

Selma Alves de Araújo

**Grafos funcionais e dinâmica de polinômios
sobre corpos finitos**

Uberlândia

2025

Selma Alves de Araújo

Grafos funcionais e dinâmica de polinômios sobre corpos finitos

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA**.

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica.

Universidade Federal de Uberlândia

Orientador: Prof. Dr. Victor Gonzalo Lopez Neumann

Uberlândia

2025

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU, MG, Brasil.

A659g Araújo, Selma Alves de, 2001-
2025 Grafos funcionais e dinâmica de polinômios sobre corpos finitos
[recurso eletrônico] / Selma Alves de Araújo. - 2025.

Orientador: Victor Gonzalo Lopez Neumann.
Dissertação (Mestrado) - Universidade Federal de Uberlândia,
Programa de Pós-graduação em Matemática.

Modo de acesso: Internet.
Disponível em: <http://doi.org/10.14393/ufu.di.2026.5025>
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. I. Neumann, Victor Gonzalo Lopez, 1974-, (Orient.).
II. Universidade Federal de Uberlândia. Programa de Pós-graduação em
Matemática. III. Título.

CDU: 51



UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 158 - Bairro Santa Mônica, Uberlândia-
MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.ppmat.ime.ufu.br - ppmat@ime.ufu.br



ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 121, PPGMAT				
Data:	25 de fevereiro de 2025	Hora de início:	9:30	Hora de encerramento:	11:30
Matrícula do Discente:	12312MAT008				
Nome do Discente:	Selma Alves de Araújo				
Título do Trabalho:	Grafos funcionais e dinâmica de polinômios sobre corpos finitos				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Propriedades de elementos especiais em corpos finitos				

Reuniu-se Reuniu-se em web conferência, através do link: <https://conferenciaweb.rnp.br/sala/victor-gonzalo-lopez-neumann>, a Banca examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Fábio Enrique Brochero Martinez - Instituto de Ciências Exatas, Departamento de Matemática/UFMG; ; Cícero Fernandes de Carvalho - IME/ UFU; e Victor Gonzalo Lopez Neumann - IME/UFU, orientador da candidata.

Iniciando os trabalhos o presidente da mesa, Dr. Victor Gonzalo Lopez Neumann , apresentou a Comissão Examinadora e a candidata, agradeceu a presença do público, e concedeu à Discente a palavra para a exposição do seu trabalho.

A duração da apresentação da Discente e o tempo de arguição e resposta foram conforme as normas do Programa. A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir a candidata. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando a candidata:

Aprovada.

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.



Documento assinado eletronicamente por **Cícero Fernandes de Carvalho, Professor(a) do Magistério Superior**, em 25/02/2025, às 11:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Fabio Enrique Brochero Martinez, Usuário Externo**, em 25/02/2025, às 11:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann, Professor(a) do Magistério Superior**, em 25/02/2025, às 16:11, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5999484** e o código CRC **6440B31E**.

Referência: Processo nº 23117.000284/2025-99

SEI nº 5999484

Ao meu padrinho Flávio (in memoriam).

Agradecimentos

Em primeiro lugar, agradeço a Deus pela força, saúde e resiliência que me permitiram superar cada desafio desta jornada acadêmica e pessoal.

Aos professores que contribuíram para minha formação. Em especial, agradeço imensamente ao meu orientador, Prof. Dr. Victor Gonzalo, por toda a paciência, orientação, conselhos e ensinamentos ao longo de meus estudos.

À minha irmã Hosana, companheira de vida cujo apoio incondicional foi meu porto seguro. Aos meus pais, pelo amor, suporte e incentivo que me acompanham desde o nascimento.

Aos meus avós, madrinhas, padrinhos, tios, primos e todos os demais familiares que de alguma maneira, contribuíram para minha trajetória. Cada gesto de apoio foi fundamental para que eu chegasse até aqui

A todos os meus amigos e colegas do mestrado, em especial à Katherine e à Mônica, por cada momento que passamos juntas nestes dois anos.

Agradeço também pelo auxílio financeiro proporcionado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), por meio da bolsa de mestrado concedida desde o primeiro semestre deste programa.

Por fim, agradeço a todos que, de forma direta ou indireta, fizeram parte desta trajetória.

ARAÚJO, S. A. *Grafos funcionais e dinâmica de polinômios sobre corpos finitos*. 2025. (55 pág) Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho, apresentamos um método de caracterizar a estrutura dos grafos funcionais de polinômios m -nice sobre corpos finitos. Iniciamos recordando conceitos elementares sobre corpos finitos e outros elementos algébricos essenciais. Em seguida, apresentamos algumas ferramentas aritméticas fundamentais para nosso objetivo, destacando os polinômios m -nice, classe de polinômios sobre a qual estabeleceremos nossos resultados sobre a estrutura dos grafos funcionais. Após isso, prosseguimos com a apresentação do conceito de grafos junto de suas classificações, com enfoque em grafos funcionais e árvores. Essas estruturas serão a base de nossos estudos sobre a dinâmica de polinômios sobre corpos finitos. Finalizamos o trabalho com a apresentação dos resultados que caracterizam detalhadamente a estrutura dos grafos de funções m -nice sobre corpos finitos.

Palavras-chave: Corpos finitos. Grafos funcionais. Polinômios m -nice.

ARAÚJO, S. A. *Functional graphs and dynamics of polynomials over finite fields*. 2025. (55 pages) p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we present a method to characterize the structure of functional graphs of m -nice polynomials over finite fields. We begin by reviewing elementary concepts about finite fields and other essential algebraic elements. Next, we introduce fundamental arithmetic tools critical to our objective, with emphasis on m -nice polynomials, a class of polynomials upon which we establish our results regarding the structure of functional graphs. Following this, we proceed to introduce the concept of graphs and their classifications, focusing on functional graphs and trees. These structures form the foundation of our study on the dynamics of polynomials over finite fields. We conclude the work by presenting results that characterize in detail the structure of functional graphs of m -nice polynomials over finite fields.

Keywords: Finite fields. Functional graphs. m -nice polynomials.

Lista de ilustrações

Figura 1 – Grafo $\mathcal{G}(f/\mathbb{F}_7)$ com $f(x) = 2x + 1$	28
Figura 2 – Grafo $\text{Cyc}(8)$	29
Figura 3 – Grafo $\text{Path}(7)$	30
Figura 4 – Grafo K_4	30
Figura 5 – Exemplo de floresta	32
Figura 6 – Exemplo de árvore com raiz e de árvore sem raiz	34
Figura 7 – Grafo $\mathcal{T}_V^1$ com $V = (3, 3)$	35
Figura 8 – Grafo $\mathcal{T}_V$ com $V = (3, 3)$	36
Figura 9 – Grafo $\mathcal{T}_V^1$ com $V = (4, 3, 2)$	36
Figura 10 – Grafo $\mathcal{T}_V^2$ com $V = (4, 3, 2)$	36
Figura 11 – Grafo $\mathcal{T}_V$ com $V = (4, 3, 2)$	37
Figura 12 – Grafo $\text{Cyc}(8, \mathcal{T})$, com $\mathcal{T} = \langle 2 \times \bullet \rangle$	39
Figura 13 – Grafos $\mathcal{G}_{f/\mathbb{F}_7}^{(0)}$ e $\mathcal{G}_{f/\mathbb{F}_7}^{(1)}$, com $f(x) = 2x + 1$	40
Figura 14 – Grafo $G_{g/\mathbb{F}_{181}}^{(0)}$, com $g(x) = 98x^{19} + 68x^{18} + 68x^{17} - 6x^{16} - 31x^{15}$	47
Figura 15 – Grafo $\mathcal{G}_{g/\mathbb{F}_{181}}^{(1)}$, com $g(x) = 98x^{19} + 68x^{18} + 68x^{17} - 6x^{16} - 31x^{15}$	52
Figura 16 – Grafo $\mathcal{G}(g/\mathbb{F}_{181})$, com $g(x) = 98x^{19} + 68x^{18} + 68x^{17} - 6x^{16} - 31x^{15}$. . .	54

Sumário

1	CONCEITOS FUNDAMENTAIS	12
1.1	Estruturas algébricas	12
1.1.1	Grupos e anéis	12
1.1.2	Corpos	14
1.1.3	Raízes da unidade	16
1.2	Polinômios m-nice	18
1.3	Função de Möbius	22
1.4	Máximo Divisor Comum Iterado	24
2	GRAFOS	26
2.1	Conceitos Iniciais e Tipos de Grafos	26
2.2	Árvores	32
3	DINÂMICA DE GRAFOS FUNCIONAIS SOBRE CORPOS FINITOS	38
3.1	Resultados auxiliares e terminologia	38
3.1.1	Terminologia	38
3.1.2	Resultados auxiliares	40
3.2	Resultados principais	44
	REFERÊNCIAS	55

Introdução

A iteração de funções polinomiais sobre corpos finitos gera sistemas dinâmicos discretos, cuja estrutura pode ser representada por grafos funcionais, que são os objetos centrais deste trabalho. Nas últimas décadas, o estudo da dinâmica de polinômios sobre corpos finitos tem atraído atenção significativa de vários autores, impulsionado principalmente pelas aplicações da dinâmica de polinômios sobre corpos finitos na criptografia. No entanto, apesar dos avanços, apenas algumas classes particulares de polinômios têm seus grafos funcionais completamente caracterizados.

Neste trabalho, apresentaremos resultados que nos fornecem um método para caracterizar a estrutura de grafos funcionais associados a uma classe específica de polinômios sobre corpos finitos, os polinômios m -nice. Esses polinômios, definidos na Seção 1.2, possuem propriedades que permitirão determinar a estrutura de seus grafos funcionais. Nossos resultados principais (Teoremas 3.12 e 3.14) descrevem a estrutura as componentes conexas do grafos desses polinômios.

A notação e os resultados apresentados neste trabalho são baseados principalmente do artigo (OLIVEIRA; BROCHERO MARTÍNEZ, 2024), que apresenta de forma sucinta um método para determinar a estrutura dos grafos funcionais relacionados aos polinômios m -nice.

Este trabalho está estruturado da seguinte maneira. No Capítulo 1 apresentamos os conceitos algébricos e aritméticos que serão utilizados ao longo deste estudo. No Capítulo 2, apresentamos uma introdução à teoria de grafos, com destaque aos conceitos relacionados a grafos funcionais. Começamos o Capítulo 3 apresentando a terminologia a ser utilizada, junto de alguns resultados auxiliares, e finalizamos apresentando os dois teoremas principais de nosso estudo, junto de um corolário que é consequência direta desses teoremas. Destacamos ainda que, ao longo dos Capítulos 2 e 3, foram adicionados diversos exemplos ilustrados a fim de auxiliar a compreensão do leitor a respeito dos conceitos e resultados.

Selma Alves de Araújo

Uberlândia-MG, 25 de fevereiro de 2025.

1 Conceitos fundamentais

Este capítulo reúne ferramentas algébricas e aritméticas essenciais para a análise de grafos funcionais associados a polinômios sobre corpos finitos, tema central deste trabalho. Na primeira seção, apresentamos os conceitos de grupos, anéis e corpos, que são estruturas algébricas fundamentais, com ênfase nas propriedades de corpos finitos, que serão utilizados ao estudarmos a dinâmica de polinômios. Nessa seção, também destacamos o papel das raízes da unidade, que terão papel fundamental para resultados que caracterizam os grafos funcionais no último capítulo.

Nas demais seções, introduzimos os conceitos de polinômios m -nice, função de Möbius e máximo divisor comum iterado. Esses conceitos fazem parte da base teórica necessária para apresentarmos os resultados mais importantes da dissertação.

As principais referências adotadas ao longo deste capítulo foram (LIDL; NIEDERREITER, 1997) e (GARCIA; LEQUAIN, 2014).

1.1 Estruturas algébricas

Nesta seção, apresentaremos definições e resultados básicos sobre estruturas algébricas, com enfoque em resultados sobre corpos finitos. Começaremos apresentando as definições de grupos e anéis, e algumas de suas propriedades. Depois apresentaremos o conceito de corpos junto de outros conceitos e resultados importantes relacionados a estes. Por fim, apresentaremos a definição de raízes da unidade, que serão fundamentais para os resultados principais deste trabalho.

1.1.1 Grupos e anéis

Definição 1.1. Um **grupo** é um conjunto G munido com uma operação binária, denotada por $*$, com as seguintes propriedades

- i. A operação $*$ é associativa, isto é, $(a * b) * c = a * (b * c)$, para todos $a, b, c \in G$.
- ii. Existe um elemento neutro, denotado por e , em G tal que, para todo $a \in G$, $e * a = a * e = a$.
- iii. Todo elemento a de G possui um elemento inverso a^{-1} em G tal que $a * a^{-1} = a^{-1} * a = e$.

Definição 1.2. Dizemos que um grupo G é **grupo abeliano** (ou **comutativo**) se $*$ é comutativa, isto é, se para todos $a, b \in G$,

$$a * b = b * a.$$

Definição 1.3. Dizemos que um grupo G é **cíclico** se existe $a \in G$ tal que para todo $b \in G$ existe um inteiro j com $b = a^j$. Tal elemento a é chamado **gerador** do grupo cíclico, e denotamos $G = \langle a \rangle$.

Definição 1.4. Um **anel** é um conjunto R munido com duas operações binárias, denotadas por $+$ e $\cdot$, com as seguintes propriedades

- i. R é grupo abeliano com respeito à operação $+$.
- ii. A operação $\cdot$ é associativa, isto é, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in R$.
- iii. As leis distributivas valem, isto é, para todo $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{e} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Notação 1.5. O elemento neutro em relação à soma em um anel será denotado por 0.

Definição 1.6. Um anel é dito **anel com unidade** se possui uma identidade multiplicativa, isto é, se existe um elemento $1 \in R$ tal que $1a = a1 = a$ para todo $a \in R$. Um anel é dito **multiplicativo** se a operação $\cdot$ é comutativa. Um anel é dito **domínio de integridade** se é um anel comutativo com unidade $1 \neq 0$ no qual não há divisores de zero, isto é, $ab = 0$ implica $a = 0$ ou $b = 0$. Um anel é dito **anel de divisão** se os elementos não nulos de R formam um grupo sobre a multiplicação.

Definição 1.7. Sejam A e B dois anéis com unidade. Definimos um **homomorfismo** como sendo um função $\varphi : A \rightarrow B$ de tal forma que, para todo $a, b \in A$, valem as seguintes propriedades:

- i. $\varphi(a + b) = \varphi(a) + \varphi(b)$,
- ii. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,
- iii. $\varphi(1) = 1$.

Definição 1.8. Seja R é um anel tal que existe um inteiro positivo n tal que $nr = 0$ para todo $r \in R$, então o menor inteiro positivo n tal que isso ocorre é chamado de **característica** de R . Além disso, neste caso dizemos que R tem **característica** n (ou **característica positiva** n). Se não existe um inteiro positivo n tal que $nr = 0$ para todo $r \in R$, então dizemos de R tem característica 0.

Teorema 1.9. *Todo anel $R \neq \{0\}$ com unidade, de característica positiva e sem divisores de zero deve ter característica prima.*

Demonstração. Como R tem elementos não nulos, R tem característica $n \geq 2$. Suponha que n não é primo, então podemos escrever $n = km$ com k e m inteiros, $1 < k$ e $m < n$. Portanto, denotando e como sendo a unidade de R , temos

$$0 = ne = (km)e = (ke)(me).$$

Logo, $ke = 0$ ou $me = 0$, pois R não tem divisores de zero. Então $kr = (ke)r = 0$ para todo $r \in R$ ou $mr = (me)r = 0$ para todo $r \in R$, contradição com a minimalidade de n . $\square$

1.1.2 Corpos

Definição 1.10. Um conjunto K é dito **corpo** se ele é um anel comutativo com unidade no qual todo elemento diferente de zero de K possui um inverso com respeito à multiplicação, ou seja

$$\forall x \in K \setminus \{0\}, \exists y \in K \text{ tal que } xy = 1.$$

Corolário 1.11. *Todo corpo finito tem característica prima.*

Demonstração. Pelo Teorema 1.9, basta mostrarmos que um corpo finito F tem característica positiva. Considere os múltiplos da identidade. Como F tem uma quantidade finita de elementos distintos, existem inteiros k e m com $1 \leq k < m$ tais que $ke = me$, então $(m - k)e = 0$. Portanto, F tem característica positiva. $\square$

Definição 1.12. Um conjunto K é dito **subcorpo** de um corpo F se $K \subseteq F$ e K é um corpo com as operações definidas em F . Também dizemos que F é uma **extensão** de K . Se $K \neq F$, dizemos que K é **subcorpo próprio** de F .

Notação 1.13. Seja K um corpo. Denotaremos K^* o conjunto dos elementos invertíveis de K , isto é, $K^* = K \setminus \{0\}$.

Definição 1.14. Um corpo que não tem subcorpos próprios é dito **corpo primo**.

Exemplo 1.15. Para todo primo p , $\mathbb{Z}_p$ é um corpo primo com p elementos. Esse corpo será denotado $\mathbb{F}_p$.

Definição 1.16. Sejam K um corpo e $f \in K[x]$ um polinômio de grau positivo e seja F uma extensão do corpo K . Dizemos que f se decompõe em F quando f pode ser escrito como produto de fatores lineares em $F[x]$, isto é, se existem elementos $\alpha_1, \dots, \alpha_n \in F$ tais que

$$f(x) = a(x - \alpha_1) \cdot (x - \alpha_n),$$

em que a é o coeficiente líder de f . O corpo F é dito **corpo de decomposição** de f sobre K se F é menor corpo que contém K em que f se decompõe em fatores lineares.

Definição 1.17. Chamaremos de **isomorfismo de corpos** a todo homomorfismo bijetor de corpos. Diremos que dois corpos são **isomorfos** quando existir um isomorfismo entre eles.

Proposição 1.18. *Seja F_q um corpo finito com q elementos. Então para todo $a \in F_q$, vale*

$$a^q = a.$$

Demonstração. A identidade $a^q = a$ é trivial para $a = 0$. Suponha $a \neq 0$. Como os elementos não nulos de F_q formam um grupo de ordem $q - 1$ sobre a multiplicação, pelo Teorema de Lagrange, temos $a^{q-1} = 1$ para todo $a \in F_q^*$. Multiplicando essa igualdade por a , obtemos $a^q = a$, o que conclui a demonstração. $\square$

Observação 1.19. *Seja F_q um corpo finito com q elementos. Então para todo $a \in F_q^*$, vale*

$$a^{q-1} = 1.$$

Teorema 1.20. *Para cada p primo e n inteiro positivo, existe um corpo finito com p^n elementos. Qualquer corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. Ver (LIDL; NIEDERREITER, 1997), Teorema 2.5. $\square$

Notação 1.21. Passaremos a denotar por $\mathbb{F}_q$ o único corpo finito com q elementos.

Teorema 1.22. *Para cada corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ dos elementos não nulos de $\mathbb{F}_q$ é cíclico.*

Demonstração. Podemos assumir $q \geq 4$, pois o resultado é trivial para $q < 4$. Seja $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ a decomposição em fatores primos da ordem $h = q - 1$ do grupo $\mathbb{F}_q^*$. Para cada i , com $1 \leq i \leq m$, o polinômio $x^{h/p_i} - 1$ tem no máximo h/p_i raízes em $\mathbb{F}_q$. Como $h/p_i < h$, segue que existem elementos não nulos em $\mathbb{F}_q$ que não são raízes desse polinômio. Seja a_i um elemento que não é raiz desse polinômio e defina $b_i = a_i^{h/p_i^{r_i}}$. Temos que $b_i^{p_i^{r_i}} = 1$, então a ordem de b_i é um divisor de $p_i^{r_i}$ e, portanto, é da forma p^{s_i} com $0 \leq s_i \leq r_i$. Por outro lado,

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1,$$

então a ordem de b_i é $p_i^{r_i}$. Mostraremos agora que $b = b_1 b_2 \cdots b_m$ tem ordem h . Suponhamos que a ordem de b é um divisor próprio de h , logo, a ordem de b é divisor de ao menos um dos m inteiros h/p_i , com $1 \leq i \leq m$. Podemos assumir sem perda de generalidade que

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1}.$$

Se $2 \leq i \leq m$, então $p_i^{r_i}$ divide h/p_1 , logo, $b_i^{h/p_1} = 1$. Portanto, $b_1^{h/p_1} = 1$. Isso implica que a ordem de b_1 deve dividir h/p_1 , contradição, pois a ordem de b_1 é p^{r_1} . Logo, $\mathbb{F}_q^*$ é um grupo cíclico com elemento gerador b . $\square$

Definição 1.23. Um gerador do grupo cíclico $\mathbb{F}_q^*$ é dito **elemento primitivo** de $\mathbb{F}_q$.

1.1.3 Raízes da unidade

Definição 1.24. Seja n um inteiro positivo. O corpo de decomposição de $x^n - 1$ sobre um corpo K é chamado de **n -ésimo corpo ciclotômico** sobre K e é denotado por $K^{(n)}$.

Definição 1.25. As raízes de $x^n - 1$ em $K^{(n)}$ são chamadas **raízes n -ésimas da unidade** sobre K e o conjunto de todas essas raízes é denotado por μ_n .

Definição 1.26. Sejam K um corpo de característica p e n um inteiro positivo não divisível por p . Então um elemento gerador do grupo cíclico μ_n é chamado de **raiz primitiva n -ésima da unidade** sobre K .

Exemplo 1.27. Considere o corpo finito $\mathbb{F}_{11}$. Vamos calcular as raízes 5-ésimas da unidade sobre $\mathbb{F}_{11}$.

Sabemos que o grupo multiplicativo $\mathbb{F}_{11}^*$ tem ordem 10, vamos encontrar uma raiz primitiva de $\mathbb{F}_{11}^*$, isto é, um elemento $\alpha \in \mathbb{F}_{11}^*$ tal que $\alpha^{10} = 1$ e $\alpha^k \neq 1$ para $1 \leq k < 10$.

Testando $\alpha = 2$, temos

$$\begin{aligned} 2^1 &= 2, & 2^2 &= 4, & 2^3 &= 8, & 2^4 &= 5, & 2^5 &= 10, \\ 2^6 &= 9, & 2^7 &= 7, & 2^8 &= 3, & 2^9 &= 6, & 2^{10} &= 1. \end{aligned}$$

Logo, 2 é uma raiz primitiva de $\mathbb{F}_{11}^*$. Como μ_5 é subgrupo de ordem 5 de $\mathbb{F}_{11}^*$, um de seus geradores é dado por $2^{10/5} = 2^2 = 4$. Por fim, temos

$$\mu_5 = \{4^0, 4^1, 4^2, 4^3, 4^4\} = \{1, 4, 5, 9, 3\}.$$

Portanto, $\mu_5 = \{1, 3, 4, 5, 9\}$ é o conjunto das raízes 5-ésimas da unidade sobre $\mathbb{F}_{11}^*$.

Exemplo 1.28. Considere o corpo finito $\mathbb{F}_{181}$. Iremos calcular as raízes 5-ésimas da unidade sobre $\mathbb{F}_{181}$.

Sabemos que o grupo multiplicativo $\mathbb{F}_{181}^*$ tem ordem 180, iremos encontrar uma raiz primitiva de $\mathbb{F}_{181}^*$, isto é, um elemento $\alpha \in \mathbb{F}_{181}^*$ tal que $\alpha^{180} = 1$ e $\alpha^k \neq 1$ para $1 \leq k < 180$.

Testando $\alpha = 2$, temos

$$2^{180} = 1, \quad 2^k \neq 1,$$

para $k \in \{36, 60, 90\}$. Logo, 2 é uma raiz primitiva de $\mathbb{F}_{181}^*$. Como μ_5 é subgrupo de ordem 5 de $\mathbb{F}_{181}^*$, um de seus geradores é dado por $2^{180/5} = 2^{36} = 59$. Por fim, obtemos

$$\mu_5 = \{59^0, 59^1, 59^2, 59^3, 59^4\} = \{1, 59, 42, 125, 135\}.$$

Logo, $\mu_5 = \{1, 42, 59, 125, 135\}$ é o conjunto das raízes 5-ésimas da unidade sobre $\mathbb{F}_{181}^*$.

1.2 Polinômios m -nice

Nesta seção, introduzimos o conceito de polinômios m -nice sobre corpos finitos e exploramos suas propriedades fundamentais. A estrutura desses polinômios permite estabelecermos resultados que serão utilizados para calcular a estrutura de seus grafos funcionais nas próximas seções.

Proposição 1.29. *Qualquer polinômio $f(x) \in \mathbb{F}_q[x]$ não nulo que satisfaça $f(0) = 0$ pode ser escrito de forma única como $f(x) = x^n h(x^{(q-1)/m})$, em que $h(0) \neq 0$, $n \geq 1$ e m é o menor inteiro satisfazendo essa propriedade.*

Demonstração. O polinômio f pode ser reescrito da forma

$$f(x) = x^n g(x),$$

em que n é um inteiro positivo determinado pela multiplicidade de 0 como raiz de f , e $g(x) = a_0 + a_1 x^{k_1} + \cdots + a_t x^{k_t}$, com $a_0 \neq 0$. Seja $S = \{k_1, \dots, k_t\}$ o conjunto dos expoentes de g e tome $d = \text{mdc}(S \cup \{q-1\})$. Definamos

$$m = \frac{q-1}{d}.$$

Sabemos que m é inteiro, pois d divide $q-1$. Além disso, cada expoente $k_i \in S$ é múltiplo de d , logo, podemos escrever $k_i = dl_i$. Definamos $h(x) = a_0 + a_1 x^{l_1} + \cdots + a_t x^{l_t}$. Como $a_0 \neq 0$, então $h(0) \neq 0$ e, além disso, $g(x) = h(x^d)$. Resta mostrar a minimalidade e unicidade de m .

Se m' satisfaz $g(x) = h'(x^{(q-1)/m'})$, então $(q-1)/m'$ seria um divisor de todos os elementos de S . Além disso, $(q-1)/m'$ divide $q-1$. Logo, $(q-1)/m'$ divide d . Isso implica que m divide m' , provando que m é o menor elemento satisfazendo essa propriedade.

Por fim, a fatorização $f(x) = x^n h(x^{(q-1)/m})$ é única, pois n é unicamente determinado pela multiplicidade de 0 como raiz, h é unicamente determinado pelos coeficientes de g , e m é unicamente determinado por $q-1$ e pelos expoentes de g .

□

Definição 1.30. O número m apresentado no resultado anterior é chamado de **índice** do polinômio f sobre $\mathbb{F}_q$.

Definição 1.31. Seja $f(x) \in \mathbb{F}_q[x]$, com $f(0) = 0$, um polinômio não nulo com índice m , definimos seu **polinômio associado**, como

$$\psi_f(x) = x^n h(x)^{\frac{q-1}{m}}.$$

Observação 1.32. Vejamos que a função $\psi_f : \mu_m \rightarrow \mu_m \cup \{0\}$, associada ao polinômio $\psi_f(x)$ da definição anterior, está bem definida. Isto é, vejamos que $\text{Im}(\psi_f) \subseteq \mu_m \cup 0$. De fato,

seja $\alpha \in \mu_m$. Se $h(\alpha) = 0$, então $\psi_f(\alpha) = 0$. Se $h(\alpha) \neq 0$, então, como $h(\alpha)^{q-1} = 1$ e $\alpha^m = 1$, temos $(\psi_f(\alpha))^m = \alpha^{nm}h(\alpha)^{q-1} = 1$, logo, $\psi_f(\alpha) \in \mu_m$. Portanto, $\psi_f : \mu_m \rightarrow \mu_m \cup \{0\}$ está bem definida.

Definição 1.33. Um polinômio $f(x) \in \mathbb{F}_q[x]$ não nulo com índice m é dito **m-nice** sobre $\mathbb{F}_q$ se a função $x \mapsto \psi_f(x)$ for injetora de $\mu_m \setminus \psi_f^{-1}(0)$ para μ_m .

Definição 1.34. Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio não nulo com índice m , definimos

$$\psi_f^{-\infty}(0) = \{\gamma \in \mu_m : \psi_f^{(i)}(\gamma) = 0 \text{ para algum inteiro positivo } i\}.$$

Proposição 1.35. *Seja $f(x) = x^n h(x^{(q-1)/m}) \in \mathbb{F}_q[x]$ um polinômio com índice m e suponha que h não tenha raízes em μ_m . Então $\psi_f^{-\infty}(0) = \emptyset$.*

Demonstração. Seja $\gamma \in \mu_m$. Mostraremos que não existe inteiro positivo i tal que $\psi_f^{(i)}(\gamma) = 0$. Sabemos que $\psi_f(\gamma) = \gamma^n h(\gamma)^{(q-1)/m}$ e que $h(\gamma) \neq 0$ por hipótese. Pela Observação 1.19,

$$h(\gamma)^{q-1} = \left(h(\gamma)^{\frac{q-1}{m}}\right)^m = 1.$$

Logo, $h(\gamma^{(q-1)/m}) \in \mu_m$ e, portanto, $\psi_f(\gamma) = \gamma^n h(\gamma^{(q-1)/m}) \in \mu_m$.

Como $\gamma \neq 0$ e $h(\gamma) \neq 0$, temos $\psi_f(\gamma) \neq 0$. Por fim, como $\psi_f \in \mu_m$ e $0 \notin \mu_m$, concluímos que $\psi_f^{(i)}(\gamma) = \psi_f(\psi_f^{(i-1)}(\gamma)) \neq 0$ para qualquer inteiro positivo i , isto é, $\psi_f^{-\infty} = 0$. $\square$

Observação 1.36. Seja $f(x) = x^n h(x^{(q-1)/m}) \in \mathbb{F}_q[x]$ um polinômio com índice m e suponha que h possua raiz em μ_m . Então $\psi_f^{-\infty}(0) \neq \emptyset$.

Exemplo 1.37. Considere a função $f(x) = x + x^3 + x^5 \in \mathbb{F}_{11}$. Reescrevendo f na forma $f(x) = x^n h(x^{(q-1)/m})$, obtemos

$$f(x) = x(1 + x^2 + x^4) = xh(x^2),$$

em que $h(y) = 1 + y + y^2$, com $h(0) \neq 0$. Sabemos do Exemplo 1.27 que $\mu_5 = \{1, 3, 4, 5, 9\}$. Verificando os valores de $\psi_f(x) = xh(x)^2$ nos elementos de μ_5 , temos

$$\psi_f(1) = 9, \quad \psi_f(3) = 1, \quad \psi_f(4) = 4, \quad \psi_f(5) = 9, \quad \psi_f(9) = 4.$$

Logo, ψ_f não é injetora de $\mu_5 \setminus \psi_f^{-1}(0)$ para μ_5 . Portanto, f não é 5-nice.

Exemplo 1.38. Considere $g(x) = 98x^{19} + 68x^{18} + 68x^{17} - 6x^{16} - 31x^{15} \in \mathbb{F}_{181}[x]$, isto é, $g(x) = x^{15}h(x^{36})$, em que

$$h(x) = 98x^4 + 68x^3 + 68x^2 - 6x - 31,$$

com $h(0) \neq 0$, e $\psi_g(x) = x^{15}h(x)^{36}$. Pelo Exemplo 1.28, sabemos que $\mu_5 = \{1, 42, 59, 125, 135\}$ e 2 é um elemento primitivo de $\mathbb{F}_{181}^*$. Além disso,

$$\psi_g(59) = 42, \quad \psi_g(42) = 0, \quad \psi_g(125) = 125, \quad \psi_g(1) = 135, \quad \psi_g(135) = 1,$$

portanto, $g(x)$ é 5-nice sobre $\mathbb{F}_{181}$.

Proposição 1.39. *Seja $f(x) = x^n h(x^{(q-1)/m})$ um polinômio com índice m e seja k um inteiro positivo. Então:*

$$f^{(k)}(x) = x^{n^k} \prod_{i=0}^{k-1} h\left(\psi_f^{(i)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{k-i-1}}.$$

Demonstração. Aplicaremos indução para mostrar esse resultado. Veja que

$$f(x) = f^{(1)}(x) = x^n h\left(x^{\frac{q-1}{m}}\right).$$

Suponha $k = 1$, então

$$\begin{aligned} x^{n^k} \prod_{i=0}^{k-1} h\left(\psi_f^{(i)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{k-i-1}} &= x^{n^1} \prod_{i=0}^0 h\left(\psi_f^{(i)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{-i}} \\ &= x^n h\left(\psi_f^{(0)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^0} \\ &= x^n h\left(x^{\frac{q-1}{m}}\right) \\ &= f^{(1)}(x). \end{aligned}$$

Suponha que o resultado seja válido para k . Provaremos que vale para $k + 1$. Note que $f^{(k+1)}(x) = f^{(k)}(f(x))$. Aplicando a hipótese de indução, temos

$$\begin{aligned} f^{(k)}(f(x)) &= (f(x))^{n^k} \prod_{i=0}^{k-1} h\left(\psi_f^{(i)}\left((f(x))^{\frac{q-1}{m}}\right)\right)^{n^{k-i-1}} \\ &= \left(x^n h\left(x^{\frac{q-1}{m}}\right)\right)^{n^k} \prod_{i=0}^{k-1} h\left(\psi_f^{(i)}\left(x^n h\left(x^{\frac{q-1}{m}}\right)^{\frac{q-1}{m}}\right)\right)^{n^{k-i-1}}. \end{aligned} \quad (1.1)$$

Antes de continuarmos a desenvolver a equação acima, vamos buscar outra forma de escrever $\psi_f^{(i)}\left(x^n h\left(x^{\frac{q-1}{m}}\right)^{\frac{q-1}{m}}\right)$. Segue da definição de ψ_f que

$$\psi_f\left(x^{\frac{q-1}{m}}\right) = \left(x^{\frac{q-1}{m}}\right)^n h\left(x^{\frac{q-1}{m}}\right)^{\frac{q-1}{m}} = \left(x^n h\left(x^{\frac{q-1}{m}}\right)\right)^{\frac{q-1}{m}} = f(x)^{\frac{q-1}{m}}.$$

Então

$$\begin{aligned} \psi_f^{(i)}\left(x^n h\left(x^{\frac{q-1}{m}}\right)^{\frac{q-1}{m}}\right) &= \psi_f^{(i)}\left(f(x)^{\frac{q-1}{m}}\right) \\ &= \psi_f^{(i)}\left(\psi_f\left(x^{\frac{q-1}{m}}\right)\right) \\ &= \psi_f^{(i+1)}\left(x^{\frac{q-1}{m}}\right). \end{aligned} \quad (1.2)$$

Continuando a desenvolver a Equação 1.1, e utilizando a Equação 1.2, temos

$$f^{(k+1)}(x) = \left(x^n h\left(x^{\frac{q-1}{m}}\right)\right)^{n^k} \prod_{i=0}^{k-1} h\left(\psi_f^{(i+1)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{k-i-1}}.$$

Definindo $j := i + 1$ e aplicando uma mudança de variável em i , obtemos

$$f^{(k+1)}(x) = \left(x^n h\left(x^{\frac{q-1}{m}}\right)\right)^{n^k} \prod_{j=1}^k h\left(\psi_f^{(j)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{k-j}}. \quad (1.3)$$

Observe que, supondo $j = 0$,

$$h\left(\psi_f^{(j)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{k-j}} = h\left(\psi_f^{(0)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{k-0}} = h\left(x^{\frac{q-1}{m}}\right)^{n^k}.$$

Prosseguindo com o desenvolvimento da Equação 1.3 e utilizando a equação acima,

$$\begin{aligned} f^{(k+1)}(x) &= x^{n^{k+1}} h\left(\psi_f^{(0)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{k-0}} \prod_{j=1}^k h\left(\psi_f^{(j)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{k-j}} \\ &= x^{n^{k+1}} \prod_{j=0}^k h\left(\psi_f^{(j)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{k-j}} \\ &= x^{n^{k+1}} \prod_{j=0}^{(k+1)-1} h\left(\psi_f^{(j)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{(k+1)-j-1}}, \end{aligned} \quad (1.4)$$

o que conclui a demonstração por indução. □

Lema 1.40. *Seja k um inteiro positivo e $b \in \mathbb{F}_q^*$. Suponhamos que $f(x) = x^n h(x^{(q-1)/m})$ seja m -nice. Se $x \in \mathbb{F}_q$ é solução da equação $f^{(k)}(x) = b$, então*

$$x^{\frac{q-1}{m}} = \psi_f^{-(k)}\left(b^{\frac{q-1}{m}}\right).$$

Demonstração. Provaremos o resultado por indução. Sejam $k = 1$ e $x \in \mathbb{F}_q$ uma solução da equação $f(x) = b$. Então

$$b^{\frac{q-1}{m}} = (f(x))^{\frac{q-1}{m}} = \psi_f\left(x^{\frac{q-1}{m}}\right).$$

isto é, $\psi_f\left(x^{(q-1)/m}\right) = b^{(q-1)/m}$. Como ψ_f é injetor, segue que $x^{(q-1)/m} = \psi_f^{-k}\left(b^{(q-1)/m}\right)$.

Suponha que o resultado seja válido para $k \geq 1$, mostremos que vale para $k + 1$. Seja $x \in \mathbb{F}_q$ uma solução de $f^{(k+1)}(x) = b$. Reescrevendo a equação,

$$f^{(k+1)}(x) = f^{(k)}(f(x)) = b.$$

Pela hipótese de indução,

$$\psi_f^{(-k)}\left(b^{\frac{q-1}{m}}\right) = (f(x))^{\frac{q-1}{m}} = \left(x^n h\left(x^{\frac{q-1}{m}}\right)\right)^{\frac{q-1}{m}} = x^{\frac{q-1}{m}n} h\left(x^{\frac{q-1}{m}}\right)^{\frac{q-1}{m}} = \psi_f\left(x^{\frac{q-1}{m}}\right).$$

Aplicando a k -ésima iteração de ψ_f nas extremidades da equação acima,

$$b^{\frac{q-1}{m}} = \psi_f^{(k)}\left(\psi_f\left(x^{\frac{q-1}{m}}\right)\right) = \psi_f^{(k+1)}\left(x^{\frac{q-1}{m}}\right).$$

Por fim, como f é m -nice, então ψ_f e suas iteradas são injetoras em μ_m . Logo,

$$x^{\frac{q-1}{m}} = \psi_f^{-(k+1)}\left(b^{\frac{q-1}{m}}\right).$$

□

1.3 Função de Möbius

Nesta seção, apresentaremos a definição da função de Möbius. Essa função e suas propriedades serão muito utilizadas no último teorema deste trabalho.

Definição 1.41. A função de Möbius, denotada μ , é definida sobre os inteiros positivos e é dada por

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ (-1)^k & \text{se } n \text{ é o produto de } k \text{ primos distintos,} \\ 0 & \text{se } p^2 | n, \text{ com } p \text{ primo.} \end{cases}$$

Lema 1.42. Seja n um inteiro positivo e μ a função de Möbius. Então

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1. \end{cases}$$

Demonstração. Se $n = 1$, então

$$\sum_{d|1} \mu(d) = \mu(1) = 1.$$

Seja $n > 1$, vamos levar em consideração apenas os divisores positivos d de n nos quais $\mu(d) \neq 0$, isto é, $d = 1$ ou d é produto de primos distintos.

Portanto, sejam $p_1, \dots, p_k$ os primos distintos divisores de n , então

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^k \mu(p_i) + \sum_{1 \leq i_1 < i_2 \leq k} \mu(p_{i_1} p_{i_2}) \\ &\quad + \sum_{1 \leq i_1 < i_2 < i_3 \leq k} \mu(p_{i_1} p_{i_2} p_{i_3}) + \dots + \mu(p_1 \dots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \dots + \binom{k}{k}(-1)^k \\ &= (1 + (-1))^k \\ &= 0. \end{aligned}$$

□

Teorema 1.43 (Fórmula da Inversão de Möbius). Sejam G e g funções definidas sobre os inteiros positivos tais que $G(n) = \sum_{d|n} g(d)$. Então,

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) G(d).$$

Demonstração. Seja n um inteiro positivo. Suponhamos que G e g são funções tais que $G(n) = \sum_{d|n} g(d)$. Então, utilizando a hipótese e o Lema 1.42, temos

$$\begin{aligned}
 \sum_{d|n} \mu\left(\frac{n}{d}\right) G(d) &= \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) \\
 &= \sum_{d|n} \mu(d) \sum_{c|n/d} g(c) \\
 &= \sum_{c|n} \sum_{d|n/c} \mu(d) g(c) \\
 &= \sum_{c|n} g(c) \sum_{d|n/c} \mu(d) \\
 &= g(n).
 \end{aligned}$$

□

1.4 Máximo Divisor Comum Iterado

Nessa seção apresentaremos o conceito de máximo divisor comum iterado de um inteiro positivo v em relação a um inteiro positivo n , denotado $\text{mdc}_n(v)$. O cálculo do $\text{mdc}_n(v)$ nos providenciará sequências não crescentes de inteiros positivos que serão muito úteis ao estudarmos sobre árvores elementares e grafos V -regulares. Além disso, os dois resultados apresentados nesta seção serão importantes para a demonstração dos resultados principais deste trabalho.

Definição 1.44. Sejam n e v inteiros positivos. Denotaremos por $\text{mdc}_n(v)$ o **máximo divisor comum iterado de v em relação a n** , definido como sendo a s -tupla $(v_1, \dots, v_s)$, em que

$$v_i = \frac{\text{mdc}(n^i, v)}{\text{mdc}(n^{i-1}, v)}$$

para $i \geq 1$, e s é o menor inteiro positivo tal que $v_{s+1} = 1$.

Exemplo 1.45. Vamos calcular o máximo divisor comum iterado de 9 em relação a 15.

$$v_1 = \frac{\text{mdc}(15, 9)}{\text{mdc}(1, 9)} = \frac{3}{1} = 3, \quad v_2 = \frac{\text{mdc}(15^2, 9)}{\text{mdc}(15, 9)} = \frac{9}{3} = 3,$$

$$v_3 = \frac{\text{mdc}(15^3, 9)}{\text{mdc}(15^2, 9)} = \frac{9}{9} = 1.$$

Então $v_i = 1$, $\forall i \geq 3$. Portanto, temos $\text{mdc}_{15}(9) = (3, 3)$.

Lema 1.46. Sejam n e v inteiros positivos e $\text{mdc}_n(v) = (v_1, \dots, v_s)$. Então, para todo $j \in \{1, \dots, s\}$, vale

$$v_1 \cdots v_j = \text{mdc}(n^j, v).$$

Demonstração. Demonstraremos esse resultado por indução sobre j . Suponha $j = 1$, então

$$v_1 = \frac{\text{mdc}(n^1, v)}{\text{mdc}(n^0, v)} = \frac{\text{mdc}(n, v)}{\text{mdc}(1, v)} = \text{mdc}(n^1, v).$$

Suponha que o resultado seja válido para j . provemos que vale para $j + 1$. Temos

$$\begin{aligned} v_1 \cdots v_j v_{j+1} &= (v_1 \cdots v_j) \cdot v_{j+1} \\ &= \text{mdc}(n^j, v) \cdot v_{j+1} \\ &= \text{mdc}(n^j, v) \cdot \frac{\text{mdc}(n^{j+1}, v)}{\text{mdc}(n^j, v)} \\ &= \text{mdc}(n^{j+1}, v). \end{aligned}$$

Logo, $v_1 \cdots v_{j+1} = \text{mdc}(n^{j+1}, v)$ e o resultado segue. $\square$

Proposição 1.47. Sejam n e v inteiros positivos e seja $\text{mdc}_n(v) = (v_1, \dots, v_s)$. Então $(v_1, \dots, v_s)$ é uma sequência não crescente de inteiros positivos.

Demonstração. Primeiramente vejamos que v_j é um inteiro positivo para todo $j \in \{1, \dots, s\}$. Por definição,

$$v_j = \frac{\text{mdc}(n^j, v)}{\text{mdc}(n^{j-1}, v)}.$$

Como n^{j-1} divide n^j , temos que $\text{mdc}(n^{j-1}, v)$ divide $\text{mdc}(n^j, v)$, logo, v_j é um inteiro positivo.

Podemos reescrever n e v na forma fatorada

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad v = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k},$$

em que p_i são primos distintos, a_i e b_i são inteiro não negativos para todo $i \in \{1, \dots, k\}$. Então

$$\begin{aligned} v_j &= \frac{\text{mdc}(n^j, v)}{\text{mdc}(n^{j-1}, v)} \\ &= \frac{p_1^{\min(ja_1, b_1)} p_2^{\min(ja_2, b_2)} \cdots p_k^{\min(ja_k, b_k)}}{p_1^{\min((j-1)a_1, b_1)} p_2^{\min((j-1)a_2, b_2)} \cdots p_k^{\min((j-1)a_k, b_k)}} \\ &= p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}, \end{aligned}$$

em que $l_i = \min(ja_i, b_i) - \min((j-1)a_i, b_i)$ com $i \in \{1, \dots, k\}$. Analogamente para v_{j+1} , obtemos

$$\begin{aligned} v_{j+1} &= \frac{\text{mdc}(n^{j+1}, v)}{\text{mdc}(n^j, v)} \\ &= \frac{p_1^{\min((j+1)a_1, b_1)} p_2^{\min((j+1)a_2, b_2)} \cdots p_k^{\min((j+1)a_k, b_k)}}{p_1^{\min(ja_1, b_1)} p_2^{\min(ja_2, b_2)} \cdots p_k^{\min(ja_k, b_k)}} \\ &= p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}, \end{aligned}$$

em que $m_i = \min((j+1)a_i, b_i) - \min(ja_i, b_i)$ com $i \in \{1, \dots, k\}$.

Basta mostrarmos que $l_i \geq m_i$ para todo $i \in \{1, \dots, k\}$. Isso é equivalente a mostrar que $l_i - m_i \geq 0$. Vamos dividir essa parte da demonstração em casos.

- Se $b_i \leq (j-1)a_i$, temos $l_i = m_i = b_i - b_i = 0$ e o resultado segue.
- Se $(j-1)a_i \leq b_i \leq ja_i$, temos $l_i = b_i - (j-1)a_i$ e $m_i = b_i - b_i = 0$, então $l_i - m_i = b_i - (j-1)a_i \geq 0$ e o resultado segue.
- Se $ja_i \leq b_i \leq (j+1)a_i$, temos $l_i = ja_i - (j-1)a_i = a_i$ e $m_i = b_i - ja_i$, então $l_i - m_i = a_i - b_i + ja_i = (j+1)a_i - b_i \geq 0$ e o resultado segue.
- Se $(j+1)a_i \leq b_i$, temos $l_i = ja_i - (j-1)a_i = a_i$ e $m_i = (j+1)a_i - ja_i = a_i$, então $l_i - m_i = a_i - a_i = 0$ e o resultado segue.

Portanto, $v_j \geq v_{j+1}$ para todo $j \in \{1, \dots, s-1\}$, isto é, $(v_1, \dots, v_s)$ é uma sequência não crescente de inteiros positivos. $\square$

2 Grafos

Este capítulo introduz os fundamentos da teoria de grafos, necessários para a análise da dinâmica de polinômios sobre corpos finitos, tema central deste trabalho.

As principais referências usadas nesse capítulo são o livro (DIESTEL, 1997) e a apostila (JURKIEWICZ, 2007), que fornecem uma base teórica para estudos sobre grafos e suas propriedades.

2.1 Conceitos Iniciais e Tipos de Grafos

Nesta primeira seção, veremos conceitos essenciais da teoria de grafos, com ênfase em grafos direcionados, ciclos e caminhos. Também definiremos formalmente os grafos funcionais, objetos centrais deste estudo, que descrevem o comportamento iterativo de funções discretas e serão utilizados amplamente no próximo capítulo para modelar a dinâmica de funções polinomiais sobre corpos finitos.

Definição 2.1. Um **grafo simples** é um par $G = (V, A)$, em que $A \subseteq [V]^2$. Os elementos de V são chamados de **vértices** e os elementos de A são chamados de **arestas** do grafo G .

Definição 2.2. A **ordem** de um grafo G é a quantidade de vértices em G e denotada $|G|$.

Notação 2.3. A quantidade de arestas em um grafo G é denotada $\|G\|$. O conjunto dos vértices de G é denotado por $V(G)$ e o conjunto das arestas por $A(G)$.

Definição 2.4. Um vértice é **incidente** com uma aresta se ele pertence a essa aresta. Os dois vértices x, y incidentes de uma aresta são ditos suas **pontas**. Dizemos que a aresta liga suas pontas e normalmente a denotamos por $\{x, y\}$.

Definição 2.5. Um **grafo** (ou **multigrafo**) é um par $G = (V, A)$ de conjuntos disjuntos (de vértices e arestas) com uma função $A \rightarrow [V]^2$ que designa cada aresta a um ou dois vértices, suas pontas.

Definição 2.6. Um **grafo direcionado** (ou **digrafo**) é um par $\mathcal{G} = (V, A)$ de conjuntos disjuntos (de vértices e arestas) com duas funções

$$\text{Inic} : A \rightarrow V \quad \text{e} \quad \text{Fin} : A \rightarrow V$$

que designam cada aresta a a um vértice inicial $\text{Inic}(a)$ e a um vértice final $\text{Fin}(a)$.

Definição 2.7. Dado um vértice v em um grafo direcionado $\mathcal{G}$, dizemos que v é **filho** de um vértice u em $\mathcal{G}$ se existe uma aresta $a \in A(\mathcal{G})$ tal que $\text{Inic}(a) = u$ e $\text{Fin}(a) = v$.

Definição 2.8. Dois vértices são ditos vértices **adjacentes** (ou **vizinhos**) se fazem parte de uma mesma aresta. Duas arestas distintas são ditas **adjacentes** (ou **vizinhas**) se possuem uma ponta em comum.

Definição 2.9. Seja G um grafo. Um subconjunto $V_1 \subseteq V(G)$ é dito um **conjunto independente de vértices** quando não existem vértices adjacentes em V_1 . Um subconjunto $A_1 \subseteq A(G)$ é dito um **conjunto independente de arestas** quando não existem arestas adjacentes em A_1 .

Definição 2.10. Consideremos dois grafos $G = (V, A)$ e $G' = (V', A')$. Uma função $\varphi : G \rightarrow G'$ é um **homomorfismo** de G em G' se preserva a adjacência dos vértices, isso é, se $\{\varphi(x), \varphi(y)\} \in A'$ sempre que $\{x, y\} \in A$.

Definição 2.11. Seja $\varphi : G = (V, A) \rightarrow G' = (V', A')$ um homomorfismo bijetor cuja inversa φ^{-1} também é um homomorfismo, isso é, $\{x, y\} \in A$ se, e somente se, $\{\varphi(x), \varphi(y)\} \in A'$ para todo $x, y \in V$. Então φ é um **isomorfismo** de G em G' e dizemos que G e G' são **isomorfos**. Um isomorfismo de G em si mesmo é chamado de **automorfismo**.

Definição 2.12. Dizemos que um grafo possui **arestas múltiplas** se existe mais de uma aresta ligando os mesmos vértices.

Definição 2.13. Uma aresta com um único vértice em ambas as pontas é chamada de **laço**.

Observação 2.14. Veja que grafos direcionados são um tipo especial de grafos no qual é adicionada uma direção a cada aresta. Uma aresta a de um grafo direcionado, com $\text{Inic}(a) = x$ e $\text{Fin}(a) = y$, normalmente será denotada por (x, y) . Além disso, grafos simples são grafos que não possuem laços ou arestas múltiplas.

Observação 2.15. Ao longo deste trabalho, consideraremos apenas grafos definidos sobre uma quantidade finita de vértices e arestas.

Definição 2.16. Seja $f \in \mathbb{F}_q[x]$. O **grafo funcional** associado ao par $(f, \mathbb{F}_q)$ é o grafo direcionado $\mathcal{G}(f/\mathbb{F}_q)$ com conjunto de vértices $V = \mathbb{F}_q$ e arestas direcionadas $A = \{(a, f(a)) : a \in \mathbb{F}_q\}$.

Exemplo 2.17. Considere $f : \mathbb{F}_7 \rightarrow \mathbb{F}_7$ tal que $f(x) = 2x + 1$. O grafo funcional $\mathcal{G}(f/\mathbb{F}_7)$ é dado pela Figura 1.

Observação 2.18. É possível estender a definição de grafos funcionais para funções $f : B \rightarrow B$, em que B é um conjunto finito qualquer. Entretanto, ao longo deste trabalho, utilizaremos apenas grafos funcionais de funções sobre corpos finitos, pois as propriedades dessas estruturas serão de extrema importância para os resultados aqui apresentados.

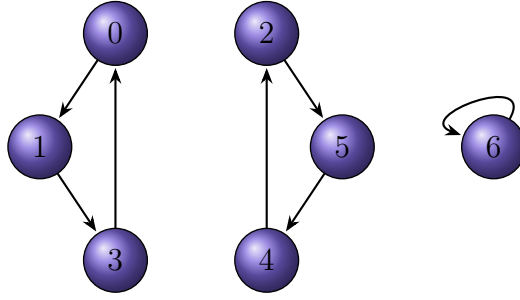


Figura 1 – $\mathcal{G}(f/\mathbb{F}_7)$: Grafo funcional de f sobre $\mathbb{F}_7$.

Definição 2.19. Um grafo G' é dito **subgrafo** de um grafo G se $V(G') \subseteq V(G)$ e $A(G') \subseteq A(G)$. Um subgrafo G' de G é dito **subgrafo induzido** pelo conjunto $S \subseteq V(G)$ se todas as arestas incidentes aos vértices $s \in S$ em G também estão presentes em G' .

Definição 2.20. A quantidade de arestas que incidem sobre um vértice v de um grafo, isto é, a quantidade de arestas que têm uma extremidade em v , é chamada de **grau** do vértice v e é denotado $\deg(v)$. Se uma das arestas for um laço, ela é contada duas vezes.

Definição 2.21. Seja $\mathcal{G}$ um grafo direcionado. Definimos o **grau interno** de um vértice v em $\mathcal{G}$, denotado $\text{Indeg}(v)$, como sendo a quantidade de arestas cuja primeira coordenada é v . E definimos o **grau externo** de v , denotado $\text{Outdeg}(v)$, como sendo a quantidade de arestas cuja segunda coordenada é v .

Observação 2.22. Dado um vértice v de grafo funcional $\mathcal{G}(f/\mathbb{F}_q)$ e considerando a definição acima, temos

$$\text{Indeg}(v) = \#f^{-1}(v) \quad \text{e} \quad \text{Outdeg}(v) = 1.$$

Teorema 2.23. Para todo grafo G , a soma dos graus de seus vértices é igual ao dobro da soma do número de suas arestas, isto é,

$$\sum_{v \in G} \deg(v) = 2m, \text{ em que } m \text{ representa o número de arestas de } G.$$

Demonstração. Ao contar os graus dos vértices, conta-se as extremidades das arestas uma vez por vértice. Logo, como cada aresta tem duas extremidades, temos que cada aresta foi contada duas vezes. $\square$

Corolário 2.24. Todo grafo G possui uma quantidade par de vértices de grau ímpar.

Demonstração. Suponha que G possui um número ímpar de vértices de grau ímpar. Então a soma dos graus dos vértices seria ímpar, contradição com o teorema anterior. Portanto, G possui uma quantidade par de vértices de grau ímpar. $\square$

Definição 2.25. A **sequência de graus** de um grafo é a sequência não crescente formada pelos graus dos vértices do grafo.

Definição 2.26. Seja G um grafo. O menor grau de um vértice em G é chamado de **grau mínimo** e denotado $\delta(G)$. O maior grau de um vértice em G é chamado de **grau máximo** e denotado $\Delta(G)$.

Definição 2.27. Um grafo é dito **grafo regular** de grau k (ou **k -regular**) quando todos os seus vértices possuem o mesmo grau k .

Definição 2.28. Um grafo é chamado de **ciclo** de comprimento k , e denotado C_k , se possui k vértices e k arestas, em que os vértices podem ser ordenados como $v_1, v_2, \dots, v_k$ de modo que cada aresta é da forma $\{v_i, v_{i+1}\}$ com $i \in 1, \dots, k-1$ e a última aresta é da forma $\{v_k, v_1\}$.

Definição 2.29. Um grafo direcionado é dito um **ciclo direcionado** de comprimento k , e denotado $\text{Cyc}(k)$, se possui k vértices e k arestas, em que os vértices podem ser ordenados como $v_1, v_2, \dots, v_k$ de modo que cada aresta é da forma (v_i, v_{i+1}) com $i \in \{1, \dots, k-1\}$ e a última aresta é da forma (v_k, v_1) .

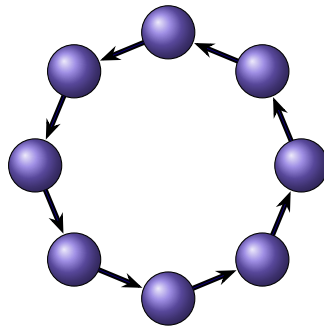


Figura 2 – $\text{Cyc}(8)$: Ciclo direcionado com 8 vértices.

Observação 2.30. Cada vértice v_i de um ciclo direcionado tem exatamente uma aresta saindo ($\text{Indeg}(v_i) = 1$) e uma aresta chegando ($\text{Outdeg}(v_i) = 1$). Além disso, todo ciclo direcionado é um ciclo, pois é um grafo 2-regular.

Definição 2.31. Dizemos que um vértice v de G é um **vértice periódico** se v está em C_k , para algum ciclo C_k contido em G .

Definição 2.32. Um grafo é chamado **caminho** se é um ciclo do qual foi retirada uma aresta, isto é, um caminho, denotado por P_k , é obtido retirando uma aresta do ciclo C_{k+1} . Além disso, dizemos que existe um caminho entre dois vértices u e v de um grafo se esse grafo contém um caminho como subgrafo e cujas extremidades são os vértices u e v .

Definição 2.33. Um **caminho direcionado** de comprimento k , denotado $\text{Path}(k)$ é um grafo direcionado obtido pela remoção de uma aresta de um ciclo direcionado $\text{Cyc}(k+1)$. Além disso, dado um grafo direcionado $\mathcal{G}$, dizemos que existe um caminho direcionado de um vértice u em $\mathcal{G}$ para um vértice v em $\mathcal{G}$ se $\mathcal{G}$ contém um subgrafo que é um caminho direcionado com vértice inicial em u e vértice final em v .

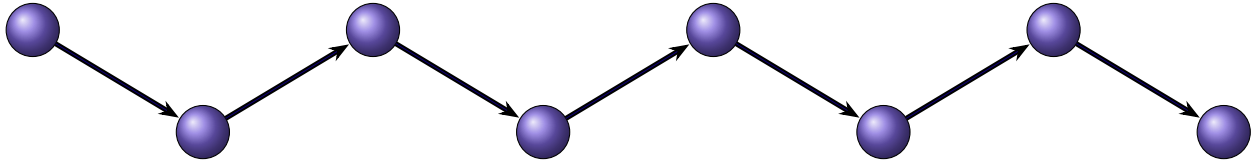


Figura 3 – Path(7): Caminho direcionado com 7 arestas.

Definição 2.34. Um grafo é dito **grafo conexo** se qualquer par de vértices é ligado por ao menos um caminho de arestas. Caso contrário, o grafo é dito um **grafo desconexo**.

Definição 2.35. Seja G um grafo, os subgrafos conexos maximais de G são chamados de **componentes conexas** de G .

Definição 2.36. Sejam b e c vértices de um grafo direcionado $\mathcal{G}$. Se existe um caminho direcionado de b a c , então b é um **antecessor** de c e c é um **sucessor** de b .

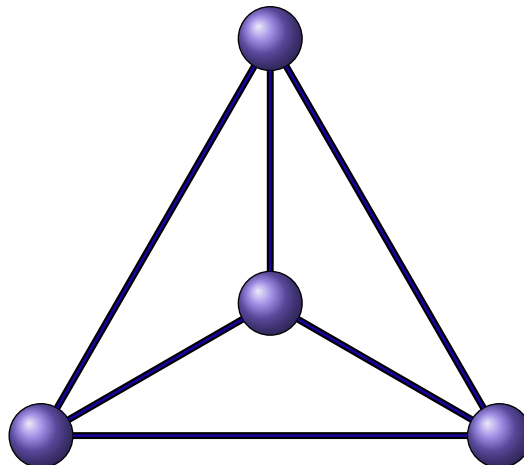
Observação 2.37. Um vértice sempre será antecessor e sucessor de si mesmo.

Definição 2.38. Dado um vértice b de um grafo direcionado G , o grafo $R_b(G)$ é o subgrafo de G contendo todos os antecessores de b .

Definição 2.39. Sejam b e c vértices de um grafo direcionado $\mathcal{G}$. Se existe um caminho direcionado minimal com $k + 1$ vértices de b a c , então b é um **antecessor k -distante** de c e c é um **sucessor k -distante** de b .

Definição 2.40. Seja G um grafo direcionado conexo, $V = (v_1, v_2, \dots, v_D)$ uma sequência não crescente de inteiros positivos e seja $v_i = 1$ para todo $i \geq D + 1$. Dizemos que G é **V -regular** se, para cada inteiro positivo k , o número de antecessores k -distantes de um vértice de G é igual a 0 ou $v_1 \cdots v_k$.

Definição 2.41. Um **grafo completo** com n vértices, denotado K_n , é definido como sendo um grafo em que todos os seus vértices são adjacentes dois a dois.

Figura 4 – K_4 : Grafo completo com 4 vértices.

Definição 2.42. O grafo complementar de um grafo G , denotado por $\overline{G}$, é definido como sendo um grafo tal que $V(G) = V(\overline{G})$, $A(G) \cap A(\overline{G}) = \emptyset$ e $A(G) \cup A(\overline{G}) = K_{|V(G)|}$.

Definição 2.43. Um grafo G é dito um **grafo nulo** (ou **grafo vazio**) se $A(G) = \emptyset$.

2.2 Árvores

Nesta segunda seção, concentraremos-nos no estudo sobre árvores, com enfoque nas árvores direcionadas com raiz, estruturas que surgem naturalmente na decomposição de grafos funcionais e que, por esse motivo, desempenham um papel fundamental na dinâmica dos grafos de funções polinomiais.

Definição 2.44. Um grafo conexo sem ciclos como subgrafos é uma **árvore** e será denotado por T .

Definição 2.45. Um grafo é dito uma **floresta** se suas componentes conexas são árvores.

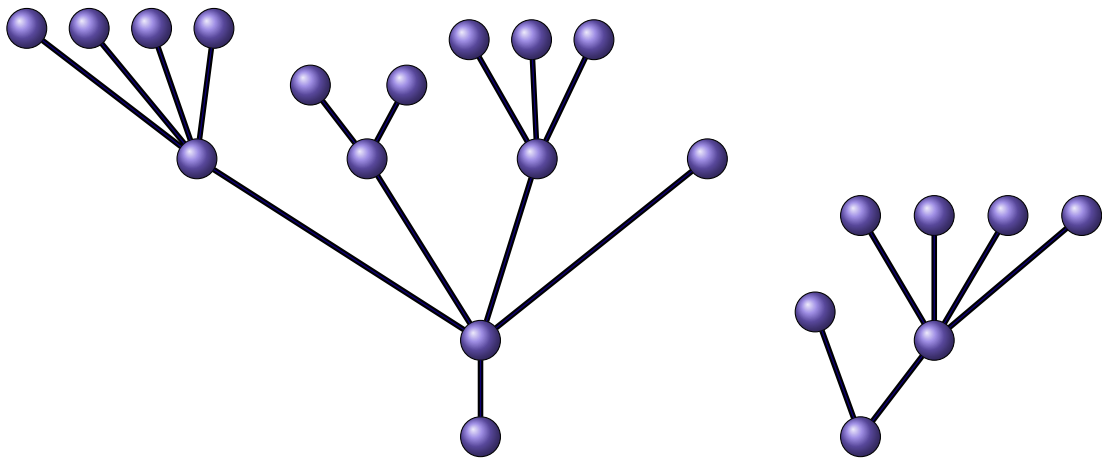


Figura 5 – Floresta com duas árvores.

Definição 2.46. Um vértice de grau 0, isto é, sem arestas incidentes, é dito **vértice isolado**. Um vértice de grau 1 é dito **vértice pendente**.

Definição 2.47. Seja T uma árvore. Um vértice de T é dito uma **folha** de T se for um vértice pendente.

Observação 2.48. Observe que, ao remover uma folha de uma árvore, ela ainda será uma árvore, pois continuará conexa e sem conter ciclos.

Notação 2.49. Uma árvore com um único vértice será denotada por $\bullet$.

Definição 2.50. Uma aresta $\{u, v\}$ de um grafo é considerada uma **ponte** se ela é o único caminho que liga os vértices u e v .

Teorema 2.51. Seja T um grafo com n vértices. As seguintes afirmações são equivalentes:

- i. T é uma árvore.
- ii. T não contém ciclos e tem $n - 1$ arestas.
- iii. T é conexo e tem $n - 1$ arestas.

- iv. T é conexo e toda aresta é uma ponte.
- v. Todo par de vértices de T é ligado por um único caminho.
- vi. T não contém ciclos, mas a adição de uma aresta produz um único ciclo.

Demonstração.

- (i) $\Rightarrow$ (ii) Pela definição de árvore, sabemos que T não contém ciclos. Resta mostrar que T tem $n - 1$ arestas.

Seja $n = 1$. Um vértice tem $0 = 1 - 1$ arestas.

Suponha que toda árvore com n vértices possua $n - 1$ arestas. Mostremos que árvores com $n + 1$ vértices têm n arestas. Remova uma folha de T . Temos então uma árvore com n vértices e, pela hipótese de indução, $n - 1$ arestas. Reconnectando a folha removida, concluímos que T possui $(n - 1) + 1 = n$ arestas.

- (ii) $\Rightarrow$ (iii) Basta mostrar que T é conexo. Denote por c o número de componentes conexas de T e por n_i com $i = 1, \dots, c$ a quantidade de vértices de cada componente de T . Como cada componente conexa é uma árvore, temos $n_i - 1$ arestas por componente. Além disso, $n = \sum_{i=1}^c n_i$. Logo, a quantidade total de arestas de T é dada por

$$\sum_{i=1}^c n_i - 1 = n - c.$$

Por hipótese, T possui $n - 1$ arestas. Portanto, $c = 1$, isto é, T é conexo.

- (iii) $\Rightarrow$ (iv) Suponha que T possua uma aresta que não é ponte. Ao remover essa aresta, o grafo continua conexo e com $n - 2$ arestas, contradição, pois um grafo conexo com n vértices possui ao menos $n - 1$ arestas. Portanto, toda aresta de T é uma ponte.

- (iv) $\Rightarrow$ (v) Suponha que existam dois caminhos distintos entre dois vértices de T . A união desses caminhos forma um ciclo. A remoção de qualquer aresta desse ciclo preserva a conexidade, logo, essas arestas não são pontes, o que contradiz a hipótese. Portanto, existe um único caminho entre quaisquer vértices de T .

- (v) $\Rightarrow$ (vi) Suponha que T possua um ciclo, então há mais de um caminho entre quaisquer dois vértices de T que estão no ciclo, contradição. Portanto, T não possui ciclos. Ao adicionar uma aresta $\{u, v\}$ ao grafo, é criado um segundo caminho entre os vértices u e v , logo, a união dessa aresta ao único caminho que ligava u e v é um ciclo.

- (vi) $\Rightarrow$ (i) Basta mostrar que T é conexo. Suponha T desconexo, então a adição de uma aresta ligando duas componentes conexas de T não criará um ciclo, contradição. Portanto, T é uma árvore.

□

Corolário 2.52. Se G é um grafo conexo com n vértices e $m \leq n$ arestas, então G possui $m - n + 1$ ciclos.

Demonstração. Provemos o resultado por indução em $k = n - m$. Seja G é um grafo conexo com n vértices e n arestas. Podemos tirar uma aresta de G de forma que G continue conexo. Então, pelo Teorema 2.51, o grafo obtido é uma árvore. Ainda pelo Teorema 2.51, temos que, ao adicionar novamente a aresta removida, cria-se um ciclo no grafo. Portanto, G possui um ciclo.

Suponha a asserção verdadeira para $k \geq n - m$. Considere um grafo conexo G com n vértices e $m + 1$ arestas. Se G não possuíse ciclos, seria uma árvore por definição e, pelo Teorema 2.51, ele teria $n - 1$ arestas. Como ele possui $m + 1 > n - 1$ arestas, então G não é uma árvore e possui ciclos. Escolhemos um ciclo de G e, retirando uma aresta do ciclo, obtemos um novo grafo conexo G' com n vértices e m arestas. Por indução, esse novo grafo possui $n - m + 1$ ciclos. O ciclo inicial não foi contado entre os $n - m + 1$ ciclos, pois esses ciclos não contêm a aresta retirada. Portanto, adicionando esse primeiro ciclo, obtemos que o grafo G possui $n - (m + 1) + 1$ ciclos. Isso prova o resultado. □

Definição 2.53. Dizemos que um vértice v em um árvore direcionada possui **profundidade** k se o maior caminho direcionado contendo v como vértice final possui $k + 1$ vértices. Além disso, uma árvore direcionada T é dita de profundidade k , se $\max \{\text{profundidade de } v, v \in V(T)\} = k$.

Definição 2.54. Por **árvore com raiz**, entendemos uma árvore direcionada com raiz, em que todas as arestas apontam para a raiz, isto é, existe um caminho direcionado de qualquer vértice até um certo vértice dessa árvore, o qual será chamado de raiz. Usaremos a letra $\mathcal{T}$ para denotar uma árvore com raiz.

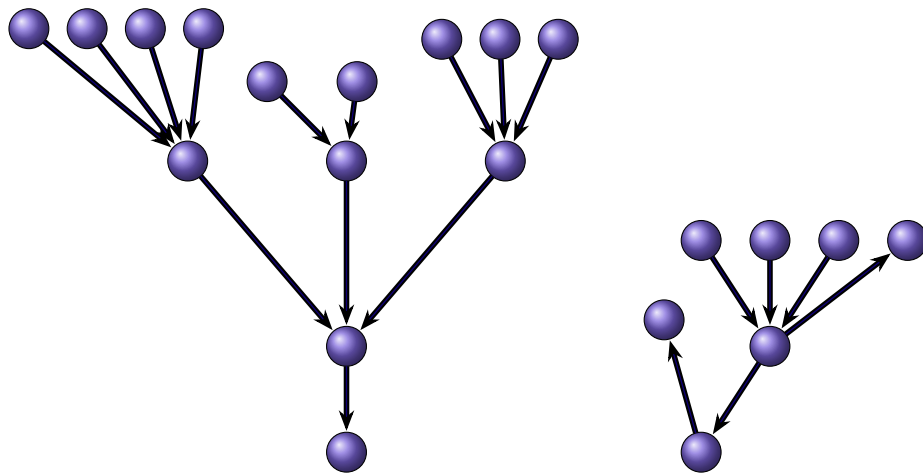


Figura 6 – Floresta com duas árvores: a árvore à esquerda é uma árvore com raiz, a árvore à direita não é uma árvore com raiz.

Notação 2.55. Usaremos $\oplus$ para denotar a união disjunta de grafos. Dado um grafo G , usaremos $k \times G$ para denotar o grafo $\oplus_{i=1}^k G_i$.

Seja $\mathcal{G} = \oplus_{i=1}^s \mathcal{T}_i$, em que $\mathcal{T}_1, \dots, \mathcal{T}_s$ são árvores com raiz, então usaremos $\langle \mathcal{G} \rangle$ para representar a árvore com raiz cuja raiz tem como filhos as raízes de grafos isomorfos a $\mathcal{T}_1, \dots, \mathcal{T}_s$.

Definição 2.56. Para uma sequência não crescente de inteiros positivos $V = (v_1, v_2, \dots, v_D)$, a sequência de árvores com raiz $\{\mathcal{T}_V^k\}_k$ é definida recursivamente como segue

$$\begin{cases} \mathcal{T}_V^0 = \bullet, \\ \mathcal{T}_V^1 = \langle v_1 \times \mathcal{T}_V^0 \rangle, \\ \mathcal{T}_V^k = \left\langle v_k \times \mathcal{T}_V^{k-1} \oplus \bigoplus_{i=1}^{k-1} (v_i - v_{i+1}) \times \mathcal{T}_V^{i-1} \right\rangle \text{ para } k \geq 1, \end{cases}$$

em que $v_i = 1$ para todo $i \geq D + 1$ e as arestas estão todas direcionadas para a raiz. A árvore com raiz $\mathcal{T}_V$, chamada de **árvore elementar**, é definida como

$$\mathcal{T}_V = \left\langle (v_D - 1) \times \mathcal{T}_V^{D-1} \oplus \bigoplus_{i=1}^{D-1} (v_i - v_{i+1}) \times \mathcal{T}_V^{i-1} \right\rangle.$$

Exemplo 2.57. Considere $V = (3, 3)$. Temos $\mathcal{T}_V^0 = \bullet$ e $\mathcal{T}_V^1 = \langle 3 \times \bullet \rangle$. A árvore $\mathcal{T}_V^1$ está representada graficamente pela Figura 7.

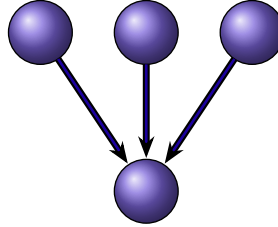


Figura 7 – Árvore $\mathcal{T}_V^1$ com $V = (3, 3)$.

Agora podemos calcular a árvore elementar $\mathcal{T}_V$.

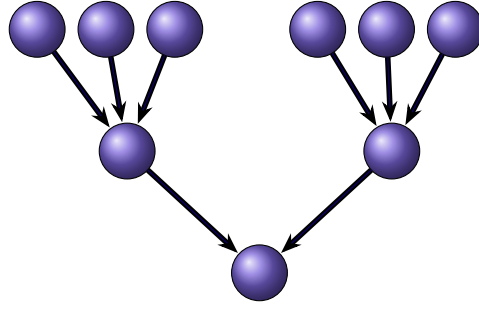
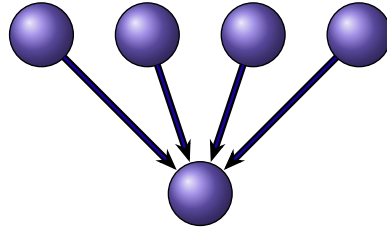
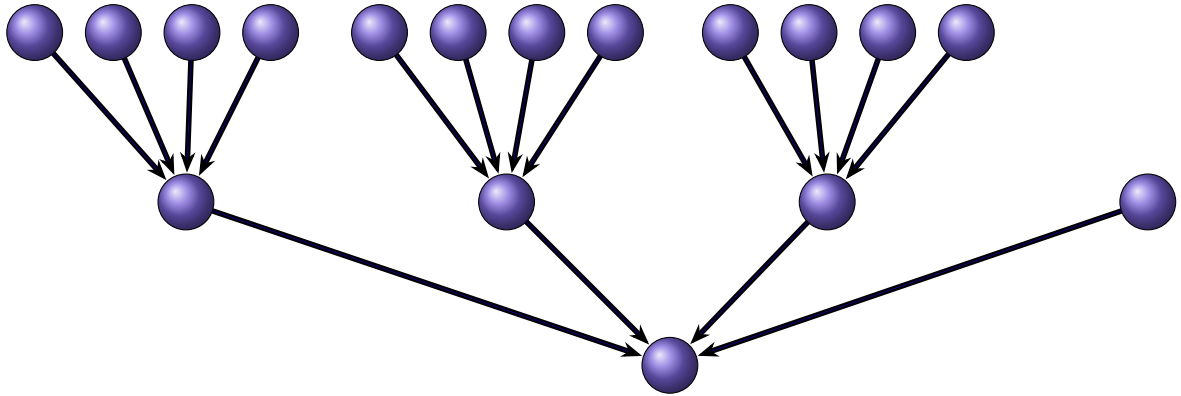
$$\begin{aligned} \mathcal{T}_V &= \langle (3 - 1) \times \mathcal{T}_V^1 \oplus (3 - 3) \times \mathcal{T}_V^0 \rangle \\ &= \langle 2 \times \mathcal{T}_V^1 \rangle. \end{aligned}$$

Logo, temos $\mathcal{T}_V = \langle 2 \times \mathcal{T}_V^1 \rangle$ e a sua representação gráfica é dada pela Figura 8.

Exemplo 2.58. Considere $V = (4, 3, 2)$. Temos $\mathcal{T}_V^0 = \bullet$ e $\mathcal{T}_V^1 = \langle 4 \times \bullet \rangle$. A árvore $\mathcal{T}_V^1$ está representada graficamente pela Figura 9.

Calculando $\mathcal{T}_V^2$, obtemos

$$\begin{aligned} \mathcal{T}_V^2 &= \langle 3 \times \mathcal{T}_V^1 \oplus (4 - 3) \times \mathcal{T}_V^0 \rangle \\ &= \langle 3 \times \mathcal{T}_V^1 \oplus \bullet \rangle, \end{aligned}$$

Figura 8 – Árvore $\mathcal{T}_V$ com $V = (3, 3)$.Figura 9 – Árvore $\mathcal{T}_V^1$ com $V = (4, 3, 2)$.Figura 10 – Árvore $\mathcal{T}_V^2$ com $V = (4, 3, 2)$.

que está representada graficamente pela Figura 10.

Agora temos as ferramentas necessárias para calcular a árvore elementar $\mathcal{T}_V$.

$$\begin{aligned}\mathcal{T}_V &= \langle (2 - 1) \times \mathcal{T}_V^2 \oplus (4 - 3) \times \mathcal{T}_V^0 \oplus (3 - 2)\mathcal{T}_V^1 \rangle \\ &= \langle \mathcal{T}_V^2 \oplus \bullet \oplus \mathcal{T}_V^1 \rangle.\end{aligned}$$

Potanto, temos $\mathcal{T}_V = \langle \mathcal{T}_V^2 \oplus \bullet \oplus \mathcal{T}_V^1 \rangle$ e a sua representação gráfica é dada pela Figura 11.

Observe que, de acordo com a Definição 2.40, as árvores $\mathcal{T}_V^0 = \bullet$, $\mathcal{T}_V^1$ (representada pela Figura 9) e $\mathcal{T}_V^2$ (representada pela Figura 10) são grafos V -regulares com $V = (4, 3, 2)$. De fato, a raiz de $\mathcal{T}_V^1$ possui 4 antecessores 1-distantes e os demais vértices não possuem antecessores. Além disso, $\mathcal{T}_V^2 = \langle 3 \times \mathcal{T}_V^1 \oplus \bullet \rangle$, possui raiz com 4 antecessores 1-distantes, que denotaremos $b_1, \dots, b_4$, e $12 = 4 \cdot 3$ antecessores 2-distantes. Sem perda de generalidade,

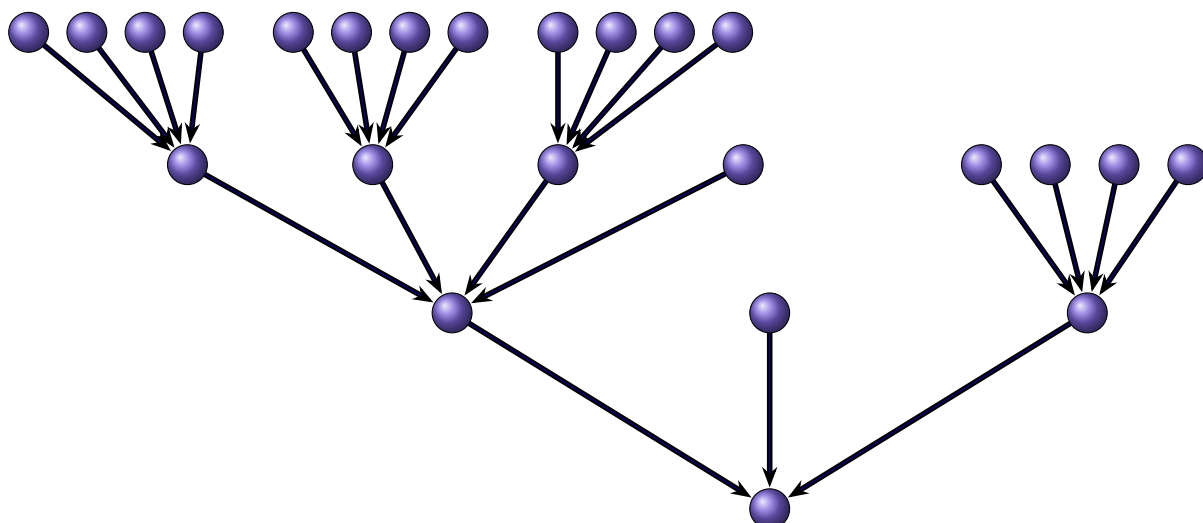


Figura 11 – Árvore elementar $\mathcal{T}_V$ com $V = (4, 3, 2)$.

temos b_1 , b_2 e b_3 com 4 antecessores 1-distantes e os demais vértices de $\mathcal{T}_V^2$ não possuem antecessores.

No próximo capítulo, veremos um resultado que mostra que todas as árvores da forma $\mathcal{T}_V^k$ são V -regulares.

3 Dinâmica de grafos funcionais sobre corpos finitos

Neste capítulo, consolidamos os resultados centrais deste trabalho, oferecendo uma classificação completa da estrutura de grafos funcionais associados à classe dos polinômios m -nice. Dividido em duas seções, iniciamos com a formalização de algumas terminologias e resultados preparatórios, essenciais para as demonstrações subsequentes, e avançamos para teoremas que descrevem as estruturas das componentes conexas dos grafos de funções m -nice.

A principal referência utilizada ao longo deste capítulo foi o artigo ([OLIVEIRA; BROCHERO MARTÍNEZ, 2024](#)).

3.1 Resultados auxiliares e terminologia

Nesta seção, apresentaremos algumas definições complementares e estabeleceremos a notação e terminologia a serem utilizadas durante o restante deste trabalho. Além disso, apresentaremos resultados auxiliares que serão amplamente utilizados ao longo das demonstrações dos resultados principais na próxima seção.

3.1.1 Terminologia

Ao longo deste trabalho, diremos que dois grafos são iguais se eles forem grafos isomorfos.

Notação 3.1. Usaremos $\text{Cyc}(k, \mathcal{T})$ para denotar um grafo direcionado composto por um ciclo de comprimento k , em que cada vértice do ciclo é a raiz de uma árvore isomorfa a $\mathcal{T}$. O ciclo $\text{Cyc}(k, \bullet)$ também é denotado por $\text{Cyc}(k)$.

Exemplo 3.2. O grafo $\text{Cyc}(8, \mathcal{T})$, com $\mathcal{T} = \langle 2 \times \bullet \rangle$ é um grafo direcionado composto por um ciclo de comprimento 8, em que cada vértice do ciclo é a raiz de uma árvore isomorfa a $\langle 2 \times \bullet \rangle$ e está graficamente representado pela Figura 12.

Definição 3.3. Seja $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ uma função m -nice. Ao longo deste capítulo, denotaremos por

- i. ω o maior divisor de $(q - 1)/m$ que é relativamente primo com n ,
- ii. ν o inteiro positivo tal que $\nu = (q - 1)/m\omega$,
- iii. ω' o maior divisor de $q - 1$ que é relativamente primo com n .

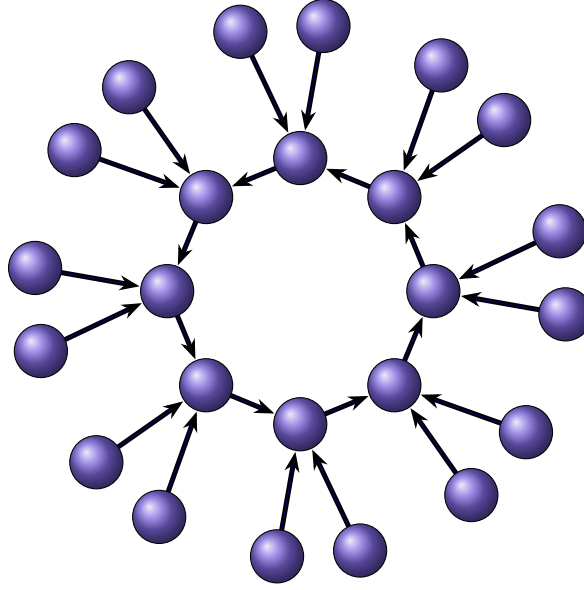


Figura 12 – $\text{Cyc}(8, \mathcal{T})$: Grafo composto por um ciclo direcionado com 8 vértices e árvores isomorfas a $\mathcal{T} = \langle 2 \times \bullet \rangle$ em cada vértice do ciclo.

Observação 3.4. As componentes conexas de um grafo funcional associado à iteração de uma função sobre um conjunto finito consistem em ciclos em que cada vértice de um ciclo é a raiz de uma árvore com raiz.

De fato, seja $\mathcal{G}'$ uma componente conexa com k elementos de um grafo funcional. Como cada vértice de $\mathcal{G}'$ é vértice inicial de uma aresta direcionada, essa componente possui k arestas. Portanto, pelo Corolário 2.52, essa componente possui um ciclo. Suponha que esse ciclo possua $l \leq k$ vértices. Sejam $a_1, a_2, \dots, a_l$ os vértices do ciclo, de forma que a_i e a_{i+1} são adjacentes para $1 \leq i \leq l-1$ e a_1 e a_l são adjacentes. Seja f a função do grafo funcional e sem perda de generalidade, podemos supor $f(a_l) = a_1$. Para cada par de índices temos $f(a_i) = a_{i+1}$ ou $f(a_{i+1}) = f(a_i)$. Como a_{l-1} e a_l estão ligados e $f(a_l) = a_1$, então $f(a_{l-1}) = a_l$. Por indução, obtemos $f(a_1) = a_2, f(a_2) = a_3, \dots, f(a_{l-1}) = a_l$ e $f(a_l) = a_1$. Assim, para cada vértice a de um ciclo, $f(a)$ pertence ao ciclo e uma das imagens inversas de a pertence ao ciclo. Os outros vértices que são pré-imagens de a são vértices fora do ciclo. Por sua vez, cada um dos vértices da pré-imagem (fora do ciclo) possuem ou não pré-imagens e, claramente, como se trata de um grafo funcional, as pré-imagens desses vértices são novos vértices. Dessa forma, continuamos a encontrar novos vértices nas pré-imagens dos vértices já encontrados. Como o número de vértices do grafo é finito, em algum momento os vértices não possuem novas pré-imagens. Assim, o vértice a , do ciclo, é raiz de uma árvore tendo a como raiz.

Notação 3.5. Ao longo deste trabalho, escreveremos um grafo funcional $\mathcal{G}(f/\mathbb{F}_q)$ como sendo a soma direta

$$\mathcal{G}(f/\mathbb{F}_q) = \mathcal{G}_{f/\mathbb{F}_q}^{(0)} \oplus \mathcal{G}_{f/\mathbb{F}_q}^{(1)},$$

em que $\mathcal{G}_{f/\mathbb{F}_q}^{(0)}$ denota a componente conexa de $\mathcal{G}(f/\mathbb{F}_q)$ contendo $0 \in \mathbb{F}_q$, e $\mathcal{G}_{f/\mathbb{F}_q}^{(1)}$ denota as

demais componentes conexas de $\mathcal{G}(f/\mathbb{F}_q)$.

Exemplo 3.6. Seja $f(x) = 2x + 1 \in \mathbb{F}_7[x]$ a função definida no Exemplo 2.17. Temos que $\mathcal{G}_{f/\mathbb{F}_7}^{(0)}$, representado graficamente pela Figura 13a, é formado por um ciclo direcionado de comprimento 3 com vértices em 0, 1 e 3. Além disso, $\mathcal{G}_{f/\mathbb{F}_7}^{(1)}$, representado graficamente pela Figura 13b, é formado por um laço no vértice 6 e por um ciclo de comprimento 3 com vértices em 2, 5 e 4.

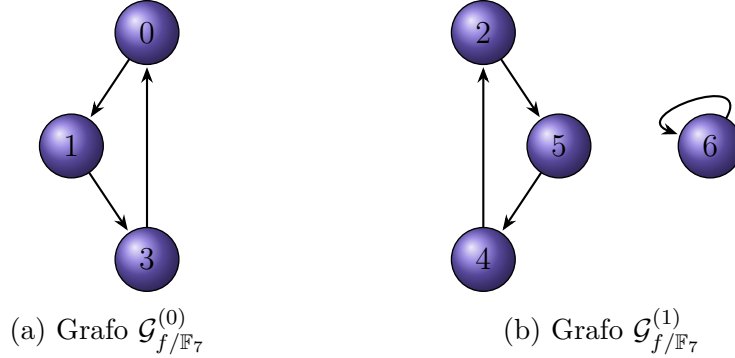


Figura 13 – Grafos $\mathcal{G}_{f/\mathbb{F}_7}^{(0)}$ e $\mathcal{G}_{f/\mathbb{F}_7}^{(1)}$, cuja soma direta resulta no grafo $\mathcal{G}(f, \mathbb{F}_7)$, com $f(x) = 2x + 1$.

3.1.2 Resultados auxiliares

Nesta subseção, apresentamos resultados auxiliares que caracterizam a relação entre grafos V -regulares, árvores elementares e polinômios m -nice, classes de objetos fundamentais para a modelagem da dinâmica de grafos funcionais. Estes resultados nos fornecerão as ferramentas necessárias para as demonstrações dos resultados principais deste trabalho, a serem apresentados na próxima seção.

Lema 3.7. *Seja $V = (v_1, v_2, \dots, v_D)$ uma sequência não crescente de inteiros positivos. Se $\mathcal{T}$ é uma árvore com raiz V -regular e de profundidade $k \leq D$, então $\mathcal{T}$ é isomorfa a $\mathcal{T}_V^k$.*

Demonstração. Seja $v_i = 1$ para $i \geq D + 1$. Provaremos o resultado por indução sobre k .

No caso $k = 1$, mostraremos que $\mathcal{T}$ é isomorfo a $\mathcal{T}_V^1$. Sabemos que $\mathcal{T}$ é uma árvore V -regular de profundidade 1, logo, $\mathcal{T}$ possui um vértice b como raiz e vértices antecessores 1-distantes de b . Assim, como $\mathcal{T}$ é V -regular, b possui v_1 antecessores 1-distantes, ou seja, $\mathcal{T} = \langle v_1 \times \bullet \rangle$. Por fim, temos

$$\mathcal{T} \cong \langle v_1 \times \bullet \rangle \cong \langle v_1 \times \mathcal{T}_v^0 \rangle \cong \mathcal{T}_V^1.$$

Agora, vamos supor que o resultado vale para um inteiro positivo k . Mostraremos que vale para $k + 1$.

Seja $\mathcal{T}$ uma árvore V -regular com raiz de profundidade $k+1$ e considere $\tilde{\mathcal{T}}$ a árvore com raiz obtida ao remover os vértices de profundidade $k+1$ de $\mathcal{T}$. Então, pela hipótese de indução, $\tilde{\mathcal{T}}$ é isomorfo a $\mathcal{T}_V^k$.

Suponhamos que $\mathcal{T}$ possui j vértices de profundidade 1 que possuem ao menos um filho de profundidade $k+1$. Cada um desses vértices possui, na verdade, $v_1 v_2 \cdots v_k$ filhos de profundidade $k+1$, pois $\mathcal{T}$ é V -regular. Dessa forma, existem $v_1 v_2 \cdots v_k j$ filhos de profundidade $k+1$. Como $\mathcal{T}$ possui exatamente $v_1 v_2 \cdots v_{k+1}$ filhos de profundidade $k+1$, então $j = v_{k+1}$.

Sejam $z_1, \dots, z_{v_{k+1}}$ os vértices de $\mathcal{T}$ de profundidade 1 que possuem ao menos um filho de profundidade k e sejam $z'_1, \dots, z'_{v_{k+1}}$ os vértices correspondentes em $\tilde{\mathcal{T}}$. Para cada $i \in \{1, \dots, v_{k+1}\}$, denotemos

$$\mathcal{T}_{z_i} = R_{z_i}(\mathcal{T}) \text{ e } \tilde{\mathcal{T}}_{z'_i} = R_{z'_i}(\tilde{\mathcal{T}}).$$

Como $\mathcal{T}$ é V -regular, temos que $\mathcal{T}_{z_i}$ é V -regular de profundidade k e, pela hipótese de indução, é isomorfo a $\mathcal{T}_V^k$ para $i \in \{1, \dots, v_k\}$. Portanto, podemos reconstruir $\mathcal{T}$ a partir de $\tilde{\mathcal{T}}$ ao trocarmos cada $\tilde{\mathcal{T}}^{z_i}$ por $\mathcal{T}_V^k$.

Por fim, segue da Definição 2.56 que a árvore obtida é isomorfa à árvore $\mathcal{T}_V^{k+1}$, isto é, $\mathcal{T} \cong \mathcal{T}_V^{k+1}$, o que conclui a demonstração. □

Lema 3.8. *Seja $V = (v_1, v_2, \dots, v_D)$ uma sequência não crescente de inteiros positivos com $v_D > 1$ e seja $\mathcal{G}$ um grafo V -regular que contém um único ciclo. Então, existe um inteiro positivo k tal que*

$$\mathcal{G} = \text{Cyc}(k, \mathcal{T}_V).$$

Demonstração. Para cada vértice b no ciclo contido em $\mathcal{G}$, existe uma árvore direcionada $\mathcal{G}_b$ com sua raiz no vértice b . Para demonstrarmos este lema, basta provar que $\mathcal{G}_b = \mathcal{T}_V$ para cada vértice periódico b .

Seja c_1 o antecessor de b que também está no ciclo contido em $\mathcal{G}$ e denotemos por $c_2, \dots, c_{v_1}$ os antecessores de b que não estão no ciclo contido em $\mathcal{G}$. Podemos escrever $\mathcal{G}_b$ utilizando os subgrafos dos antecessores de b que não estão no ciclo, obtendo

$$\mathcal{G}_b = \left\langle \bigoplus_{i=2}^{v_1} R_{c_i}(\mathcal{G}_b) \right\rangle.$$

Além disso, como cada $R_{c_i}(\mathcal{G}_b)$ é uma árvore V -regular, o Lema 3.7 nos garante que existe um inteiro k_i tal que $R_{c_i}(\mathcal{G}_b) = \mathcal{T}_V^{k_i}$. Seja w_k a quantidade de inteiros i com $2 \leq i \leq v_1$ tais que $R_{c_i}(\mathcal{G}_b) = \mathcal{T}_V^k$. Então temos

$$\mathcal{G}_b = \left\langle \bigoplus_{k=0}^{\infty} w_k \times \mathcal{T}_V^k \right\rangle. \quad (3.1)$$

Definamos $v_i = 1$ para $i > D$ e $v_0 = 1$. Como $\mathcal{G}$ é V -regular, o número de antecessores l -distantes de b em $\mathcal{G}_b$ é dado pela diferença do número de antecessores l -distantes de b em $\mathcal{G}$ e o número de antecessores $(l-1)$ -distantes de b em $\mathcal{G}$, isto é,

$$v_1 \cdots v_l - v_1 \cdots v_{l-1} = v_1 \cdots v_{l-1} (v_l - 1). \quad (3.2)$$

Então, das Equações (3.1) e (3.2), segue que

$$v_1 \cdots v_l (w_l + w_{l+1} + \cdots) = v_1 \cdots v_l (v_{l+1} - 1)$$

para cada $l \geq 0$. Desse sistema de equações, obtemos $w_k = v_{k+1} - v_{k+2}$ para cada $k \geq 0$. Por fim, substituindo na Equação (3.1), temos que

$$\begin{aligned} \mathcal{G}_b &= \left\langle \bigoplus_{k=1}^{\infty} (v_k - v_{k+1}) \times \mathcal{T}_V^{k-1} \right\rangle \\ &= \left\langle \bigoplus_{k=1}^D (v_k - v_{k+1}) \times \mathcal{T}_V^{k-1} \right\rangle \\ &= \left\langle (v_D - 1) \mathcal{T}_V^{D-1} \oplus \bigoplus_{k=1}^{D-1} (v_k - v_{k+1}) \times \mathcal{T}_V^{k-1} \right\rangle \\ &= \mathcal{T}_V, \end{aligned}$$

o que completa a demonstração. $\square$

Proposição 3.9. *Seja $a \in \mathbb{F}_q^*$. Se $f(x)$ é m -nice, então $R_a(\mathcal{G}(f/\mathbb{F}_q))$ é $\text{mdc}_n(\nu)$ -regular.*

Demonstração. Sejam b um vértice de $R_a(\mathcal{G}(f/\mathbb{F}_q))$ e k um inteiro positivo. Como $\mathcal{G}(f/\mathbb{F}_q)$ é grafo funcional, temos que o número de antecessores k -distantes de b é igual ao número de soluções da equação

$$f^{(k)}(x) = b \quad (3.3)$$

sobre $\mathbb{F}_q$. Pelo Lema 1.40, a solução $x \in \mathbb{F}_q$ da Equação 3.3 satisfaz a relação

$$x^{\frac{q-1}{m}} = \psi_f^{(-k)} \left(b^{\frac{q-1}{m}} \right).$$

Denotemos $\xi := \psi_f^{(-k)} \left(b^{(q-1)/m} \right) \in \mu_m$ e consideremos α um elemento primitivo de $\mathbb{F}_q$ e t um inteiro positivo tal que $\xi = \alpha^{(q-1)t/m}$. Então a igualdade $x^{(q-1)/m} = \alpha^{(q-1)t/m}$ implica

$$x = \alpha^{t+ml} \quad (3.4)$$

para algum $l \in \{1, \dots, (q-1)/m\}$. Agora, da Proposição 1.39 e das Equações 3.3 e 3.4, obtemos

$$\alpha^{(t+ml)n^k} c = b, \quad (3.5)$$

em que

$$c = \sum_{i=0}^{k-1} h \left(\psi_f^{(i)}(\xi) \right)^{n^{k-i-1}}$$

e $l \in \{1, \dots, (q-1)/m\}$. Mostraremos agora que, dadas as hipóteses desta proposição, a quantidade de $l \in \{1, \dots, (q-1)/m\}$ satisfazendo a Equação 3.5 é 0 ou $(q-1)/m$.

De fato, seja u um inteiro tal que $b/c = \alpha^u$. Precisamos encontrar os valores de $l \in \{1, \dots, (q-1)/m\}$ tais que $\alpha^{(t+ml)n^k} = \alpha^u$, isto é, tais que

$$(t + ml)n^k \equiv u \pmod{q-1}. \quad (3.6)$$

Se a Equação 3.6 não possui solução, então $l = 0$. Suponha que essa equação possua solução. Podemos reescrever a Equação 3.6, obtendo

$$mn^k l \equiv u - tn^k \pmod{q-1}.$$

Então $\text{mdc}(mn^k, q-1)$ deve dividir $u - tn^k$. Nesse caso, a equação se torna

$$\frac{n^k}{\text{mdc}(n^k, s)} l \equiv \frac{u - tn^k}{\text{mdc}(mn^k, q-1)} \pmod{\frac{q-1}{m \cdot \text{mdc}(n^k, s)}},$$

em que $s = (q-1)/m$.

Como $n^k / \text{mdc}(n^k, s)$ é relativamente primo com $(q-1) / (m \cdot \text{mdc}(n^k, s))$, existe exatamente uma solução l para essa equação no intervalo $[1, (q-1) / (m \cdot \text{mdc}(n^k, s))]$. Logo, a Equação 3.6 tem $\text{mdc}(n^k, s)$ soluções com $l \in \{1, \dots, (q-1)/m\}$.

Portanto, como $l = 0$ ou $l = \text{mdc}(n^k, s)$, temos que o número de antecessores k -distantes de b é 0 ou $\text{mdc}(n^k, s)$, que, pelo Lema 1.46, é o produto dos k primeiros termos de $\text{mdc}_n(\nu)$, em que $\nu = (q-1)/m\omega = s$ e $\omega = 1$. Dessa forma, como $b \in V(R_a(\mathcal{G}(f/\mathbb{F}_q)))$ e k são arbitrários, concluímos que $R_a(\mathcal{G}(f/\mathbb{F}_q))$ é $\text{mdc}_n(\nu)$ -regular. $\square$

Corolário 3.10. *Seja $f(x)$ um polinômio m -nice sobre $\mathbb{F}_q$. Se G é uma componente conexa de $\mathcal{G}(f/\mathbb{F}_q)$ que contém um único ciclo e não contém o vértice $0 \in \mathbb{F}_q$, então existe um inteiro positivo k tal que $G = \text{Cyc}(k, \mathcal{T}_{\text{mdc}_n(\nu)})$.*

Demonstração. Pela Proposição 3.9, $G = R_a(\mathcal{G}(f/\mathbb{F}_q))$ é $\text{mdc}_n(\nu)$ -regular para qualquer $a \in \mathbb{F}_q^*$. Como G é uma componente conexa que contém um único ciclo e é $\text{mdc}_n(\nu)$ -regular, segue do Lema 3.8 que existe um inteiro positivo k tal que $G = \text{Cyc}(k, \mathcal{T}_{\text{mdc}_n(\nu)})$. $\square$

Corolário 3.11. *Seja $f(x)$ um polinômio m -nice sobre $\mathbb{F}_q$. Para qualquer $a \in \mathbb{F}_q^*$, a árvore $R_a(\mathcal{G}(f/\mathbb{F}_q))$ é $\text{mdc}_n(\nu)$ -regular e, portanto, é isomorfa a $\mathcal{T}_{\text{mdc}_n(\nu)}^k$, em que k é a profundidade da árvore para algum k .*

Demonstração. Pela Proposição 3.9, $R_a(\mathcal{G}(f/\mathbb{F}_q))$ é $\text{mdc}_n(\nu)$ -regular. Como $R_a(\mathcal{G}(f/\mathbb{F}_q))$ é uma árvore com raiz $\text{mdc}_n(\nu)$ -regular de profundidade k , segue do Lema 3.7 que ela é isomorfa a $\mathcal{T}_{\text{mdc}_n(\nu)}^k$. $\square$

3.2 Resultados principais

Esta seção apresenta os dois resultados principais deste trabalho, que apresentam uma classificação completa da estrutura de grafos funcionais associados a polinômios m -nice sobre corpos finitos. O Teorema 3.12 caracteriza a componente conexa contendo o vértice 0, formada por um laço em 0 anexado à raiz de uma árvore. Por sua vez, o Teorema 3.14 descreve a estrutura de todas as demais componentes conexas desse grafo funcional e garante que, em cada componente conexa, todas as árvores conectadas aos pontos cíclicos de $\mathcal{G}_{f/\mathbb{F}_q}^{(1)}$ são isomorfas.

Complementando os resultados apresentados, incluímos exemplos detalhados com diagramas que ilustram a decomposição gráfica do polinômio $g(x) = x^{15}h(x^{36})$ em $\mathbb{F}_{181}[x]$.

Teorema 3.12. *Seja $f(x) = x^n h(x^{(q-1)/m})$ um polinômio m -nice sobre $\mathbb{F}_q$ e seja $d_j = \text{mdc}(\nu, n^j)$. Para cada $i = 1, \dots, m+1$, denotemos por*

$$r_i = \left| \{ \xi \in \mu_m : \psi_f^{(i)}(\xi) = 0, \psi_f^{(i-1)}(\xi) \neq 0 \} \right|.$$

Então,

$$\mathcal{G}_{f/\mathbb{F}_q}^{(0)} = \text{Cyc}(1, T),$$

em que

$$T = \left\langle \bigoplus_{i=0}^{m-1} \left(\frac{(q-1)r_{i+1}}{md_i} - \frac{(q-1)r_{i+2}}{md_{i+1}} \right) \times \mathcal{T}_{\text{mdc}_n(\nu)}^i \right\rangle.$$

Demonstração. Primeiramente, vejamos que

$$r_1 = |\{ \xi \in \mu_m : \psi_f(\xi) = 0, \xi \neq 0 \}|,$$

isto é, r_1 representa a quantidade de raízes m -ésimas da unidade não nulas que anulam o polinômio associado de f .

Denotemos o conjunto dos filhos do vértice 0 em $\mathcal{G}(f/\mathbb{F}_q)$ por $\{0, w_1, \dots, w_{r_1(q-1)/m}\}$, que consiste nas soluções da equação

$$x^n h(x^{\frac{q-1}{m}}) = 0$$

sobre $\mathbb{F}_q$, isto é, nas soluções de $f(x) = 0$ sobre $\mathbb{F}_q$.

Para cada $j = 1, \dots, r_1(q-1)/m$, seja $T_j = R_{w_j}(\mathcal{G}(f/\mathbb{F}_q))$. Como $f(0) = 0$, o vértice 0 é o único vértice da parte cíclica dessa componente, então cada T_j é uma árvore. Portanto,

$$\mathcal{G}_{f/\mathbb{F}_q}^{(0)} = \text{Cyc}(1, T),$$

em que

$$T = \left\langle \bigoplus_{j=1}^{r_1(q-1)/m} T_j \right\rangle. \quad (3.7)$$

Lembremos também que $\nu = (q-1)/m\omega$, em que ω é o maior divisor de $(q-1)/m$ que é relativamente primo com n . Pelo Corolário 3.11, cada T_j é isomorfo a $\mathcal{T}_{mdc_n(\nu)}^{i_j}$, em que i_j é a profundidade de T_j . Portanto, basta determinar a cardinalidade de cada conjunto

$$A_i = \{j \in \{1, \dots, r_1(q-1/m)\} : T_j \text{ é isomorfo a } \mathcal{T}_{mdc_n(\nu)}^i\}.$$

Para determinar essa cardinalidade, precisaremos definir o conjunto a seguir

$$B_i = \{j \in \{1, \dots, r_1(q-1/m)\} : T_j \text{ tem um vértice de profundidade } i\}.$$

Veja que $|A_i| = |B_i| - |B_{i+1}|$. De fato, como $\mathcal{T}_{mdc_n(\nu)}^i$ é uma árvore com profundidade i , temos que $T_i \in A_i$ se, e somente se, T_i tem profundidade i . Isso significa que T_i possui ao menos um vértice de profundidade i e, portanto, $T_i \in B_i$. Entretanto, T_i não possui vértices de profundidade $i+1$, logo, $T_i \notin B_{i+1}$. Então $A_i \subseteq B_i - B_{i+1}$. Reciprocamente, se $j \in B_i \setminus B_{i+1}$, então T_j tem pelo menos um vértice de profundidade i , mas não possui vértices de profundidade $i+1$, logo é uma árvore de profundidade i . Isso implica $j \in A_i$. Concluimos que $A_i = B_i \setminus B_{i+1}$ e, como $B_{i+1} \subseteq B_i$, então

$$|A_i| = |B_i| - |B_{i+1}|. \quad (3.8)$$

Para calcular a cardinalidade de B_i , denotemos por $z_1, \dots, z_{r_1}$ os elementos em μ_m que são soluções da equação $h(x) = 0$. Pelo Lema 1.40, qualquer vértice x de T_j com profundidade i é uma solução da equação

$$x^{\frac{q-1}{m}} = \psi_f^{(-i)} \left(w_j^{\frac{q-1}{m}} \right).$$

Por outro lado, como f é m -nice, qualquer solução da equação acima deve ser um vértice com profundidade i de T_j para algum $j \in \{1, \dots, r_1(q-1/m)\}$. Portanto, estamos interessados no número de soluções de equações

$$x^{\frac{q-1}{m}} = \psi_f^{(-i)}(z_l), \quad (3.9)$$

em que $l = 1, \dots, r_1$.

Tomando $x^{(q-1)/m} = \xi \in \mu_m$, a Equação (3.9) se torna

$$\xi = \psi_f^{(-i)}(z_l),$$

que, para algum l , é satisfeita para r_{i+1} valores distintos $\xi \in \mu_m$. Logo, o número de soluções $x \in \mathbb{F}_q$ da Equação (3.9) é igual a $r_1 \times (q-1/m)$. Como T_j é $mdc_n(\nu)$ -regular, o número de antecessores i -distantes de w_j em T_j é igual a 0 ou a $d_i = mdc(\nu, n^i)$. Portanto,

$$|B_i| = \frac{r_{i+1}(q-1)}{md_i}.$$

Ademais, segue das Equações (3.7) e (3.8) que

$$T = \left\langle \bigoplus_{i=1}^{\infty} (|B_i| - |B_{i+1}|) \times \mathcal{T}_{\text{mdc}_n(\nu)}^i \right\rangle.$$

Como existem, no máximo, m elementos em μ_m , a soma terá parcelas não nulas no máximo até $i = m - 1$. Logo, podemos assumir sem perda de generalidade que $i \leq m - 1$. Portanto,

$$T = \left\langle \bigoplus_{i=0}^{m-1} \left(\frac{(q-1)r_{i+1}}{md_i} - \frac{(q-1)r_{i+2}}{md_{i+1}} \right) \times \mathcal{T}_{\text{mdc}_n(\nu)}^i \right\rangle,$$

o que conclui a demonstração. $\square$

Exemplo 3.13. Seja $g(x) = x^{15}h(x^{36}) \in \mathbb{F}_{181}[x]$ definido como no Exemplo 1.38, e considere a notação usada no teorema anterior. Nosso objetivo é aplicar o Teorema 3.12 ao polinômio g .

Como $n = 15$, $m = 5$ e $(q-1)/m = 36$, temos $\omega = 2$, pois 2 é o maior divisor de $(181-1)/5$ que é relativamente primo com 15, $\nu = (181-1)/(5 \cdot 4) = 9$ e $\text{mdc}_n(\nu) = (3, 3)$.

Pelo Exemplo 1.28, temos $\mu_5 = \{1, 42, 59, 125, 135\}$. Além disso, pelo Exemplo 1.38 obtemos

$$r_1 = r_2 = 1, \quad r_i = 0, \text{ para } i \geq 3.$$

Além disso,

$$d_0 = \text{mdc}(9, 15^0) = 1, \quad d_1 = \text{mdc}(9, 15) = 3, \quad d_i = \text{mdc}(9, 15^i) = 9$$

para $i \geq 2$. Logo, aplicando Teorema 3.12 em g , temos que

$$\begin{aligned} T &= \left\langle \bigoplus_{i=0}^{5-1} \left(\frac{(181-1)r_{i+1}}{5d_i} - \frac{(181-1)r_{i+2}}{5d_{i+1}} \right) \times \mathcal{T}_{\text{mdc}_{15}(9)}^i \right\rangle \\ &= \left\langle \left(\frac{180r_1}{5d_0} - \frac{180r_2}{5d_1} \right) \times \mathcal{T}_{(3,3)}^0 \oplus \left(\frac{180r_2}{5d_1} - \frac{180r_3}{5d_2} \right) \times \mathcal{T}_{(3,3)}^1 \oplus \left(\frac{180r_3}{5d_2} - \frac{180r_4}{5d_3} \right) \times \mathcal{T}_{(3,3)}^2 \right. \\ &\quad \left. \oplus \left(\frac{180r_4}{5d_3} - \frac{180r_5}{5d_4} \right) \times \mathcal{T}_{(3,3)}^3 \oplus \left(\frac{180r_5}{5d_4} - \frac{180r_6}{5d_5} \right) \times \mathcal{T}_{(3,3)}^4 \right\rangle \\ &= \left\langle \left(\frac{180}{5} - \frac{180}{15} \right) \times \mathcal{T}_{(3,3)}^0 \oplus \left(\frac{180}{15} - 0 \right) \times \mathcal{T}_{(3,3)}^1 \oplus 0 \times \mathcal{T}_{(3,3)}^2 \oplus 0 \times \mathcal{T}_{(3,3)}^3 \oplus 0 \times \mathcal{T}_{(3,3)}^4 \right\rangle \\ &= \left\langle (36 - 12) \times \mathcal{T}_{(3,3)}^0 \oplus 12 \times \mathcal{T}_{(3,3)}^1 \right\rangle \\ &= \left\langle 24 \times \mathcal{T}_{(3,3)}^0 \oplus 12 \times \mathcal{T}_{(3,3)}^1 \right\rangle. \end{aligned}$$

Portanto,

$$G_{g/\mathbb{F}_{181}}^{(0)} = \text{Cyc}(1, T),$$

em que

$$T = \left\langle 24 \times \mathcal{T}_{(3,3)}^0 \oplus 12 \times \mathcal{T}_{(3,3)}^1 \right\rangle.$$

O grafo $G_{g/\mathbb{F}_{181}}^{(0)}$ está graficamente representado pela Figura 14.

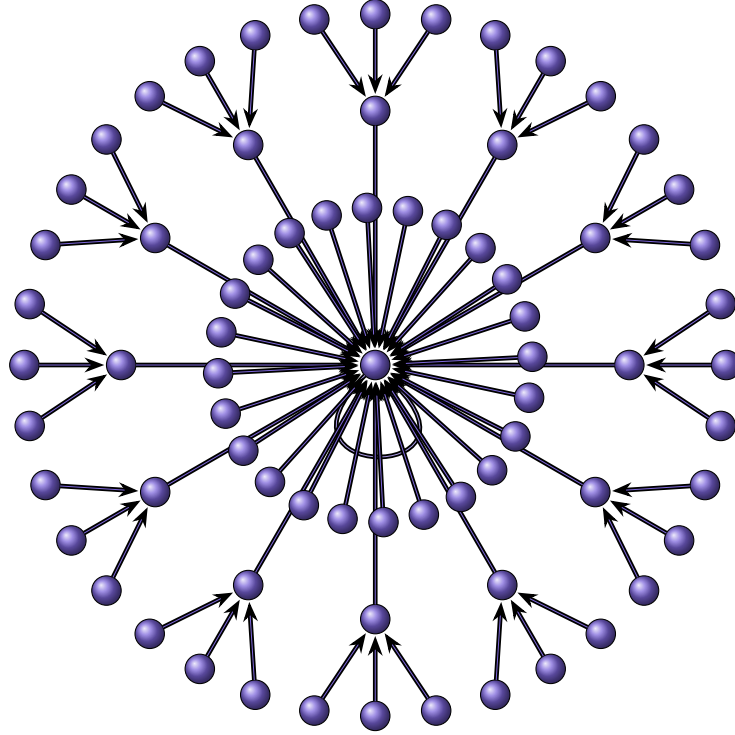


Figura 14 – $G_{g/\mathbb{F}_{181}}^{(0)}$: Componente conexa do 0 da função g sobre $\mathbb{F}_{181}$.

Teorema 3.14. *Suponhamos que $f(x) = x^n h(x^{(q-1)/m})$ seja m -nice sobre $\mathbb{F}_q$ e sejam $S_1, \dots, S_t$ conjuntos tais que $\mu_m \setminus \psi_f^{-\infty}(0) = S_1 \cup \dots \cup S_t$ e $\mathcal{G}(\psi_f/S_i) = \text{Cyc}(k_i)$. Para cada $i \in \{1, \dots, t\}$, sejam $\xi_i \in S_i$ e ℓ_i, r_i inteiros tais que*

$$\xi_i = \alpha^{\frac{q-1}{m} r_i} \quad e \quad \alpha^{\ell_i} = \prod_{j=0}^{k_i-1} h\left(\psi_f^{(j)}(\xi_i)\right)^{n^{k_i-j-1}}.$$

Então,

$$G_{f/\mathbb{F}_q}^{(1)} = \bigoplus_{\substack{i=1, \dots, t \\ u \mid \text{ord}_{\omega'(n^{k_i-1})}(n^{k_i})}} \left(\sum_{d \mid u} \frac{\mu(\frac{u}{d}) \tau_i(d)}{u} \times \text{Cyc}(k_i u, \mathcal{T}_{\text{mdc}_n(\nu)}) \right),$$

em que

$$\tau_i(d) := \begin{cases} \text{mdc}\left(\frac{q-1}{m}, n^{dk_i} - 1\right), & \text{se } \text{mdc}(q-1, (n^{dk_i} - 1)m) \\ & \text{divide } \frac{\ell_i \cdot (n^{dk_i} - 1)}{n^{k_i} - 1} + r_i(n^{dk_i} - 1); \\ 0, & \text{caso contrário.} \end{cases}$$

Demonstração. Recordemos que cada componente de $\mathcal{G}_{f/\mathbb{F}_q}^{(1)}$ é da forma $\text{Cyc}(k, \mathcal{T})$, com k inteiro positivo, cada vértice do k -ciclo é um elemento não nulo de $\mathbb{F}_q$ e é raiz de uma árvore. Pelo Corolário 3.10, tais árvores são isomorfas a $\mathcal{T}_{\text{mdc}_n(\nu)}$. Portanto, basta determinarmos a quantidade de ciclos existentes com comprimento ℓ em $\mathcal{G}_{f/\mathbb{F}_q}^{(1)}$.

Sabemos, através do Lema 1.40, que o comprimento de um ciclo está diretamente relacionado à dinâmica de ψ_f sobre μ_m . De fato, se $f^{(\ell)}(a) = a$ para algum inteiro positivo

ℓ , então, pelo Lema 1.40,

$$a^{\frac{q-1}{m}} = \psi_f^{(-\ell)} \left(a^{\frac{q-1}{m}} \right),$$

o que implica

$$\psi_f^{(\ell)} \left(a^{\frac{q-1}{m}} \right) = a^{\frac{q-1}{m}},$$

pois f é m -nice e, portanto, ψ_f é injetora em a .

Logo, se $a^{(q-1)/m} \in S_i$, então k_i divide ℓ . Além disso, qualquer vértice b no mesmo ciclo de a satisfaz $b^{(q-1)/m} \in S_i$. Em particular, isso significa que ciclos cujas dinâmicas estão relacionadas a conjuntos S_i e S_j distintos não estão conectados. Portanto, podemos determinar separadamente cada um desses ciclos.

Sejam d e u inteiros positivos, $i \in \{1, \dots, t\}$ fixado, e definamos

$$A_i(u) = \left\{ a \in \mathbb{F}_q : a^{\frac{q-1}{m}} = \xi_i \text{ e } f^{(uk_i)}(a) = a \right\},$$

$$B_i(d) = \left\{ a \in \mathbb{F}_q : a^{\frac{q-1}{m}} = \xi_i \text{ e } d \text{ é o menor inteiro positivo tal que } f^{(dk_i)}(a) = a \right\}.$$

Precisamos calcular $|B_i(u)|$ para determinar quantos ciclos, com vértices a tais que $a^{(q-1)/m} = \xi_i$, existem com comprimento uk_i . Dado um elemento $a \in A_i(u)$, temos que, como d é o menor inteiro positivo tal que $f^{(dk_i)}(a) = a$, o comprimento do ciclo contendo a é exatamente dk_i . Além disso, como $f^{(uk_i)}(a) = a$, temos que dk_i divide uk_i , então d divide u .

Logo, como todo $a \in A_i(u)$ está em um ciclo de comprimento dk_i tal que d divide u , temos que A_i é formado pela união disjunta dos conjuntos $B_i(d)$, em que d percorre os divisores de u , isto é,

$$A_i(u) = \bigcup_{d|u} B_i(d),$$

em que $B_i(d) \cap B_i(d') = \emptyset$ se $d \neq d'$. Portanto, temos

$$|A_i(u)| = \sum_{d|u} |B_i(d)|.$$

Aplicando a fórmula de inversão de Möbius (Teorema 1.43) nessa igualdade, obtemos

$$|B_i(u)| = \sum_{d|u} \mu \left(\frac{u}{d} \right) |A_i(d)|. \quad (3.10)$$

Calculemos agora o valor de $|A_i(d)|$. Seja $a \in A_i(d)$. Como $a^{(q-1)/m} = \xi_i$ e $f^{(dk_i)}(a) = a$, segue que $a = \alpha^{sm+r_i}$ para alguns valores de $s \in \{1, \dots, (q-1)/m\}$, então, da Proposição 1.35, temos que

$$\left(\alpha^{sm+r_i} \right)^{n^{dk_i}} \prod_{j=0}^{dk_i-1} h \left(\psi_f^{(i)}(\xi) \right)^{n^{dk_i-j-1}} = \alpha^{sm+r_i}. \quad (3.11)$$

Como $\psi_f^{(k_i)}(\xi_i) = \xi_i$ e $\psi_f^{(k_it+j)}(\xi_i) = \psi_f^{(j)}(\xi_i)$, podemos reescrever o produtório da Equação (3.11). Então

$$\prod_{j=0}^{dk_i-1} h \left(\psi_f^{(j)}(\xi) \right)^{n^{dk_i-j-1}} = \prod_{t=0}^{d-1} \prod_{j=0}^{k_i-1} h \left(\psi_f^{(k_it+j)}(\xi_i) \right)^{n^{d_i-k_it-j-1}}. \quad (3.12)$$

Além disso, $dk_i - k_i t - j - 1 = (d - t - 1)k_i + k_i - j - 1$, logo, $n^{dk_i - k_i t - j - 1} = n^{k_i - j - 1} n^{(d - t - 1)k_i}$. Substituindo na Equação (3.12) obtemos

$$\prod_{j=0}^{dk_i-1} h(\psi_f^{(j)}(\xi))^{n^{dk_i-j-1}} = \prod_{t=0}^{d-1} \prod_{j=0}^{k_i-1} h(\psi_f^{(j)}(\xi_i)^{n^{k_i-j-1}})^{n^{(d-t-1)k_i}}. \quad (3.13)$$

Sabemos que $\alpha^{\ell_i} = \prod_{j=0}^{k_i-1} h(\psi_f^{(j)}(\xi_i))^{n^{k_i-j-1}}$. Substituindo esse valor na Equação (3.13) e fazendo algumas manipulações algébricas, temos

$$\begin{aligned} \prod_{j=0}^{dk_i-1} h(\psi_f^{(j)}(\xi))^{n^{dk_i-j-1}} &= \prod_{t=0}^{d-1} (\alpha^{\ell_i})^{n^{(d-t-1)k_i}} \\ &= \alpha^{\ell_i n^{(d-1)k_i}} \alpha^{\ell_i n^{(d-2)k_i}} \dots \alpha^{\ell_i n^{k_i}} \alpha^{\ell_i} \\ &= \alpha^{\ell_i(1+n^{k_i}+\dots+n^{(d-1)k_i})}. \end{aligned}$$

Substituindo, na Equação (3.11), o valor encontrado, obtemos

$$(\alpha^{sm+r_i})^{n^{dk_i}} \alpha^{\ell_i(1+n^{k_i}+\dots+n^{(d-1)k_i})} = \alpha^{sm+r_i}.$$

Considerando os expoentes dessa equação, temos

$$(sm + r_i) n^{dk_i} + \ell_i(1 + n^{k_i} + \dots + n^{(d-1)k_i}) \equiv sm + r_i \pmod{q-1}.$$

Reescrevendo a progressão geométrica $(1 + n^{k_i} + \dots + n^{(d-1)k_i})$, obtemos

$$(sm + r_i) n^{dk_i} + \ell_i \frac{n^{dk_i} - 1}{n^{k_i} - 1} \equiv sm + r_i \pmod{q-1}.$$

Colocando $sm + r_i$ em evidência no lado esquerdo da congruência, temos

$$(sm + r_i) (n^{dk_i} - 1) + \ell_i \frac{n^{dk_i} - 1}{n^{k_i} - 1} \equiv 0 \pmod{q-1}.$$

Por fim, colocando $\frac{n^{dk_i}-1}{n^{k_i}-1}$ em evidência, obtemos

$$\left(\frac{n^{dk_i} - 1}{n^{k_i} - 1} \right) ((sm + r_i) (n^{k_i} - 1) + \ell_i) \equiv 0 \pmod{q-1}. \quad (3.14)$$

Veremos agora que o número de soluções $s \in \{1, \dots, (q-1)/m\}$ da Equação (3.14) é dada por

$$\tau_i(d) := \begin{cases} \text{mdc}\left(\frac{q-1}{m}, n^{dk_i} - 1\right), & \text{se } \text{mdc}\left((n^{dk_i} - 1)m, q-1\right) \\ & \text{divide } \ell_i \frac{n^{dk_i}-1}{n^{k_i}-1} + r_i(n^{dk_i} - 1); \\ 0, & \text{caso contrário.} \end{cases}$$

De fato, denotemos

$$\begin{aligned} \tilde{a} &= \frac{n^{dk_i} - 1}{n^{k_i} - 1} m (n^{k_i} - 1) = m (n^{dk_i} - 1), \\ \tilde{b} &= \frac{n^{dk_i} - 1}{n^{k_i} - 1} (r_i (n^{k_i} - 1) + \ell_i) = \ell_i \frac{n^{dk_i} - 1}{n^{k_i} - 1} + r_i (n^{dk_i} - 1), \\ \tilde{m} &= q - 1. \end{aligned}$$

Veja que a Equação (3.14) é uma equação da forma $\tilde{a}x \equiv \tilde{b} \pmod{\tilde{m}}$, que possui solução se

$$\text{mdc}(\tilde{a}, \tilde{m}) \mid \tilde{b}.$$

Se a equação não possui solução, então $\tau_i(d) = 0$. Suponha que essa equação possua solução, então existem $\tilde{c}$ soluções módulo $\tilde{c} \cdot \tilde{m} / \text{mdc}(\tilde{a}, \tilde{m})$ no intervalo $[1, \tilde{c} \cdot \tilde{m} / \text{mdc}(\tilde{a}, \tilde{m})]$. Logo, a solução $\text{mdc}(\tilde{a}, \tilde{m}) \mid \tilde{b}$ é

$$\text{mdc}\left(m\left(n^{dk_i} - 1\right), q - 1\right) \mid \ell_i \frac{n^{dk_i} - 1}{n^{k_i} - 1} + r_i\left(n^{dk_i} - 1\right).$$

O número de soluções módulo $\tilde{c}(q - 1) / \text{mdc}\left(m\left(n^{dk_i} - 1\right), q - 1\right)$ é $\tilde{c}$. Como

$$\tilde{c} \cdot \frac{q - 1}{\text{mdc}\left(m\left(n^{dk_i} - 1\right), q - 1\right)} = \frac{q - 1}{m},$$

temos $\tilde{c} = \text{mdc}\left(n^{dk_i} - 1, (q - 1)/m\right)$. Então $\tau_i(d) = \text{mdc}\left(n^{dk_i} - 1, (q - 1)/m\right)$ se

$$\text{mdc}\left(m\left(n^{dk_i} - 1\right), q - 1\right) \mid \ell_i\left(n^{dk_i} - 1\right) / \left(n^{k_i} - 1\right) + r_i\left(n^{dk_i} - 1\right).$$

Isso prova a afirmação.

Por outro lado, cada solução $s \in \{1, \dots, (q - 1)/m\}$ da Equação (3.14) cria um elemento em $A_i(d)$ e, portanto,

$$|A_i(d)| = \tau_i(d). \quad (3.15)$$

Logo, das Equações (3.10) e (3.15) segue que

$$|B_i(u)| = \sum_{d|u} \mu\left(\frac{u}{d}\right) \tau_i(d).$$

Resta provar que, se u é um inteiro para o qual existe um ciclo em $\mathcal{G}_{f/\mathbb{F}_q}^{(1)}$ de comprimento uk_i , então

$$u \mid \text{ord}_{\omega'(n^{k_i}-1)}(n^{k_i}).$$

Primeiramente, vejamos que se $a = \alpha^{sm+r_i}$ é um elemento em um ciclo de comprimento uk_i , então a Equação (3.14) implica que u é o menor inteiro tal que

$$\left(\frac{n^{uk_i} - 1}{n^{k_i-1}}\right) \left((sm + r_i)(n^{k_i} - 1) + \ell_i\right) \equiv 0 \pmod{q - 1},$$

o que implica que

$$u = \text{ord}_{t(n^{k_i}-1)}(n^{k_i}),$$

em que t é divisor de $q - 1$ e é relativamente primo com n . Então t divide ω' , pois ω' é o maior divisor de $q - 1$ que é relativamente primo com n . Logo,

$$\text{ord}_{t(n^{k_i}-1)}(n^{k_i}) \mid \text{ord}_{\omega'(n^{k_i}-1)}(n^{k_i}),$$

o que completa a demonstração. $\square$

Exemplo 3.15. Seja $g(x) \in \mathbb{F}_{181}[x]$ definido como no Exemplo (1.28) e a notação usada no teorema anterior. Iremos aplicar o Teorema 3.14 ao polinômio $g(x) = x^{15}h(x^{36})$.

Do Exemplo 1.38, em que calculamos os valores de ψ_g aplicado nos elementos de μ_5 e concluímos que g é 5-nice sobre $\mathbb{F}_{181}$, podemos escolher $S_1 = \{125\}$ e $S_2 = \{1, 135\}$. Dessa forma, como $\mathcal{G}(\psi_g/S_1) = \text{Cyc}(1)$ e $\mathcal{G}(\psi_g/S_2) = \text{Cyc}(2)$, temos $k_1 = 1$ e $k_2 = 2$.

Do Exemplo 3.13, temos $\omega = 2$ e $\nu = 9$. Além disso, $\omega' = 4$, pois 4 é o maior divisor de $181 - 1$ que é relativamente primo com 15. Logo,

$$\text{ord}_{4(15-1)}(15) = 2, \quad \text{ord}_{4(15^2-1)}(15^2) = 4$$

e, pelo Exemplo 1.45, $\mathcal{T}_{\text{mdc}_n(\nu)} = \mathcal{T}_{\text{mdc}_{15}(9)} = \mathcal{T}_{(3,3)}$.

Dos dados já obtidos e das expressões $\xi_i = \alpha^{r_1(q-1)/m}$ e $\alpha^{\ell_i} = \prod_{j=0}^{k_i-1} h\left(\psi_f^{(j)}(\xi_i)\right)^{n^{k_i-j-1}}$, temos

$$\ell_1 = 18, \quad \ell_2 = 75, \quad r_1 = 3, \quad r_2 = 0.$$

Calculando os valores de $\tau_i(d)$ obtemos

$$\tau_1(1) = 2, \tau_1(2) = 4, \tau_2(1) = 0, \tau_2(2) = 0 \text{ e } \tau_2(4) = 4.$$

Portanto, aplicando Teorema 3.14, temos que

$$\begin{aligned} G_{g/\mathbb{F}_{181}}^{(1)} &= \bigoplus_{u|\text{ord}_{4(15^{k_1}-1)}(15^{k_1})} \left(\sum_{d|u} \frac{\mu(\frac{u}{d})\tau_1(d)}{u} \times \text{Cyc}(k_1 u, \mathcal{T}_{(3,3)}) \right) \\ &\quad \bigoplus_{u|\text{ord}_{4(15^{k_2}-1)}(15^{k_2})} \left(\sum_{d|u} \frac{\mu(\frac{u}{d})\tau_2(d)}{u} \times \text{Cyc}(k_2 u, \mathcal{T}_{(3,3)}) \right) \\ &= \bigoplus_{u|2} \left(\sum_{d|u} \frac{\mu(\frac{u}{d})\tau_1(d)}{u} \times \text{Cyc}(1 \cdot u, \mathcal{T}_{(3,3)}) \right) \\ &\quad \bigoplus_{u|4} \left(\sum_{d|u} \frac{\mu(\frac{u}{d})\tau_2(d)}{u} \times \text{Cyc}(2 \cdot u, \mathcal{T}_{(3,3)}) \right) \\ &= \left(\sum_{d|1} \frac{\mu(\frac{1}{d})\tau_1(d)}{1} \times \text{Cyc}(1, \mathcal{T}_{(3,3)}) \right) \oplus \left(\sum_{d|2} \frac{\mu(\frac{2}{d})\tau_1(d)}{2} \times \text{Cyc}(2, \mathcal{T}_{(3,3)}) \right) \\ &\quad \left(\sum_{d|1} \frac{\mu(\frac{1}{d})\tau_2(d)}{1} \times \text{Cyc}(2 \cdot 1, \mathcal{T}_{(3,3)}) \right) \oplus \left(\sum_{d|2} \frac{\mu(\frac{2}{d})\tau_2(d)}{2} \times \text{Cyc}(2 \cdot 2, \mathcal{T}_{(3,3)}) \right) \\ &\quad \oplus \left(\sum_{d|4} \frac{\mu(\frac{4}{d})\tau_2(d)}{4} \times \text{Cyc}(2 \cdot 4, \mathcal{T}_{(3,3)}) \right) \end{aligned}$$

$$\begin{aligned}
&= \left(\tau_1(1) \times \text{Cyc} \left(1, \mathcal{T}_{(3,3)} \right) \right) \oplus \left(\frac{(-\tau_1(1) + \tau_1(2))}{2} \times \text{Cyc} \left(2, \mathcal{T}_{(3,3)} \right) \right) \\
&\quad \oplus \left(\tau_2(1) \times \text{Cyc} \left(2 \cdot 1, \mathcal{T}_{(3,3)} \right) \right) \oplus \left(\frac{(-\tau_2(1) + \tau_2(2))}{2} \times \text{Cyc} \left(4, \mathcal{T}_{(3,3)} \right) \right) \\
&\quad \oplus \left(\frac{(0 \cdot \tau_2(1) - \tau_2(2) + \tau_2(4))}{4} \times \text{Cyc} \left(8, \mathcal{T}_{(3,3)} \right) \right) \\
&= \left(2 \times \text{Cyc} \left(1, \mathcal{T}_{(3,3)} \right) \right) \oplus \left(1 \times \text{Cyc} \left(2, \mathcal{T}_{(3,3)} \right) \right) \oplus \left(0 \times \text{Cyc} \left(2, \mathcal{T}_{(3,3)} \right) \right) \\
&\quad \oplus \left(0 \times \text{Cyc} \left(4, \mathcal{T}_{(3,3)} \right) \right) \oplus \left(\frac{4}{4} \times \text{Cyc} \left(8, \mathcal{T}_{(3,3)} \right) \right) \\
&= 2 \times \text{Cyc} \left(1, \mathcal{T}_{(3,3)} \right) \oplus \text{Cyc} \left(2, \mathcal{T}_{(3,3)} \right) \oplus \text{Cyc} \left(8, \mathcal{T}_{(3,3)} \right),
\end{aligned}$$

isto é,

$$G_{g/\mathbb{F}_{181}}^{(1)} = 2 \times \text{Cyc} \left(1, \mathcal{T}_{(3,3)} \right) \oplus \text{Cyc} \left(2, \mathcal{T}_{(3,3)} \right) \oplus \text{Cyc} \left(8, \mathcal{T}_{(3,3)} \right).$$

O grafo $G_{g/\mathbb{F}_{181}}^{(1)}$ está graficamente representado pela Figura 15.

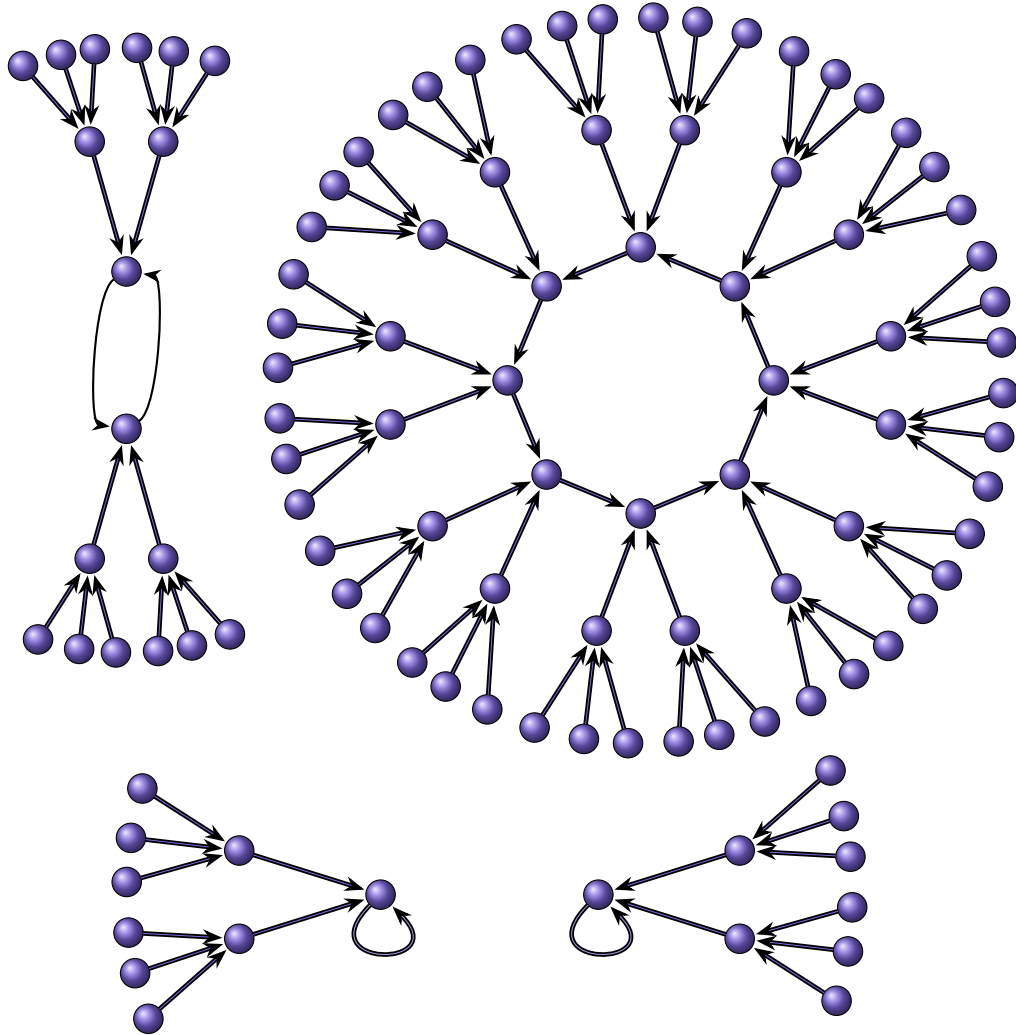


Figura 15 – $\mathcal{G}_{g/\mathbb{F}_{181}}^{(1)}$: Grafo das componentes conexas da função g sobre $\mathbb{F}_{181}$ que não contêm o vértice 0.

Teorema 3.16. *Seja $f(x) = x^n h(x^{(q-1)/m})$ função m -nice sobre $\mathbb{F}_q$ e considere as notações apresentadas no Teorema 3.12 e no Teorema 3.14. Então o grafo funcional $\mathcal{G}(f/\mathbb{F}_q)$ é dado por*

$$\mathcal{G}(f/\mathbb{F}_q) = \text{Cyc}(1, T) \bigoplus_{\substack{i=1, \dots, t \\ u | \text{ord}_{\omega'(n^{k_i-1})}(n^{k_i})}} \left(\sum_{d|u} \frac{\mu(\frac{u}{d}) \tau_i(d)}{u} \times \text{Cyc}(k_i u, \mathcal{T}_{\text{mdc}_n(\nu)}) \right),$$

em que

$$T = \left\langle \bigoplus_{i=0}^{m-1} \left(\frac{(q-1)r_{i+1}}{md_i} - \frac{(q-1)r_{i+2}}{md_{i+1}} \right) \times \mathcal{T}_{\text{mdc}_n(\nu)}^i \right\rangle.$$

Exemplo 3.17. Aplicando o Teorema 3.16 na função $g(x) = x^{15}h(x^{36}) \in \mathbb{F}_{181}[x]$ e utilizando as estruturas de $\mathcal{G}_{g/\mathbb{F}_{181}}^{(0)}$ e de $\mathcal{G}_{g/\mathbb{F}_{181}}^{(1)}$ obtidas no Exemplo 3.13 e no Exemplo 3.15. Temos

$$\begin{aligned} \mathcal{G}(g/\mathbb{F}_{181}) = & \text{Cyc}\left(1, \left\langle 24 \times \mathcal{T}_{(3,3)}^0 \oplus 12 \times \mathcal{T}_{(3,3)}^1 \right\rangle\right) \oplus 2 \times \text{Cyc}\left(1, \mathcal{T}_{(3,3)}\right) \\ & \oplus \text{Cyc}\left(2, \mathcal{T}_{(3,3)}\right) \oplus \text{Cyc}\left(8, \mathcal{T}_{(3,3)}\right). \end{aligned}$$

O grafo $\mathcal{G}(g/\mathbb{F}_{181})$ está graficamente representado pela Figura 16.

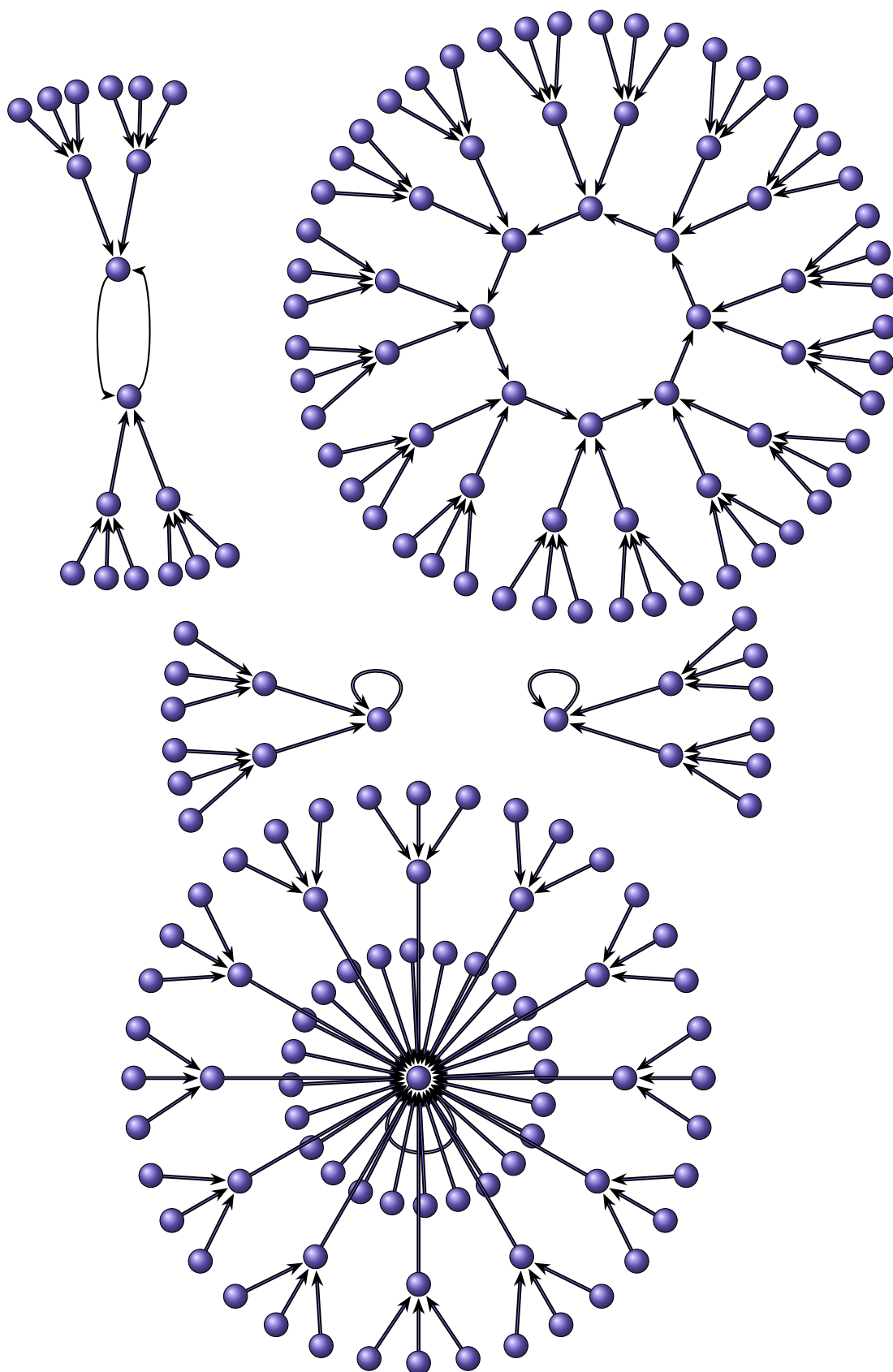


Figura 16 – $\mathcal{G}(g/\mathbb{F}_{181})$: Grafo da função $g(x) = x^{15}h(x^{36})$ sobre $\mathbb{F}_{181}$.

Referências

- DIESTEL, R. *Graph Theory*. 6. ed. Heidelberger Platz 3, 14197 Berlin, Germany: Springer, 1997.
- GARCIA, A.; LEQUAIN, Y. *Elementos de Álgebra*. 6. ed. Rio de Janeiro: IMPA, 2014.
- JURKIEWICZ, S. *Grafos: Uma introdução*. 1. ed. Rio de Janeiro: IMPA, 2007.
- LIDL, R.; NIEDERREITER, H. *Finite Fields*. 2. ed. Cambridge, Reino Unido: Cambridge University Press, 1997.
- OLIVEIRA, J. A.; BROCHERO MARTÍNEZ, F. E. *Dynamics of polynomial maps over finite fields*. *Des. Codes Cryptogr.* 92, no. 5, 1113–1125. Springer, 2024. Disponível em: <https://doi.org/10.1007/s10623-023-01332-3>.