KATHERINE ANGIE MOLINA LUCIANO

O grafo funcional de uma família de polinômios sobre uma extensão quadrática de um corpo finito

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
2025

KATHERINE ANGIE MOLINA LUCIANO

O grafo funcional de uma família de polinômios sobre uma extensão quadrática de um corpo finito

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.

Orientador(a): Dr(a). Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2025

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

L937g 2025

Luciano, Katherine Angie Molina, 1999-
O grafo funcional de uma família de polinômios sobre uma extensão quadrática de um corpo finito [recurso eletrônico] / Katherine Angie Molina Luciano. - 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.2026.5050
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

Nelson Marcos Ferreira
Bibliotecário-Documentalista - CRB-6/3074

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 - pgmat@ime.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 124, PPGMAT				
Data:	30/06/2025	Hora de início:	15:00	Hora de encerramento:	17:00
Matrícula do Discente:	12312MAT002				
Nome do Discente:	Katherine Angie Molina Luciano				
Título do Trabalho:	O grafo funcional de uma família de polinômios sobre uma extensão quadrática de um corpo finito				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Estudo de elementos primitivos e normais em corpos finitos				

Reuniu-se em web conferência, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Abílio Lemos Cardoso Júnior - Universidade Federal de Viçosa/UFV; Guilherme Chaud Tizziotti - Instituto de Matemática e Estatística - IME/UFU e Victor Gonzalo Lopez Neumann - Instituto de Matemática e Estatística - 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 **Guilherme Chaud Tizziotti**, **Professor(a) do Magistério Superior**, em 30/06/2025, às 17:05, 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 30/06/2025, às 20:21, 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 **Abílio Lemos Cardoso Júnior**, **Usuário Externo**, em 30/06/2025, às 20:24, 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 **5999518** e o código CRC **A12FFD51**.

Referência: Processo nº 23117.000290/2025-46 SEI nº 5999518

Dedicatória

Dedicado a Deus e aos meus pais, Carlos e Maruja, que sempre me acompanharam e me motivaram a ser uma pessoa melhor e a alcançar meus objetivos. Sou profundamente grata pelo cuidado, amor e atenção que me dedicam até hoje.
Aos meus avós, Margarita e Máximo, cujo apoio e impulso senti desde os meus primeiros anos de vida. Agradeço por sua ternura, pelos valores que me transmitiram e pelo amor infinito que sempre me deram.
Às minhas irmãs, Yhadira e Saomi, e ao meu irmãozinho, Carlos Max Angelo — vocês são a minha maior motivação para seguir em frente. Por vocês, procuro ser uma irmã mais velha cada vez melhor. Amo vocês profundamente.

Agradecimentos

Gostaria de começar este texto expressando minha profunda gratidão a Deus, que foi meu melhor amigo. Não teria sido possível chegar a este momento tão especial sem Ele.

À minha família — em especial, agradeço aos meus pais, Carlos e Maruja, pelo amor e apoio incondicionais que sempre recebi, pela motivação constante ao longo de todos esses anos. Faltam-me palavras para agradecer verdadeiramente.

Agradeço à bolsa da CAPES durante o primeiro ano do mestrado e à bolsa da FAPEMIG pelo apoio por meio do projeto APQ-00470-22 durante o segundo ano do mestrado.

Agradeço a todos os meus professores do mestrado e ao meu orientador, Víctor Gonzalo Lopez Neumann, que não apenas compartilharam seu conhecimento, mas também seu tempo e dedicação. Em especial, ressalto a paciência e o acompanhamento constante do meu orientador.

Finalmente, agradeço aos meus amigos no Brasil que estiveram ao meu lado nos momentos em que mais precisei, oferecendo motivação, consolo e força para continuar. Alguns deles me deram sentido de vida e motivos para me superar e crescer. Sou e sempre serei grata a todos, pois foram como uma família para mim — chegaram até a assumir o papel de parentes em situações importantes.

Ao lembrar dessa etapa, fico sensível. É inevitável sentir certa tristeza, mas também um sorriso nasce ao perceber que não estive sozinha: tive a presença e o apoio deles. Seus gestos foram impulso e grande suporte emocional durante minha estadia em Uberlândia.
Agradeço especialmente ao professor Fernando Rodrigo R., à Aida Câmera, à Geiza, pela alegria contagiante, e à minha colega de mestrado Selma Alves.
E a duas pessoas importantes do Peru, cujo apoio incondicional senti em momentos decisivos. Apesar da distância, estiveram sempre me incentivando e apoiando como puderam, desde Huaraz(Peru) e Rio de Janeiro. Lhes agradeço de coração. Obrigada a todos eles, porque fizeram parte do meu percurso.

LUCIANO, K. A. M. *O grafo funcional de uma família de polinômios sobre uma extensão quadrática de um corpo finito.* 2025. 66 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Seja X um conjunto finito e $f : X \to X$ uma função arbitraria. A iteração de f sobre X nos dá um sistema dinâmico que pode ser representado como um grafo. De fato, o grafo funcional de f é o grafo dirigido $\mathscr{G}(f) = (\mathcal{V}, \mathcal{E})$, onde $\mathcal{V} = X$ e $\mathcal{E} = \{\langle x, f(x)\rangle \mid x \in X\}$. O sistema dinâmico obtido tem aplicações em muitas áreas tais como a criptografia, as comunicações e física.

Seja $\mathbb{F}_q$ um corpo finito com q elementos de característica ímpar. Neste trabalho, descreveremos completamente a dinâmica da função $f(X) = c\,(X^{q+1} + aX^2)$ sobre o corpo finito $\mathbb{F}_{q^2}$, para $a \in \{\pm 1\}$ e $c \in \mathbb{F}_q^*$. Também, daremos alguns resultados parciais para $a \in \mathbb{F}_q \setminus \{0, 1, -1\}$.

Palavras-chave: Grafo funcional, Funções iterativas, Dinâmica de funções, Corpos Finitos, Extensões quadráticas, Pontos periódicos.

LUCIANO, K. A. M. *The functional graph of a family of polynomials over a quadratic extension of a finite field* 2025. 66 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

Let X be a finite set and $f : X \to X$ an arbitrary function. The iteration of f over X yields a dynamical system that can be represented as a graph. In fact, the functional graph of f is the directed graph $\mathscr{G}(f) = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = X$ and $\mathcal{E} = \{\langle x, f(x)\rangle \mid x \in X\}$. The obtained dynamical system has applications in many areas such as cryptography, communications and physics.

Let $\mathbb{F}_q$ be a finite field with q elements of odd characteristic. In this work, we will fully describe the dynamics of the function $f(X) = c\,(X^{q+1} \pm aX^2)$ over the finite field $\mathbb{F}_{q^2}$, for $a \in \{\pm 1\}$ and $c \in \mathbb{F}_q^*$. We will also provide partial results for $a \in \mathbb{F}_q^* \backslash \{\pm 1\}$.

Keywords: Functional graph, Iterated functions, Function dynamics, Finite fields, Quadratic extensions, Periodic points.

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

1. $\mathbb{F}_q$: Corpo finito com q elementos.
2. $\mathbb{F}_q^*$: Grupo multiplicativo do $\mathbb{F}_q$.
3. $F^* = F \setminus \{0\}$: O conjunto dos elementos não nulos de F.
4. (a, b) : Intervalo aberto com extremos a e b.
5. $\chi_2(a)$: Carácter quadrático de a.
6. $a \equiv b \pmod{m}$: a congruente a b módulo m.
7. $a|b$: a divide b.
8. $\mathrm{Ord}(\theta)$: Ordem multiplicativa de θ em um corpo finito.
9. $\mathrm{Ord}_d(a)$: Ordem multiplicativa de a módulo d.
10. $\mathrm{mcd}(a, b)$: Máximo comum divisor de a e b.
11. $\mathrm{mmc}(a, b)$: Mínimo múltiplo comum de a e b.
12. $\mathbb{N}$: Conjunto dos números Naturais $\{1, 2, 3, 4, \ldots\}$.
13. $\mathbb{Q}$: Conjunto dos números Racionais.
14. $\mathbb{R}$: Corpo dos números Reais.
15. $\mathbb{C}$: Corpo dos números complexos.
16. $\mathrm{Nu}(\varphi)$: Núcleo de φ.
17. $\mathrm{Car}(F)$: Característica do corpo F.
18. 1_F: É a unidade do corpo F.
19. $F \mid K$: F é uma extensão de corpos sobre K
20. $[L : K]$: Grau da extensão L sobre K.
21. ζ_n: raiz n-ésima primitiva da unidade.
22. $\mathscr{G}\left(f|_{\mathbb{F}_q}\right)$: O grafo funcional de f restrito a $\mathbb{F}_q$.

Conteúdo

Introdução

A dinâmica de funções, também conhecida como dinâmica iterativa, é uma área da matemática que estuda o comportamento de funções sob iterações repetidas. Em outras palavras, trata-se de um processo contínuo, no qual cada repetição se baseia nos resultados da anterior, buscando aprimorar ou ajustar o processo ou produto a cada ciclo. Esse mecanismo gera sequências (ou órbitas) a partir de um ponto inicial, permitindo analisar como o sistema evolui ao longo das iterações — seja estabilizando-se, entrando em ciclos periódicos ou exibindo comportamentos transitórios.

Particularmente a dinâmica de iterações de polinômios e funções racionais tem despertado grande interesse recentemente, em parte devido às suas aplicações como por exemplo em criptografia, e algumas outras aplicações como por exemplo métodos de fatoração de inteiros como algoritmo Pollard rho para algumas aplicações em criptografia de curva elíptica (Wiener & Zuccherato, 1999).

De maneira geral, se consideramos T_m o conjunto de funções que mapeiam o conjunto $\{1, 2, 3, \ldots, m\}$ em si mesmo. Para cada $f \in T_m$, está associado um grafo funcional com m vértices, onde existe uma aresta direcionada do vértice u para o vértice v se, e somente se, $f(u) = v$. Os grafos funcionais das funções são compostos por conjuntos de componentes conexas, onde cada componente conexa consiste em ciclos direcionados de vértices, e cada um desses vértices é a raiz de uma árvore.

Neste trabalho forneceremos o grafo funcional de uma família de polinômios sobre uma extensão quadrática de um corpo finito de característica ímpar. Essa família de polinômios a considerar será

$$f(X) = c(X^{q+1} + aX^2),$$

com $a, c \in \mathbb{F}_q^*$.

Imediatamente nos Capítulos 2 e 3 serão apresentadas, para $a = -1$ e $a = 1$, respectivamente, a determinação dos pontos fixos, a análise das pré-imagens, o número de ciclos e seus comprimentos, a descrição dos pré-ciclos e, por último, os teoremas principais (ver Teoremas 2.5.1 e 3.5.1), cujas formulações serão construídas com base nas análises desenvolvidas ao longo dos capítulos mencionados.

Finalmente, no Capítulo 4 um resultado parcial, com alguns exemplos referenciais que se experimenta em esse tipo de casos. A maior parte deste trabalho tem referência ao artigo (Brochero Martínez & Teixeira, 2023).

Katherine Angie Molina Luciano
Uberlândia-MG, 30 de Junho de 2025.

Capítulo 1

Fundamentação Teórica

1.1 Corpos Finitos

Com base nos conceitos apresentados nos livros de (Gonçalves, 2020) e (Rudolf Lidl, 2003), selecionamos e adaptamos algumas ideias gerais de álgebra e algumas que consideramos essenciais para a compreensão dos corpos finitos. Esses conceitos serviram como alicerce para a formulação das definições que serão expostas a seguir, com o objetivo de fornecer uma base teórica sólida e acessível ao leitor.

Definição 1.1.1 (Anel)**.** *Seja F um conjunto diferente do vazio no qual estão definidas duas operações binarias, $+$ adição e $\cdot$ multiplicação:*

$$\begin{array}{rccccc} +: & F\times F & \longrightarrow & F & & \\ & (a,b) & \rightsquigarrow & a+b & & \end{array} \quad e \quad \begin{array}{rccccc} \cdot: & F\times F & \longrightarrow & F & & \\ & (a,b) & \rightsquigarrow & a\cdot b. & & \end{array}$$

Se para todos $a, b, c \in F$:

1) Tem-se $(a+b)+c = a+(b+c)$ (Associatividade da soma);

2) Existe $0 \in F$ tal que $a+0 = 0+a$ (Existência de elemento neutro para a soma);

3) Para $x \in F$ existe um único $y \in F$, denotado por $y = -x$, tal que $x+y = y+x$ (Existência de inverso aditivo);

4) Tem-se $a+b = b+a$ (Comutatividade da soma);

5) Tem-se $(a\cdot b)\cdot c - a\cdot(b\cdot c)$ (Associatividade do produto);

6) Tem-se $a\cdot(b+c) = a\cdot b + a\cdot c$; $(a+b)\cdot c = a\cdot c + b\cdot c$ (Distributividade à esquerda e à direita),

dizemos que $F = (F, +, \cdot)$ é um Anel.

Se um anel $F = (F, +, \cdot)$ satisfaz:

7) Existe $1 \in F, 0 \neq 1$, tal que $x\cdot 1 = 1\cdot x = x$ para todo $x \in F$,

dizemos que $(F, +, \cdot)$ é um anel com unidade 1.

Se um anel $F = (F, +, \cdot)$ satisfaz:

8) Para todos $x, y \in F$, $x\cdot y = y\cdot x$,

dizemos que $(F, +, \cdot)$ *é um anel comutativo.*

Se um anel $F = (F, +, \cdot)$ *satisfaz:*

9) Para todos $x, y \in F$*, se* $x \cdot y = 0$ *então* $x = 0$ *ou* $y = 0$*,*

dizemos que $(F, +, \cdot)$ *é um anel sem divisores de zero.*

Definição 1.1.2 (Domínio de Integridade)**.** *Se* $F = (F, +, \cdot)$ *é um anel comutativo, com unidade e sem divisores de zero, dizemos que* $(F, +, \cdot)$ *é um domínio de Integridade.*

Definição 1.1.3 (Corpo)**.** *Um anel comutativo com unidade* $F = (F, +, \cdot)$ *é um corpo se todo elemento* $a \in F \setminus \{0\}$ *possui inverso multiplicativo. Isto se, para todo* $a \in F \setminus \{0\}$*, existe* $b \in F$ *tal que* $a \cdot b = 1$*. O inverso multiplicativo de um elemento* a *é denotado* a^{-1}*.*

Em outras palavras, F é um corpo se for um anel comutativo com unidade tal que todo elemento não nulo possui inverso multiplicativo. O fato de não ter divisores de zero, é uma consequência da existência de inverso multiplicativo. Isso nos leva ao seguinte resultado.

Proposição 1.1.4. *Todo corpo é um domínio de integridade.*

Demostração. Seja F um corpo e sejam $x, y \in F$ tais que $x \cdot y = 0$. Se $x \neq 0$, então existe $x^{-1} \in F$. Daí, $y = x^{-1} \cdot 0 = 0$. Consequentemente, F é um domínio de integridade. □

Definição 1.1.5 (Corpo Finito)**.** *Um corpo com um número finito de elementos é chamado de corpo finito.*

Definição 1.1.6 (Característica de um domínio de integridade)**.** *Seja* F *um domínio de integridade com elemento unidade* 1*. O menor inteiro positivo* r *tal que* $r \cdot 1 = 0$ *é chamado de característica de* F*. Se tal inteiro positivo não existe, dizemos que a característica de* F *é zero.*

Teorema 1.1.7. *Se a característica de um domínio de integridade* F *é um número positivo* p*, então* p *é um número primo.*

Demostração. Como F contém elementos não nulos, F tem característica $p \geqslant 2$. Se p não fosse primo, poderíamos escrever $p = km$ com $k, m \in \mathbb{Z}, 1 < k, m < p$. Então

$$0 = p \cdot 1 = (k \cdot m) \cdot 1 = (k \cdot 1) \cdot (m \cdot 1),$$

o que implica que $k \cdot 1 = 0$ ou $m \cdot 1 = 0$, já que F não tem divisores de zero. Mas, isso contradiz a definição da característica p. □

Corolário 1.1.8. *A característica de um corpo finito é um número primo.*

Demostração. Pelo Teorema 1.1.7, basta mostrar que um corpo finito F tem característica positiva.

Considere os múltiplos $1, 2 \cdot 1, 3 \cdot 1, \ldots$ da unidade do corpo. Como F possui apenas um número finito de elementos distintos, existem inteiros k e m com $1 \leq k < m$ tais que $k \cdot 1 = m \cdot 1$, ou seja, $(m - k) \cdot 1 = 0$. Assim, a característica de F é positiva. Pelo Teorema 1.1.7, conclui-se que a característica é um número primo.

□

Teorema 1.1.9. *Seja* F *um corpo de característica* $p > 0$*. Para todo inteiro positivo* n *e todos* $\alpha, \beta \in F$*, tem-se*

$$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n}.$$

Demostração. Para $n = 1$, temos

$$(\alpha + \beta)^p = \alpha^p + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^{p-i}\beta^i + \beta^p.$$

Veja que para $1 \leq i \leq p-1$, temos

$$\binom{p}{i} = \frac{p!}{(p-i)!i!}.$$

Como p só aparece uma vez na fatoração de $p!$, não aparece na fatoração de $(p-i)!$ e $i!$ e $\binom{p}{i}$ é um inteiro, então $\binom{p}{i}$ é múltiplo de p. Como a característica de F é p, então

$$\binom{p}{i} \alpha^{p-i}\beta^i = 0.$$

Assim, $(\alpha + \beta)^p = \alpha^p + \beta^p$. Observe que, mesmo se $p = 2$, temos $(-\beta)^p = -\beta^p$. Logo, $(\alpha \pm \beta)^p = \alpha^p \pm \beta^p$.

Suponha agora que $(\alpha \pm \beta)^{p^{n-1}} = \alpha^{p^{n-1}} \pm \beta^{p^{n-1}}$. Então,

$$(\alpha \pm \beta)^{p^n} = ((\alpha \pm \beta)^{p^{n-1}})^p = (\alpha^{p^{n-1}} \pm \beta^{p^{n-1}})^p = \alpha^{p^n} \pm \beta^{p^n}.$$

Conclui-se por indução. □

Definição 1.1.10 (Subcorpo)**.** *Seja F um corpo e $K \subseteq F$ tal que K é não vazio. Dizemos que K é um subcorpo de F se ele é fechado sob a adição e multiplicação de F, e se K tem estrutura de corpo. Nesse contexto, dizemos que F é uma extensão de K, ou ainda que $F \mid K$ é uma extensão de corpos. Adicionalmente, se $K \neq F$, dizemos que K é um subcorpo próprio de F.*

Seja p um número primo. O anel de inteiros módulo p é um corpo com p elementos e será denotado por $\mathbb{F}_p$.

Se K é um subcorpo do corpo finito $\mathbb{F}_p$, com p primo, então K deve conter os elementos 0 e 1, e portanto todos os outros elementos de $\mathbb{F}_p$ pelo fechamento de K sob adição. Segue-se que $\mathbb{F}_p$ não contém subcorpos próprios. Somos assim levados ao seguinte conceito.

Definição 1.1.11 (Subcorpo primo)**.** *Seja F um corpo. Um corpo que não contém subcorpos próprios é chamado de corpo primo, em outras palavras, um subcorpo primo do corpo F é o menor subcorpo que ele pode conter.*

Pelo argumento acima, qualquer corpo finito de ordem p, com p primo, é um corpo primo. Outro exemplo de corpo primo é o corpo $\mathbb{Q}$ dos números racionais.

A interseção de qualquer coleção não vazia de subcorpos de um dado corpo F é novamente um subcorpo de F. Se formarmos a interseção de todos os subcorpos de F, obtemos o subcorpo primo de F.

Apresentamos a seguir um lema importante, que será utilizado na demonstração do próximo teorema.

Lema 1.1.12. *Sejam F um corpo e 1_F a unidade de F. Considere o homomorfismo de anéis*

$$\varphi : \mathbb{Z} \to F, \quad \varphi(n) = n \cdot 1_F.$$

Se φ é injetivo, então a característica de F é zero. Nesse caso, a imagem de $\mathbb{Z}$ em F é isomorfa a $\mathbb{Z}$, e o subcorpo primo de F é isomorfo a $\mathbb{Q}$.

Demostração. Suponha que o homomorfismo $\varphi : \mathbb{Z} \to F$, dado por $\varphi(n) = n \cdot 1_F$, seja injetivo. Isso significa que $\ker(\varphi) = \{0\}$, ou seja, não existe inteiro positivo n tal que $n \cdot 1_F = 0$ em F.

Pela definição de característica, concluímos que a característica de F é zero.

Como $\mathbb{Z}$ é um domínio de integridade e φ é um homomorfismo injetivo, sua imagem $\varphi(\mathbb{Z})$ é isomorfa a $\mathbb{Z}$ e constitui um subanel de F. Além disso, como F é um corpo, ele contém os inversos multiplicativos dos elementos não nulos de $\mathbb{Z} \cdot 1_F$.

Logo, podemos considerar frações do tipo

$$\frac{a \cdot 1_F}{b \cdot 1_F}, \quad \text{com } a, b \in \mathbb{Z},\ b \neq 0,$$

as quais pertencem a todo subcorpo de F e formam um subcorpo isomorfo ao corpo de frações de $\mathbb{Z}$, ou seja, $\mathbb{Q}$.

Portanto, o subcorpo primo de F é isomorfo a $\mathbb{Q}$. □

Teorema 1.1.13. *O subcorpo primo de um corpo F é isomorfo a $\mathbb{F}_p$ ou a $\mathbb{Q}$ conforme a característica de F seja um primo p ou 0 (zero), respectivamente.*

Demostração. Como no lema anterior, consideramos o homomorfismo de anéis

$$\varphi : \mathbb{Z} \to F, \quad \varphi(n) = n \cdot 1_F,$$

onde 1_F é a unidade do corpo F. O núcleo de φ é do tipo $p\mathbb{Z}$ para algum inteiro $p \geq 0$.

Se a característica de F é zero, então φ é injetora ($\ker(\varphi) = 0$) e, pelo Lema 1.1.12, o subcorpo primo de F é isomorfo a $\mathbb{Q}$.

Por outro lado, se a característica de F é um número positivo p, então $\ker(\varphi) = p\mathbb{Z}$. Observe que, pelo Corolário 1.1.8, p é um número primo.

Pelo Teorema de Isomorfismo de anéis (ver (Judson, 2009, Theorem 14.11)), temos

$$\mathbb{Z}/p\mathbb{Z} \cong \varphi(\mathbb{Z}) \subseteq F.$$

Como $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ é um corpo, sua imagem também é um subcorpo de F. Assim, o subcorpo primo de F é isomorfo a $\mathbb{F}_p$. □

A partir deste momento, p denotará um número primo e q a potência desse número primo.

Definição 1.1.14. *Seja $F \mid K$ uma extensão de corpos. Se F, considerado como um espaço vetorial sobre K, for de dimensão finita, então dizemos que F é uma extensão finita de K. A dimensão do espaço vetorial F sobre K é chamada de grau da extensão F sobre K, e é denotada por $[F : K]$.*

Lema 1.1.15. *Seja F um corpo finito contendo um subcorpo K com q elementos. Então F tem q^m elementos, onde $m = [F : K]$.*

Demostração. Como F é um espaço vetorial sobre K e F é finito, então ele é de dimensão finita como espaço vetorial sobre K. Se $[F : K] = m$, então F tem uma base sobre K consistindo de m elementos, digamos $b_1, b_2, \ldots, b_m$. Assim, cada elemento de F pode ser representado de forma única como

$$a_1 b_1 + a_2 b_2 + \cdots + a_m b_m,$$

onde $a_1, a_2, \ldots, a_m \in K$. Como cada a_i pode ter q valores, F tem exatamente q^m elementos. □

Teorema 1.1.16. *Seja F um corpo finito. Então F tem p^n elementos, onde p é a característica prima de F e n é o grau de F sobre seu subcorpo primo.*

Demostração. Como F é finito, sua característica é um número primo p, de acordo com o Corolário 1.1.8. Portanto, o subcorpo primo K de F é isomorfo a $\mathbb{F}_p$ pelo Teorema 1.1.13 e, assim, contém p elementos. O restante segue do Lema 1.1.15. □

Definição 1.1.17 (Ordem de um grupo)**.** *Seja $(H, *)$ um grupo. Chamamos de ordem de um grupo ao número de elementos que ele possui, e denotaremos por $|H|$.*

Definição 1.1.18 (Ordem de um elemento)**.** *Seja $(H, *)$ um grupo e $a \in H$. Chamamos de ordem de um elemento de um grupo ao menor exponente do elemento cuja potência nos da o elemento neutro do grupo. Isto é, a ordem de a é o menor inteiro positivo r satisfazendo $a^r = e$.*

Definição 1.1.19. *Sejam n um inteiro e m um inteiro positivo. Se n e m são primos entre si, então a ordem de n módulo m, denotado $\mathrm{Ord}_m(n)$, é o menor inteiro positivo d satisfazendo $n^d \equiv 1 \pmod{m}$.*

Proposição 1.1.20. *Seja F um corpo finito com q elementos. Os elementos não nulos de F formam um grupo de ordem $q-1$ sob a multiplicação.*

Demostração. Consideremos o conjunto $F^* = F \setminus \{0\}$. Como a multiplicação em um corpo é associativa e possui um elemento neutro multiplicativo 1, temos que para todo $a \in F^*$, vale $a \cdot 1 = 1 \cdot a = a$. Além disso, dado qualquer $a \in F^*$, pela Definiçaõ 1.1.3 existe $a^{-1} \in F$ tal que $a \cdot a^{-1} = 1$, e como $a^{-1} \neq 0$, segue que $a^{-1} \neq 0 \in F^*$. Como o produto de dois elementos não nulos em um corpo continua sendo um elemento não nulo, concluímos que F^* é fechado para a multiplicação. Assim, $(F^*, \cdot)$ satisfaz os axiomas de grupo e sua ordem é $|F^*| = q-1$, pois excluímos o elemento zero de F. Portanto, os elementos não nulos de F formam um grupo multiplicativo de ordem $q-1$.

□

Teorema 1.1.21. *Seja F um corpo finito com q elementos. O grupo multiplicativo F^* dos elementos não nulos de F é cíclico.*

Demostração. Podemos assumir que $q \geqslant 3$. 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 F^*.

Para cada i, com $1 \leqslant i \leqslant m$, o polinômio $x^{h/p_i} - 1$ possui no máximo h/p_i raízes em F. Como $h/p_i < h$, segue que existem elementos não nulos em F que **não** são raízes desse polinômio.

Para cada i, seja $a_i \in \mathbb{F}_q^*$ tal que $a_i^{h/p_i} \neq 1$, e definimos:

$$b_i = a_i^{h/p_i^{r_i}}.$$

Temos $b_i^{p_i^{r_i}} = \left(a_i^{h/p_i^{r_i}}\right)^{p_i^{r_i}} = a_i^h = 1$, pois F^* tem ordem h. Logo, a ordem de b_i divide $p_i^{r_i}$ e é, portanto, da forma $p_i^{s_i}$, com $0 \leqslant s_i \leqslant r_i$.

Por outro lado, como

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

então a ordem de b_i é exatamente $p_i^{r_i}$.

Agora definimos o elemento:

$$b = b_1 b_2 \cdots b_m.$$

Afirmamos que a ordem de b é h. Suponha, por absurdo, que a ordem de b seja um divisor próprio de h, e portanto divide algum dos h/p_i. Suponha que divida h/p_1. Então:

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

Veja que para cada $i \geqslant 2$, temos $p_i^{r_i}$ divide h/p_1. Isso implica $b_i^{h/p_1} = 1$. Logo, a equação acima reduz-se a $b_1^{h/p_1} = 1$, o que implicaria que a ordem de b_1 divide h/p_1, contradizendo o fato de que a ordem de b_1 é $p_1^{r_1}$ (veja que $p_1^{r_1} \nmid h/p_1$).

Portanto, a ordem de b é realmente h, e F^* é um grupo cíclico gerado por b. □

Definição 1.1.22. *Seja F um grupo finito. Um gerador $b \in F^*$ do grupo cíclico $F^* = \langle b \rangle$ é chamado de elemento primitivo de F.*

Definição 1.1.23. *Sejam F um corpo finito e $\alpha \in F^*$. A ordem de α no grupo multiplicativo F^* é denotada* $\mathrm{Ord}(\alpha)$.

Lema 1.1.24. *Sejam F um corpo finito, $\alpha \in F^*$ e i um inteiro. Se* $\mathrm{Ord}(\alpha) = n$, *então*

$$\mathrm{Ord}(\alpha^i) = \frac{n}{\mathrm{mdc}(n, i)}.$$

Demostração. Seja $d = \mathrm{mdc}(n, i)$. Então, existem $a, b \in \mathbb{Z}$ tais que $n = da$, $i = db$ e $\mathrm{mdc}(a, b) = 1$. Veja que

$$(\alpha^i)^a = \alpha^{dba} = (\alpha^n)^b = 1^b = 1.$$

Por outro lado, seja m um inteiro satisfazendo $(\alpha^i)^m = 1$. Como $(\alpha^i)^m = \alpha^{im}$ e a ordem de α é n, então $n \mid im$. Daí, $da \mid dbm$, ou seja, $a \mid bm$. Como $\mathrm{mdc}(a, b) = 1$, então $a \mid m$. Isso prova que a ordem α^i é

$$a = \frac{n}{d} = \frac{n}{\mathrm{mdc}(n, i)}.$$

□

Lema 1.1.25. *Seja F um corpo finito com q elementos. Para cada divisor positivo d de $q - 1$ existem exatamente $\varphi(d)$ elementos de F^* de ordem d.*

Demostração. Considere α um elemento primitivo de F. Os elementos de F^* são exatamente os elementos da forma α^i para $0 < i \leq q - 1$. Pelo lema anterior, o elemento α^i é de ordem d se, e somente se,

$$\frac{q-1}{\mathrm{mdc}(q-1, i)} = d.$$

Ou seja, i deve ser um múltiplo de $(q-1)/d$. Escrevendo $i = a(q-1)/d$, temos $0 < a \leq d$ e

$$\mathrm{mdc}(d, a) = \mathrm{mdc}\left(d, \frac{i}{(q-1)/d}\right) = 1.$$

Por definição da função totiente de Euler o qual denotaremos por φ, existem exatamente $\varphi(d)$ inteiros a primos com d satisfazendo $0 < a \leq d$. □

A partir do lema anterior, vemos que o número de elementos primitivos de um corpo finito com q elementos é $\varphi(q - 1)$.

Lema 1.1.26. *Seja F um corpo finito com q elementos. Para todo $\alpha \in F$ tem-se $\alpha^q = \alpha$.*

Demostração. A identidade $\alpha^q = \alpha$ é trivial para $\alpha = 0$. Por outro lado, pela Proposição 1.1.20 os elementos não nulos de F formam um grupo de ordem $q-1$ sob multiplicação. Assim, $\alpha^{q-1} = 1$ para todo $\alpha \in F^*$. Multiplicando a igualdade por α obtemos o resultado desejado. □

Definição 1.1.27. *Seja F um corpo, $F[x]$ o anel de polinômios com coeficientes em F e $f(x) \in F[x]$ um polinômio não constante. Um corpo de decomposição de $f(x)$ sobre F é um corpo K que contém F, no qual f se fatora como*

$$f(x) = a\prod_{i=1}^{m}(x - u_i),$$

com $a \in F^*$ e $K = F[u_1, \ldots, u_m]$.

Lema 1.1.28. *Se F é um corpo finito com q elementos e K é um subcorpo de F, então o polinômio $x^q - x \in K[x]$ se fatora em $F[x]$ como*

$$x^q - x = \prod_{\alpha \in F}(x - \alpha)$$

e F é o corpo de decomposição de $x^q - x$ sobre K.

Demostração. Pelo Lema 1.1.26, todos os elementos de F são raízes do polinômio $x^q - x$. Como esse polinômio é de grau q, então todas as suas raízes são exatamente os elementos de F. Dessa forma, o corpo de decomposição de $x^q - x$ é F e, como os polinômios $x^q - x$ e $\prod_{\alpha \in F}(x - \alpha)$ são mônicos, então eles são iguais. □

Teorema 1.1.29 (Caracterização)**.** *O número de elementos de um corpo finito é uma potência de um número primo. Reciprocamente, para cada potência prima existe um corpo finito cujo número de elementos é exatamente tal potência prima.*

Demostração.
$\Longrightarrow$) Seja F um corpo finito. Pelo Corolário 1.1.8, a característica de F, denotada por p, é um número primo. Assim, pelo Teorema 1.1.13, F contém um subcorpo isomorfo a $\mathbb{F}_p$, o corpo com p elementos.

Como F é um espaço vetorial sobre $\mathbb{F}_p$ e F é um corpo finito, então a dimensão de F sobre $\mathbb{F}_p$ é finita. Seja $n = \dim_{\mathbb{F}_p}(F)$. Cada elemento de F pode ser escrito como uma combinação linear dos n vetores de uma base do espaço vetorial F com coeficientes em $\mathbb{F}_p$. Logo, o número total de elementos de F é dado por $|F| = p^n$. Em outras palavras, o número de elementos de qualquer corpo finito é uma potência de um número primo.

$\Longleftarrow$) Agora, seja $q = p^n$, onde p é um número primo e $n \geq 1$. Precisamos mostrar que existe um corpo finito com q elementos.
Considere $\mathbb{F}_p$, o corpo com p elementos. Seja F o corpo de decomposição de $f(x) = x^q - x \in \mathbb{F}_p[x]$. Como $f'(x) = qx^{q-1} - 1 = -1$, então $f(x)$ e $f'(x)$ não têm raízes em comum. Logo, $f(x) = x^q - x$ tem exatamente q raízes distintas. Considere

$$L = \{\alpha \in F \mid \alpha^q = \alpha\}.$$

Veja que L é subcorpo de F, pois

1. $0, 1 \in L$;

2. se $\alpha, \beta \in L$, então, pelo Teorema 1.1.9,

$$(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta;$$

3. se $\alpha, \beta \in L$, com $\beta \neq 0$, então

$$(\alpha\beta^{-1})^p = \alpha^p(\beta^p)^{-1} = \alpha\beta^{-1}.$$

Pelo Lema 1.1.28, L é o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Logo, $L = F$ e F é um corpo com q elementos. □

Teorema 1.1.30. *Sejam p um número primo e n um inteiro positivo. Todos os corpos com $q = p^n$ são isomorfos ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Tal corpo será denotado por $\mathbb{F}_q$.*

Demostração. Seja F um corpo com q elementos. Pelo Teorema 1.1.16, F é um corpo de característica p e, portanto, contem $\mathbb{F}_p$ como subcorpo. Pelo Lema 1.1.28, F é um corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Pelo (Rudolf Lidl, 2003, Theorem 1.91), o corpo F é único a menos de isomorfismo. □

A seguir, apresentamos alguns conceitos extraídos do livro de (Bondy & Murty, 1982), os quais foram fundamentais para o desenvolvimento das definições que se encontram abaixo.

1.2 Grafos

Definição 1.2.1 (Grafo). *Um grafo* G *é uma tripla ordenada* $(V(\mathrm{G}), E(\mathrm{G}), \psi_{\mathrm{G}})$ *consistindo de um conjunto não vazio de vértices* $V(\mathrm{G})$*, um conjunto* $E(\mathrm{G})$*, disjunto de* $V(\mathrm{G})$*, de arestas, e uma função de incidência* ψ_{G} *que associado a cada aresta de* G *um par não ordenado de (não necessariamente distintos) vértices de* G*. Se* e *é uma aresta e* u *e* v *são vértices tais que* $\psi_{\mathrm{G}}(e) = [uv]$*, diz-se que* e *une* u *e* v*; os vértices* u *e* v *são chamados de extremidades de* e*.*

Definição 1.2.2 (Laço e elo). *Uma aresta cujos extremos são idênticos é chamada de laço, e uma aresta com extremos distintos é chamada de elo (ou ligação ou aresta).*

Definição 1.2.3 (Grafo Simples). *Um grafo é dito simples quando não possui laços e nem arestas múltiplas, ou seja, nenhuma de suas arestas conecta o mesmo par de vértices mais de uma vez. Em outro caso, o grafo é dito não simples.*

Definição 1.2.4 (Grafo Dirigido). *Um grafo dirigido* D *é uma tripla ordenada* $(V(\mathrm{D}), E(\mathrm{D}), \psi_{\mathrm{D}})$ *consistindo de um conjunto não vazio de vértices* $V(\mathrm{D})$*, um conjunto* $E(\mathrm{D})$*, disjunto de* $V(\mathrm{D})$*, de arcos, e uma função de incidência* ψ_{D} *que associado a cada aresta de* D *um par ordenado de (não necessariamente distintos) vértices de* D*.*

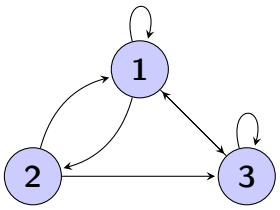


Figura 1.1: Exemplo de grafo dirigido.

Definição 1.2.5 (Passeio). *Um passeio em um grafo* G *é uma sequência finita não nula* $W = v_0e_1v_1e_2v_2\ldots e_{\mathrm{k}}v_{\mathrm{k}}$*, cujos termos são alternadamente vértices e arestas, de modo que, para* $1 \leq i \leq k$*, as extremidades de* e_i *são* $v_{\mathrm{i}-1}$ *e* v_{i}*.*

Exemplo 1.2.6. *Seja*

$$H = (V(H), E(H), \psi_{\mathrm{H}})$$

sendo

$$V(H) = \{u, v, w, x, y\},$$
$$E(H) = \{a, b, c, d, e, f, g, h\}$$

e ψ_{H} *definido por*

$$\psi_{\mathrm{H}}(a) = uv, \quad \psi_{\mathrm{H}}(b) = uu, \quad \psi_{\mathrm{H}}(c) = vw, \quad \psi_{\mathrm{H}}(d) = wx,$$
$$\psi_{\mathrm{H}}(e) = vx, \quad \psi_{\mathrm{H}}(f) = wx, \quad \psi_{\mathrm{H}}(g) = ux, \quad \psi_{\mathrm{H}}(h) = xy.$$

A representação gráfica do grafo H *é apresentada a seguir (ver Figura 1.2).*

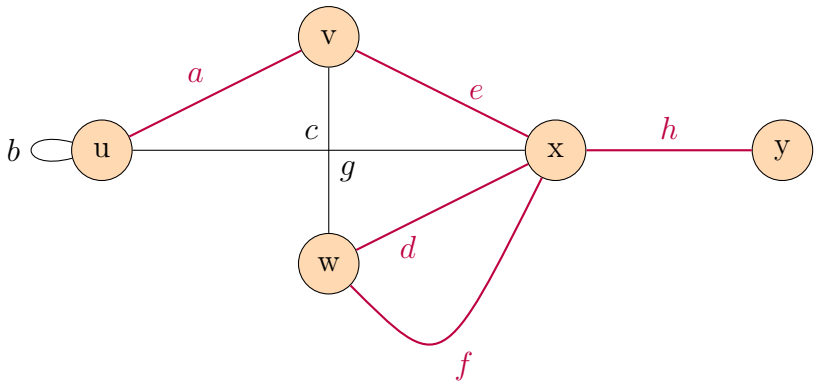


Figura 1.2: Passeio: $W = uavexhyhxfwdx$ do grafo H.

Definição 1.2.7 (Caminho)**.** *Um caminho* R *em um grafo* G*, é um passeio cujas arestas são distintas (uma trilha) e além disso, seus vértices são distintos.*

Exemplo 1.2.8. *Seguindo o grafo do Exemplo 1.2.6, podemos visualizar que o passeio de vértices e arestas dado por* $uavexhy$ *representa um caminho. A esse passeio chamaremos de* R*. (ver Figura 1.3).*

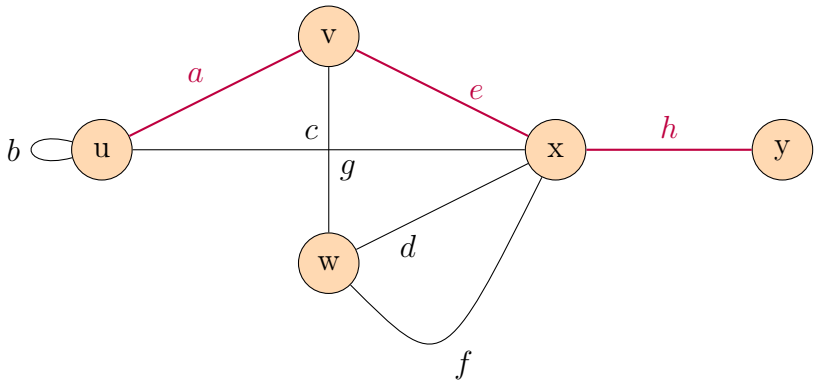


Figura 1.3: Um caminho no grafo H: $R = u \leftrightarrow v \leftrightarrow x \leftrightarrow y$.

Definição 1.2.9 (Caminho fechado)**.** *Um caminho é considerado fechado se possui comprimento positivo e sua origem coincide com o seu término.*

Exemplo 1.2.10. *Seguindo o grafo do Exemplo 1.2.6, observamos que ele possui pelo menos um caminho fechado, cuja sequência de vértices e arestas é dada por* $S = vexfwcv$. *A representação desse caminho fechado é apresentada a seguir (ver Figura 1.4).*

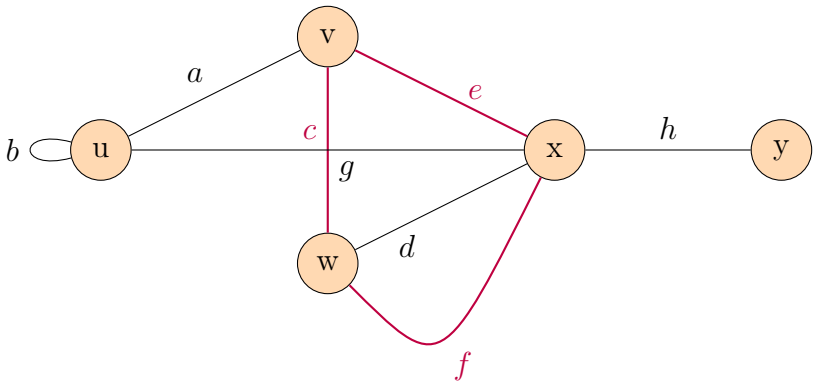


Figura 1.4: Caminho fechado: $S = v \leftrightarrow x \leftrightarrow w \leftrightarrow v$.

Definição 1.2.11 (Grafo conexo)**.** *Dois vértices* u *e* v *de um grafo* G *dizem-se conexos se existe um caminho de* u *até* v *em* G. *A conexidade é uma relação de equivalência no conjunto de vértices* V. *Assim, há uma partição de* V *em subconjuntos não vazios* $V_1, V_2, \ldots, V_a$, *tal que dois vértices* u *e* v *estão conectados se, e somente se, ambos pertencem ao mesmo conjunto* V_i. *Os subgrafos* $G[V_1], G[V_2], \ldots, G[V_a]$ *são chamados de componentes de* G. *Se* G *possui exatamente uma componente, dizemos que* G *é conexo; caso contrário,* G *é desconexo. Denotamos o número de componentes de* G *por* $\omega(G)$.

Exemplo 1.2.12. *A seguir, apresentamos um exemplo de grafo conexo (ver Figura 1.5).*

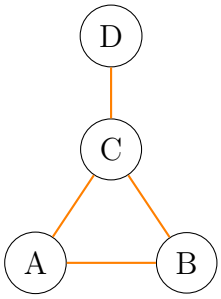


Figura 1.5: Grafo conexo N.

Exemplo 1.2.13. *Vejamos um exemplo de grafo desconexo (ver Figura 1.6).*

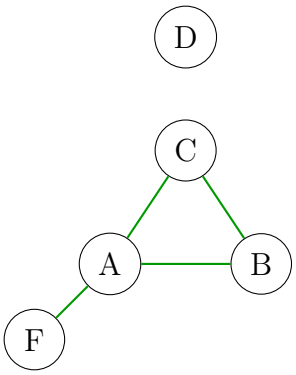


Figura 1.6: Grafo desconexo $\hat{N}$.

Definição 1.2.14 (Ciclo)**.** *Um ciclo é um caminho fechado de comprimento positivo, na qual todos os vértices (exceto o inicial/final) são distintos.*

Exemplo 1.2.15. *A seguir, vejamos um exemplo de grafo com ciclo. Denotemo-lo por L (ver Figura 1.7).*

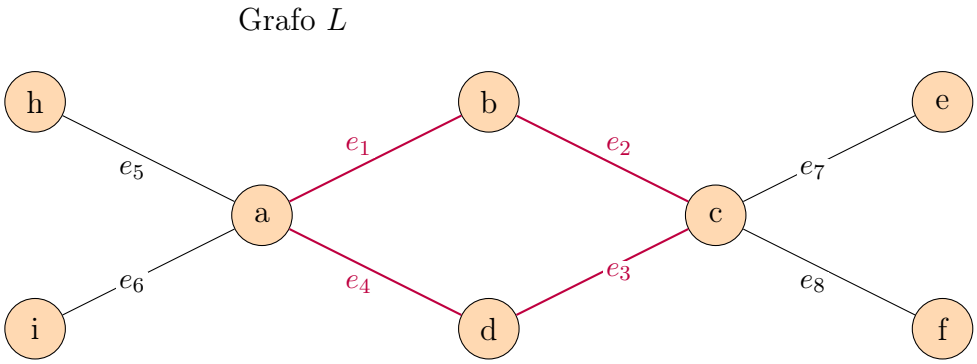


Figura 1.7: Ciclo $\mathcal{C} = ae_1be_2ce_3de_4a$ no grafo L.

Definição 1.2.16 (Grafo acíclico)**.** *Um grafo acíclico é aquele que não contém ciclos.*

Exemplo 1.2.17. *A seguir, apresentaremos o grafo acíclico M (ver Figura 1.8).*

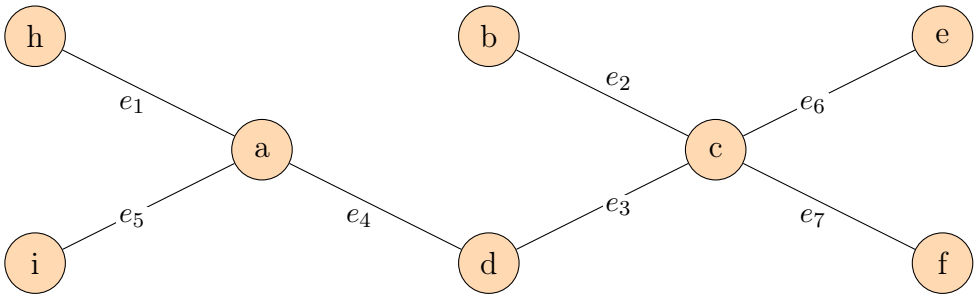


Figura 1.8: Grafo acíclico M.

Definição 1.2.18 (Árvores)**.** *Uma árvore é um grafo acíclico conexo.*

Exemplo 1.2.19. *Considere-se a árvore seguinte, denotado por J (ver Figura 1.9).*

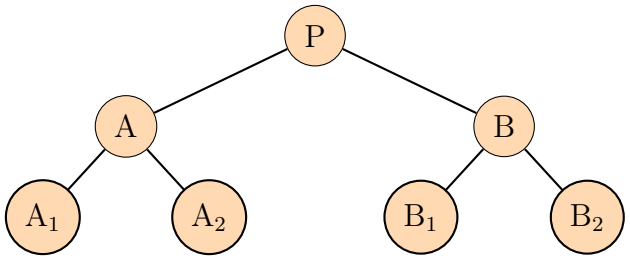


Figura 1.9: Árvore J.

Definição 1.2.20 (Árvore dirigida)**.** *Uma árvore dirigida é um grafo acíclico conexo dirigido, é dizer, um tipo de grafo dirigido sem ciclos e conexo.*

Exemplo 1.2.21. *A seguir, apresenta-se uma árvore dirigida; denotemos essa árvore por F (ver Figura 1.10).*

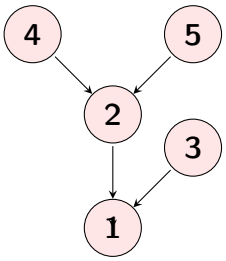


Figura 1.10: Árvore dirigida F.

Definição 1.2.22. *Dois grafos* G *e* H *são idênticos* ($\mathrm{G} = \mathrm{H}$) *se* $V(\mathrm{G}) = V(\mathrm{H})$, $E(\mathrm{G}) = E(\mathrm{H})$, *e* $\psi_{\mathrm{G}} = \psi_{\mathrm{H}}$.

Definição 1.2.23 (Isomorfismo de Grafos)**.** *Dois grafos* G *e* H *são ditos isomorfos e escrevemos* ($\mathrm{G} \cong \mathrm{H}$) *se houver bijeções* $\theta : V(\mathrm{G}) \to V(\mathrm{H})$ *e* $\phi : E(\mathrm{G}) \to E(\mathrm{H})$ *tais que* $\psi_{\mathrm{G}}(e) = [uv]$ *se, e somente se,* $\psi_{\mathrm{H}}(\phi(e)) = [\theta(u)\theta(v)]$*; tal par* (θ, ϕ) *de mapeamentos é chamado um isomorfismo entre* G *e* H.

Exemplo 1.2.24. *A seguir, temos dois grafos que são isomorfos. No grafo* G *(à esquerda), os vértices são rotulados como* u, w, x, y, z *e no grafo* H *(à direita), não há rótulos explícitos, mas podemos definir a bijeção:*

$$\theta : \{u \mapsto C, w \mapsto B, x \mapsto A, y \mapsto D, z \mapsto E\}$$

e a bijeção correspondente entre as arestas:

$$\phi : \{a \mapsto a', b \mapsto b', c \mapsto c', d \mapsto d', e \mapsto e', f \mapsto f', g \mapsto g'\}$$

de forma que as conexões (incidências) são preservadas.

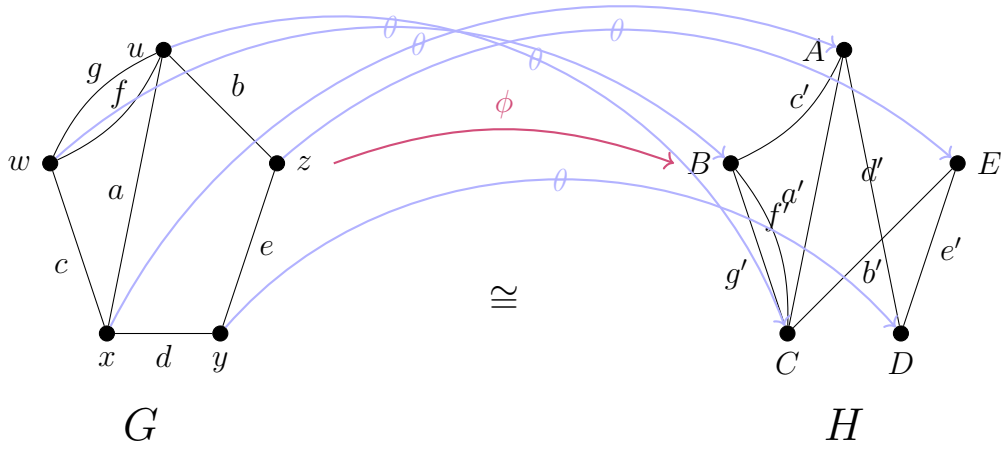


Figura 1.11: Grafos isomorfos G e H.

As estruturas são preservadas: as conexões entre vértices, o número de vértices e arestas, e o grau de cada vértice. Portanto, $G \cong H$.

Definição 1.2.25. *Para* m *e* n*, números inteiros positivos, sejam:*

a) $Cyc(n)$ *o grafo cíclico direcionado de comprimento* n*;*

b) $\mathcal{T}(1)$ *a árvore composta por dois pontos,* P_1 *e* P*, onde* P_1 *é direcionado a* P*. Para* $m \geq 1$*,* $\mathcal{T}(m+1)$ *é a árvore obtida após anexar 2 pontos direcionados a cada ponto no último nível de* $\mathcal{T}(m)$*;*

c) $(Cyc(n), \mathcal{T}(m))$ *o grafo obtido após substituir cada ponto de* $Cyc(n)$ *por uma árvore isomorfa a* $\mathcal{T}(m)$*;*

d) $\mathcal{Z}(q)$ *o grafo obtido ao anexar* $\frac{q-1}{2}$ *árvores disjuntas isomorfas a* $\mathcal{T}(1)$ *e* $\frac{q-1}{2}$ *árvores disjuntas isomórficas a* $\mathcal{T}(2)$ *a* $Cyc(1)$*.*

Exemplo 1.2.26. *Para* $m = 1$ *obtemos o grafo* $\mathcal{T}(1)$*(ver Figura 1.12):*

Figura 1.12: Grafo $\mathcal{T}(1)$.

Para $m = 2$ *obtemos o grafo* $\mathcal{T}(2)$*(ver Figura 1.13):*

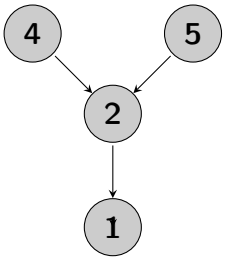


Figura 1.13: Grafo $\mathcal{T}(2)$.

Exemplo 1.2.27. *Para* $n = 2$ *e* $m = 1$*(ver Figura 1.14):*

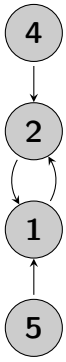


Figura 1.14: Grafo $Cyc(2), \mathcal{T}(1)$.

Exemplo 1.2.28. *Para* $q = 7$ *apresentamos o grafo* $\mathcal{Z}^(7)$ *(ver Figura 1.15):*

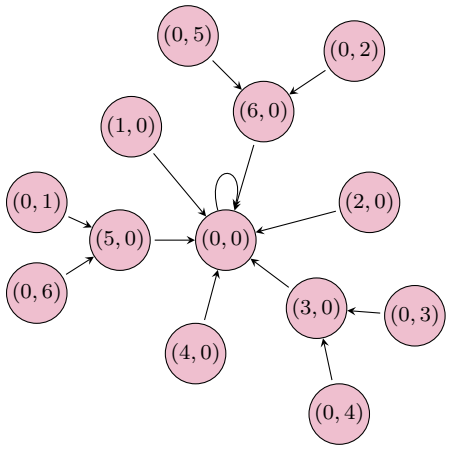


Figura 1.15: Grafo $\mathcal{Z}(7)$.

Definição 1.2.29. *Definimos $\mathcal{Z}^*(q)$ como o grafo direcionado $Cyc(1)$ com $q-1$ árvores isomorfas a $\mathcal{T}(1)$ conectadas a ele.*

Exemplo 1.2.30. *Para $q = 7$, apresentamos a grafo $\mathcal{Z}^*(7)$ (ver Figura 1.16):*

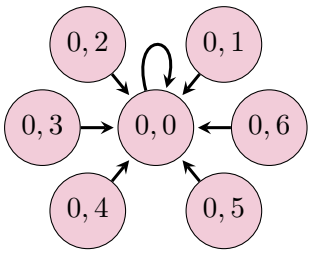


Figura 1.16: Grafo $\mathcal{Z}^*(7)$.

Nos grafos que iremos estudar a função de incidência ψ_G é uma função injetora. Isto é, para cada par de vértices $a, b \in V$ existe no máximo uma aresta dirigida de a em b. Essa aresta dirigida, se existir, será denotada por $\langle a, b\rangle$. Dessa forma, o conjunto de arestas E é um subconjunto de $V \times V$.

1.3 Grafo Funcional

Definição 1.3.1. *Seja $\mathcal{V}$ um conjunto e $f : \mathcal{V} \longrightarrow \mathcal{V}$ uma função. O grafo funcional de f é o grafo dirigido $\mathcal{G}(f) = (\mathcal{V}, \mathcal{E})$, onde $\mathcal{E} = \{\langle x, f(x)\rangle \mid x \in \mathcal{V}\}$.*

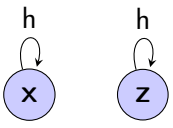
Alguns exemplos de grafos funcionais		
1	Descrição	Grafo
Grafo funcional da função identidade $h : X \longrightarrow X$.		 Figura 1.17: Grafo da função identidade.

Tabela 1.1: Exemplo 1 – Função identidade.

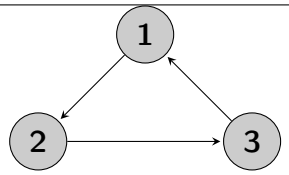
Alguns exemplos de grafos funcionais		
2	Descrição	Grafo
Grafo com ciclo representando uma função periódica (forma triangular).		 Figura 1.18: Grafo de uma função periódica.

Tabela 1.2: Exemplo 2 – Função periódica.

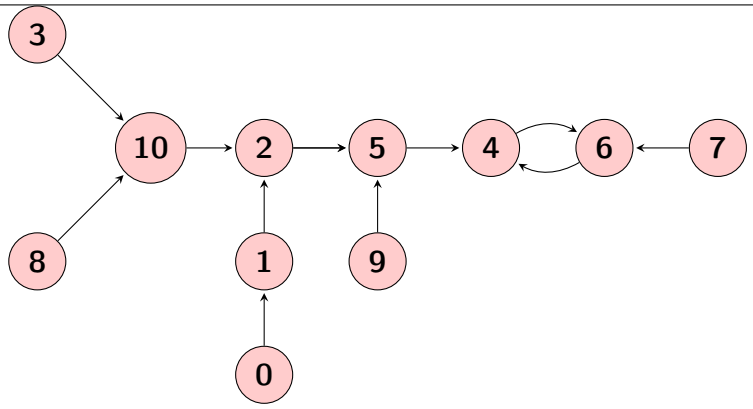
Alguns exemplos de grafos funcionais		
3	Descrição	Grafo
Grafo funcional de $f_c(x) = x^2 + c$, com $c \in \mathbb{F}_q^*$, em que q é um primo ímpar. Ver (Peinado, 2001).		 Figura 1.19: Grafo funcional $f_1(x) = x^2 + 1$ definido sobre $\mathbb{F}_{11}$ com $c = 1 \in \mathbb{F}_{11}^*$.

Tabela 1.3: Exemplo de grafo funcional de uma função do tipo $x^2 + c$ sobre $\mathbb{F}_q$.

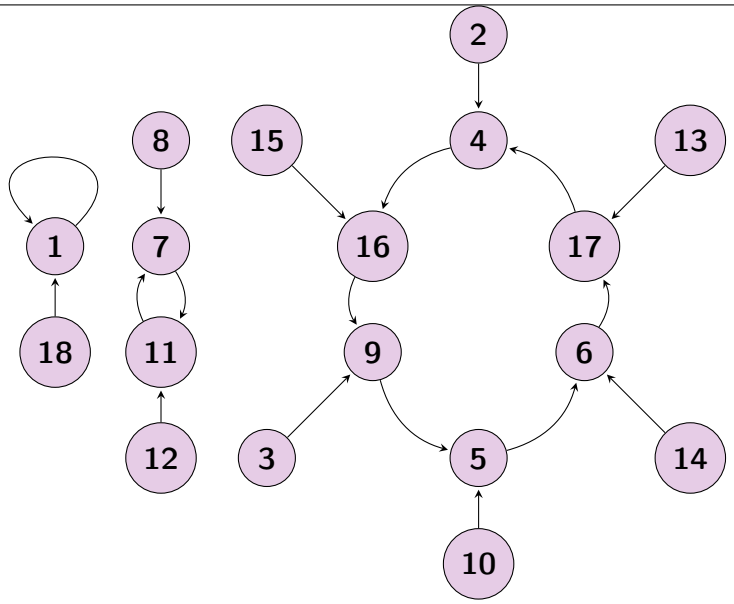
Alguns exemplos de grafos funcionais		
4	Descrição	Grafo
O grafo denotado por G_p para primos $p \geq 3$ relativo à função $f : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$ definida por $f(x) = x^2$. Ver (Rogers, 1996).		 Figura 1.20: Grafo funcional G_{19}.

Tabela 1.4: Exemplo de grafo funcional da função $f(x) = x^2$ sobre $\mathbb{F}_p^*$.

Definição 1.3.2. *(Pontos fixos) Um ponto $\alpha \in \mathcal{V}$ é um ponto fixo de f se $f(\alpha) = \alpha$.*

Definição 1.3.3. *Dado $\alpha \in \mathcal{V}$, definimos as iteradas de α por recorrência:*

$$f^{(1)}(\alpha) = f(\alpha) \quad e \quad f^{(n)}(\alpha) = f^{(n-1)}(f(\alpha)) \text{, para } n \geq 2.$$

Definição 1.3.4 (Pontos periódicos)**.** *Um ponto $\alpha \in \mathcal{V}$ é chamado de ponto periódico do grafo funcional $\mathcal{G}(f)$ se existe um inteiro positivo $i > 0$ tal que $f^{(i)}(\alpha) = \alpha$. Em outras palavras, α é periódico se pertence a um ciclo do grafo $\mathcal{G}(f)$.*

Definição 1.3.5. *Se $\mathcal{V}$ é um corpo finito, define-se $Cyc(\mathcal{G}(f)) = (\mathcal{V}_1, \mathcal{E}_1)$ o subgrafo de $\mathcal{G}(f)$ cujos vértices são os vértices periódicos de $\mathcal{G}(f)$ que não pertencem à componente conexa de zero e $\mathcal{E}_1 = \{\langle x, f(x)\rangle \mid x \in \mathcal{V}_1\}$.*

1.4 Conceitos Complementares

Definição 1.4.1. *(Caráter) Seja G um grupo abeliano finito. Um caráter é um homomorfismo de G em U, sendo U o grupo multiplicativo dos números complexos de valor absoluto 1, isto é, um caráter*

$$\chi : G \longrightarrow U$$

é uma função tal que para todos $g, h \in G$ tem-se

$$\chi(gh) = \chi(g)\chi(h).$$

Definição 1.4.2. *Um caráter multiplicativo sobre $\mathbb{F}_q$ é um caráter do grupo multiplicativo $\mathbb{F}_q^*$ em U. Se $\chi : \mathbb{F}_q^* \longrightarrow U$ é o caráter definido por $\chi(a) = 1$, para todo $a \in \mathbb{F}_q^*$, então definimos $\chi(0) = 1$. Caso contrário, definimos $\chi(0) = 0$.*

Definição 1.4.3. *Seja $\alpha \in \mathbb{F}_q$. Dizemos que α é um quadrado em $\mathbb{F}_q$ se existe $\beta \in \mathbb{F}_q$ tal que $\beta^2 = \alpha$.*

Definição 1.4.4. *Seja q a potência de um primo ímpar p. Para todo $\alpha \in \mathbb{F}_q$, seja χ_2 o* ***caráter quadrático*** *sobre $\mathbb{F}_q$ definido como*

$$\chi_2(\alpha) = \begin{cases} 1 & \text{se } \alpha \text{ for um quadrado em } \mathbb{F}_q, \\ -1 & \text{se } \alpha \text{ não for um quadrado em } \mathbb{F}_q, \\ 0 & \text{se } \alpha = 0. \end{cases}$$

De agora em diante, q será sempre a potência de um primo ímpar p.

Proposição 1.4.5. *A função χ_2 é um caráter multiplicativo sobre $\mathbb{F}_q$.*

Demostração . Sejam $a, b \in \mathbb{F}_q$. Caso $a = 0$ ou $b = 0$, então $\chi_2(ab) = 0$ e $\chi_2(ab) = \chi_2(a)\chi_2(b)$. Considere α um elemento primitivo em $\mathbb{F}_q$ e suponha $a \neq 0$ e $b \neq 0$. Nesse caso, existem $0 \leq i, j < q-1$ tais que $a = \alpha^i$ e $b = \alpha^j$. Veja que a é um quadrado se existe $c \in \mathbb{F}_q^*$ tal que $c^2 = a$. Como c também é da forma $c = \alpha^k$, então

$$2k \equiv i \pmod{q-1}.$$

Como q é ímpar, então a é um quadrado se, e somente se, i é par. O mesmo raciocínio vale para b e ab. Isto é,

$$\chi_2(a) = (-1)^i, \quad \chi_2(b) = (-1)^j \quad \text{e} \quad \chi_2(ab) = (-1)^{i+j}.$$

Isso implica

$$\chi_2(ab) = (-1)^{i+j} = (-1)^i(-1)^j = \chi_2(a)\chi_2(b).$$

□

Proposição 1.4.6. *As seguintes propriedades são válidas:*

a) Caráter quadrático do inverso:

$$\chi_2(a^{-1}) = \chi_2(a), \quad \forall a \in \mathbb{F}_q^*.$$

b) Caráter quadrático de -1:

$$\chi_2(-1) = \begin{cases} 1 & \text{se } q \equiv 1 \pmod 4, \\ -1 & \text{se } q \equiv 3 \pmod 4. \end{cases}$$

c) Distribuição dos valores de χ no grupo multiplicativo $\mathbb{F}_q^*$:

$$\#\{a \in \mathbb{F}_q^* : \chi(a) = 1\} = \frac{q-1}{2}, \quad \#\{a \in \mathbb{F}_q^* : \chi(a) = -1\} = \frac{q-1}{2}.$$

d) Propriedade de simetria:

$$\chi(-a) = \chi(a) \cdot \chi(-1), \quad \forall a \in \mathbb{F}_q^*.$$

Demostração.

a) Seja $a \in \mathbb{F}_q^*$. Como χ_2 é um caráter multiplicativo, então

$$1 = \chi_2(1) = \chi_2(aa^{-1}) = \chi_2(a)\chi_2(a^{-1}).$$

Logo, $\chi_2(a^{-1}) = \chi_2(a)^{-1}$.

b) Considere $\alpha \in \mathbb{F}_q^*$ um elemento primitivo. Como $\mathbb{F}_q^*$ é um grupo cíclico de ordem $q-1$, então $\alpha^{q-1} = 1$ e $\alpha^i \neq 1$ para todo $1 \leq i \leq q-2$. Observe que

$$0 = \alpha^{q-1} - 1 = (\alpha^{\frac{q-1}{2}} - 1)(\alpha^{\frac{q-1}{2}} + 1).$$

Como $\alpha^{\frac{q-1}{2}} \neq 1$, então

$$\alpha^{\frac{q-1}{2}} = -1.$$

Usando as ideias da prova da Proposição 1.4.5, temos

$$\chi_2(-1) = (-1)^{\frac{q-1}{2}}.$$

Observe que a paridade de $\frac{q-1}{2}$ depende do valor de q módulo 4:

- Se $q \equiv 1 \pmod 4$, então $q-1$ é múltiplo de 4, e $\frac{q-1}{2}$ é par, logo:

$$(-1)^{\frac{q-1}{2}} = 1.$$

- Se $q \equiv 3 \pmod 4$, então $q-1$ é da forma $4s+2$, e $\frac{q-1}{2}$ é ímpar, logo:

$$(-1)^{\frac{q-1}{2}} = -1.$$

Portanto, concluímos que:

$$(-1)^{\frac{q-1}{2}} = \begin{cases} 1, & \text{se } q \equiv 1 \pmod 4, \\ -1, & \text{se } q \equiv 3 \pmod 4. \end{cases}$$

c) Se α é um elemento primitivo de $\mathbb{F}_q$, então

$$\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}.$$

Como vimos na Proposição 1.4.5, os elementos $a = \alpha^i$ são quadrados se, e somente se, i é par. Logo, a metade dos $q-1$ elementos $a \in \mathbb{F}_q^*$ satisfazem $\chi_2(a) = 1$ e a outra metade satisfazem $\chi_2(a) = -1$.

d) Segue da Definição 1.4.1 $\chi_2(-a) = \chi_2((-1)\cdot a) = \chi_2(a)\cdot\chi_2(-1)$, para todo $a \in \mathbb{F}_q^*$.

□

Lema 1.4.7. *Seja $b \in \mathbb{F}_q$. Temos*

$$b^{\frac{q-1}{2}} = 1 \iff \chi_2(b) = 1.$$

Demostração. Se $\chi_2(b) = 1$, então existe $a \in \mathbb{F}_q^*$ tal que $b = a^2$. Daí

$$b^{\frac{q-1}{2}} = (a^2)^{\frac{q-1}{2}} = a^{q-1} = 1.$$

Reciprocamente, suponha $b^{\frac{q-1}{2}} = 1$. Considere $\alpha \in \mathbb{F}_q^*$ um elemento primitivo. Nesse caso, existe $0 \leq i \leq q-2$ tal que $b = \alpha^i$. Como $b^{\frac{q-1}{2}} = 1$, então

$$\alpha^{i\frac{q-1}{2}} = 1.$$

Isso implica que $q-1$ divide $\frac{i(q-1)}{2}$. Em outras palavras, existe um inteiro j tal que

$$\frac{i(q-1)}{2} = j(q-1).$$

Assim, $i = 2j$ e $\chi_2(b) = 1$. □

Definição 1.4.8 (Raiz primitiva)**.** *Seja K um corpo e m um inteiro positivo. Um elemento $\zeta \in K$ é uma raiz m-ésima primitiva da unidade se $\zeta^m = 1$ e $\zeta^k \neq 1$ para todo $1 \leq k < m$.*

Lema 1.4.9. *Seja m um inteiro positivo. Uma raiz m-ésima primitiva da unidade pertence a $\mathbb{F}_q$ se, e somente se, $q \equiv 1 \pmod{m}$.*

Demostração. Seja α um elemento primitivo em $\mathbb{F}_q$. O elemento α^j, para algum $0 \leq j \leq q-2$, é uma raiz m-ésima primitiva da unidade se, e somente se, $\mathrm{Ord}(\alpha^j) = m$. Pelo Lema 1.1.24,

$$\mathrm{Ord}(\alpha^j) = \frac{q-1}{\mathrm{mdc}(q-1, j)}.$$

Logo, se $m|q-1$, escolhemos $j = \frac{q-1}{m}$. Reciprocamente, se $\mathrm{Ord}(\alpha^j) = m$, então $m|q-1$. □

Proposição 1.4.10. *Sejam K um corpo, m um inteiro positivo par e $\zeta \in K$ uma raiz m-ésima primitiva da unidade. Então, ζ^2 é uma raiz $\frac{m}{2}$-ésima primitiva da unidade.*

Demostração. Veja que

$$(\zeta^2)^{\frac{m}{2}} = \zeta^m = 1.$$

Por outro lado, para $1 \leq j < \frac{m}{2}$, temos $2 \leq 2j < m$. Logo,

$$(\zeta^2)^j = \zeta^{2j} \neq 1.$$

Em outras palavras, ζ^2 é uma raiz $\frac{m}{2}$-ésima primitiva da unidade. □

Definição 1.4.11. *Dado um inteiro positivo d e um inteiro n primo com d, o número $\mathrm{Ord}_d(n)$ é o menor inteiro positivo j satisfazendo $n^j \equiv 1 \pmod{d}$.*

Capítulo 2

O grafo funcional de $f(X) = c\left(X^{q+1} - X^2\right)$

Como mencionado na introdução, este capítulo é dedicado à análise do grafo funcional da função $f(X) = c(X^{q+1} + aX^2)$ sobre $\mathbb{F}_{q^2}$, com $a, c \in \mathbb{F}_q^*$, a partir dos resultados obtidos em (Brochero Martínez & Teixeira, 2023). Focaremos especificamente no caso $a = -1$.

2.1 Determinação dos pontos fixos da função $f(X)$

Antes de começar encontrando os pontos fixos de $f(X) = c\,(X^{q+1} - X^2)$, vamos reescrevê-la em função das coordenadas de uma base de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$.

Proposição 2.1.1. *Seja $\{1, \beta\}$ uma base de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$ tal que $\beta^2 = b \in \mathbb{F}_q^*$. Então, para todos $x, y \in \mathbb{F}_q$, temos*

$$f(x + y\beta) = -2bcy^2 - 2cxy\beta.$$

Demonstração. Como $\{1, \beta\}$ é uma base de $\mathbb{F}_{q^2}$, então $\beta \notin \mathbb{F}_q$ e β, β^q são raízes de $x^2 - b \in \mathbb{F}_q[x]$. Logo,

$$\beta^q = -\beta \quad \text{e} \quad \beta^{q+1} = -b = -\beta^2.$$

Dessa forma, para $\alpha = x + y\beta \in \mathbb{F}_{q^2}$, com $x, y \in \mathbb{F}_q$, temos

$$\begin{aligned} f(\alpha) &= c(\alpha^{q+1} - \alpha^2) = c\alpha(\alpha^q - \alpha) = c(x + y\beta)(x + y\beta^q - x - y\beta) \\ &= c(x + y\beta)(-2y\beta) = -2bcy^2 - 2cxy\beta. \end{aligned}$$

□

Fixando um elemento c em $\mathbb{F}_q^*$, vamos determinar os pontos fixos de $f(X) = c\,(X^{q+1} - X^2)$.

Lema 2.1.2. *O único ponto fixo de $f(X) = c\,(X^{q+1} - X^2)$ em $\mathbb{F}_{q^2}$ é $\alpha = 0$.*

Demostração. Seja $\alpha \in \mathbb{F}_{q^2}$. Observe que

$$f(\alpha) = c\alpha\,(\alpha^q - \alpha) = \alpha \quad \text{se, e somente se,} \quad \alpha = 0 \text{ ou } c\,(\alpha^q - \alpha) = 1. \tag{2.1}$$

Logo, $\alpha = 0$ é um ponto fixo de $f(X)$.

Seja $\alpha \in \mathbb{F}_{q^2}^*$ tal que $c\,(\alpha^q - \alpha) = 1$. Nesse caso,

$$\alpha^q = \alpha + c^{-1}.$$

Considerando que $\alpha^{q^2} = \alpha$, temos

$$\alpha = \alpha^{q^2} = (\alpha^q)^q = (\alpha + c^{-1})^q = \alpha^q + c^{-1} = \alpha + 2c^{-1}.$$

Como $\mathbb{F}_{q^2}$ é um corpo de característica ímpar, então $2c^{-1} \neq 0$, o que contradiz $c\,(\alpha^q - \alpha) = 1$. Dessa forma, $\alpha = 0$ é o único ponto fixo de $f(X)$. □

O lema anterior nos diz que o grafo funcional de f possui apenas um ciclo de comprimento 1 (um único laço).

2.2 Análise das pré-imagens de $f(X)$

Definição 2.2.1. *Para cada elemento $\alpha \in \mathbb{F}_{q^2}$, definimos $f^{-1}(\alpha) = \{\gamma \in \mathbb{F}_{q^2} \mid f(\gamma) = \alpha\}$. Chamamos esse conjunto de pré-imagem de α.*

Suponha que $\alpha \in \mathbb{F}_{q^2}^*$ e seja $\{1, \beta\}$ uma base de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$ tal que $\beta^2 = b \in \mathbb{F}_q^*$. De acordo com a Proposição 2.1.1, $X = x + y\beta \in f^{-1}(\alpha)$, com $x, y \in \mathbb{F}_q$, se, e somente se,

$$\alpha = -2cxy\beta - 2bcy^2 \tag{2.2}$$

Antes de prosseguir, b não é um quadrado em $\mathbb{F}_q$, pois se fosse teríamos $\beta^2 = b = g^2$ com $g \in \mathbb{F}_q$ e isso implicaria em $\beta = \pm g$, ou seja, $\beta \in \mathbb{F}_q$.

A partir de agora, fixamos $\beta \in \mathbb{F}_{q^2}$ e $b = \beta^2 \in \mathbb{F}_q$, de forma que $\{1, \beta\}$ seja uma base de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$. Assim, pelo lema anterior, $\chi_2(b) = -1$ e da Proposição 2.1.1,

$$f(x + y\beta) = -2bcy^2 - 2cxy\beta.$$

Identificando os elementos $x + y\beta \in \mathbb{F}_{q^2}$ com os pares $\langle x, y\rangle \in \mathbb{F}_q^2$, podemos reescrever a função $f(X)$ como

$$f(x, y) = \langle -2bcy^2, -2cxy\rangle.$$

Teorema 2.2.2. *Seja $\alpha \in \mathbb{F}_q$. Então,*

1. $$\#f^{-1}(\alpha) = \begin{cases} 2 & \text{se } \chi_2(-2\alpha c) = -1, \\ 0 & \text{se } \chi_2(-2\alpha c) = 1, \\ q & \text{se } \alpha = 0. \end{cases} \tag{2.3}$$

2. *Se $\alpha \neq 0$ e $\gamma \in f^{-1}(\alpha)$, então temos $f^{-1}(\gamma) = \emptyset$ e $\gamma = k\beta$ para algum $k \in \mathbb{F}_q^*$. Reciprocamente, se tivermos $\gamma = k\beta$ para algum $k \in \mathbb{F}_q$, então $f(\gamma) \in \mathbb{F}_q$.*

Demostração.

1. Seja $\gamma \in \mathbb{F}_{q^2}$. Temos $\gamma \in f^{-1}(0)$ se, e somente se, $0 = c(\gamma^{q+1} - \gamma^2) = c\gamma(\gamma^q - \gamma)$. Dos Lemas 1.1.26 e 1.1.28, $\gamma \in f^{-1}(0)$ se, e somente se, $\gamma \in \mathbb{F}_q$. Portanto, $\#f^{-1}(0) = q$.

   Da Equação (2.2), se $\alpha \in \mathbb{F}_q^*$ e $\gamma = x + y\beta \in f^{-1}(\alpha)$, então $-2cxy = 0$ e $-2bcy^2 = \alpha$. O que implica que $x = 0$ e $y^2 = -\frac{\alpha}{2bc}$. Como $\chi_2(b) = -1$, temos que se $\chi_2(-2\alpha c) = 1$, então $f^{-1}(\alpha)$ é vazio, isto é, $\#f^{-1}(\alpha) = 0$. Por outro lado, se $\chi_2(-2\alpha c) = -1$, então $f^{-1}(\alpha) = \{\pm k\beta\}$, onde $k^2 = -\frac{\alpha}{2bc}$.

2. $\Longrightarrow$) Pelo item anterior, se $\gamma \in f^{-1}(\alpha)$, então $\gamma = k\beta$, para algum $k \in \mathbb{F}_q$. Da Proposição 2.1.1, se $x + y\beta \in f^{-1}(\gamma)$, então

   $$-2cxy\beta - 2bcy^2 = k\beta.$$

   Consequentemente, obtemos que $-2bcy^2 = 0$ e $-2cxy = k$. Como $-2bc \neq 0$, então $y = 0$ e, portanto, $-2cxy = 0 \neq k$. Assim, $f^{-1}(\gamma) = \emptyset$.

   $\Longleftarrow$) Seja $\gamma = k\beta$ para algum $k \in \mathbb{F}_q$. Pela Proposição 2.1.1

   $$f(k\beta) = -2bck^2 \in \mathbb{F}_q.$$

   Isso conclui a demonstração.

□

Agora que conhecemos o número de pré-imagens do elemento $\alpha = 0$, bem como o número de pré-imagens de um elemento de $\mathbb{F}_q^*$ ou o número de pré-imagens de uma pré-imagem de um elemento em $\mathbb{F}_q$ (que é vazia), podemos descrever a componente conexa de zero no seguinte teorema.

Teorema 2.2.3. *A componente conexa que contém zero é composta por ele e pelos $q-1$ elementos de $\mathbb{F}_q^*$, todos eles direcionados para zero, e dois elementos de $\mathbb{F}_{q^2}\backslash\mathbb{F}_q$ associados a cada um dos $\frac{q-1}{2}$ elementos $\alpha \in \mathbb{F}_q^*$ que satisfazem $\chi_2(-2\alpha c) = -1$. Essa componente contém todos os elementos de $\mathbb{F}_q \cup \mathbb{F}_q\beta$.*

Demostração. Pelo Teorema 2.2.2, temos $f^{-1}(0) = \mathbb{F}_q$. Isto é, $0 \in \mathbb{F}_q$ possui q pre-imagens.

Se $\alpha \in \mathbb{F}_q$, temos que α não possui pré-imagem, caso $\chi_2(-2\alpha c) = 1$. Caso $\chi_2(-2\alpha c) = -1$, então α possui 2 pré-imagens da forma $\pm k\beta$. Por sua vez, esses elementos não possuem pré-imagem. Além disso, a imagem de $k\beta$, para todo $k \in \mathbb{F}_q$, se encontra em $\mathbb{F}_q$. □

Exemplo 2.2.4. *Tomando $q = 7$ e $c = 3$, seja $\{1, \beta\}$ uma base para $\mathbb{F}_{7^2}$ sobre $\mathbb{F}_7$, tal que $\beta^2 = 5$. Então, a componente conexa que contém o vértice $\langle 0, 0\rangle \in \mathbb{F}_7 \oplus \beta\mathbb{F}_7$ é a seguinte:*

- *Há $7 - 1 = 6$ elementos de $\mathbb{F}_7$ dirigidos a zero e dois elementos de $\mathbb{F}_{7^2}\backslash\mathbb{F}_7$ conectados a cada um dos $\frac{7-1}{2} = 3$ elementos de $\mathbb{F}_7^*$, estes últimos elementos satisfazem $\chi_2(-2\alpha c) = -1$.*
  Utilizando a Equação (2.2), conseguimos que $f(0, y) = -2bcy^2$ e substituindo os valores de b e c conseguimos que $f(0, y) = \langle -30y^2, 0\rangle = \langle 5y^2, 0\rangle$. Assim, obtemos os seguintes valores de $\mathbb{F}_7^*$ e $\mathbb{F}_{7^2}\backslash\mathbb{F}_7$:

$f(0, 1) = \langle 5, 0\rangle$
$f(0, 2) = \langle 20, 0\rangle = \langle 6, 0\rangle$
$f(0, 3) = \langle 45, 0\rangle = \langle 3, 0\rangle$
$f(0, 4) = \langle 80, 0\rangle = \langle 3, 0\rangle$
$f(0, 5) = \langle 125, 0\rangle = \langle 6, 0\rangle$
$f(0, 6) = \langle 180, 0\rangle = \langle 5, 0\rangle$

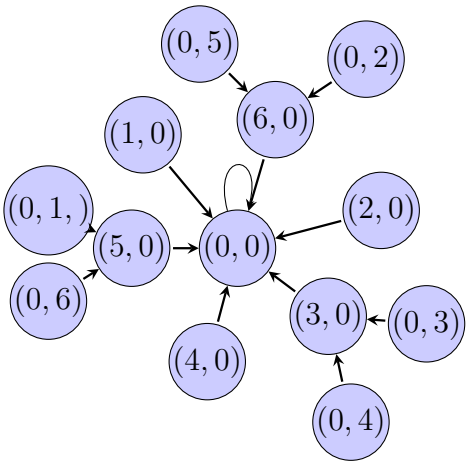


Figura 2.1: Componente conexa do zero para $q = 7$.

Lema 2.2.5. *Seja $\alpha \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$. Escrevendo $\alpha = u + v\beta$, onde $u, v \in \mathbb{F}_q$ e $v \neq 0$, temos*

$$\#f^{-1}(\alpha) = \begin{cases} 2 & \text{se } \chi_2(-2bcu) = 1 \\ 0 & \text{caso contrário} \end{cases}$$

Além disso, se $\gamma \in f^{-1}(\alpha)$, então $-\gamma \in f^{-1}(\alpha)$.

Demostração. Queremos saber se existe uma solução para $c\,(X^{q+1} - X^2) = \alpha$ em $\mathbb{F}_{q^2}$. Escrevendo $X = x + y\beta$, pela Equação (2.2) basta resolver

$$-2bcy^2 - 2cxy\beta = u + v\beta.$$

Se existe $y \in \mathbb{F}_q^*$ satisfazendo a equação acima, então $-2bcy^2 = u$. Isto implica que, $y^2 = -\frac{u}{2bc}$ e $x = -\frac{v}{2cy}$, obtendo assim uma solução. Se $u = 0$, então $y = 0$. No Teorema 2.2.2 mostramos que, nesse caso, $\#f^{-1}(\alpha) = 0$.

Se $u \neq 0$, então α possui pré-imagem se, e somente se, existe $y \in \mathbb{F}_q^*$ tal que $y^2 = -\frac{u}{2bc}$. Observe que

$$\chi_2\left(\frac{u}{-2bc}\right) = \chi_2(u)\chi_2\left(\frac{1}{-2bc}\right) = \chi_2(u)\chi_2(-2bc) = \chi_2(-2bcu).$$

Se $\chi_2(-2bcu) = 1$, então existe $y \in \mathbb{F}_q$ tal que $y^2 = -\frac{u}{2bc}$. Note que $-y$ também é uma solução. Como $y^2 = -\frac{u}{2bc}$ tem no máximo duas soluções, estas são as únicas.

Se $\chi_2(-2cbu) = -1$, não há solução e $\#f^{-1}(\alpha) = 0$. □

Corolário 2.2.6. *Seja $\alpha \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$ tal que $\#f^{-1}(\alpha) = 2$. Se $q \equiv 3 \pmod 4$ e $\gamma \in f^{-1}(\alpha)$, então $\#f^{-1}(\gamma) = 2$ e $\#f^{-1}(-\gamma) = 0$ ou $\#f^{-1}(-\gamma) = 2$ e $\#f^{-1}(\gamma) = 0$.*

Demostração. Se $q \equiv 3 \pmod 4$, então pela Proposição 1.4.6(b), tem-se $\chi_2(-1) = -1$. Tomando $\gamma = u + v\beta$ com $u, v \in \mathbb{F}_q^*$, e pelo Lema 2.2.5 basta analisar $\chi_2(-2bcu)$ para saber se γ possui pré-imagens. De fato, pela Equação (2.2), $f(x + y\beta) = \gamma$ é equivalente a

$$-2cxy\beta - 2bcy^2 = u + v\beta.$$

Segue que,

$$\begin{matrix} -2bcy^2 = u \\ -2cxy = y \end{matrix} \implies \begin{cases} y^2 = -\frac{u}{2bc} \\ x = -\frac{v}{2cy}. \end{cases}$$

Daí, se $\chi_2(-2bcu) = 1$, então $\chi_2(-2bc(-u)) = -1$ e, consequentemente, $\#f^{-1}(\gamma) = 2$ e $\#f^{-1}(-\gamma) = 0$.

Se $\chi_2(-2bcu) = -1$, então $\chi_2(-2bc(-u)) = 1$ e, consequentemente, $\#f^{-1}(\gamma) = 0$ e $\#f^{-1}(-\gamma) = 2$. □

Em outras palavras, se $q \equiv 3 \pmod 4$ e $\alpha \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$, este corolário nos mostra que, quando não vazia, a pré-imagem de α possui dois elementos. Um deles com duas pré-imagens e o outro sem nenhuma pré-imagem.

Consequentemente, se $\alpha \neq 0$ é um elemento de um ciclo, ou seja, pertence a um ciclo da função $f(X)$, então ele ele possui pelo menos um elemento em sua pré-imagem. Pelo Teorema 2.2.2 e pelo Lema 2.2.5, ele deve possuir exatamente duas pré-imagens. Seja γ o elemento periódico e ρ o elemento não periódico na pré-imagem de α. Note que, como γ é periódico, ele debe possuir uma pré-imagem não vazia (pois está em um ciclo). Logo, pelo Corolário 2.2.6, a pré-imagem de ρ é vazia, confirmando que ρ não está em um ciclo — ou seja, é um ponto fora da órbita periódica da função.

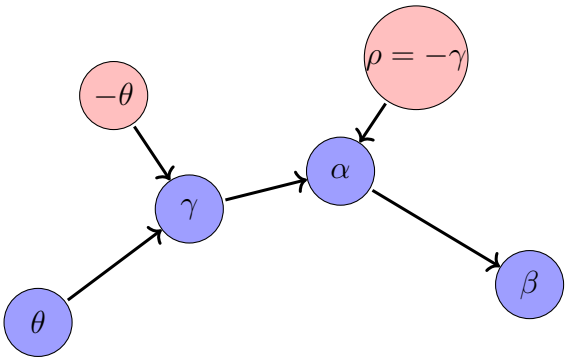


Figura 2.2: Ilustração da prova do Corolário 2.2.6.

Em conclusão, se $q \equiv 3 \pmod 4$, para cada componente conexa diferente da componente conexa de zero (isomorfa a $\mathcal{Z}(q)$), existe $n \in \mathbb{N}$ tal que essa componente é isomorfa a $(Cyc(n), \mathcal{T}(1))$.

Exemplo 2.2.7. *Tomando $q = 7$, $b = 5$ e $c = 4$, as duas componentes conexas não isomorfas, além de $\mathcal{Z}(q)$, que aparecem no grafo funcional, são isomorfas às componentes conexas da Figura 2.3.*

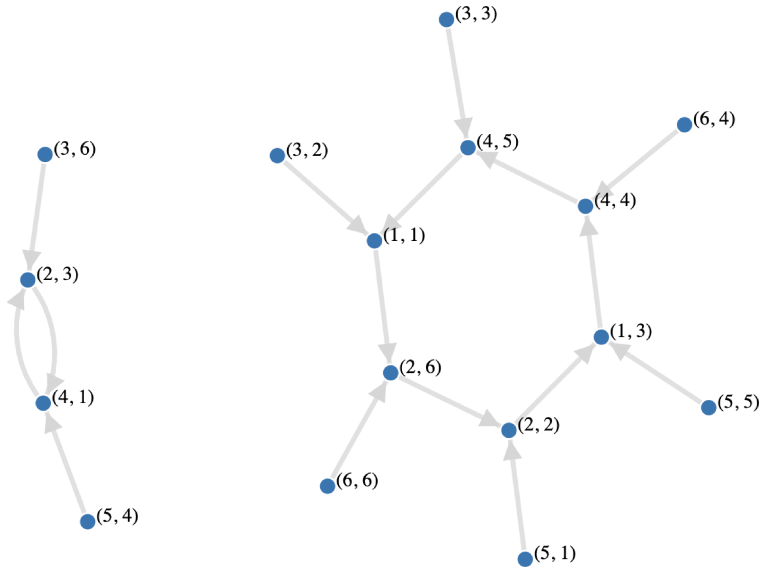


Figura 2.3: Componentes conexas isomorfas a $(Cyc(2), \mathcal{T}(1))$ e $(Cyc(6), \mathcal{T}(1))$.

Corolário 2.2.8. *Seja $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ tal que $\#f^{-1}(\alpha) = 2$. Se $q \equiv 1 \pmod 4$ e $\gamma \in f^{-1}(\alpha)$, então $\#f^{-1}(\gamma) = \#f^{-1}(-\gamma) = 2$ ou $\#f^{-1}(\gamma) = \#f^{-1}(-\gamma) = 0$.*

Demostração. Se $q \equiv 1 \pmod 4$, então, pela Proposição 1.4.6(b), $\chi_2(-1) = 1$. Seja $\gamma = u + v\beta$, com $u, v \in \mathbb{F}_q^*$. Pelo Lema 2.2.5, para saber o número de elementos de $f^{-1}(\gamma)$ e $f^{-1}(-\gamma)$, basta analisar $\chi_2(-2bcu) = \chi_2(-2bc(-u))$. Observe que como $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ e $\gamma \in f^{-1}(\alpha)$, então $u \neq 0$ e $v \neq 0$.

Assim, se $\chi_2(-2bcu) = 1$, então $\#f^{-1}(\gamma) = 2$ e $\#f^{-1}(-\gamma) = 2$, e se $\chi_2(-2bcu) = -1$, então $\#f^{-1}(\gamma) = 0$ e $\#f^{-1}(-\gamma) = 0$.

□

O corolário acima implica que, quando a pré-imagem de α é não vazia e $q \equiv 1 \pmod 4$, ou ambos os elementos da pré-imagem de α têm pré-imagem não vazia, ou ambos têm pré-imagem vazia, como mostrado no exemplo a seguir.

Exemplo 2.2.9. *Tomando $q = 13$, $b = 11$ e $c = 3$, as componentes conexas diferentes de $\mathcal{Z}(q)$ são isomorfas aos grafos das Figuras 2.4 e 2.5.*

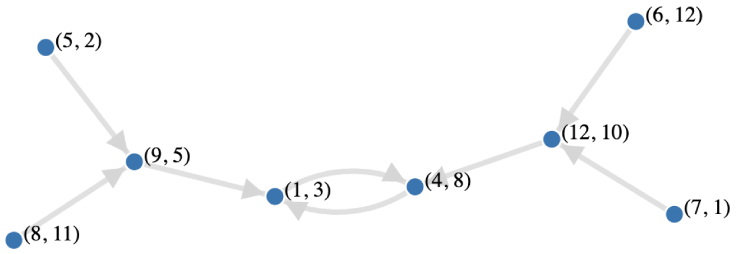


Figura 2.4: Grafo $(Cyc(2), \mathcal{T}(2))$

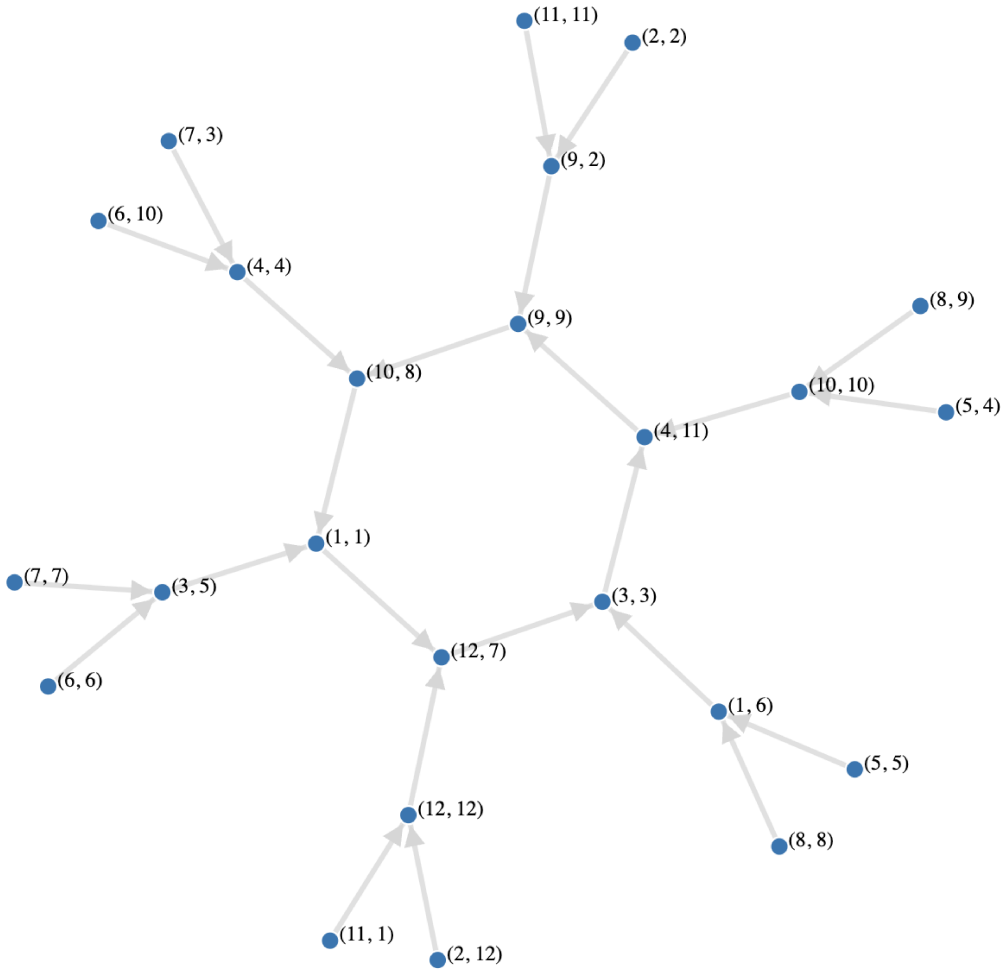


Figura 2.5: Grafo $(Cyc(6), \mathcal{T}(2))$

Observe que, na componente da Figura 2.4, o elemento $\langle 4, 8\rangle$ possui dois elementos em sua pré-imagem, isto é $\langle 1, 3\rangle$ e $\langle 12, 10\rangle$. Ambos esses elementos também têm pré-imagens não vazias. Por outro lado, o elemento $\langle 12, 10\rangle$ tem dois elementos em sua pré-imagem, mas ambos possuem pré-imagens vazias.

2.3 Número de ciclos e comprimentos de ciclos

Agora, vamos encontrar os comprimentos dos ciclos do grafo funcional de $f(X)$ e a quantidade de ciclos existentes de cada comprimento. Antes disso, precisamos do seguinte lema.

Lema 2.3.1. *O comprimento de um ciclo de comprimento maior que 1 é par.*

Demostração. Do Teorema 2.2.3, temos que se $\gamma = x + y\beta \in \mathbb{F}_q$, com $x = 0$ ou $y = 0$, então γ pertence à componente conexa de zero, e zero é o único elemento que pertence a um ciclo de comprimento 1.

Dessa forma, podemos supor que $x, y \neq 0$. Pela Proposição 2.1.1, temos

$$f(x + y\beta) = -2bcy^2 - 2cxy\beta.$$

Considerando $\mathbb{F}_{q^2}$ como um espaço vetorial sobre $\mathbb{F}_q$ com base $\{1, \beta\}$, temos:

$$\begin{aligned} \left(\mathbb{F}_q^*\right)^2 &\xrightarrow{f} \left(\mathbb{F}_q^*\right)^2 \\ \langle x, y\rangle &\mapsto \langle -2bcy^2, -2cxy\rangle. \end{aligned} \tag{2.4}$$

Para simplificar a notação, denotaremos $f(\langle x, y\rangle)$ como $f(x, y)$. Aplicando f novamente, obtemos:

$$\begin{aligned} f^{(2)}(x, y) &= \langle -2bc(-2cxy)^2, -2c(-2bcy^2)(-2cxy)\rangle \\ &= \langle -8bc^3x^2y^2, -8bc^3xy^3\rangle \\ &= -8bc^3xy^2\langle x, y\rangle. \end{aligned} \tag{2.5}$$

Definindo $g(x, y) = -8bc^3xy^2$, para todo $v \in \mathbb{F}_q^*$, obtemos:

$$\begin{aligned} f^{(2)}(vx, vy) &= f(f(vx, vy)) \\ &= f(-2cb(vy)^2, -2c(vx)(vy)) \\ &= \langle -2bc(-2cv^2xy)^2, -2c(-2cbv^2y^2)(-2cv^2xy)\rangle \\ &= \langle -8bc^3v^{4x2}y^2, -8c^3bv^4xy^3\rangle \\ &= -8bc^3xy^2v^4\langle x, y\rangle \\ &= v^4g(x, y)\langle x, y\rangle. \end{aligned}$$

Além disso, tomando $v = g(x, y)$, temos:

$$\begin{aligned} f^{(4)}(x, y) &= f^{(2)}\left(f^{(2)}(x, y)\right) \\ &= f^{(2)}(g(x, y)\langle x, y\rangle) \\ &= f^{(2)}(vx, vy) \\ &= v^4g(x, y)\langle x, y\rangle \\ &= g(x, y)^5\langle x, y\rangle. \end{aligned}$$

Afirmação 2.3.2. $f^{(2n)}(x, y) = g(x, y)^{1+4+4^2+\cdots+4^{n-1}}\langle x, y\rangle$.

Demostração. Observe que a afirmação já foi provada acima para $n = 1$ e $n = 2$:

$$f^{(2)}(x, y) = g(x, y)\langle x, y\rangle \quad \text{e} \quad f^{(4)}(x, y) = g(x, y)^{1+4}\langle x, y\rangle.$$

Suponha a afirmação verdadeira para $n = k$, isto é,

$$f^{(2k)} = g(x, y)^{1+4+4^2+\cdots+4^{k-1}}\langle x, y\rangle.$$

Para $n = k+1$, temos:

$$\begin{aligned} f^{(2(k+1))}(x,y) &= f^{(2k+2)}(x,y) = f^{(2)}\left(f^{(2k)})(x,y)\right) \\ &= f^{(2)}(g(x,y)^{1+4+4^2+\cdots+4^{k-1}}\langle x,y\rangle) \\ &= g(x,y)\left[(g(x,y)^{1+4+4^2+\cdots+4^{k-1}}\right]^4\langle x,y\rangle \\ &= g(x,y)(g(x,y)^{\left[1+4+4^2+\cdots+4^{k-1}\right]\cdot 4}\langle x,y\rangle) \\ &= g(x,y)(g(x,y)^{\left[4+4^2+\cdots+4^{k}\right]}\langle x,y\rangle) \\ f^{(2(k+1))}\langle x,y\rangle &= g(x,y)^{\left[1+4+4^2+\cdots+4^{k}\right]}\langle x,y\rangle. \end{aligned}$$

Portanto, por indução, concluímos que:

$$f^{(2n)}(x,y) = g(x,y)^{1+4+4^2+\cdots+4^{n-1}}\langle x,y\rangle, \quad \forall n \in \mathbb{N}. \tag{2.6}$$

A expressão $1+4+4^2+\cdots+4^{n-1}$ é a soma de uma progressão geométrica de primeiro termo $a=1$ e razão $r=4$. A soma é dada por

$$S_n = 1+4+4^2+\cdots+4^{n-1} = \frac{4^n-1}{4-1} = \frac{4^n-1}{3}. \tag{2.7}$$

A partir das Equações (2.6) e (2.7), podemos concluir que:

$$f^{(2n)}(x,y) = g(x,y)^{\frac{4^n-1}{3}}\langle x,y\rangle. \tag{2.8}$$

□

Aplicando f mais uma vez em (2.8), segue que:

$$\begin{aligned} f^{(2n+1)}(x,y) &= f\left(g(x,y)^{\frac{4^n-1}{3}}\langle x,y\rangle\right) \\ &= f\left(v^{S_n}x, v^{S_n}y\right) \\ &= \langle -2bc\left(v^{S_n}y\right)^2, -2cv^{S_n}xv^{S_n}y\rangle \\ &= \langle -2bcv^{2S_n}y^2, -2cv^{2S_n}xy\rangle \\ &= v^{2S_n}\langle -2bcy^2, -2cxy\rangle \\ &= -2cyg(x,y)^{\frac{2(4^n-1)}{3}}\langle by, x\rangle \\ &= k_{x,y,n}\langle by, x\rangle, \end{aligned}$$

onde $v = g(x,y)$ e $k_{x,y,n} = -2cyg(x,y)^{\frac{2(4^n-1)}{3}}$. Note que $k_{x,y,n} \in \mathbb{F}_q$.

Se houver um ciclo de comprimento ímpar, então devemos ter $k_{x,y,n}\langle by, x\rangle = \langle x,y\rangle$, para algum $\langle x,y\rangle \in \left(\mathbb{F}_q^*\right)^2$. Isso implica que $\langle k_{x,y,n}by, k_{x,y,n}x\rangle = \langle x,y\rangle$. Daí,

$$\begin{cases} k_{x,y,n}by = x \\ k_{x,y,n}x = y \end{cases} \implies k_{x,y,n} = \frac{x}{by} = \frac{y}{x} \in \mathbb{F}_q.$$

Em particular, segue que $b = \frac{x^2}{y^2} = \left(\frac{x}{y}\right)^2$. Como b não é um quadrado em $\mathbb{F}_q$, isso leva a uma contradição. Isso prova o resultado. □

Teorema 2.3.3. *Seja $q-1 = 2^s r$, com r ímpar. Então, para cada divisor d de r, existem $\frac{\varphi(d)(q-1)}{2\,\mathrm{Ord}_{3d}(4)}$ ciclos de comprimento $2\,\mathrm{Ord}_{3d}(4)$, e esses são os únicos ciclos de comprimento maior que 1 no grafo funcional de $f(X)$.*

Demostração. Suponha que $X = \langle x, y\rangle$ seja um elemento de um ciclo de comprimento $m > 1$. Então, pelo Lema 2.3.1, $m = 2n$ para algum $n \in \mathbb{N}$ e

$$\begin{aligned} f^{(2n)}(X) = X &\implies g(x,y)^{\frac{4^n-1}{3}} X = X \\ &\implies \left(-8bc^3xy^2\right)^{\frac{4^n-1}{3}} = 1. \end{aligned}$$

Seja $\theta = -8bc^3xy^2 \in \mathbb{F}_q^*$. Então $n \in \mathbb{N}$ é o menor inteiro positivo tal que $\frac{4^n-1}{3} \equiv 0 \pmod{\operatorname{Ord}(\theta)}$. Isso equivale a $4^n \equiv 1 \pmod{3\operatorname{Ord}(\theta)}$.

Afirmação 2.3.4. *Existe n tal que $\frac{4^n-1}{3} \equiv 0 \pmod{\operatorname{Ord}(\theta)}$ se, e somente se, $\operatorname{Ord}(\theta)$ é ímpar.*

Demostração. Seja $n \in \mathbb{N}$ tal que $\frac{4^n-1}{3} \equiv 0 \pmod{\operatorname{Ord}(\theta)}$. Isso significa que $\operatorname{Ord}(\theta)$ divide $\frac{4^n-1}{3}$. Como $\frac{4^n-1}{3}$ é ímpar, então $\operatorname{Ord}(\theta)$ é ímpar.

Reciprocamente, suponha que $\operatorname{Ord}(\theta)$ é ímpar. Nesse caso, $3\operatorname{Ord}(\theta)$ é primo com 4. Isso significa que existe um inteiro positivo n tal que $4^n \equiv 1 \pmod{3\operatorname{Ord}(\theta)}$. Isso equivale a $\frac{4^n-1}{3} \equiv 0 \pmod{\operatorname{Ord}(\theta)}$.

□

Uma vez que $\theta \in \mathbb{F}_q^*$, temos $\operatorname{Ord}(\theta) | q-1$. Isto é, $\operatorname{Ord}(\theta) | 2^s r$. Como $\operatorname{Ord}(\theta)$ é ímpar, então $\operatorname{Ord}(\theta) | r$.

Assim, para cada ciclo de comprimento $2n$, existe um divisor ímpar d de $q-1$ (isto é, um divisor de r) tal que $n = \operatorname{Ord}_{3d}(4)$.

Agora, contaremos o número de ciclos desse comprimento.

Suponha que α seja um gerador de $\mathbb{F}_q^*$ e α^j um elemento de ordem d. Do Lema 1.1.24 temos

$$\operatorname{Ord}\left(\alpha^j\right) = d = \frac{q-1}{\operatorname{mdc}(q-1, j)}.$$

Assim, como $2^s | \operatorname{mdc}(q-1, j)$, podemos escrever $j = 2^s t$, sendo t um inteiro positivo que satisfaz a restrição:

$$j \leq q-1 \implies 2^s t \leq 2^s r.$$

Dividindo ambos os lados por 2^s, obtemos:

$$t \leq r.$$

Como $r = \frac{q-1}{2^s}$, isso nos dá:

$$1 \leq t \leq \frac{q-1}{2^s},$$

com t variando entre 1 e $\frac{q-1}{2^s}$. Em resumo, $j = 2^s t$ com $1 \leq t \leq \frac{q-1}{2^s}$.

Por outro lado, para qualquer $\langle x, y\rangle \in \mathbb{F}_q^2$ tal que $-8bc^3xy^2 = \alpha^j \left((\alpha^j)^{\frac{4^n-1}{3}} = 1\right)$, o elemento $x + \beta y \in \mathbb{F}_{q^2}$ é um nó de um ciclo de comprimento $2\operatorname{ord}_{3d}(4)$, com $n = \operatorname{Ord}_{3d}(4)$.

Note que t satisfaz $\operatorname{mdc}\left(\frac{q-1}{2^s}, t\right) = \frac{q-1}{2^s d}$ se, e somente se, $t = \frac{q-1}{2^s d} t'$, com $\operatorname{mdc}(t', d) = 1$. Como

$$1 \leq t \leq \frac{q-1}{2^s} \implies 1 \leq \frac{q-1}{2^s d} t' \leq \frac{q-1}{2^s},$$

então $1 \leq t' \leq d$.

Assim, existem $\varphi(d)$ escolhas para t e, consequentemente, $\varphi(d)$ escolhas para j tal que $\operatorname{Ord}(\alpha^j) = d$. Além disso, para cada j existem $q-1$ pares ordenados $\langle x, y\rangle$ tais que $-8bc^3xy^2 = \alpha^j$. Isso acontece porque para cada $y \in \mathbb{F}_q^*$ existe um único $x \in \mathbb{F}_q^*$ satisfazendo $-8bc^3xy^2 = \alpha^j$. Consequentemente, o número de elementos em ciclos de comprimento $2\operatorname{Ord}_{3d}(4)$ é $\varphi(d)(q-1)$. Como há $2\operatorname{Ord}_{3d}(4)$ elementos em cada ciclo, existem $\frac{\varphi(d)(q-1)}{2\operatorname{Ord}_{3d}(4)}$ ciclos. □

Corolário 2.3.5. *Existem $\frac{q-1}{2}$ ciclos de comprimento dois.*

Demostração. Como 1 é sempre um divisor ímpar de $q-1$, tomando $d=1$, temos

$$2\,\mathrm{Ord}_{3d}(4) = 2\,\mathrm{Ord}_3(4) = 2.$$

Note que, se $d \geq 3$ for um divisor de r, então $3d \geq 9$ e $2\,\mathrm{Ord}_{3d}(4) \neq 2$, pois $\mathrm{Ord}_{3d}(4) > 1$. Portanto, o número de ciclos de comprimento 2 é

$$\frac{\varphi(1)(q-1)}{2} = \frac{q-1}{2}.$$

□

Agora que encontramos todos os comprimentos de ciclos deste grafo funcional, só precisamos descrever os pré-ciclos.

2.4 Descrição dos pré-ciclos

Definição 2.4.1. *Seja $Cyc(\mathscr{G}) = (\mathcal{V}, \mathcal{E})$ o subgrafo de $\mathscr{G}\backslash\mathcal{Z}(q)$ tal que $\mathcal{V}$ é o conjunto de pontos periódicos e*

$$\mathcal{E} = \{\langle x, f(x)\rangle \mid x \in \mathcal{V}\}.$$

Teorema 2.4.2. *Se $q-1 = 2^s r$, com r ímpar, então, para cada nó de $Cyc(\mathscr{G})$, há uma árvore isomorfa a $\mathcal{T}(s)$ conectada a ele.*

Demostração. Seja d um divisor de r. Mais uma vez, seja $\mathbb{F}_{q^2}$ gerado por $\{1, \beta\}$ sobre $\mathbb{F}_q$, em que $\beta^2 = b \in \mathbb{F}_q$. Consideremos $\mathbb{F}_{q^2}$ como um espaço vetorial sobre $\mathbb{F}_q$.
Seja $\langle x_0, y_0\rangle$ um elemento periódico e, para todo $i \geq 1$, seja $\langle x_i, y_i\rangle$ um ponto periódico tal que

$$f(x_i, y_i) = \langle x_{i-1}, y_{i-1}\rangle.$$

Como visto no Lema 2.2.5, $\langle -x_i, -y_i\rangle$ também satisfaz

$$f(-x_i, -y_i) = \langle x_{i-1}, y_{i-1}\rangle,$$

mas não é um elemento periódico. Suponha que $\langle x, y\rangle \in f^{-1}(-x_1, -y_1)$.

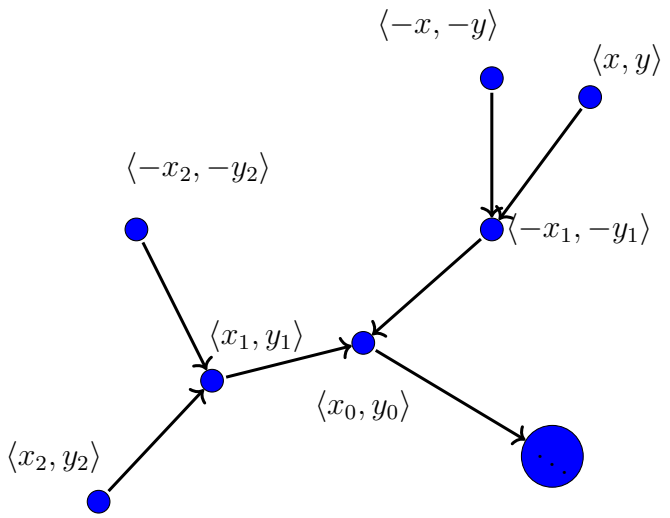


Figura 2.6: Esquema ilustrativo de $\langle x, y\rangle \in f^{-1}(-x_1, -y_1)$.

Usando a Equação (2.4), temos

$$\begin{aligned} f(x,y) &= \langle -x_1, -y_1 \rangle \\ &= \langle -2bcy^2, -2cxy \rangle. \end{aligned}$$

Logo, $-2bcy^2 = -x_1$ e $-2cxy = -y_1$. No entanto, $-2bcy_2^2$ e $-2cx_2y_2$ também são iguais a x_1 e y_1, respectivamente. Logo, $-2bcy^2 = 2bcy_2^2$ e $-2cxy = 2cx_2y_2$. Isso implica $y^2 = -y_2^2$.

Se $\chi_2(y^2) = \chi_2(-y_2^2) = 1$, então $\chi_2(-1) = 1$. Dessa forma, $\langle -x_1, -y_1 \rangle$ tem pré-imagem não vazia se, e somente se, -1 for um quadrado em $\mathbb{F}_q$, ou, equivalentemente, se $q \equiv 1 (\mathrm{mod}\, 4)$.

Sabemos que no corpo finito $\mathbb{F}_q$, quando $q \equiv 1 \pmod 4$, existem raízes quartas da unidade. Seja ζ_4 uma raiz quarta primitiva da unidade. Então o conjunto de raízes de $X^4 = 1$ é

$$\{\zeta_4, \quad \zeta_4^2, \quad \zeta_4^3, \quad \zeta_4^4 = 1\} = \{1, \zeta_4, -1, -\zeta_4\}. \tag{2.9}$$

pois $\zeta_4^2 = -1$. Assim, se $q \equiv 1 \pmod 4$, então os valores de y e x podem ser expressos como:

$$y = \zeta_4 y_2, \quad x = \zeta_4 x_2 \quad \text{ou} \quad y = -\zeta_4 y_2, \quad x = -\zeta_4 x_2. \tag{2.10}$$

Esses elementos são os únicos vértices na altura 2 da árvore de pontos não periódicos acima do ponto $\langle x_0, y_0 \rangle$.

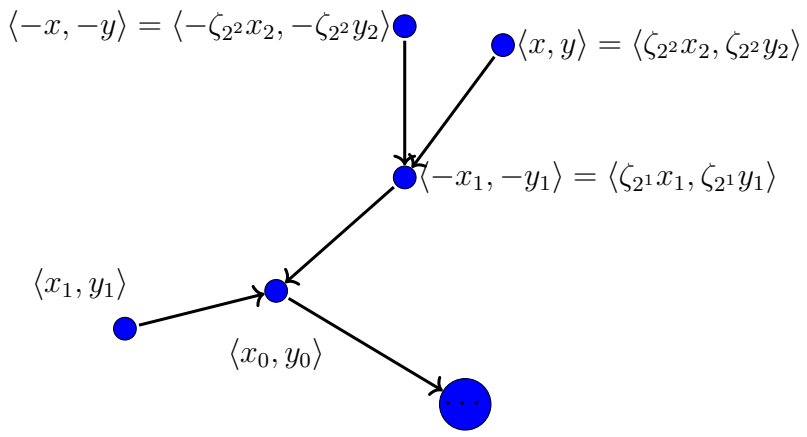


Figura 2.7: Esquema ilustrativo dos vértices nas altura 2 da árvore de pontos não periódicos acima do ponto $\langle x_0, y_0 \rangle$.

Suponha agora que para cada $0 < k \leq s$ e para cada raiz 2^{k-1}-primitiva da unidade $\zeta_{2^{k-1}}$, o par $\langle \zeta_{2^{k-1}} x_{k-1}, \zeta_{2^{k-1}} y_{k-1} \rangle$ seja um elemento não periódico satisfazendo

$$f^{(k-1)} \left(\zeta_{2^{k-1}} x_{k-1}, \zeta_{2^{k-1}} y_{k-1} \right) = \langle x_0, y_0 \rangle .$$

Em outras palavras, $\langle \zeta_{2^{k-1}} x_{k-1}, \zeta_{2^{k-1}} y_{k-1} \rangle$ é um vértice na altura $k-1$ da árvore de elementos não periódicos. Se $\langle x, y \rangle \in f^{-1} \left(\zeta_{2^{k-1}} x_{k-1}, \zeta_{2^{k-1}} y_{k-1} \right)$, então $-2bcy^2 = \zeta_{2^{k-1}} x_{k-1}$. Por definição $f(x_k, y_k) = \langle -2bcy_k^2, -2cx_k y_k \rangle = \langle x_{k-1}, y_{k-1} \rangle$. Logo,

$$-2bcy^2 = \zeta_{2^{k-1}} x_{k-1} = -\zeta_{2^{k-1}} 2bcy_k^2.$$

Daí, segue que

$$y^2 = \zeta_{2^{k-1}} y_k^2,$$

e, consequentemente, $f^{-1}\left(\zeta_{2^{k-1}}x_{k-1}, \zeta_{2^{k-1}}y_{k-1}\right) \neq \emptyset$ se, e somente se, $\zeta_{2^{k-1}}$ for um quadrado em $\mathbb{F}_q$, isto é, $\mathbb{F}_q$ possui raiz 2^k-ésima primitiva da unidade. Pelo Lema 1.4.9, isso é equivalente a $q \equiv 1 \pmod{2^k}$. Como para todo par $\langle x, y\rangle$ temos $f(x,y) = f(-x,-y)$, então

$$f\left(\pm\langle\zeta_{2^k}x_k, \zeta_{2^k}y_k\rangle\right) = \langle\zeta_{2^{k-1}}x_{k-1}, \zeta_{2^{k-1}}y_{k-1}\rangle\,.$$

Como esses elementos estão na pré-imagem dos vértices na altura $k-1$, eles devem ser os elementos na altura k da árvore de elementos não periódicos.

Isso mostra que, se $q-1 = 2^s r$, onde r é ímpar, então para cada $\langle x_0, y_0\rangle$ em $Cyc(\mathscr{G})$, existe uma árvore $\mathcal{T}(s)$ conectada a ele. Como isso vale para cada elemento de cada ciclo, concluímos a demonstração. □

Finalmente, podemos descrever todo o grafo funcional de $f(X) = c\left(X^{q+1} - X^2\right)$ sobre $\mathbb{F}_{q^2}$. Primeiro, há uma componente conexa isomorfa a $\mathcal{Z}(q)$, sendo zero o único ponto fixo. Escrevendo $q-1 = 2^s r$, para cada divisor d de r, existem

$$\frac{\varphi(d)(q-1)}{2\,\mathrm{Ord}_{3d}(4)}$$

componentes conexas isomorfas a $\left(Cyc\left(2\,\mathrm{Ord}_{3d}(4)\right), \mathcal{T}(s)\right)$. Em conclusão, temos o seguinte teorema.

2.5 Teorema principal

Teorema 2.5.1. *Seja q uma potência de um primo ímpar com $q-1 = 2^s r$ e r ímpar. O grafo funcional da função $f(X) = c\left(X^{q+1} - X^2\right)$ sobre $\mathbb{F}_{q^2}$, com $c \in \mathbb{F}_q^*$, é isomorfo a*

$$\mathscr{G} = \mathcal{Z}(q) \oplus \bigoplus_{d|r} \frac{\varphi(d)(q-1)}{2\,\mathrm{Ord}_{3d}(4)} \times \left(Cyc\left(2\,\mathrm{Ord}_{3d}(4)\right), \mathcal{T}(s)\right). \tag{2.11}$$

2.5.1 Exemplos

Exemplo 2.5.2. *Sejam $q = 7$, $b = 5$ e $c = 2$. Note que $q-1 = 2\cdot 3$, então temos árvores isomorfas a $\mathcal{T}(1)$ anexadas a cada ponto periódico. Observe que os divisores ímpares de $q-1$ são 1 e 3. Assim, os comprimentos dos ciclos devem ser $2\,\mathrm{Ord}_{3\cdot 1}(4) = 2$ e $2\,\mathrm{Ord}_{3\cdot 3}(4) = 6$. Logo, o grafo funcional estará composto por uma componente conexa isomorfa a $\mathcal{Z}(7)$ (ver Figura 2.8).*

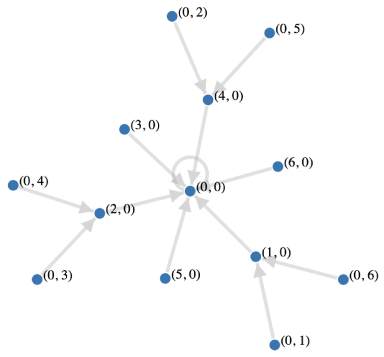


Figura 2.8: Componente conexa $\mathcal{Z}(7)$ para $a = -1$.

Existem $\frac{7-1}{2} = 3$ componentes conexas isomorfas a $\left(Cyc\left(2\,\mathrm{Ord}_3(4)\right), \mathcal{T}(1)\right)$ (ver Figura 2.9).

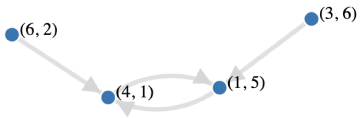


Figura 2.9: $(Cyc\,(2\,\mathrm{Ord}_3(4))\,,\,\mathcal{T}(1))$.

E existem $\frac{\varphi(3)(q-1)}{6} = \frac{2\cdot 6}{6} = 2$ *componentes conexas isomorfas a* $(Cyc\,(2\,\mathrm{Ord}_9(4))\,,\,\mathcal{T}(1))$ *(ver Figura 2.10).*

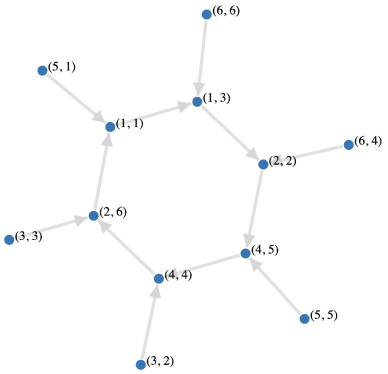


Figura 2.10: Componente conexa $(Cyc\,(2\,\mathrm{Ord}_9(4))\,,\,\mathcal{T}(1))$.

Em outras palavras, o grafo funcional de $f(X) = 2\,(X^8 - X^2)$ *sobre* $\mathbb{F}_{7^2}$ *é*

$$\mathscr{G} = \mathcal{Z}(7) \oplus 4 \times (Cyc(2), \mathcal{T}(1)) \oplus 3 \times (Cyc(6), \mathcal{T}(1))\,. \tag{2.12}$$

Exemplo 2.5.3. *Sejam* $q = 5$, $b = 2$ *e* $c = 3$. *Como* $q-1 = 2^2 \cdot 1$, *então temos árvores isomorfas a* $\mathcal{T}(2)$ *anexadas a cada ponto periódico. Observe que, nesse caso, o único divisor ímpar de* $q - 1$ *é* 1. *Assim, o comprimento de seus ciclos (que não se encontram na componente conexa de zero) deve ser* $2\,\mathrm{Ord}_{3\cdot 1}(4) = 2$. *Logo, o grafo funcional estará composto pela componente conexa de zero* $\mathcal{Z}(q)$ *e duas componentes conexas isomorfas a* $(Cyc(2), \mathcal{T}(2))$ *(ver Figura 2.11).*

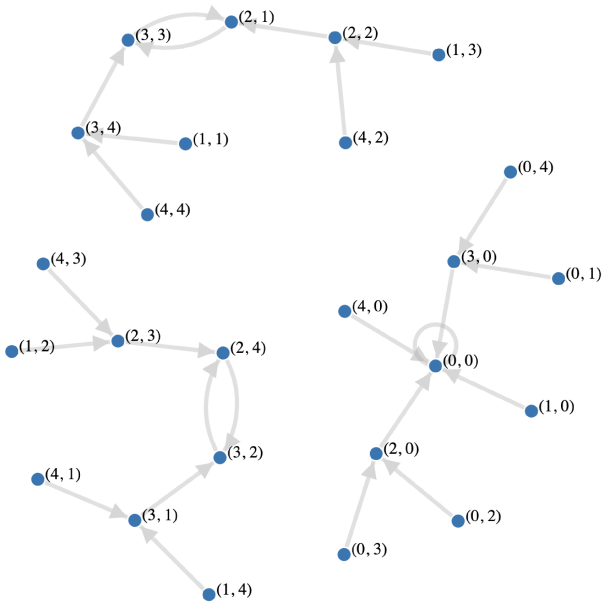


Figura 2.11: Grafo funcional sobre $\mathbb{F}_{5^2}$.

Exemplo 2.5.4. *Sejam* $q = 13$, $b = 11$ *e* $c = 3$. *Como* $q - 1 = 2^2 \cdot 3$, *então temos árvores isomorfas a* $\mathcal{T}(2)$ *anexadas a cada ponto periódico. Observe que os divisores ímpares de* $q - 1$ *são 1 e 3, portanto os comprimentos dos ciclos devem ser* $2\,\mathrm{Ord}_3(4) = 2$ *e* $2\,\mathrm{Ord}_9(4) = 6$. *Finalmente, concluímos que o grafo funcional é composto por uma componente isomorfa a* $\mathcal{Z}_{13}$ *(ver Figura 2.12),*

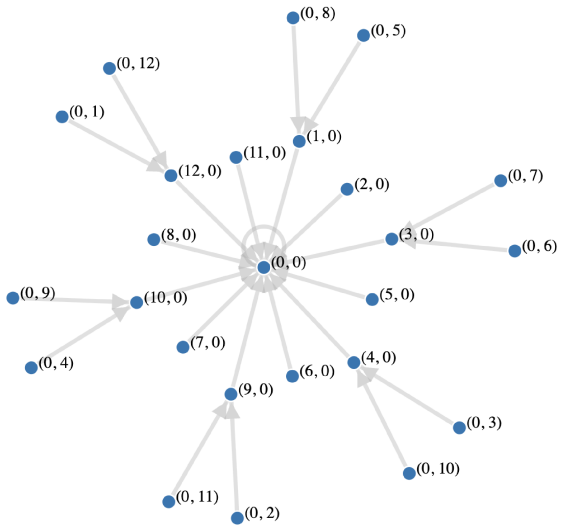


Figura 2.12: Componente conexa $\mathcal{Z}_{13}$.

$\frac{q-1}{2} = 6$ *componentes conexas isomorfas a* $(Cyc\,(2\,\mathrm{Ord}_3(4))\,, \mathcal{T}(2))$ *(ver Figura 2.13)*

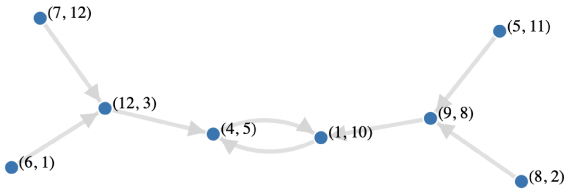


Figura 2.13: Componente conexa $(Cyc\,(2\,\mathrm{Ord}_3(4))\,, \mathcal{T}(2))$.

e $\frac{\varphi(3)(q-1)}{6} = \frac{2 \cdot 12}{6} = 4$ *componentes conexas isomorfas a* $(Cyc\,(2\,\mathrm{Ord}_9(4))\,, \mathcal{T}(2))$ *(ver Figura 2.14).*

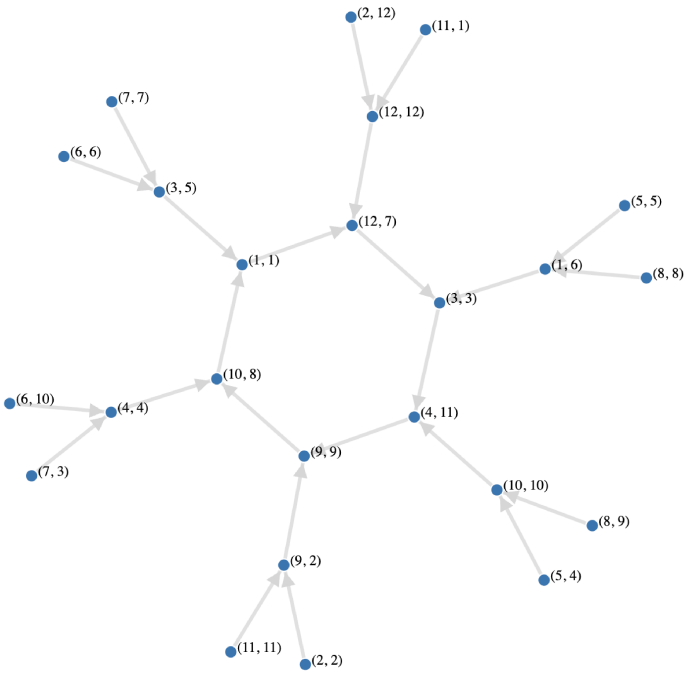


Figura 2.14: Componente conexa $(Cyc\,(2\,\mathrm{Ord}_9(4))\,,\mathcal{T}(2))$.

Em outras palavras, o grafo funcional de $f(X) = 3\,(X^{14} - X^2)$ *sobre* $\mathbb{F}_{13^2}$ *é*

$$\mathscr{G} = \mathscr{Z}(13) \oplus 4 \times (Cyc(6), \mathcal{T}(2)) \oplus 6 \times (Cyc(2), \mathcal{T}(2)). \tag{2.13}$$

Capítulo 3

O grafo funcional de $f(X) = c(X^{q+1} + X^2)$

Nesse capítulo analisaremos o grafo funcional de $f(X) = c(X^{q+1} + X^2)$. Ou seja, vamos considerar $a = 1$. Seguiremos o mesmo caminho do capítulo anterior, no qual analisamos o grafo funcional de $f(X)$ com $a = -1$.

3.1 Determinação dos pontos fixos da função $f(X)$

Como no capítulo anterior, vamos reescrever $f(X) = c(X^{q+1} + X^2)$ em função das coordenadas de uma base de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$.

Proposição 3.1.1. *Seja $\{1, \beta\}$ uma base de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$ tal que $\beta^2 = b \in \mathbb{F}_q^*$. Então, para todos $x, y \in \mathbb{F}_q$, temos*

$$f(x + y\beta) = 2cx^2 + 2cxy\beta.$$

Demonstração. Como $\{1, \beta\}$ é uma base de $\mathbb{F}_{q^2}$, com $\beta^2 = b \in \mathbb{F}_q$, concluímos, como no capítulo anterior,

$$\beta^q = -\beta \quad \text{e} \quad \beta^{q+1} = -b = -\beta^2.$$

Dessa forma, para $\alpha = x + y\beta \in \mathbb{F}_{q^2}$, com $x, y \in \mathbb{F}_q$, temos

$$\begin{aligned} f(\alpha) &= c\alpha(\alpha^q + \alpha) = c(x + y\beta)\left(x + y\beta^q + x + y\beta\right) \\ &= = c(x + y\beta)\left(x - y\beta + x + y\beta\right) = 2cx^2 + 2cxy\beta. \end{aligned}$$

□

Observe que ao identificar $\mathbb{F}_{q^2}$ com $\mathbb{F}_q^2$, podemos representar um elemento α nesse corpo (ou espaço vetorial) da forma $\alpha = x + y\beta$ ou $\alpha = \langle x, y\rangle$. Podemos então reescrever a função $f(X)$ da seguinte forma:

$$\begin{array}{ccc} \mathbb{F}_q^2 & \xrightarrow{f} & \mathbb{F}_q^2 \\ \langle x, y\rangle & \longmapsto & \langle 2cx^2, 2cxy\rangle . \end{array} \tag{3.1}$$

Agora, determinemos os pontos fixos de $f(X) = c\left(X^{q+1} + X^2\right)$.

Lema 3.1.2. *A função $f(X) = c\left(X^{q+1} + X^2\right)$ possui $q + 1$ pontos fixos: $\langle 0, 0\rangle$ e $\langle (2c)^{-1}, y\rangle$, para todo $y \in \mathbb{F}_q$.*

Demostração. Seja $\alpha \in \mathbb{F}_{q^2}$. Observe que

$$f(\alpha) = c\alpha\,(\alpha^q + \alpha) = \alpha \quad \text{se, e somente se,} \quad \alpha = 0 \text{ ou } c\,(\alpha^q + \alpha) = 1. \tag{3.2}$$

Logo, $\alpha = 0$ é um ponto fixo de $f(X)$.

Seja $\alpha = \langle x, y\rangle \in \mathbb{F}_q^2$ um ponto fixo de f tal que $\alpha \neq 0$. Como $\alpha^q = x - y\beta$, então $c\,(\alpha^q + \alpha) = 1$ equivale a

$$c\,(2x) = 1.$$

Ou seja, $x = (2c)^{-1}$ e y é um ponto qualquer de $\mathbb{F}_q$. Consequentemente, $\langle x, y\rangle$ é um ponto fixo de $f(X)$ se, e somente se, $x = y = 0$ ou $x = (2c)^{-1}$ e y é um elemento arbitrário de $\mathbb{F}_q$. Assim, existem $q + 1$ pontos fixos: $\langle 0, 0\rangle$ e $\langle (2c)^{-1}, y\rangle$, para todo $y \in \mathbb{F}_q$. □

3.2 Análise das pré-imagens de f

De (4.1), para $\alpha = \langle x, y\rangle \in \mathbb{F}_q^2$, temos $f(\alpha) = 0$ se, e somente se, $x = 0$. Em outras palavras, $f^{-1}(0, 0) = \{\langle 0, y\rangle \mid y \in \mathbb{F}_q\}$, isto é, zero possui q pré-imagens. Segue diretamente de (4.1), que $\#f^{-1}(0, y) = \langle 0, 0\rangle$, se $y \neq 0$. Em conclusão, temos um teorema análogo ao Teorema 2.2.2.

Teorema 3.2.1. *Se $\alpha \in \beta\mathbb{F}_q$, então*

$$\#f^{-1}(\alpha) = \begin{cases} q & \text{se } \alpha = 0, \\ 0 & \text{se } \alpha \neq 0. \end{cases}$$

Portanto, a componente conexa de zero do grafo funcional da função $X \mapsto c\,(X^{q+1} + X^2)$ é zero direcionado para si mesmo e os $q - 1$ elementos de $\beta\mathbb{F}_q^*$ direcionados para zero.

Dessa forma, a componente conexa de zero do grafo funcional de $f(X)$ é isomorfa ao grafo da próxima definição.

Definição 3.2.2. *Definimos $\mathcal{Z}^*(q)$ como o grafo direcionado $Cyc(1)$ com $q-1$ árvores isomorfas a $\mathcal{T}(1)$ anexadas a ele.*

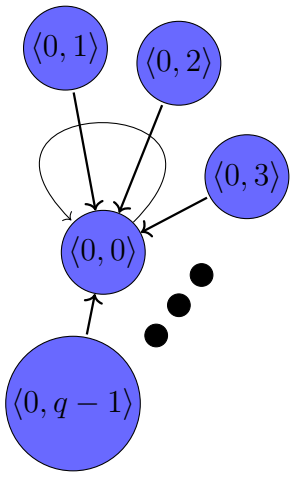


Figura 3.1: Componente conexa $\mathcal{Z}^*(q)$.

Na próxima seção vamos contar os ciclos do grafo funcional de $f(X)$.

3.3 Número de ciclos e comprimentos de ciclos

Teorema 3.3.1. *Seja $q-1=2^s r$, com r ímpar. Para cada divisor $d\neq 1$ de r, existem $\frac{q\cdot\varphi(d)}{\mathrm{Ord}_d(2)}$ ciclos de comprimento $\mathrm{Ord}_d(2)$, e esses são todos os ciclos de comprimento maior que 1. Para $d=1$, há $q+1$ ciclos de comprimento 1 (laços do grafo funcional).*

Demostração. Usando (4.1), temos

$$f^{(2)}(x,y)=f(2cx^2,2cxy)=\langle 8c^3x^4,8c^3x^3y\rangle.$$

Por indução, podemos provar que $f^{(n)}(x,y)=\langle (2c)^{2^n-1}x^{2^n},(2cx)^{2^n-1}y\rangle$, para todo $n\in\mathbb{N}$. Suponha a asserção verdadeira para $n-1$. Então,

$$\begin{aligned} f^{(n)}(x,y) &= f\left((2c)^{2^{n-1}-1}x^{2^{n-1}},(2cx)^{2^{n-1}-1}y\right)\\ &= \langle (2c)\left((2c)^{2^{n-1}-1}x^{2^{n-1}}\right)^2,2c(2c)^{2^{n-1}-1}x^{2^{n-1}}(2cx)^{2^{n-1}-1}y\rangle\\ &= \langle (2c)^{2^n-1}x^{2^n},(2c)^{2^n-1}x^{2^n-1}y\rangle. \end{aligned}$$

Isso prova $f^{(n)}(x,y)=\langle (2c)^{2^n-1}x^{2^n},(2cx)^{2^n-1}y\rangle=(2cx)^{2^n-1}\langle x,y\rangle$, para todo $n\in\mathbb{N}$.

Seja $\langle x,y\rangle\neq\langle 0,0\rangle$ um elemento de um ciclo de comprimento $n\geq 1$. Nesse caso, $f^{(n)}(x,y)=\langle x,y\rangle$ e n é o menor inteiro positivo tal que $(2cx)^{2^n-1}=1$. Como no Teorema 2.3.3, escrevemos $\theta=2cx\in\mathbb{F}_q^*$. Portanto, 2^n-1 é um múltiplo de $\mathrm{Ord}(\theta)$ e para todo $m<n$, 2^m-1 não é um múltiplo de $\mathrm{Ord}(\theta)$. Tal n existe se, e somente se, $\mathrm{Ord}(\theta)$ for ímpar (de forma similar à Afirmação 2.3.4). Observe que n é o menor inteiro positivo satisfazendo $2^n\equiv 1 \pmod{\mathrm{Ord}(\theta)}$. Como $\theta\in\mathbb{F}_q^*$ e $\mathbb{F}_q^*$ é um grupo cíclico de ordem $q-1$, então $d=\mathrm{Ord}(\theta)$ é um divisor ímpar de $q-1$. Além disso, $n=\mathrm{Ord}_d(2)$.

Seja α um gerador de $\mathbb{F}_q^*$. Para cada divisor ímpar d de $q-1$ (como visto no Teorema 2.3.3) existem $\varphi(d)$ escolhas para j de forma que $\mathrm{Ord}\,(\alpha^j)=d$ e q pares ordenados $\langle x,y\rangle$ tais que $2cx=\alpha^j$ (ou seja, para cada j temos um único valor de x e q escolhas para y em $\mathbb{F}_q$). Consequentemente, o número de elementos nos ciclos de comprimento $\mathrm{Ord}_d(2)$ é $q\cdot\varphi(d)$. Logo, há $\frac{q\cdot\varphi(d)}{\mathrm{Ord}_d(2)}$ ciclos de comprimento $\mathrm{Ord}_d(2)$.

Note que, se $d=1$, então $\mathrm{Ord}_1(2)=1$ e temos $\frac{q\cdot\varphi(d)}{\mathrm{Ord}_d(2)}=q$ ciclos de comprimento um, além do ciclo do elemento zero. Isto é, há $q+1$ ciclos de comprimento um. □

Por fim, para descrever completamente o grafo funcional de $f(X)$, basta entender o comportamento dos pré-ciclos. Com o seguinte lema, concluiremos que os pré-ciclos do grafo funcional de $f(X)$, com $a=1$, são exatamente os mesmos do caso $a=-1$.

3.4 Descrição dos pré-ciclos

Lema 3.4.1. *Seja $\alpha\in\mathbb{F}_{q^2}\backslash\beta\mathbb{F}_q$. Escrevendo $\alpha=u+v\beta$, onde $u,v\in\mathbb{F}_q$ e $v\neq 0$, temos $\#f^{-1}(\alpha)\in\{0,2\}$.*

Demostração. *Se $\alpha=u+v\beta$ e $X=x+y\beta\in f^{-1}(\alpha)$, então*

$$2cx^2+2cxy\beta=u+v\beta$$

Se $u=0$, temos $2cx^2=0$, e assim $v=0-$absurdo. Portanto $\#f^{-1}(\alpha)=0$.
Se $\chi_2(u)\chi_2((2c)^{-1})=\chi_2(2cu)=-1$ então x^2 não é um quadrado. Portanto, $\#f^{-1}(\alpha)=0$.
Em resumo, se $u=0$ ou $\chi_2(2cu)=-1$, então $f^{-1}(\alpha)=\emptyset$.

Se $\chi_2(2cu) = 1$, *então existe* $x \in \mathbb{F}_q$ *tal que* $x^2 = \frac{u}{2c}$ *e* $y = \frac{v}{2cx}$. *Como* $\pm x$ *são ambas soluções, essas são as únicas, logo* $\#f^{-1}(\alpha) = 2$.

□

Usando $Cyc(\mathscr{G})$ como na Definição 2.4.1, onde $\mathscr{G}$ agora é o grafo funcional da função $f(X) = c\left(X^{q+1} + X^2\right)$, o seguinte teorema segue com a mesma prova do Teorema 2.4.2, apenas substituindo $-2bcy^2$ por $2cx^2$.

Concluindo, o grafo funcional da função $c\left(X^{q+1} + X^2\right)$ tem uma componente conexa isomorfa a $\mathcal{Z}^*(q)$, na qual zero é o ponto fixo. Além disso, escrevendo $q - 1 = 2^s r$, com r inteiro positivo ímpar, temos que para cada divisor d de r, há $\frac{q \cdot \varphi(d)}{\mathrm{Ord}_d(2)}$ componentes conexas isomorfas a $\left(Cyc\left(\mathrm{Ord}_d(2)\right), \mathcal{T}(s)\right)$.

3.5 Teorema principal

Teorema 3.5.1. *Se* $q - 1 = 2^s r$, *com* r *ímpar, então o grafo funcional da função* $f(X) = c\left(X^{q+1} + X^2\right)$ *sobre* $\mathbb{F}_{q^2}$ *é isomorfo a*

$$\mathscr{G} = \mathcal{Z}^*(q) \bigoplus_{d|r} \frac{q \cdot \varphi(d)}{\mathrm{Ord}_d(2)} \times \left(Cyc\left(\mathrm{Ord}_d(2)\right), \mathcal{T}(s)\right).$$

3.5.1 Exemplos

Exemplo 3.5.2. *Sejam* $q = 7$, $b = 3$ *e* $c = 2$. *Como* $q - 1 = 2 \cdot 3$, *então temos árvores isomorfas a* $\mathcal{T}(1)$ *anexadas a cada ponto periódico. Observe que os divisores ímpares de* $q - 1$ *são* 1 *e* 3, *assim os comprimentos dos ciclos devem ser* $\mathrm{Ord}_1(2) = 1$ *e* $\mathrm{Ord}_3(2) = 2$. *Logo, o grafo funcional estará composto por uma componente conexa isomorfa a* $\mathcal{Z}^*(7)$ *(ver Figura 3.2),*

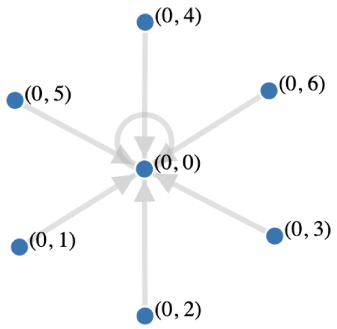


Figura 3.2: Componente conexa $\mathcal{Z}^*(7)$ para $a = 1$.

$\frac{7 \cdot 1}{1} = 7$ *componentes conexas isomorfas a* $\left(Cyc\left(\mathrm{Ord}_1(2)\right), \mathcal{T}(1)\right)$ *(ver Figura 3.3)*

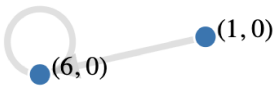


Figura 3.3: $\left(Cyc\left(\mathrm{Ord}_1(2)\right), \mathcal{T}(1)\right)$.

e $\frac{7 \cdot \varphi(3)}{2} = \frac{7 \cdot 2}{2} = 7$ *componentes conexas isomorfas a* $\left(Cyc\left(\mathrm{Ord}_3(2)\right), \mathcal{T}(1)\right)$ *(ver Figura 3.4).*

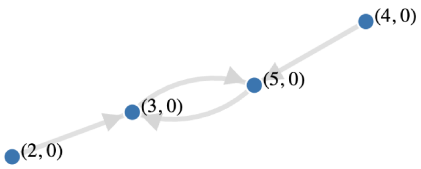


Figura 3.4: Componente conexa $(Cyc\left(\mathrm{Ord}_3(2)\right), \mathcal{T}(1))$.

Em outras palavras, o grafo funcional de $f(X) = 2\left(X^8 + X^2\right)$ *sobre* $\mathbb{F}_{7^2}$ *é*

$$\mathscr{G} = \mathcal{Z}^*(7) \oplus 7 \times (Cyc(1), \mathcal{T}(1)) \oplus 7 \times (Cyc(2), \mathcal{T}(1)). \tag{3.3}$$

Exemplo 3.5.3. *Sejam* $q = 5$, $b = 2$ *e* $c = 3$. *Como* $q - 1 = 2^2$, *então temos árvores isomorfas a* $\mathcal{T}(2)$ *anexadas a cada ponto periódico diferente de* $\langle 0, 0\rangle$. *Observe que o único divisor ímpar de* $q - 1$ *é* 1. *Assim, o único comprimento de ciclo que existe é* $\mathrm{Ord}_1(2) = 1$. *Logo, o grafo funcional estará composto por uma componente conexa isomorfa a* $\mathcal{Z}^*(5)$ *(ver Figura 3.5),*

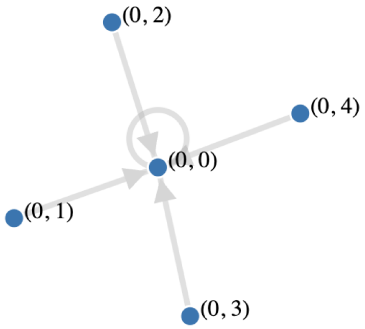


Figura 3.5: Componente conexa $\mathcal{Z}^*(5)$ para $a = 1$.

e $\frac{5\cdot 1}{1} = 5$ *componentes conexas isomorfas a* $(Cyc(1), \mathcal{T}_2)$ *(ver Figura 3.6).*

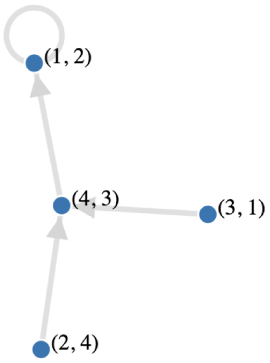


Figura 3.6: Componente conexa $(Cyc(1), \mathcal{T}_2)$.

Exemplo 3.5.4. *Sejam* $q = 13$, $b = 11$ *e* $c = 3$. *Como* $q - 1 = 2^2 \cdot 3$, *então temos árvores isomorfas a* $\mathcal{T}(2)$ *anexadas a cada ponto periódico diferente de* $\langle 0, 0\rangle$. *Observe que os únicos divisores ímpares de* $q - 1$ *são* 1 *e* 3. *Assim, os únicos comprimentos de ciclos que existem são o*$\mathrm{Ord}_1(2) = 1$ *e* $\mathrm{Ord}_3(2) = 2$. *Logo, o grafo funcional estará composto por uma componente conexa isomorfa a* $\mathcal{Z}^*(13)$ *(ver Figura 3.7),*

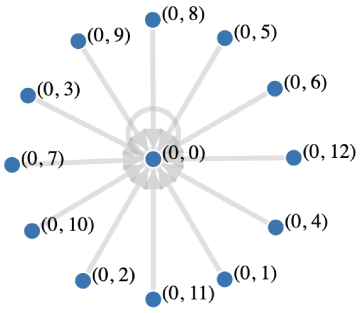


Figura 3.7: Componente conexa $\mathcal{Z}^*(13)$.

$\frac{13 \cdot 1}{1} = 13$ *componentes conexas isomorfas a* $(Cyc(1), \mathcal{T}_2)$ *(ver Figura 3.8)*

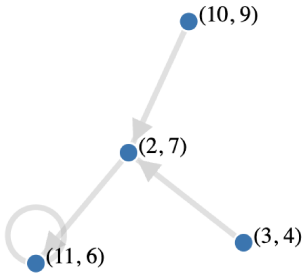


Figura 3.8: Componente conexa $(Cyc(1), \mathcal{T}_2)$.

e $\frac{13 \cdot 2}{2} = 13$ *componentes conexas isomorfas a* $(Cyc(2), \mathcal{T}_2)$ *(ver Figura 3.9).*

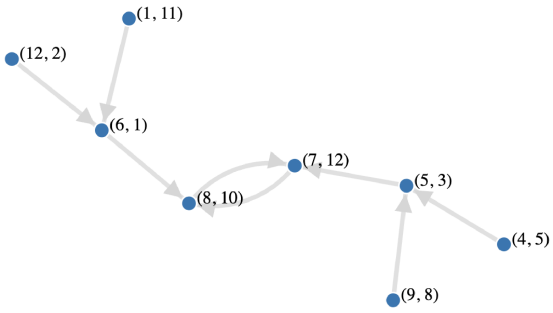


Figura 3.9: Componente conexa $(Cyc(2), \mathcal{T}_2)$.

Capítulo 4

Resultados parciais para $a \notin \{\pm 1\}$

Antes de prosseguirmos, apresentamos o Lema 4.0.1, que é importante pois mostra que os grafos funcionais das funções $f_c(X) = cX(X^q + aX)$ e $f(X) = X(X^q + aX)$ são isomorfos sobre $\mathbb{F}_{q^2}$, ou seja, $\mathscr{G}_f \cong \mathscr{G}_{f_c}$.

Lema 4.0.1. *Para todo $c \in \mathbb{F}_q^*$, os grafos funcionais de $f_c(X) = cX(X^q + aX)$ e $f(X) = X(X^q + aX)$ são isomorfos sobre $\mathbb{F}_{q^2}$.*

Demostração. Considere a função $\theta : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ definida por:

$$\theta(x) = cx,$$

com $c \in \mathbb{F}_q^*$.
Provemos que a função θ é bijetora. Sejam $x_1, x_2, x, y \in \mathbb{F}_{q^2}$. Se $\theta(x_1) = \theta(x_2)$, então $cx_1 = cx_2$. Como $c \neq 0$, então $x_1 = x_2$. Isto é, θ é injetora. Como $\mathbb{F}_{q^2}$ é um conjunto finito, então θ também é sobrejetora.
A bijeção θ entre os vértices induz naturalmente uma bijeção entre as arestas E_c do grafo funcional de f_c e as arestas E do grafo funcional de f:

$$\varphi : E_c \to E, \quad \varphi((x, f_c(x))) = (\theta(x), \theta(f_c(x))) = (\theta(x), f(\theta(x)))\,.$$

Essa correspondência é válida porque a relação funcional é preservada:

$$f(\theta(x)) = cX\left((cX)^q + acX\right) = cX\left(cX^q + acX\right) = c\left(cX\left(X^q + aX\right)\right) = \theta\left(f_c(x)\right).$$

O comportamento da bijeção pode ser visualizado no seguinte diagrama comutativo:

$$\begin{array}{ccc} x & \xrightarrow{\quad f_c \quad} & f_c(x) \\ \Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle \theta} \\ \theta(x) = cx & \xrightarrow{\quad f \quad} & f\left(\theta(x)\right) = \theta\left(f_c(x)\right) \end{array}$$

Esse diagrama ilustra que $\theta(f_c(x)) = f\left(\theta(x)\right)$, ou seja, a aplicação θ respeita a estrutura funcional do grafo.

Portanto, a função $\theta(x) = cx$, com $c \in \mathbb{F}_q^*$, define um isomorfismo entre os grafos $\mathscr{G}_{f_c}$ e $\mathscr{G}_f$. Como θ é uma bijeção entre os vértices, preserva as conexões entre vértices (isto é, as arestas são levadas em arestas), e satisfaz $\theta(f_c(x)) = f\left(\theta(x)\right)$, garantindo que a estrutura dos grafos é a mesma.

Assim,

$$\mathscr{G}_f \cong \mathscr{G}_{f_c}.$$

□

A partir de agora, assumimos $c = 1$ e $f(X) = X\left(X^q + aX\right)$, com $a \neq \pm 1$.

4.1 Determinação dos pontos fixos da função $f(X)$ quando $a \notin \{\pm 1\}$

Como nos capítulos anteriores, consideramos a base $\{1, \beta\}$ de $\mathbb{F}_{q^2}$, com $\beta^2 = b \in \mathbb{F}_q$. Relembramos que valem as seguintes relações

$$\beta^q = -\beta \quad \text{e} \quad \beta^{q+1} = -b = -\beta^2.$$

Proposição 4.1.1. *Para todos $x, y \in \mathbb{F}_q$, temos*

$$f(x + y\beta) = (a+1)x^2 + (a-1)by^2 + 2axy\beta.$$

Demonstração. Considerando $\alpha = x + y\beta \in \mathbb{F}_{q^2}$, com $x, y \in \mathbb{F}_q$, temos

$$\begin{aligned} f(\alpha) &= \alpha\left(\alpha^q + a\alpha\right) = (x+y\beta)(x+y\beta^q + a(x+y\beta)) \\ &= (x+y\beta)(x - y\beta + a(x+y\beta)) = (x+y\beta)((1+a)x + (a-1)y\beta) \\ &= \left((1+a)x^2 + (a+1)xy\beta + (a-1)xy\beta + (a-1)y^2\beta^2\right) \\ &= \left((a+1)x^2 + (a-1)by^2\right) + 2axy\beta. \end{aligned}$$

□

Usando a base $\{1, \beta\}$, identificamos $\mathbb{F}_{q^2}$ com $\mathbb{F}_q^2$. Um elemento $\alpha \in \mathbb{F}_{q^2}$ é representado da forma $\alpha = x + y\beta$ ou $\alpha = \langle x, y\rangle$. Podemos então reescrever a função $f(X)$ da seguinte forma:

$$\begin{array}{rccc} f: & \mathbb{F}_q^2 & \longrightarrow & \mathbb{F}_q^2 \\ & \langle x, y\rangle & \longmapsto & \langle (a+1)x^2 + (a-1)by^2, 2axy\rangle . \end{array} \tag{4.1}$$

Lema 4.1.2. *A função $f(X) = X^{q+1} + aX^2$, com $a \in \mathbb{F}_q \setminus \{0, 1, -1\}$, possui como pontos fixos $\langle 0, 0\rangle$ e $\left\langle \frac{1}{a+1}, 0\right\rangle$, sendo $\langle 0, 0\rangle$ um ponto fixo sem pré-ciclo.*

Demostração. Calculemos primeiro $f^{-1}(0,0)$. Se $\alpha = x + y\beta \in \mathbb{F}_{q^2}$ satisfaz $f(x + y\beta) = 0$, então

$$(a+1)x^2 + (a-1)by^2 = 0 \quad \text{e} \quad 2axy = 0.$$

Como $a \neq 0$, então $x = 0$ ou $y = 0$.

Se $x = 0$, então $(a-1)by^2 = 0$. Como $a \neq 1$, então $y = 0$. De forma similar, se $y = 0$, então $(a+1)x^2 = 0$. Como $a \neq -1$, então $x = 0$. Isso implica $f^{-1}(0,0) = \{\langle 0, 0\rangle\}$. Logo, zero é um ponto fixo sem pré-ciclo.

Note que se $\langle x, y\rangle$ for outro ponto fixo, então ele deve satisfazer as seguintes equações:

$$\begin{cases} (a+1)x^2 + (a-1)by^2 = x \\ 2axy = y \end{cases}$$

Se $y \neq 0$, a segunda equação implica $x = \frac{1}{2a}$. Substituindo esse valor de x na primeira equação, temos

$$\begin{aligned}
\frac{a+1}{4a^2} + (a-1)by^2 &= \frac{1}{2a} \\
y^2 &= \left(\frac{1}{2a} - \frac{a+1}{4a^2}\right)\frac{1}{(a-1)b} \\
y^2 &= \left(\frac{2a-(a+1)}{4a^2}\right)\frac{1}{(a-1)b} \\
y^2 &= \left(\frac{a-1}{4a^2}\right)\frac{1}{(a-1)b} \\
y^2 &= \frac{1}{4ba^2}.
\end{aligned}$$

Como b não é um quadrado em $\mathbb{F}_q$, essa equação não tem solução. Isso implica $y = 0$. Nesse caso, temos

$$\begin{aligned}
(a+1)x^2 + (a-1)b \cdot 0 &= x \\
x^2 &= \frac{x}{a+1}.
\end{aligned}$$

Como $\langle x, y\rangle \neq \langle 0, 0\rangle$, então $x \neq 0$. Logo, $x = \frac{1}{a+1}$ e $\left\langle \frac{1}{a+1}, 0\right\rangle$ é o único ponto fixo de f diferente de $\langle 0, 0\rangle$. □

4.2 Analise das pré-imagens

Agora analisaremos as pré-imagens de dois tipos distintos de pontos: $\hat{x}$ e $\hat{x}\beta$, sendo $\hat{x} \in \mathbb{F}_q$.

Teorema 4.2.1. *Para $\hat{x} \in \mathbb{F}_q^*$, temos:*

1. $\#f^{-1}(\hat{x}) = \begin{cases} 0 & \text{se } \chi_2(\hat{x}(a-1)) = 1 \text{ e } \chi_2(\hat{x}(a+1)) = -1, \\ 4 & \text{se } \chi_2(\hat{x}(a-1)) = -1 \text{ e } \chi_2(\hat{x}(a+1)) = 1, \\ 2 & \text{caso contrário.} \end{cases}$

2. *Se $q \equiv 3 \pmod 4$, então*

$$\#f^{-1}(\alpha\beta) = \begin{cases} 0 & \text{se } \chi_2\left(-a^2+1\right) = 1, \\ 2 & \text{se } \chi_2\left(-a^2+1\right) = -1. \end{cases}$$

3. *Se $q \equiv 1 \pmod 4$, então*

$$\#f^{-1}(\hat{x}\beta) = \begin{cases} 4 & \text{se } \chi_2\left(-a^2+1\right) = -1 \text{ e } \chi_2\left(2\gamma_a \hat{x} a\right) = -1, \\ 0 & \text{caso contrário.} \end{cases}$$

em que $\gamma_a^2 = -\frac{(a-1)b}{a+1}$.

Demostração. Se $\hat{x} \in \mathbb{F}_q$, então $\langle x, y\rangle \in f^{-1}(\hat{x})$ implica

$$\left\langle (a+1)x^2 + (a-1)by^2, 2axy\right\rangle = \langle \hat{x}, 0\rangle .$$

Logo,

$$\begin{cases} (a+1)x^2 + (a-1)by^2 &= \hat{x}, \\ 2axy &= 0. \end{cases}$$

Se $x = 0$, temos $y^2 = \frac{\hat{x}}{(a-1)b}$, que possui duas soluções se $\chi_2(\hat{x}(a-1)) = -1$ e nenhuma solução caso contrário.

Se $y = 0$, temos $x^2 = \frac{\hat{x}}{a+1}$, que possui duas soluções se $\chi_2(\hat{x}(a+1)) = 1$ e nenhuma solução caso contrário. Isso prova o primeiro resultado.

Seja $\langle x, y\rangle \in f^{-1}(0, \hat{x})$. Nesse caso,

$$\begin{cases} (a+1)x^2 + (a-1)by^2 &= 0, \\ 2axy &= \hat{x}. \end{cases}$$

De forma equivalentemente, temos

$$\begin{cases} \left(\frac{x}{y}\right)^2 &= -\frac{(a-1)b}{a+1}, \\ xy &= \frac{\hat{x}}{2a}. \end{cases}$$

A primeira equação tem solução se, e somente se, $\chi_2\left(-a^2+1\right) = -1$, já que $\chi_2(b) = -1$.

Supondo que $\chi_2\left(-a^2+1\right) = -1$, existe $\gamma_a \in \mathbb{F}_q$ tal que $\gamma_a^2 = -\frac{(a-1)b}{a+1}$. Então,

$$x^2 = \frac{x}{y} \cdot xy = \pm\gamma_a \cdot \frac{\hat{x}}{2a} = \pm\frac{\gamma_a \hat{x}}{2a}.$$

Se $q \equiv 3 \pmod 4$, então

$$x^2 = \pm\frac{\gamma_a \hat{x}}{2a}$$

possui duas soluções, pois -1 não é um quadrado e podemos escolher o sinal de modo que a equação possua solução. Denotando x_1, x_2 as duas soluções da equação acima e escrevendo $y_i = \frac{\hat{x}}{2ax_i}$, para $i \in \{1, 2\}$, obtemos

$$f^{-1}(\hat{x}\beta) = \{\langle x_1, y_1\rangle, \langle x_2, y_2\rangle\}.$$

Suponha agora $q \equiv 1 \pmod 4$. Nesse caso, -1 é um quadrado em $\mathbb{F}_q$ e

$$x^2 = \pm\frac{\gamma_a \hat{x}}{2a}$$

possui 4 soluções se $\chi_2\left(2\gamma_a \hat{x} a\right) = 1$ ou nenhuma solução caso $\chi_2\left(2\gamma_a \hat{x} a\right) = -1$, concluindo assim a prova. □

O seguinte corolário é uma consequência direta da prova do teorema anterior.

Corolário 4.2.2. *Se $\hat{x} \in \mathbb{F}_q^*$ e $\chi_2(\hat{x}(a-1)) = 1$, então $f^{-1}(\hat{x}) \subseteq \mathbb{F}_q$.*

Demostração. Como $\chi_2(\hat{x}(a-1)) = 1$, de acordo com o teorema anterior, temos $f^{-1}(\hat{x})$ não vazio se $\chi_2(\hat{x}(a+1)) = 1$. Nesse caso, $\langle x, y\rangle \in f^{-1}(\hat{x})$ se $y = 0$. □

Proposição 4.2.3. *A restrição de f a $\mathbb{F}_q$ está dada por*

$$\begin{array}{rccc} f|_{\mathbb{F}_q}: & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ & x & \longmapsto & (a+1)x^2. \end{array}$$

Se $q - 1 = 2^s r$, com r ímpar, então o grafo funcional de f sobre $\mathbb{F}_q$ é isomorfo a

$$Cyc(1) \bigoplus_{d|r} \frac{\varphi(d)}{\mathrm{Ord}_d(2)} \times \left(Cyc\left(\mathrm{Ord}_d(2)\right), \mathcal{T}(s)\right).$$

Demostração. Claramente, restringindo f a $\mathbb{F}_q$, temos

$$\begin{array}{rccc} f|_{\mathbb{F}_q}: & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ & x & \longmapsto & (a+1)x^2. \end{array}$$

Defina $\varphi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ dada por $\varphi(x) = \lambda x$, em que $\lambda \in \mathbb{F}_q^*$ é fixo. Observamos que φ é um automorfismo de $\mathbb{F}_q$ e que $(\hat{x}, f(\hat{x}))$ é uma aresta do grafo funcional de f restrito a $\mathbb{F}_q$ se, e somente se, $(\varphi^{-1}(\hat{x}), \varphi^{-1}(f(\hat{x})))$ é uma aresta do grafo funcional de $\varphi^{-1} \circ f \circ \varphi$ sobre $\mathbb{F}_q$. Isso pode ser visto, através do seguinte diagrama.

$$\begin{array}{ccc} \mathbb{F}_q & \xrightarrow{\quad f \quad} & \mathbb{F}_q \\ {\scriptstyle\varphi}\uparrow & & \uparrow{\scriptstyle\varphi} \\ \mathbb{F}_q & \xrightarrow[\varphi^{-1}\circ f\circ\varphi]{} & \mathbb{F}_q \end{array}$$

Veja que, escolhendo $\lambda = (a+1)^{-1}$, obtemos

$$\begin{aligned} \varphi^{-1} \circ f \circ \varphi(x) &= f^{-1} \circ f\left((a+1)^{-1}x\right) \\ &= \varphi^{-1}\left((a+1)\left((a+1)^{-1}x\right)^2\right) \\ &= \varphi^{-1}\left((a+1)\cdot(a+1)^{-2}\cdot x^2\right) \\ &= (a+1)(a+1)(a+1)^{-2}\cdot x^2 = x^2. \end{aligned}$$

Assim, podemos concluir que o grafo de $f|_{\mathbb{F}_q}$ é isomorfo ao grafo de x^2. De (Rogers, 1996, Section 4), considerando $\mathbb{F}_q^*$ como um grupo multiplicativo cíclico de ordem par $q-1 = 2^s r$, com r ímpar, temos que o grafo funcional de x^2 sobre $\mathbb{F}_q^*$ é isomorfo a

$$\bigoplus_{d|r} \frac{\varphi(d)}{\mathrm{Ord}_d(2)} \times \left(Cyc\left(\mathrm{Ord}_d(2)\right), \mathcal{T}(s)\right).$$

Concluímos adicionando o laço isolado em $0 \in \mathbb{F}_q$. □

Dessa forma, o comportamento de $f|_{\mathbb{F}_q}$ é bem conhecido e aqui será denotado simplesmente como $\mathscr{G}\left(f|_{\mathbb{F}_q}\right)$.

Teorema 4.2.4. *Seja r um número inteiro positivo ímpar tal que $q-1 = 2^s r$ e seja $f(X) = c\left(X^{q+1} + aX^2\right)$, em que $a \in \mathbb{F}_q \setminus \{0, 1, -1\}$. Se $\chi_2\left(1-a^2\right) = 1$, então as componentes conexas que contêm os elementos de $\mathbb{F}_q$ podem ser obtidos anexando dois nós a cada ponto $\hat{x} \in \mathscr{G}\left(f|_{\mathbb{F}_q}\right)$ que satisfaz $\chi_2(\hat{x}(a-1)) = -1$. Em particular, 0 é um ponto fixo isolado e $\frac{1}{a+1}$ é um ponto fixo com componente conexa isomorfa a $\mathcal{Z}^*(4)$ se $s = 1$, ou isomorfa a $(\mathrm{Cyc}(1), \mathcal{T}(s+1))$ se $s \geq 2$.*

Demostração. Quando $\chi_2\left(1-a^2\right) = 1$, do Corolário 4.2.2 concluímos que para cada ponto $\hat{x} \in \mathscr{G}\left(f|_{\mathbb{F}_q}\right)$, se $\chi_2(\hat{x}(a-1)) = 1$, então não há pontos fora de $\mathscr{G}\left(f|_{\mathbb{F}_q}\right)$ em sua pré-imagem. Por outro lado, se $\chi_2(\hat{x}(a-1)) = -1$, então há exatamente dois pontos fora de $\mathscr{G}\left(f|_{\mathbb{F}_q}\right)$ em sua pré-imagem: $\{\lambda_{\hat{x}}, -\lambda_{\hat{x}}\} \in \beta\mathbb{F}_q$ tal que $\lambda_{\hat{x}}^2 = \frac{\hat{x}}{(a-1)b}$. Além disso, $\pm\lambda_{\hat{x}}$ não têm pré-imagem.

Em particular, podemos descrever precisamente o pré-ciclo do ponto fixo $\left\langle \frac{1}{a+1}, 0\right\rangle$. Primeiro, assumindo $q \equiv 3 \pmod 4$, observe que a pré-imagem de $\left\langle \frac{1}{a+1}, 0\right\rangle$ tem 4 elementos. Como visto na prova do Teorema 4.2.1, eles são $\left\langle \pm\frac{1}{a+1}, 0\right\rangle$ e $\langle 0, \pm\lambda\rangle$, para $\lambda^2 = \frac{1}{(a^2-1)b}$. Como $\chi_2\left(1-a^2\right) = 1$, pela parte 2 do Teorema 4.2.1, temos $\#f^{-1}(0, \pm\lambda) = \langle 0, 0\rangle$. Como $\chi_2(-1) = -1$, então

pela parte 1 do mesmo Teorema, temos $\#f^{-1}\left(-\frac{1}{a+1},0\right)=\langle 0,0\rangle$. Em conclusão, a componente conexa de $\frac{1}{a+1}$ é isomorfa a $\mathcal{Z}^*(4)$.

Agora, para $q\equiv 1 \pmod 4$, a pré-imagem de $\frac{1}{a+1}$ é

$$f^{-1}\left(\frac{1}{a+1},0\right)=\left\{\left\langle\frac{1}{a+1},0\right\rangle,\left\langle-\frac{1}{a+1},0\right\rangle\right\}.$$

Como -1 é um quadrado, a pré-imagem de $\left\langle-\frac{1}{a+1},0\right\rangle$ tem 2 elementos:

$$f^{-1}\left(-\frac{1}{a+1},0\right)=\left\{\left\langle\pm\frac{\zeta_4}{a+1},0\right\rangle\right\}$$

em que ζ_n é uma raiz primitiva n-ésima da unidade em $\mathbb{F}_q$. Se $q\equiv 5 \pmod 8$, então ζ_4 não é um quadrado e

$$f^{-1}\left(\frac{\zeta_4}{a+1},0\right)=\{\langle 0,\pm\lambda\rangle\},$$

para $\lambda^2=\frac{\zeta_4}{(a^2-1)b}$. Observe que a partir deste caso em diante -1 é um quadrado, portanto $-\zeta_4$ também não é um quadrado. Além disso, observe que este é o último nível da árvore, uma vez que $\chi_2\left(-a^2+1\right)=1$ e a parte 3 do Teorema 4.2.1 implica que $\#f^{-1}(0,\pm\lambda)=\langle 0,0\rangle$.

Se $q\equiv 1 \pmod 8$, então ζ_4 é um quadrado e

$$f^{-1}\left(\frac{\zeta_4}{a+1},0\right)=\left\{\left\langle\pm\frac{\zeta_8}{a+1},0\right\rangle\right\}.$$

Suponhamos que $q\equiv 1 \pmod{2^n}$ para algum $n\geq 3$. Pela hipótese de indução, uma vez que $\pm\zeta_{2^{n-1}}$ é um quadrado em $\mathbb{F}_q$, segue que

$$f^{-1}\left(\frac{\zeta_{2^{n-1}}}{a+1},0\right)=\left\{\left\langle\pm\frac{\zeta_{2^n}}{a+1},0\right\rangle\right\}.$$

Além disso, se $q\equiv 2^{n-1}+1 \pmod{2^n}$, então $\zeta_{2^{n-1}}\in\mathbb{F}_q$ não é um quadrado em $\mathbb{F}_q$ e

$$f^{-1}\left(\frac{\zeta_{2^{n-1}}}{a+1},0\right)=\{\langle 0,\pm\lambda\rangle\},$$

com $\lambda^2=\frac{\zeta_{2n-1}}{(a^2-1)b}$. Seguindo um processo semelhante ao Teorema 2.4.2, obtemos o resultado. □

Exemplo 4.2.5. *Para $q=13$ e $a=2$, temos $s=2$ e $\chi_2(1-2^2)=\chi_2(10)=1$. Tomando $b=2$, as componentes conexas dos elementos em $\mathbb{F}_q$ são isomorfas a $Cyc(1)$, $(Cyc(1),\mathcal{T}(3))$ e $(Cyc(2),\mathcal{T}(3))$ (ver Figura 4.1).*

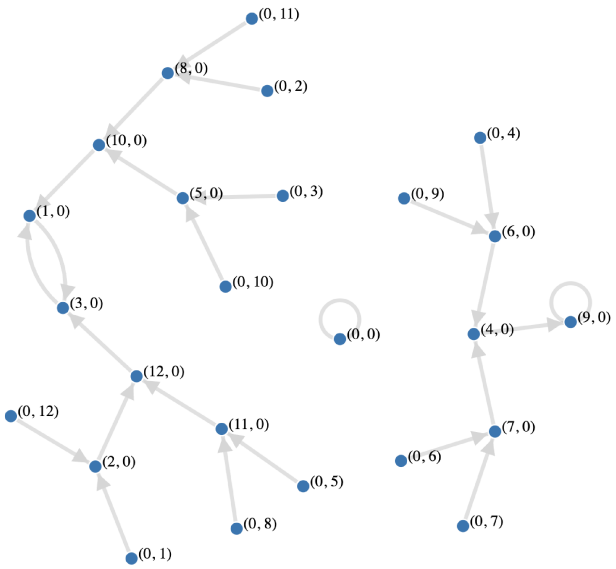


Figura 4.1: Componentes conexas dos elementos de $\mathbb{F}_q$.

A componente que contém zero é um ciclo isolado, a componente de $\frac{1}{a+1} = 9$ *é isomorfa a* $(Cyc(1), \mathcal{T}(3))$ *e todos os pontos* $\hat{x} \in \mathbb{F}_q$ *que satisfazem* $\chi_2(\hat{x}(a-1)) = -1$ *têm dois pontos em* $\beta\mathbb{F}_q$ *direcionados a eles.*

Quando $\chi_2(1-a^2) = -1$, as condições que controlam o crescimento de tais componentes são mais difíceis de obter. Por exemplo, se $q \equiv 3 \pmod 4$, para fazer com que essas árvores tenham exatamente um nível a mais, ou seja, que os elementos em $\beta\mathbb{F}_q$ estejam ligados aos pontos $\hat{x} \in \mathscr{G}\left(f|_{\mathbb{F}_q}\right)$ que satisfazem $\chi_2(\hat{x}(a-1)) = -1$ e têm duas pré-imagens que não têm pré-imagem, devemos exigir que $ba^2 + (a+1)^2$ seja um quadrado em $\mathbb{F}_q$.

Nos exemplos seguintes, mostraremos a componente conexa que contém $\frac{1}{a+1}$ para $\chi_2(1-a^2) = -1$.

Exemplo 4.2.6. *Sejam* $q = 13$, $b = 2$ *e* $a = 3$. *Mais uma vez,* $\chi_2(1-3^2) = -1$. *Então, a componente conexa do ponto fixo* $\langle (a+1)^{-1}, 0\rangle = \langle 4^{-1}, 0\rangle = \langle 10, 0\rangle$ *no grafo funcional de* $f(X) = X^{q+1} + 3X^2$ *sobre* $\mathbb{F}_{13^2}$ *é o grafo da Figura 4.2.*

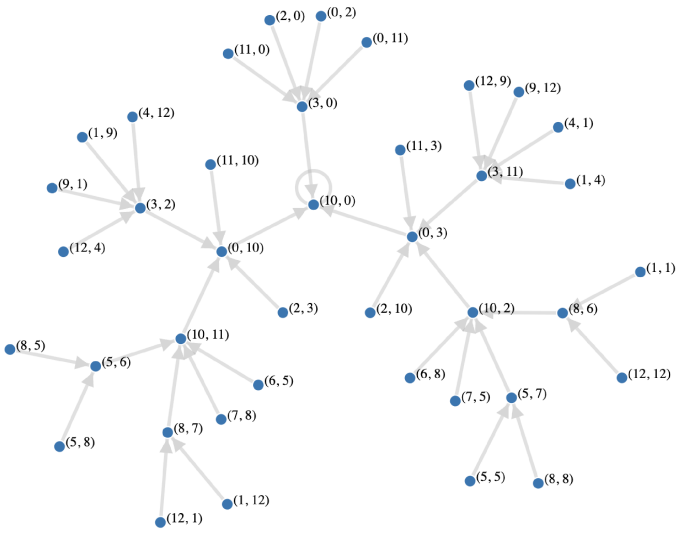


Figura 4.2: Componente conexa do ponto fixo $\langle 4^{-1}, 0\rangle = \langle 10, 0\rangle$ no grafo funcional $f(X) = X^{q+1} + 3X^2$ sobre $\mathbb{F}_{13^2}$.

Exemplo 4.2.7. *Sejam* $q = 19$, $b = 2$ *e* $a = 5$. *Note que* $\chi_2(1-5^2) = -1$. *Então, a componente conexa do ponto fixo* $\langle 6^{-1}, 0\rangle = \langle 16, 0\rangle$ *no grafo funcional de* $f(X) = X^{q+1} + 5X^2$ *sobre* $\mathbb{F}_{19^2}$ *é o grafo da Figura 4.3.*

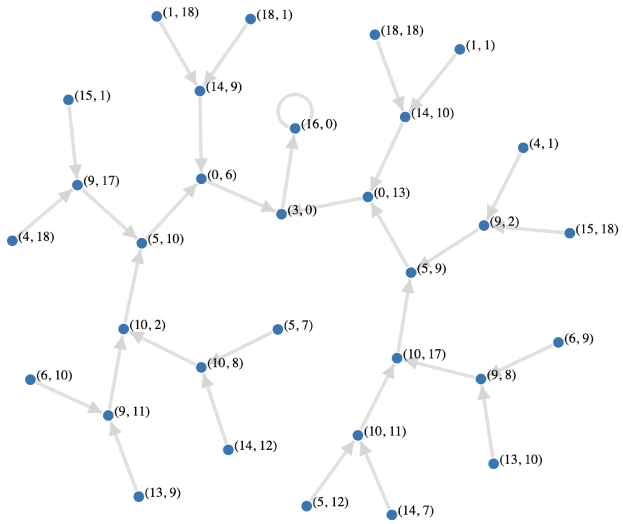


Figura 4.3: Componente conexa de $\langle (a+1)^{-1}, 0\rangle = \langle 16, 0\rangle$.

O comportamento de outros ciclos e pré-ciclos quando $a \notin \{\pm 1\}$ também é difícil de prever. Por exemplo, pode haver ciclos com o mesmo comprimento, mas com pré-ciclos diferentes, como visto no próximo exemplo.

Exemplo 4.2.8. *Seja* $q = 29$ *e* $a = 3$. *Então, o grafo funcional de* $f(X) = X^{q+1} + 3X^2$ *sobre* $\mathbb{F}_{29^2}$ *terá quatro tipos diferentes de componentes conexas. Um ciclo de comprimento 1 sem pré-ciclo, cujo vértice é* 0. *Outro ciclo de comprimento* 1, *com vértice em* $\langle (a+1)^{-1}, 0\rangle = \langle 22, 0\rangle$, *mas com um pré-ciclo, como visto na Figura 4.4.*

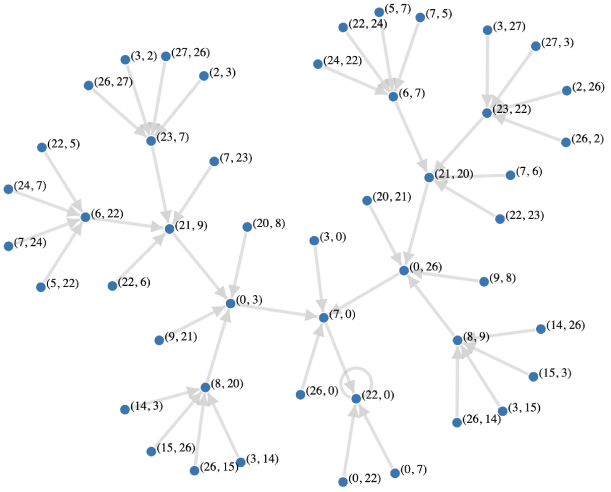


Figura 4.4: Componente conexa de $\langle (a+1)^{-1}, 0\rangle = \langle 22, 0\rangle$.

Três ciclos de comprimento 3, *com seus respectivos pré-ciclos isomorfos ao grafo da Figura 4.5.*

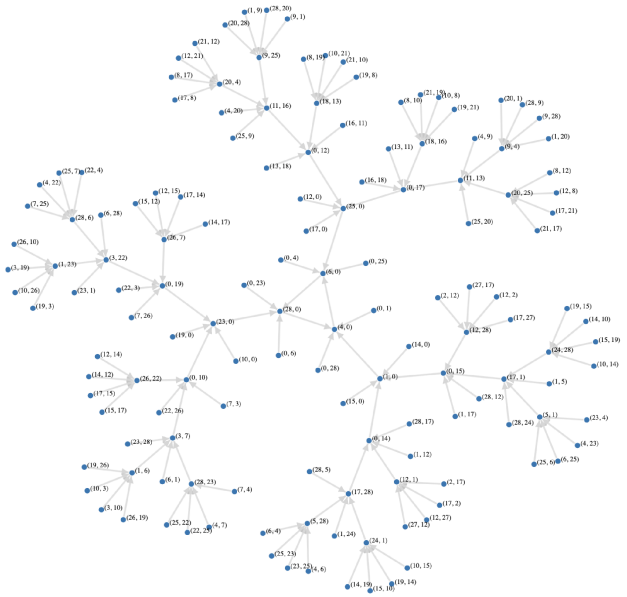


Figura 4.5: Componente conexa de um ciclo de comprimento 3.

Por último, um ciclo de comprimento 42 *com três tipos diferentes de pré-ciclos, como visto parcialmente na Figura 4.6.*

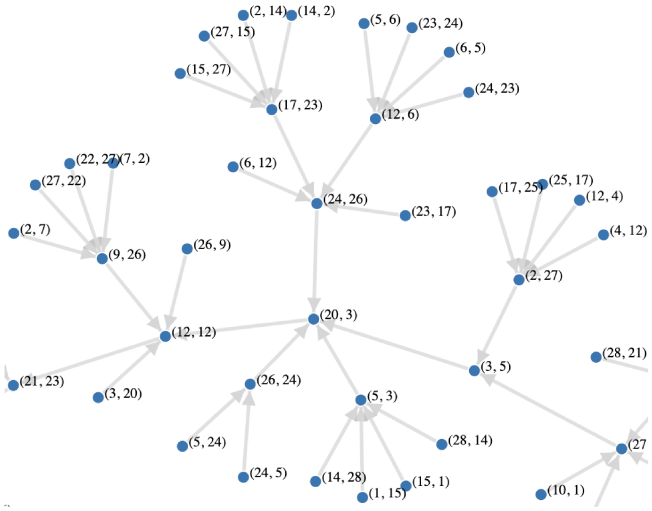


Figura 4.6: Ciclo de comprimento 42 e seus três tipos de pré-ciclos.

Capítulo 5

Conclusões

Neste trabalho, foi estudada a dinâmica da função

$$f(X) = c(X^{q+1} + aX^2),$$

com $a, c \in \mathbb{F}_q^*$, definido sobre o corpo finito $\mathbb{F}_{q^2}$. Apresentamos uma descrição detalhada dos grafos funcionais associados nos casos em que $a = 1$ e $a = -1$, com resultados completos para essas situações. O caso $a \notin \{\pm 1\}$ ainda não foi completamente explorado. Apesar de algumas propriedades estruturais terem sido discutidas, uma caracterização abrangente da dinâmica nesse caso permanece em aberto. Além disso, destacamos dois caminhos promissores para investigações futuras:

- Estudar o comportamento do mapa quando a característica do corpo for par, ou seja, quando a caraterística de $\mathbb{F}_{q^2}$ é par. Nessa situação, propriedades fundamentais utilizadas ao longo do trabalho, como o fato de $-1 \neq 1$, deixam de valer, o que pode modificar substancialmente a estrutura dos grafos funcionais.

- Investigar possíveis simetrias entre os grafos funcionais associados aos mapas $f_1(X) = X^{q+1} + X^2$ e $f_{-1}(X) = X^{q+1} - X^2$. Embora os casos $a = \pm 1$ tenham sido tratados separadamente, observações experimentais sugerem que, para alguns valores de q, os grafos apresentam estruturas semelhantes.

Essas direções podem enriquecer a compreensão da dinâmica desses mapas e revelar novas conexões entre álgebra, geometria, teoria de números e teoria dos grafos.

Bibliografia

Bondy, J., & Murty, U. R. (1982). *Graph theory with applications*. Elsevier Science Publishing Co., Inc.

Brochero Martínez, F., & Teixeira, H. (2023). On the functional graph of $f(x) = c(x^{q+1} + ax^2)$ over quadratic extensions of finite fields. *Finite Fields and Their Applications*. doi: https://doi.org/10.1016/j.ffa.2023.102180

Gonçalves, A. (2020). *Introdução à Álgebra* (2nd ed.). São Paulo: Editora Livraria da Física.

Judson, T. W. (2009). *Abstract algebra: Theory and applications*. Stephen F. Austin State University. Retrieved from https://judsonbooks.org/aata-files/aata-original.pdf (Accessed: 2025-06-15)

Peinado, M. F. M. J. Y. A., A. (2001). *Applied algebra, algebraic algorithms and error-correcting codes*. Springer Berlin Heidelberg.

Rogers, T. D. (1996). The graph of the square mapping on the prime fields. *Discrete Mathematics*, *148*(1), 317-324. Retrieved from https://www.sciencedirect.com/science/article/pii/0012365X9400250M doi: https://doi.org/10.1016/0012-365X(94)00250-M

Rudolf Lidl, H. N. (2003). *Finite fields*. The press syndicate of the university of cambridge.

Wiener, M. J., & Zuccherato, R. J. (1999). *Faster attacks on elliptic curve cryptosystems*. Springer Berlin Heidelberg. doi: https://doi.org/10.1007/3-540-48892-8_15