : V \to V$ uma transformação linear. Então podemos escrever $V = \bigoplus_{i=1}^{m} V_i$, onde cada V_i tem as seguintes propriedades:*

1. *V_i é T-invariante, i.e., $T(V_i) \subseteq V_i$;*
2. *$m_{V_i,T}(x)$ é um polinômio da forma $p(x)^s$, onde $p(x) \in \mathbb{F}[x]$ é irredutível, mônico tal que a dimensão de V_i é igual a $s \cdot \deg(p(x))$.*

Em outras palavras, V se decompõe em subspespaços T-invariantes, onde a restrição de T em cada subespaço é uma transformação linear cujo polinômio característico e minimal coincidem, e são iguais a potência de um polinômio irredutível sobre $\mathbb{F}$.

Observação 3.14. *Se $\mathbb{F}$ é algebricamente fechado, todo polinômio mônico irredutível é da forma $x - a, a \in \mathbb{F}$. Logo cada espaço V_i no teorema anterior corresponderia a um "bloco de Jordan" ao representar T em forma matricial. Em particular, o teorema anterior pode ser visto como uma generalização do Teorema de Jordan para transformações lineares sobre um corpo (não necessariamente algebricamente fechado)*

3.2.2 SDFL's bijetivos minimais

Já vimos que o grafo funcional de um SDF bijetivo se decompõe em ciclos $\mathrm{Cyc}(m)$ e já sabemos como calcular $\mathrm{Cyc}(m) \otimes \mathrm{Cyc}(n) = \mathrm{mdc}(m,n) \times \mathrm{Cyc}(\mathrm{mmc}(m,n))$. Logo, pelo Teorema 3.13, basta considerar os subespaços "legais" que aparecem no resultado de decomposição de tal teorema.

Teorema 3.15. *Seja V um espaço de dimensão finita sobre o corpo finito $\mathbb{F}_q$ de q elementos e seja $T : V \to V$ uma transformação linear bijetiva. Suponha que o polinômio*

característico e minimal de T coincidem e são iguais a $f(x)^s$, onde $f(x) \in \mathbb{F}_q[x]$ é um polinômio mônico irredutível de grau d. Então temos que

$$G(T/V) = \mathrm{Cyc}(1) \oplus \bigoplus_{i=1}^{s} \left(\frac{q^{di} - q^{d(i-1)}}{\mathrm{ord}(f(x)^i)} \times \mathrm{Cyc}(\mathrm{ord}(f(x)^i)) \right),$$

onde $\mathrm{ord}(f(x)^i)$ *é o menor inteiro positivo M tal que $f(x)^i$ divide $x^M - 1$.*

Demonstração. Como $d = \deg(f(x))$, temos que V possui dimensão ds, ou seja, V possui q^{ds} elementos. Lembremos que o polinômio minimal de T é simplesmente o MMC dos polinômios minimais $m_{v,T}(x), v \in V$. Como tal polinômio é uma potência de um polinômio irredutível, devemos ter $m_{w,T}(x) = f(x)^s$ para algum $w \in V$.

Afirmação 1. *Seja $w \in V$ como antes. Então para todo $v \in V$ existe um único polinômio $h(x) = h_v(x)$ no conjunto*

$$\mathcal{C}_{ds} = \{g \in \mathbb{F}_q[x] \mid \deg(g) < ds\},$$

tal que $v = h_v(T) \cdot w$. Neste caso, temos que $m_{v,T}(x) = \frac{f(x)^s}{\mathrm{mdc}(f(x)^s, h_v(x))}$.

Prova da Afirmação 1. Como $m_{w,T}(x) = f(x)^s$, um polinômio de grau ds, segue que os elementos $T^{(i)}w$ com $0 \leq i \leq ds - 1$ são linearmente independentes. Logo o espaço gerado por eles tem dimensão ds, a dimensão de V. Em particular, todo elemento de V é combinação linear destes elementos, e tal combinação é única. É direto de verificar que cada combinação corresponde a uma expressão $g(T) \cdot w$ com $g(x) \in \mathcal{C}_{ds}$.

Para a igualdade de polinômios, tome $v = h(T) \cdot w$. Observe que $g(T) \cdot v = 0$ se, e somente se,

$$(g \times h)(T) \cdot w = 0.$$

Como $m_{w,T}(x) = f(x)^s$, a última igualdade ocorre se, e somente se, $f(x)^s$ divide $g(x) \cdot h(x)$, i.e., $\frac{f(x)^s}{\mathrm{mdc}(f(x)^s, h_v(x))}$ divide $g(x)$. Como queremos o $g(x) = m_{v,T}(x)$ não nulo, mônico e de menor grau possível, concluimos que

$$m_{v,T}(x) = \frac{f(x)^s}{\mathrm{mdc}(f(x)^s, h_v(x))}. \quad \square$$

Observe que, para todo $v \in V$, temos que $m_{v,T}(x) = f(x)^j$ para algum $0 \leq j \leq s$.

Afirmação 2. *Para cada $1 \leq i \leq s$, seja $\mathcal{E}_i$ o conjunto dos elementos $v \in V$ tais que $m_{v,T}(x) = f(x)^i$. Então $\mathcal{E}_i$ tem cardinalidade $q^{di} - q^{d(i-1)}$ e $T(\mathcal{E}_i) = T^{-1}(\mathcal{E}_i) = \mathcal{E}_i$. Em particular, os elementos de $\mathcal{E}_i$ compreendem componentes conexas de $G(T/V)$.*

Prova da Afirmação 2. Pela Afirmação 1, observamos que $v \in \bigcup_{i=1}^{j} \mathcal{E}_i$ se, e somente se,

$$\frac{f(x)^s}{\mathrm{mdc}(f(x)^s, h_v(x))} = f(x)^i,$$

com $i \leq j$. Em outras palavras, $\mathrm{mdc}(h_v(x), f(x)^s)$ é divisível por $f(x)^{s-j}$. O último é equivalente a $h_v(x) = f(x)^{s-j} \cdot F(x)$ com

$$\deg(F(x)) < ds - d(s-j) = dj.$$

Como $F(x) \in \mathbb{F}_q[x]$, temos q^{dj} escolhas para $F(x)$. Logo $\cup_{i=1}^{j} \mathcal{E}_i$ possui q^{dj} elementos e então $\mathcal{E}_i$ tem cardinalidade $q^{di} - q^{d(i-1)}$.

Observe que, se $v = h_v(T) \cdot w$, então

$$Tv = T(h_v(T) \cdot w) = H(T) \cdot w,$$

onde $H(x) = x \cdot h_v(x)$. Como T **é bijetiva**, temos que $\mathrm{mdc}(f(x), x) = 1$ e então

$$\mathrm{mdc}(f(x)^s, h_v(x)) = \mathrm{mdc}(f(x)^s, h_v(x) \cdot x).$$

Em conclusão, $m_{v,T}(x) = m_{Tv,T}(x)$. Isto mostra que $T(\mathcal{E}_i) \subseteq \mathcal{E}_i$. Novamente, como T é bijetiva, temos que $T(\mathcal{E}_i) = \mathcal{E}_i$ e então $\mathcal{E}_i = T^{-1}(\mathcal{E}_i)$. □

Observamos que $\mathcal{E}_0 = \{0\}$ e $T(0) = 0$, gerando o ciclo Cyc(1) do teorema. Além disto, $\bigcup_{i=0}^{s} \mathcal{E}_i = V$. Logo, pela Afirmação 2, basta mostrar o seguinte.

Afirmação 3. *Na restrição de T sobre $\mathcal{E}_i$, cada ciclo possui tamanho* $\mathrm{ord}(f(x)^i)$.

Prova da Afirmação 3. Fixe $v \in \mathcal{E}_i$. Observamos que v pertence a um ciclo de tamanho M em $G(T/V)$ se, e somente se, M é o menor inteiro positivo tal que $T^{(M)}v = v$, i.e, $(x^M - 1)(T) \cdot v = 0$. Pela definição de polinômio minimal, segue que o último ocorre se, e somente se, $m_{v,T}(x) = f(x)^i$ divide $x^M - 1$. Por definição, o menor M com tal propriedade é $M = \mathrm{ord}(f(x)^i)$. □

Observação 3.16. *Observamos que, fixado $F \in \mathbb{F}_q[x]$ tal que* $\mathrm{mdc}(x, F(x)) = 1$*, então de fato existe inteiro positivo M tal que $F(x)$ divide $x^M - 1$. Para provar isto, note que os possíveis restos na divisão por $F(x)$ é finito (pois $\mathbb{F}_q$ é finito). Logo existem $0 < i < j$ tais que $F(x)$ divide $x^i - x^j = x^j(x^{i-j} - 1)$. Em particular $F(x)$ divide $x^{i-j} - 1$ pois* $\mathrm{mdc}(F(x), x) = 1$.

Tal resultado não é válido em geral sobre um corpo qualquer. Por exemplo, se $\mathbb{F}$ possui característica 0, o polinômio $x^M - 1$ não possui raízes múltiplas (em qualquer extensão), logo nunca pode ser divisível por um polinômio não constante da forma $f(x)^i$ com $i > 1$.

3.2.3 Calculando $\mathrm{ord}(f(x)^i)$

Já vimos que $\mathrm{ord}(f(x)^i)$ sempre existe sobre corpos finitos se $\mathrm{mdc}(f(x), x) = 1$, e aqui daremos um método para calcular tal valor. O seguinte resultado é clássico, mas omitiremos a prova.

Lema 3.17. *Se $f \in \mathbb{F}_q[x]$ é irredutível de grau d e $f(x) \neq x$, então* $\mathrm{ord}(f(x))$ *divide $q^d - 1$.*

Temos ainda o seguinte resultado.

Lema 3.18. *Seja $q = p^r$ um potência de primo e $f \in \mathbb{F}_q[x]$ um polinômio irredutível. Para cada inteiro positivo i, seja $\varepsilon(i)$ o menor inteiro positivo j tal que $p^j \geq i$. Então* $\mathrm{ord}(f(x)^i) = p^{\varepsilon(i)} \cdot \mathrm{ord}(f(x))$.

Demonstração. Seja $M = \mathrm{ord}(f(x)^i)$ e $L = \mathrm{ord}(f(x))$. Observamos que $f(x) | x^M - 1$ e então M é divisível por L, que não é divisível por p. Escreva $M = p^j \cdot L \cdot u$, onde $\mathrm{mdc}(u, p) = 1$. Temos que

$$x^M - 1 = (x^{Lu} - 1)^{p^j}.$$

Pelo teste da derivada, $x^{Lu} - 1$ não possui raízes múltiplas. Ainda, tal polinômio é divisível por $f(x)$. Logo a maior potência de $f(x)$ que divide $x^M - 1$ é $f(x)^{p^j}$. Queremos $f(x)^i$ dividindo $x^M - 1$, logo devemos ter $p^j \geq i$. O menor inteiro positivo j com tal

propriedade é $j = \varepsilon(i)$. E então concluímos que $M = p^{\varepsilon(i)} \cdot L \cdot u$. Como não temos nenhuma condição em u e queremos M mínimo, temos $u = 1$. □

Logo basta calcular $\text{ord}(f(x))$ onde $f(x) \neq x$ é um polinômio irredutível. Isto pode ser feito usando programas como *Singular* ou SageMath, e os comandos podem ser facilmente encontrados na web.

3.3 Alguns exemplos

Exemplo 3.19. *Considere a transformação* $T : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ *dada por*

$$T(a, b, c, d, e) = (a + b, a, c + d, d, e).$$

Se $V_1 = \{(\mathbb{F}_2, \mathbb{F}_2, 0, 0, 0)\}$, $V_2 = \{(0, 0, \mathbb{F}_2, \mathbb{F}_2, 0)\}$ *e* $V_3 = \{(0, 0, 0, 0, \mathbb{F}_2)\}$, *temos que* $\mathbb{F}_2^5 = V_1 \oplus V_2 \oplus V_3$ *e* $m_{V_1,T}(x) = m_{V_2,T}(x) = x^2 + x + 1$ *e* $m_{V_3,T}(x) = x - 1$. *Logo*

$$G(T/\mathbb{F}_2^5) = \bigotimes_{i=1}^{3} G(T/V_i).$$

Temos que $\text{ord}(x^2 + x + 1) = 3$ *(pois* $x^2 + x + 1$ *divide* $x^3 - 1$*)* *e* $\text{ord}(x - 1) = 1$. *Pelo Teorema 3.15, temos que*

$$G(T/V_1) = G(T/V_2) = \text{Cyc}(1) \oplus \frac{2^2 - 1}{3} \times \text{Cyc}(3) = \text{Cyc}(1) \oplus \text{Cyc}(3),$$

e

$$G(T/V_3) = \text{Cyc}(1) \oplus \frac{2 - 1}{1} \times \text{Cyc}(1) = 2 \times \text{Cyc}(2).$$

Usando a distributividade e a fórmula $\text{Cyc}(m) \otimes \text{Cyc}(n) = \text{mdc}(m, n) \times \text{Cyc}(\text{mmc}(m, n))$, *temos que*

$$G(T/\mathbb{F}_2^5) = (2 \times \text{Cyc}(1)) \oplus (10 \times \text{Cyc}(3)).$$

Exemplo 3.20. *Considere a transformação* $T : \mathbb{F}_5^3 \to \mathbb{F}_5^3$ *dada por*

$$T(a, b, c) = (a, a + b, 2c).$$

Se $V = \{(\mathbb{F}_5, \mathbb{F}_5, 0)\}$ *e* $U = \{(0, 0, \mathbb{F}_5)\}$, *temos* $\mathbb{F}_5^3 = V \oplus U$ *e* $m_{V,T}(x) = (x - 1)^2$ *e* $m_{U,T}(x) = x - 2$. *Logo*

$$G(T/\mathbb{F}_5^3) = G(T/V) \otimes G(T/U).$$

Temos que $\mathrm{ord}(x-2) = 4$ *(pois* $x^4 \equiv 1 \pmod{x-2}$ *em* $\mathbb{F}_5$*) e* $\mathrm{ord}((x-1)^2) = \mathrm{ord}(x-1) \cdot 5^1 = 1 \cdot 5 = 5$. *Pelo Teorema 3.15, temos que*

$$G(T/U) = \mathrm{Cyc}(1) \oplus \mathrm{Cyc}(4),$$

e

$$G(T/V) = \mathrm{Cyc}(1) \oplus \left(\frac{5-1}{1} \times \mathrm{Cyc}(1)\right) \oplus \left(\frac{25-5}{5} \times \mathrm{Cyc}(5)\right) = (5 \times \mathrm{Cyc}(1)) \oplus (4 \times \mathrm{Cyc}(5)).$$

Usando a distributividade e a fórmula $\mathrm{Cyc}(m) \otimes \mathrm{Cyc}(n) = \mathrm{mdc}(m,n) \times \mathrm{Cyc}(\mathrm{mmc}(m,n))$, *temos que*

$$G(T/\mathbb{F}_5^3) = (5 \times \mathrm{Cyc}(1)) \oplus (5 \times \mathrm{Cyc}(4)) \oplus (4 \times \mathrm{Cyc}(5)) \oplus (4 \times \mathrm{Cyc}(20)).$$

3.4 Um problema em aberto

Fixado um corpo finito $\mathbb{F}_q$ com q elementos e n um inteiro positivo, seja $A_q(n)$ o número de grafos não isomorfos gerados por transformações lineares de um espaço vetorial U de dimensão n sobre si mesmo. Observe que $A_q(n)$ conta exatamente o número de classes de conjugação de sistemas dinâmicos finitos lineares sobre U.

Problema. *Estime a função* $A_q(n)$ *com* q *fixo e* $n \to +\infty$.

Bach e Bridy [3] provaram o seguinte:

Teorema 3.21. *Existem constantes* $c_1, c_2 > 0$ *(que não dependem de* n*) tais que*

$$e^{c_1 \cdot n^{1/2}} < A_q(n) < e^{c_2 \frac{n}{\log \log n}}.$$

Aparentemente, a cota inferior ainda está longe do crescimento real da função $A_q(n)$. Em particular, podemos melhorar a cota inferior para $e^{c \cdot n^{1-\varepsilon}}$ para todo $\varepsilon > 0$ (trabalho do autor deste texto).

De qualquer forma, o problema aparenta ser bem complicado: qualquer abordagem deve passar por estimar *a quantidade de divisores* dos números $q^i - 1$ com $1 \leq i \leq n$, problema amplamente aberto.

4 Funções monomiais em grupos abelianos

Nesta seção consideramos o grafo funcional associado a funções monomiais sobre um grupo abeliano finito.

Definição 4.1. *Seja G um grupo abeliano finito e t um inteiro positivo. Definimos $\varphi_t : G \to G$ com $\varphi_t(g) = g^t$.*

O objetivo aqui é descrever o grafo $G(\varphi_t/G)$. Como na seção anterior, temos uma redução natural do problema: grupos abelianos finitos se decompõem como produto direto de grupos cíclicos.

Teorema 4.2. *Seja G um grupo abeliano finito. Então existem inteiros positivos $m_1|\cdots|m_k$, e um isomorfismo de grupos (não necessariamente único)*

$$\pi : G \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k},$$

onde cada $\mathbb{Z}_{m_i}$ é escrito aditivamente. Neste caso, se Ψ_t é a função $y \to ty$ sobre $H = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$, temos que

$$\pi(\varphi_t(g)) = \Psi_t(\pi(g)).$$

Em particular, $G(\varphi_t/G) = G(\Psi_t/H)$.

Demonstração. A existência de π decorre do Teorema da estrutura de grupos abelianos finitamente gerados. Basta então provar a igualdade $\pi \circ \varphi_t = \Psi_t \circ \pi$, uma vez que a mesma implica que os SDF's (G, φ_t) e (H, Ψ_t) são conjugados. Ora, como π é um homomorfismo, para $g \in G$ temos que

$$\pi(\varphi_t(g)) = \pi(g^t) = t \cdot \pi(g) = \Psi_t(\pi(g)).$$

□

Observe que temos o isomorfismo de grafos

$$G(\Psi_t/H) = \bigotimes_{i=1}^{k} G(\Psi_t/\mathbb{Z}_{m_i}).$$

SPOILER: *Os grafos $G(\Psi_t/\mathbb{Z}_m)$ só possuem componentes conexas da forma*

$$\mathrm{Cyc}(m) \otimes \mathcal{T},$$

onde $\mathcal{T}$ é uma árvore de uma sequência ν.

Logo, uma vez que sabemos calcular o produto tensorial entre ciclos e árvores vindo de sequências ν's, basta focarmos no caso de **grupos cíclicos**. Ainda faremos mais uma redução!

Definição 4.3. *Dados inteiros positivos n, t, a t-decomposição de n é a decomposição $n = n_0 \cdot n_1$, onde n_1 é o maior divisor de n, relativamente primo com t.*

Em outras palavras, n_0 colecta somente os fatores primos (e suas multiplicadades em n), comuns a n e t. Observe que $\mathbb{Z}_n$ é isomorfo a $\mathbb{Z}_{n_0} \times \mathbb{Z}_{n_1}$ (Teorema Chinês dos Restos). Obtemos o seguinte resultado.

Lema 4.4. *Sejam n, t inteiros positivos e seja $n = n_0 \cdot n_1$ sua t-decomposição. Então os seguintes valem*

1. $G(\Psi_t/\mathbb{Z}_n) = G(\Psi_t/\mathbb{Z}_{n_0}) \otimes G(\Psi_t/\mathbb{Z}_{n_1})$;
2. $\mathbb{T} = G(\Psi_t/\mathbb{Z}_{n_0})$ *é uma árvore;*
3. $G(\Psi_t/\mathbb{Z}_{n_1})$ *é da forma* $\bigoplus_{i=1}^{d} \mathrm{Cyc}(m_i)$.

Em particular, para a árvore $\mathbb{T}$ no item (i) e os mesmos inteiros m_i no item (ii), temos que

$$G(\Psi_t/\mathbb{Z}_n) = \bigoplus_{i=1}^{d} \mathrm{Cyc}(m_i, \mathbb{T}).$$

Demonstração. De maneira análoga ao que foi feito no caso de transformações lineares, basta mostrar que $(\mathbb{Z}_{n_0}, \Psi_t)$ é nilpotente e $(\mathbb{Z}_{n_1}, \Psi_t)$ é bijetivo.

Observe que os fatores primos de n_0 dividem t. Logo se α é o maior exponente que aparece na fatoração de n_0 como produto de primos, temos que $n_0 | t^\alpha$. Logo, para todo $y \in \mathbb{Z}_{n_0}$, temos que

$$\Psi_t^{(\alpha)}(y) = t^\alpha \cdot y \equiv 0 \pmod{n_0}.$$

Logo $(\mathbb{Z}_{n_0}, \Psi_t)$ é nilpotente com atrator $0 \in \mathbb{Z}_{n_0}$. Para mostrar que $(\mathbb{Z}_{n_1}, \Psi_t)$ é bijetivo, basta mostrar que Ψ_t é injetivo em $\mathbb{Z}_{n_1}$. Ora, se $x, y \in \mathbb{Z}_{n_1}$ são tais que $\Psi_t(x) = \Psi_t(y)$, temos que

$$tx \equiv ty \pmod{n_1}.$$

Logo $t(x-y) \equiv 0 \pmod{n_1}$, onde concluimos que $x = y$ pois $\mathrm{mdc}(t, n_1) = 1$. □

Logo para entender o grafo funcional da função monomial sobre grupos abelianos, basta estudar a função Ψ_t sobre grupos aditivos $\mathbb{Z}_n$, onde tal função é do tipo nilpotente ou bijetiva.

4.1 Funções Ψ_t bijetivas sobre grupos cíclicos

Obtemos o seguinte resultado.

Teorema 4.5. *Sejam N, t inteiros relativamente primos e considere a função $\Psi_t : \mathbb{Z}_N \to \mathbb{Z}_N$ tal que $\Psi_t(y) = t \cdot y \pmod{N}$. Então vale que*

$$G(\Psi_t/\mathbb{Z}_n) = \bigoplus_{d|N} \frac{\varphi(d)}{\mathrm{ord}_d\, t} \times \mathrm{Cyc}(\mathrm{ord}_d\, t),$$

onde $\varphi(d) = |\mathbb{Z}_d^*| = \#\{0 < r < d \,|\, \mathrm{mdc}(r, d) = 1\}$ é a função de Euler, e $\mathrm{ord}_d\, t$ é a ordem de t módulo d, i.e., o menor inteiro positivo e tal que $t^e \equiv 1 \pmod{d}$.

Demonstração. A prova deste teorema é, de certa forma, similar a prova do Teorema 3.15. Vamos tomar a simples representação $\mathbb{Z}_N = \{0, \ldots, N-1\}$.

Afirmação 1. *Para cada divisor d de N, seja $\mathcal{E}_d$ o conjunto dos elementos $y \in \mathbb{Z}_N$ tais que $\mathrm{mdc}(y, N) = \frac{N}{d}$. Então $\mathcal{E}_d$ possui cardinalidade $\varphi(d)$ e $\Psi_t(\mathcal{E}_d) = \mathcal{E}_d = \Psi_t^{-1}(\mathcal{E}_d)$. Em particular, os elementos de $\mathcal{E}_d$ compreendem componentes conexas de $G(T/V)$.*

Prova da Afirmação 1. Observe que $\mathrm{mdc}(y, N) = N/d$ se, e somente se, $y = N/d \cdot r$ com $0 \le r < d$ (pois $0 \le y < N$) e $\mathrm{mdc}(r, d) = 1$. Por definição, existem $\varphi(d)$ escolhas para r, onde concluímos que $\mathcal{E}_d$ possui $\varphi(d)$ elementos. Como Ψ_t é bijetivo, para concluir

basta mostrar que $\Psi_t(\mathcal{E}_d) \subseteq \mathcal{E}_d$. Para isto, seja $y \in \mathcal{E}_d$, logo $\Psi_t(y) \equiv ty \pmod N$ e então $\mathrm{mdc}(\Psi_t(y), N) = \mathrm{mdc}(ty, N)$, pelo lema de Euclides. Mas, como $\mathrm{mdc}(N, t) = 1$, temos que $\mathrm{mdc}(ty, N) = \mathrm{mdc}(y, N)$. Logo

$$\mathrm{mdc}(\Psi_t(y), N) = \mathrm{mdc}(y, N),$$

ou seja, $\Psi_t(y) \in \mathcal{E}_d$. □

Para concluir, basta mostrar a seguinte afirmação.

Afirmação 2. *Se $y \in \mathcal{E}_d$, então y pertence a um ciclo de comprimento $\mathrm{ord}_d\, t$ no grafo $G(\Psi_t/\mathbb{Z}_N)$.*

Prova da Afirmação 1. Por definição, o comprimento do ciclo ao qual $y \in \mathcal{E}_d$ pertence é igual ao menor inteiro positivo M tal que $\Psi_t^{(M)}(y) = y$, i.e.,

$$t^m \cdot y \equiv y \pmod N.$$

O último é equivalente a N dividir $y(t^M - 1)$, i.e., $\frac{N}{\mathrm{mdc}(N,y)} = d$ dividir $t^M - 1$. Segue da definição que o menor inteiro positivo com tal propriedade é $M = \mathrm{ord}_d\, t$. □

Exemplo 4.6. *Considere $t = 3$ e $G = \mathbb{Z}_{32}$. Pelo Teorema 4.5, temos que*

$$G(\Psi_3/\mathbb{Z}_{32}) = \bigoplus_{d|32} \frac{\varphi(d)}{\mathrm{ord}_d\, 3} \times \mathrm{Cyc}(\mathrm{ord}_d\, 3) = (2\times\mathrm{Cyc}(1)) \oplus (3\times\mathrm{Cyc}(2)) \oplus (2\times\mathrm{Cyc}(4)) \oplus (2\times\mathrm{Cyc}(8)).$$

Exemplo 4.7. *Considere $t = 2$ e $G = \mathbb{Z}_{21}$. Pelo Teorema 4.5, temos que*

$$G(\Psi_2/\mathbb{Z}_{21}) = \bigoplus_{d|21} \frac{\varphi(d)}{\mathrm{ord}_d\, 3} \times \mathrm{Cyc}(\mathrm{ord}_d\, 3) = \mathrm{Cyc}(1) \oplus \mathrm{Cyc}(2) \oplus (2 \times \mathrm{Cyc}(3)) \oplus (2 \times \mathrm{Cyc}(6)).$$

Exemplo 4.8. *Seja p um primo e r uma raiz primitiva módulo p, i.e., $\mathrm{ord}_p\, r = \varphi(p) = p - 1$. Temos que*

$$G(\Psi_r/\mathbb{Z}_p) = \mathrm{Cyc}(1) \oplus \mathrm{Cyc}(p-1).$$

Em geral podemos mostrar que, se $\mathrm{mdc}(t, N) = 1$ e $N > 1$, então $G(\Psi_t/N)$ possui pelo menos duas componentes conexas. Além disto, tal grafo possui exatamente 2 componentes conexas se, e somente se, N é primo e t é uma raiz primitiva módulo N.

4.2 Funções Ψ_t nilpotentes sobre grupos cíclicos

Aqui consideramos o SDF $(\Psi_t, \mathbb{Z}_N)$ onde todos os fatores primos de N dividem t. Como já mencionado, $G(\Psi_t/\mathbb{Z}_N)$ será uma árvore. O objetivo aqui é exatamente descrever tal árvore. Começamos com a seguinte definição.

Definição 4.9. *Dados inteiros N, t tais que todo divisor primo de $N > 1$ divide t, definimos $\nu_t(N) = (N_1, \ldots, N_k)$ como sendo a sequência definida recursivamente por $N_1 = \text{mdc}(N, t)$ e, para $i \geq 2$, temos que*

$$N_i = \text{mdc}\left(\frac{N}{N_1 \cdots N_{i-1}}, t\right),$$

onde k é o maior inteiro positivo tal que $N_k > 1$.

Para fixar tal conceito, vamos dar alguns exemplos.

Exemplo 4.10. *1.* $\nu_{15}(75) = (15, 5)$*;*

2. $\nu_{36}(384) = (12, 4, 4, 2)$*;*

3. $\nu_{20}(1000) = (20, 10, 5)$.

Observe que, em geral, temos que $\prod_{i=1}^{k} N_i = N$, i.e., a sequência $\nu_t(N)$ nos dá uma decomposição de N como produto de inteiros maiores que 1 onde cada termo divide o anterior.

O principal resultado desta seção é o seguinte teorema.

Teorema 4.11. *Sejam N, t inteiros tais que $N > 1$ e todo fator primo de N divide t. Então temos que*

$$G(\Psi_t/\mathbb{Z}_N) = \mathcal{T}_{\nu_t(N)},$$

onde $\mathcal{T}_{\nu_t(N)}$ é dada como na Subsec. 2.3.

Observamos primeiramente que se $N = \prod_{i=1}^{m} p_i^{\alpha_i}$ é a fatoração de N em primos, temos o isomorfismo $\mathbb{Z}_N = \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_m^{\alpha_m}}$ e então

$$G(\Psi_t/\mathbb{Z}_N) = \bigotimes_{i=1}^{m} G(\Psi_t/\mathbb{Z}_{p_i^{\alpha_i}}).$$

Além disto, podemos ver que $\nu_t(N)$ **é multiplicativa** com respeito ao produto estendido, i.e.,

$$\nu_t(N) = \nu_t(p_1^{\alpha_1}) * \cdots * \nu_t(p_m^{\alpha_m}).$$

Logo, pelo Teorema 2.10, basta mostrar nosso teorema para o caso em que N é **uma potência de um primo**.

4.2.1 Prova do Teorema 4.11

Precisamos da seguinte definição (clássica).

Definição 4.12. *Seja m um inteiro positivo e p um número primo. Definimos $\delta_p(m)$ como sendo o maior inteiro não negativo j tal que p^j divide m.*

Seja p um número primo, $N = p^\alpha$ e seja t tal que $\delta_p(t) = \beta \geq 1$. Quando $\beta < \alpha$, temos o seguinte resultado.

Lema 4.13. *Seja $N = p^\alpha$ com $\alpha \geq 1$ e t um inteiro positivo tal que $1 \leq \delta_p(t) = \beta < \alpha$. Sejam $d = \lfloor \frac{\alpha}{\beta} \rfloor$ e $E = \alpha - d\beta < \beta$ (quociente e resto da divisão de α por β). Se $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$, então os seguintes valem:*

1. *A equação $\Psi_t(y) = 0$ tem p^β soluções $y \in \mathbb{Z}_N$, uma sendo $y = 0$. Além disto, o conjunto das soluções não nulas de tal equação é a união (disjunta) dos conjuntos $A = \{y \in \mathbb{Z}_N \setminus \{0\} \,|\, \delta_p(y) \geq \alpha - E\}$ e $B = \{y \in \mathbb{Z}_N \,|\, \alpha - \beta \leq \delta_p(y) < \alpha - E\}$.*

2. *Suponha que $b \in \mathbb{Z}_N$ é não nulo. Então $\Psi_t(y) = b$ tem soluções $y \in \mathbb{Z}_N$ se, e somente se, $\delta_p(b) \geq \beta$. Neste caso, tal equação possui p^β soluções distintas e, para qualquer y solução, temos que $\delta_p(y) = \delta_p(b) - \beta$.*

Demonstração. Vamos fazer a prova de cada item separadamente.

1. Observe que $\Psi_t(y) = 0$ se, e somente se, $ty \equiv 0 \pmod{p^\alpha}$, ou seja, y é divisível por $p^{\alpha-\beta}$. Logo $y = 0$ ou $y \neq 0$ e $\delta_p(y) \geq \alpha - \beta$. A segunda condição compreende exatamente a união dos conjuntos A e B. Além disto, $\delta_p(y) \geq \alpha - \beta$ equivale a $y = p^{\alpha-\beta}z$ com $1 \leq z < p^\beta - 1$. Adicionando a solução nula $y = 0$, temos p^β soluções.

2. Observe que se $\Psi_t(y) = b$ tem solução, então possui p^β soluções (equação afim - equação homogênea). Observe que temos solução se e somente se existe y inteiro tal que $ty \equiv b \pmod{N}$. Equivalentemente, a equação diofantina

$$b = ty + Nx,$$

tem solução. Sabemos que isto ocorre se, e somente se, b é divisível por $\mathrm{mdc}(t, N) = p^\beta$, i.e., $\delta_p(b) \geq \beta$.

Se $y \in \mathbb{Z}_N$ é solução, temos que $ty \equiv b \pmod{p^\alpha}$ e assim $b = kp^\alpha + ty$. Neste caso, como b é não nulo, temos $\delta_p(b) < \alpha$ e então concluímos que

$$\delta_p(b) = \delta_p(ty) = \delta_p(t) + \delta_p(y)$$

Logo $\delta_p(y) = \delta_p(b) - \beta$.

□

Podemos agora provar o teorema para o caso $N = p^\alpha$.

Lema 4.14. *Sejam $N = p^\alpha$ e t com $\beta = \delta_p(t) \geq 1$ Então temos que*

$$G(\Psi_t/\mathbb{Z}_N) = \mathcal{T}_{\nu_t(N)}.$$

Demonstração. O caso em que $\beta \geq \alpha$ é trivial, uma vez que $\Psi_t(y) = 0$ para todo $y \in \mathbb{Z}_N$ e obtemos a árvore com $N - 1$ vertíces direcionados a raiz ($0 \in \mathbb{Z}_N$), que possui um loop. É simples de verificar que tal árvore de fato coincide com $\mathcal{T}_{\nu_t(N)}$, uma vez que $\nu_t(N) = (N)$.

Suponha agora que $\alpha > \beta$ e sejam d, E como no Lema 4.13. Observamos diretamente que

$$\nu_t(N) = (\underbrace{p^\beta, \ldots, p^\beta}_{d \text{ vezes}}, p^E).$$

Pelo item 2 do Lema 4.13, cada solução não nula $y \in \mathbb{Z}_N$ da equação $\Psi_t(y) = 0$ pode ser vista como a raiz de $\mathbb{T}(s(y))$, a árvore p^β-ádica completa de profundidade $s(y) = \left\lfloor \frac{\delta_p(y)}{\beta} \right\rfloor$. Se A, B são os conjuntos definidos no item 1 do Lema 4.13, vemos que $s(y) = d$ se $y \in A$ e $s(y) = d - 1$ se $y \in B$.

Segue então que

$$\mathbb{T}(s(y)) = \begin{cases} \mathcal{T}^{(d)}_{\nu_t(N)} & \text{se } y \in A, \\ \\ \mathcal{T}^{(d-1)}_{\nu_t(N)} & \text{se } y \in B. \end{cases}$$

Logo $G(\Psi_t/\mathbb{Z}_N)$ é a árvore $\mathbb{T}$ obtida a partir de $p^\alpha - 1$ vértices direcionados a raiz (com um loop), onde em $|A| = p^e - 1$ de tais vértices "penduramos" uma árvore isomorfa a $T^{(d)}_{\nu_t(N)}$ e em $|B| = p^\alpha - p^e$ vértices "penduramos" uma árvore isomorfa a $T^{(d-1)}_{\nu_t(N)}$. Olhando para a sequência $\nu_t(N)$, vemos que $\mathbb{T}$ é exatamente a árvore $\mathcal{T}_{\nu_t(N)}$. □

Exemplo 4.15. *Se $t = 12$ e $N = 54$, temos que $\nu_{12}(54) = (6, 3, 3)$ e então*

$$G(\Psi_{12}/\mathbb{Z}_{54}) = \mathcal{T}_{(6,3,3)}.$$

Usando o software SageMath, obtemos uma imagem de $G(\Psi_{12}/\mathbb{Z}_{54})$ na Figura 8.

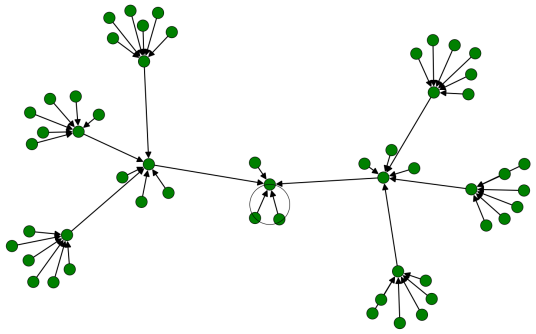

Figure 8: A árvore $\mathcal{T}_{(6,3,3)}$.

4.3 Estendendo para grupos abelianos: alguns exemplos

Observamos que, a partir das fórmulas para grafos funcionais de funções monomiais bijetivas e nilpotentes sobre grupos cíclicos, conseguimos obter o grafo funcional de funções monomiais sobre qualquer grupo abeliano. A receita é basicamente a seguinte:

1. Pegamos G grupo finito abeliano, com $G \cong \mathbb{Z}_{m_1} \times \cdots \mathbb{Z}_{m_k}$.

2. Dado t inteiro positivo, escrevemos $m_i = m_i^{(0)} \cdot m_i^{(1)}$, onde $m_i^{(1)}$ é o maior divisor de m_i, relativamente primo com t.

3. Temos $G \cong G_0 \times G_1$, onde $G_0 = \mathbb{Z}_{m_1^{(0)}} \times \cdots \times \mathbb{Z}_{m_k^{(0)}}$ e $G_1 = \mathbb{Z}_{m_1^{(1)}} \times \cdots \times \mathbb{Z}_{m_k^{(1)}}$.

4. Em particular, $G(\varphi_t/G) = G(\Psi_t/G_0 \times G_1) = G(\Psi_t/G_0) \otimes G(\Psi_t/G_1)$.

5. $G(\Psi_t/G_1) = \bigotimes_{i=1}^{k} G(\Psi_t/\mathbb{Z}_{m_i^{(1)}})$, onde cada $G(\Psi_t/\mathbb{Z}_{m_i^{(1)}})$ é soma de grafos do tipo $\mathrm{Cyc}(s)$(e sabemos operar com eles). Além disto, tal soma de grafos é precisamente descrita no Teorema 4.5.

6. $G(\Psi_t/G_0) = \bigotimes_{i=1}^{k} G(\Psi_t/\mathbb{Z}_{m_i^{(0)}}) = \bigotimes_{i=1}^{k} \mathcal{T}_{\nu_t(m_i^{(0)})} = \mathcal{T}_\nu$, onde

$$\nu = \nu_t(m_1^{(0)}) * \cdots * \nu_t(m_k^{(0)}),$$

é o produto estendido das sequências $\nu_t(m_i^{(0)})$.

Vamos a alguns exemplos.

Exemplo 4.16. *Seja $t = 3$ e $G \cong \mathbb{Z}_6 \times \mathbb{Z}_{18}$. Na notação do procedimento anterior, temos que:*

1. *$m_1 = 6, m_2 = 18$ e então $m_1^{(0)} = 3, m_2^{(0)} = 9$ e $m_1^{(1)} = 2 = m_2^{(1)} = 2$.*

2. *A parte bijetiva gera $G(\Psi_3/\mathbb{Z}_2) \otimes G(\Psi_3/\mathbb{Z}_2) = 4 \times \mathrm{Cyc}(1)$.*

3. *Temos que $\nu = \nu_3(3) * \nu_3(9) = (3) * (3,3) = (9,3)$.*

4. *Logo $G(\varphi_3/G) = 4 \times \mathrm{Cyc}(1, \mathcal{T}_{(9,3)})$.*

Utilizando o software SageMath, obtemos uma imagem de $G(\varphi_3/G)$ na Figura 9 (mostramos apenas uma componente, uma vez que temos 4 cópias de um mesmo grafo).

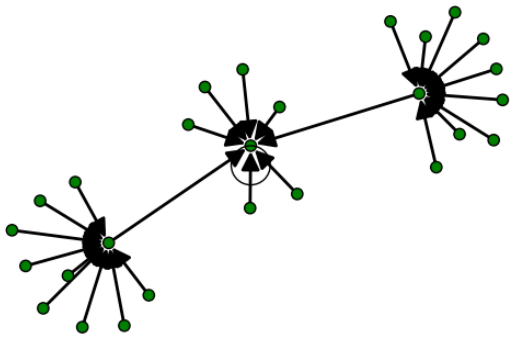

Figure 9: O grafo $G(\varphi_3/G)$.

Exemplo 4.17. *Seja* $t = 6$ *e* $G \cong \mathbb{Z}_{15} \times \mathbb{Z}_{18} \times \mathbb{Z}_{35} \times \mathbb{Z}_{40}$. *Na notação do procedimento anterior, temos que:*

1. $m_1 = 15, m_2 = 18, m_3 = 35, m_4 = 40$ *e então*

$$m_1^{(0)} = 3, m_2^{(0)} = 18, m_3^{(0)} = 1, m_4^{(0)} = 8,$$

   e

$$m_1^{(1)} = 5, m_2^{(1)} = 1, m_3^{(1)} = 35, m_4^{(1)} = 5.$$

2. *A parte bijetiva gera*

$$\bigotimes_{i=1}^{4} G(\Psi_6/\mathbb{Z}_{m_i^{(1)}}) = (125 \times \mathrm{Cyc}(1)) \oplus (375 \times \mathrm{Cyc}(2)).$$

3. *Temos que* $\nu = \nu_6(3) * \nu_6(18) * \nu_6(1) * \nu_6(8)$ *e então*

$$\nu = (3) * (6, 3) * (1) * (2, 2, 2) = (36, 6, 2).$$

4. *Logo*

$$G(\varphi_6/G) = (125 \times \mathrm{Cyc}(1, \mathcal{T}_{(36,6,2)})) \oplus (375 \times \mathrm{Cyc}(2, \mathcal{T}_{(36,6,2)})).$$

5 Algumas observações e referências para pesquisa

Nestas notas vimos alguns conceitos básicos de iterações de funções f sobre conjuntos finitos X, focando no grafo funcional $G(f/X)$ associado ao par (X, f) (chamado sistema dinâmico finito, SDF).

Discutimos em detalhes dois casos especiais: tranformações lineares em espaços vetoriais sobre corpos finitos e funções monomiais sobre grupos abelianos. Em particular, vimos como descrever o grafo funcional de tais SDF's.

5.1 Dinâmica sobre domínios de Dedekind

No caso de funções monomiais, vimos que era suficiente considerar grupos cíclicos, e reduzimos o último a considerar a função $\Psi_t : y \to ty \pmod N$ (multiplicação por t, módulo N). É digno de menção que em [5], consideramos uma generalização desta função para um ambiente mais geral: consideramos a função $\Psi_t : y \mapsto ty \pmod I$ onde $t \in \mathcal{D}$, $I \subset \mathcal{D}$ é um ideal não trivial e $\mathcal{D}$ é um **domínio de Dedekind residualmente finito**, i.e., o anel quociente $\mathcal{D}/I$ é sempre finito e I se decompõe (unicamente) como produto de ideais primos.

Observe que recuperamos o caso dos inteiros pois $\mathbb{Z}$ é um domínio com tais propriedades. De fato, os resultados dados em [5] generalizam o que fizemos para o caso dos inteiros. Os resultados e provas seguem de maneira bem semelhante, onde adaptamos certas funções para este ambiente mais geral (função norma de um ideal, função de Euler para ideais, etc).

5.2 Algumas referências

Para o leitor interessado, em [5] temos várias referências de artigos que trabalham dinâmica sobre diversas estruturas algébricas finitas.

No contexto de funções monomiais sobre grupos finitos, pouco sabemos sobre o caso **não abeliano**. Temos alguns artigos que nos dá descrições parciais do grafo [1, 2, 4] mas, em todos os casos, o resultado principal é bem implícito: precisamos descrever os elementos de G e localizá-los no grafo para ter uma visão geral do próprio grafo.

Em um trabalho em finalização do autor do texto com C. Qureshi (Universidad de la Republica, Uruguai), procuramos melhorar a descrição dos grafos funcionais com respeito aos grupos que são considerados em [1, 2, 4].

Bibliografia

[1] U. Ahmad. The power digraphs associated with generalized dihedral groups. *Discrete Math. Algorithms Appl.* 7(4): 1550057 (2015).

[2] U. Ahmad and M. Moeen. The digraphs arising by the power maps of generalized Quaternion groups. *J. Algebra Appl.* 16(9): 1750179 (2017).

[3] E. Bach, A. Bridy. *On the number of distinct functional graphs of affine-linear transformations over finite fields.* **Linear Algebra Appl.** (439) pp. 1312–1320 (2013).

[4] G. Deng and J. Zhao. Digraph from power mapping on noncommutative groups. *J. Algebra Appl.* 19(5): 2050084 (2020).

[5] C. Qureshi and L. Reis, *Dynamics of the a-map over residually finite Dedekind domains*, **J. Number Theory** (204) pp. 134–154 (2019).

[6] R. Toledo, *Linear finite dynamical systems*, **Commun. Algebra** (33) pp. 2977–2989 (2005).