Instituto de Matemática
Universidade Federal do Rio de Janeiro

UFRJ

Contagem de Elementos Primitivos em Grupos Livres

Natália Jordana dos Santos Stanescon

Rio de Janeiro, Brasil

21 de agosto de 2021

Contagem de Elementos Primitivos em Grupos Livres

Natália Jordana dos Santos Stanescon

Dissertação de mestrado apresentada ao Programa de Pós-graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática

Universidade Federal do Rio de Janeiro

Instituto de Matemática

Programa de Pós-Graduação em Matemática

Orientador: Ilir Snopche

Rio de Janeiro, Brasil

21 de agosto de 2021

Contagem de Elementos Primitivos em Grupos Livres

Dissertação de mestrado apresentada ao Programa de Pós-graduação do Instituto de Matemática, Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Trabalho aprovado por

Ilir Snopche
Orientador

Slobodan Tanushevski
Convidado 1

Francesco Noseda
Convidado 2

Rio de Janeiro, Brasil
9 de agosto de 2021

A matemática, vista corretamente, possui
não apenas verdade, mas também suprema beleza.
- Bertrand Russell

Agradecimentos

Agradeço primeiramente a Deus, por me guiar e me dar forças durante toda essa caminhada.

Aos meus pais e a minha vó que sempre estiveram ao meu lado me apoiando e investindo no meu sonho.

Aos meus amigos que sempre me incentivaram e tornaram essa caminhada mais leve.

Aos meus professores, por toda dedicação e aprendizado, que me permitiram chegar até aqui.

E em especial ao meu orientador, Ilir Snopche, pela orientação, paciência, incentivo e por todo esforço para a conclusão deste trabalho.

Agradeço também a Capes e a FAPERJ pelo apoio financeiro que foi fundamental para o desenvolvimento do projeto.

Resumo

Grupos livres são objetos matemáticos importantes, que desempenham um papel central em diferentes áreas, em particular, em Álgebra, Geometria e Topologia.

Um elemento de um grupo livre é chamado de um elemento primitivo se fizer parte de uma base livre do grupo. O objetivo principal deste trabalho é provar que o conjunto dos elementos primitivos de um grupo livre não abeliano tem densidade zero, o que basicamente significa que a proporção desses elementos em bolas cada vez maiores é arbitrariamente pequena. Em particular, vamos estudar como os elementos primitivos estão espalhados dentro do grupo, mostrando que eles ficam cada vez mais espalhados de acordo com que o raio das bolas aumenta. Daremos também limites mais específicos da quantidade de elementos primitivos em cada bola. Esse trabalho é baseado no artigo "Counting Primitive Elements in Free Groups", de J. Burillo e E. Ventura.

Palavras-chave: Grupos livres, elementos primitivos.

Abstract

Free groups are important mathematical objects, which play a central role in different areas, in particular, in Algebra, Geometry and Topology.

An element of a free group is called a primitive element if it is part of a free base of the group. The main purpose of this work is to prove that the set of primitive elements of a non-abelian free group has density zero, which basically means that the proportion of these elements in bigger and bigger balls is arbitrarily small. In particular, we will study how primitive elements are spread out within the group, showing that they get more and more spread out as the radius of the balls increases. We will also give more specific limits on the amount of primitive elements in each ball. This work is based on the article "Counting Primitive Elements in Free Groups", by J. Burillo and E. Ventura.

Keywords: Free groups, primitive elements.

Sumário

1 Introdução

Grupos livres são objetos matemáticos importantes, que desempenham um papel central em diferentes áreas, em particular, em Álgebra, Geometria e Topologia. Os grupos livres surgiram primeiro no estudo da geometria hiperbólica, como exemplos de grupos Fuchsianos (grupos discretos agindo por isometrias no plano hiperbólico). Em um artigo de 1882, Walther von Dyck apontou que esses grupos têm as apresentações mais simples possíveis. O estudo algébrico de grupos livres foi iniciado por Jakob Nielsen em 1924, que lhes deu seu nome e estabeleceu muitas de suas propriedades básicas. Max Dehn percebeu a conexão com a topologia.

Um grupo F é chamado de grupo livre se existe um conjunto gerador X de F tal que cada palavra de grupo reduzido não vazio em X define um elemento não trivial de F. Nesse caso, X é chamado de base livre de F e F é chamado de livre em X ou gerado livremente por X. Alternativamente, um grupo é chamado de grupo livre se nenhuma relação existe entre seus geradores de grupo além da relação entre um elemento e seu inverso exigido como uma das propriedades definidoras de um grupo. Cada grupo livre é o grupo fundamental de um buquê de círculos (tendo um ponto de base comum); cada círculo representa um gerador. Grupos livres são objetos centrais na Teoria dos Grupos. Por exemplo, cada grupo é um quociente de um grupo livre.

Elementos primitivos de um grupo livre são aqueles que podem ser completados para formar uma base livre. Tem havido muita pesquisa sobre elementos primitivos. O presente trabalho é baseado no artigo "*Counting Primitive Elements in Free Groups*", de J. Burillo e E. Ventura, publicado em *Geometriae Dedicata*. O objetivo principal deste trabalho é provar que o conjunto dos elementos primitivos de um grupo livre não abeliano tem densidade zero, o que basicamente significa que a proporção desses elementos em bolas cada vez maiores é arbitrariamente pequena. Estaremos interessados em estudar como esses elementos estão espalhados dentro do grupo, mostrando que eles ficam cada vez mais espalhados de acordo com que o raio das bolas aumentam. Daremos também limites mais específicos da quantidade de elementos em cada bola.

Para concluirmos nosso objetivo estaremos estudando dois tipos de densidade, natural e exponencial, e algumas de suas propriedades. A densidade natural, como o próprio nome induz, é a noção mais logica de densidade, mas esta nos da menos precisão em grupos com crescimento exponencial; nesses grupos será interessante estudar a densidade exponencial e compara-las.

2 Grupos Livres

Dado um grupo G, dizemos que o conjunto $X \subset G$ é um conjunto de geradores de G se todo elemento de G pode ser escrito como combinação, sob a operação do grupo, dos elementos de X e de seus inversos.

Seja X um conjunto de geradores de um grupo G. Algumas operações entre elementos de X resultarão em 1 independente de qual seja o grupo G e o conjunto X. Alguns exemplos são: xx^{-1}, $xyy^{-1}x^{-1}$, yy^{-1}. Já outras operações podem resultar em 1 dependendo de cada grupo G e conjunto X. Por exemplo, num grupo abeliano G temos que $xy = yx$ e logo $xyx^{-1}y^{-1} = 1$. Os grupos em que a operação entre elementos do conjunto de geradores só resultará em 1 quando assim for para todo grupo, isto é, apenas resultará em 1 se for operação entre inversos, são os grupos que estaremos interessados em estudar aqui. Chamamos estes grupos de *Grupos Livres*.

2.1 Definição e Propriedades

Definição 2.1. *Seja X um conjunto, F um grupo e $i : X \to F$ uma função. O par (F, i) é chamado livre sobre X se para qualquer grupo G e qualquer função $\varphi : X \to G$ existe um único homomorfismo $\phi : F \to G$ tal que $\phi \circ i = \varphi$.*

Exemplo 2.2. *O grupo ciclico infinito $\mathbb{Z}$ é livre sobre qualquer conjunto $X = \{x\}$. De fato, tome $i : X \to \mathbb{Z}$ definida por $i(x) = 1$. Seja G um grupo e $\varphi : X \to G$ uma função tal que $\varphi(x) = g \in G$. A função $\phi : \mathbb{Z} \to G$ dada por $\phi(1) = g$ pode ser extendida unicamente a um homomorfismo da seguinte maneira: $\phi(n) = \phi(1^n) = \phi(1)^n = g^n$, onde $n \in \mathbb{Z}$.*

Proposição 2.3. *Se (F, i) é livre sobre X então i é uma função injetiva.*

Demonstração. Suponha que i não seja injetiva. Então existem $x_1 \neq x_2$ tais que $i(x_1) = i(x_2)$. Tomemos G tal que $|G| \geq 2$. Sejam $g_1 \neq g_2$ e $\varphi : X \to G$ tal que $\varphi(x_1) = g_1$ e $\varphi(x_2) = g_2$. Como (F, i) é livre sobre X, existe um único homomorfismo $\phi : F \to G$ tal que $\phi \circ i = \varphi$. Logo temos $g_1 = \varphi(x_1) = \phi \circ i(x_1) = \phi(i(x_1)) = \phi(i(x_2)) = \phi \circ i(x_2) = \varphi(x_2) = g_2$, que é uma contradição já que tomamos $g_1 \neq g_2$. Logo i deve ser injetiva. ∎

Proposição 2.4. *Se (F_1, i_1) e (F_2, i_2) são livres sobre X então existe um isomomorfismo $\phi : F_1 \to F_2$*

Demonstração. Primeiro observe que, se $f : F_1 \to F_1$ é um homomorfismo tal que $f \circ i_1 = i_1$ então f deve ser I_{F_1}, a função identidade, pois tomando $G = F_1$ e $\varphi = i_1$ temos que existe apenas um homomorfismo $f : F_1 \to F_1$ tal que $f \circ i_1 = i_1$. Como a função identidade é um homomorfismo que satisfaz essa condição, temos $f = 1_{F_1}$. Analogamente, se $h : F_2 \to F_2$ é um homomorfismo tal que $h \circ i_2 = i_2$ então h também deve ser I_{F_2}

Agora, como (F_1, i_1) e (F_2, i_2) são livres sobre X temos que existe um homomorfismo $\phi_1 : F_1 \to F_2$ tal que $\phi_1 \circ i_1 = i_2$ e também um homomorfismo $\phi_2 : F_2 \to F_1$ tal que $\phi_2 \circ i_2 = i_1$. Logo temos $(\phi_1 \circ \phi_2) \circ i_2 = i_2$ e $(\phi_2 \circ \phi_1) \circ i_1 = i_1$. Como $\phi_1 \circ \phi_2$ e $\phi_2 \circ \phi_1$ são homomorfismo, temos que $\phi_1 \circ \phi_2 = I_{F_2}$ e $\phi_2 \circ \phi_1 = I_{F_1}$. Logo $\phi_1 = \phi_2^{-1}$ e $\phi : F_1 \to F_2$ é uma bijeção, e consequentemente um isomorfismo. ■

Teorema 2.5. *Seja X um conjunto qualquer não vazio. Então existe um par (F, i) livre sobre X.*

Demonstração. Para começar a construção do grupo livre sobre X tomaremos um conjunto que denotaremos por X^{-1} tal que, exista uma bijeção entre X e X^{-1} e $X \bigcap X^{-1} = \emptyset$. Para cada elemento $x \in X$ denotaremos o elemento de X^{-1} associado a x por x^{-1}.

Uma palavra em X é uma sequência finita de elementos de $X \bigcup X^{-1}$, isto é, w é uma palavra em X se $w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n}$, onde $x_{i_j} \in X$ e $\epsilon_j = \pm 1$ para todo $j \in \{1, ..., n\}$.

Dizemos que o comprimento de w, denotado por $|w|$, é igual a quantidade de elementos da sequência de w, isto é, se $w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n}$ então $|w| = n$. A palavra vazia denotada por 1 tem comprimento 0. Definiremos a multiplicação entre duas palavras em X como a justaposição das palavras, isto é, se $w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n}$ e $v = x_{j_1}^{\eta_1} x_{j_2}^{\eta_2} ... x_{j_m}^{\eta_m}$ teremos $wv = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n} x_{j_1}^{\eta_1} x_{j_2}^{\eta_2} ... x_{j_m}^{\eta_m}$. Claramente temos que $|wv| = |w| + |v|$

Definiremos agora a seguinte relação de equivalencia nas palavras em X: $w \sim v$ se podemos transformar w em v realizando as seguintes operações em w uma quantidade finita de vezes

1. Acrescentando $x_i x_i^{-1}$ ou $x_i^{-1} x_i$ no inicio, fim ou entre duas letras consecutivas de w.
2. Retirando $x_i x_i^{-1}$ ou $x_i^{-1} x_i$ no inicio, fim ou entre duas letras consecutivas de w.

Claramente $\sim$ é uma relação de equivalência. Denotaremos a classe de equivalencia de w por $[w]$.

Afirmação: O conjunto $F(X)$ das classes de equivalências das palavras em X com a operação $[w][v] = [wv]$ é um grupo.

De fato, a operação em F(X) está bem definida, pois se $[w_1] = [w_2]$ e $[v_1] = [v_2]$ temos que $w_1 v_1 \sim w_2 v_2$, já que podemos fazer operações finitas em w_1 para tranformar em w_2 e tambem em v_1 para transformar em v_2. Logo $[w_1 v_1] = [w_2 v_2]$. Claramente a operação é associativa já que a justaposição das palavras é associativa. Temos que [1], a classe da palavra vazia, é o elemento neutro, pois $[w][1] = [w1] = [w]$. Agora, seja

$w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n}$. Defina $w^{-1} = x_{i_n}^{-\epsilon_n} x_{i_{n-1}}^{\epsilon_{n-1}} ... x_{i_1}^{-\epsilon_1}$. Claramente temos que $ww^{-1} \sim 1$ e logo $[w][w^{-1}] = [ww^{-1}] = [1]$. Então cada elemento de $F(X)$ possui um elemento inverso. Logo, finalmente podemos afirmar que $F(X)$ é um grupo

Afirmação: Seja $i : X \to F(X)$ definida por $i(x) = [x]$. Então $(F(X), i)$ é livre sobre X.

Seja G um grupo e $\varphi : X \to G$ uma função. Defina $\phi : F(X) \to G$ por $\phi([w]) = \varphi(x_{i_1})^{\epsilon_1} ... \varphi(x_{i_n})^{\epsilon_n}$, onde $w = x_{i_1}^{\epsilon_1} ... x_{i_n}^{\epsilon_n}$. Observe que ϕ está bem definida pois se $[w_1] = [w_2]$ então temos que $w_1 \sim w_2$ e logo uma palavra se difere da outra por acrescimos de $x_i x_i^{-1}$ ou $x_i^{-1} x_i$ e consequentemente terão a mesma imagem, pois $\varphi(x_i)\varphi(x_i)^{-1} = 1_G$.

Claramente temos que ϕ é um homomorfismo e que para cada $x \in X$ temos $\phi \circ i(x) = \phi([x]) = \varphi(x)$. A unicidade de ϕ vem do fato de que a imagem de X é um conjunto de geradores de F(X). Logo $(F(X), i)$ é livre sobre X. ∎

Definição 2.6. *Uma palavra w em X é dita reduzida se não tem dois elementos consecutivos da forma $x_i x_i^{-1}$ ou $x_i^{-1} x_i$.*

Proposição 2.7. *Cada classe de equivalência em F(X) possui apenas uma palavra reduzida.*

Demonstração. Seja M o conjunto de todas as palavras em X. Definiremos $\lambda : M \to M$ por indução da seguinte maneira: $\lambda(1) = 1,\ \lambda(x^\epsilon) = x^\epsilon$ e

$$\lambda(wx^\epsilon) = \begin{cases} \lambda(w)x^\epsilon, & \text{se } \lambda(w) \text{ não termina por } x^{-\epsilon} \\ u, & \text{se } \lambda(w) = ux^{-\epsilon} \end{cases}$$

Vamos mostrar agora as seguintes propriedades de λ:

- Se w é uma palavra reduzida então $\lambda(w) = w$
- Para todo $w \in M$ temos que $\lambda(w)$ é uma palavra reduzida
- se $w_1 \sim w_2$ então $\lambda(w_1) = \lambda(w_2)$

Mostraremos essas propriedades por indução no comprimento de w.

Seja w tal que $|w| = 1$. Claramente temos que w é reduzida pois $w = x^\epsilon$ e por definição temos $\lambda(w) = \lambda(x^\epsilon) = x^\epsilon = w$. Se $|w| = 2$ e w é reduzida, temos que $w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}$ com $x_{i_1}^{\epsilon_1} \neq x_{i_2}^{-\epsilon_2}$. Logo

$$\lambda(w) = \lambda(x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}) = \lambda(x_{i_1}^{\epsilon_1}) x_{i_2}^{\epsilon_2} = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} = w.$$

Agora suponha que a primeira propriedade vale para todas as palavras reduzidas w, tais que $|w| = n$. Se v é uma palavra reduzida tal que $|v| = n + 1$, isto é, $v = x_{i_1}^{\epsilon_1} ... x_{i_n}^{\epsilon_n} x_{i_{n+1}}^{\epsilon_{n+1}}$, temos que $v = ux_{i_{n+1}}^{\epsilon_{n+1}}$ onde $u = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$ e logo u é uma palavra reduzida com $|u| = n$. Por hipotese temos $\lambda(u) = u$ e também $x_{i_n}^{\epsilon_n} \neq x_{i_{n+1}}^{-\epsilon_{n+1}}$ já que w é reduzida, logo temos

$$\lambda(v) = \lambda(ux_{i_{n+1}}^{\epsilon_{n+1}}) = \lambda(u)x_{i_{n+1}}^{\epsilon_{n+1}} = ux_{i_{n+1}}^{\epsilon_{n+1}} = v.$$

Vale então que $\lambda(w) = w$ para todo $w \in M$ reduzida.

Novamente por indução no comprimento de w, mostraremos agora que para todo $w \in M$, $\lambda(w)$ é uma palavra reduzida. Se w é tal que $|w| = 1$ então w é reduzida e logo $\lambda(w) = w$ é reduzida. Seja w uma palavra tal que $|w| = 2$. Então se w é reduzida, novamente temos $\lambda(w) = w$ uma palavra reduzida. Se w não for reduzida então $w = x^\epsilon x^{-\epsilon}$. Logo temos que $\lambda(x^\epsilon) = x^\epsilon$ e por definição $\lambda(x^\epsilon x^{-\epsilon}) = u$, onde $\lambda(x^\epsilon) = ux^\epsilon$, isto é, $u = 1$. Logo $\lambda(w) = 1$ que é uma palavra reduzida.
Suponha então que para todo $w \in M$ tal que $|w| = n$ temos $\lambda(w)$ uma palavra reduzida. Seja v uma palavra tal que $|v| = n + 1$, isto é, $v = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}x_{i_{n+1}}^{\epsilon_{n+1}}$. Temos que $v = ux_{i_{n+1}}^{\epsilon_{n+1}}$, onde $u = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$. Por hipotese $\lambda(u)$ é uma palavra reduzida. Se $\lambda(u)$ não termina por $x_{i_{n+1}}^{-\epsilon_{n+1}}$ então

$$\lambda(v) = \lambda(ux_{i_{n+1}}^{\epsilon_{n+1}}) = \lambda(u)x_{i_{n+1}}^{\epsilon_{n+1}}.$$

Logo $\lambda(v)$ é uma palavra reduzida, pois $\lambda(u)$ é reduzida e não termina por $x_{i_{n+1}}^{-\epsilon_{n+1}}$. Se $\lambda(u)$ é uma palavra reduzida que termina por $x_{i_{n+1}}^{-\epsilon_{n+1}}$ temos que $\lambda(u) = wx_{i_{n+1}}^{-\epsilon_{n+1}}$ e w também é uma palavra reduzida. Por definição teriamos

$$\lambda(v) = \lambda(ux_{i_{n+1}}^{\epsilon_{n+1}}) = w.$$

Concluimos que para todo $w \in M$, $\lambda(w)$ é uma palavra reduzida.

Vamos mostrar agora a ultima propriedade: Se $w_1 \sim w_2$ então $\lambda(w_1) = \lambda(w_2)$. Para mostrar essa propriedade vamos mostrar que $\lambda(ux^\epsilon x^{-\epsilon}v) = \lambda(uv)$ onde u é uma palavra reduzida que não termina por $x^{-\epsilon}$. Faremos a demonstração por indução no comprimento de v. Para $|v| = 1$ temos que $v = y^\eta$ e como u é uma palavra reduzida, temos $\lambda(u) = u$ que não termina por $x^{-\epsilon}$, logo $\lambda(ux^\epsilon) = ux^\epsilon$ o que implica que $\lambda(ux^\epsilon x^{-\epsilon}) = u$. Se u nao termina por $y^{-\eta}$, temos $\lambda(ux^\epsilon x^{-\epsilon}v) = \lambda(ux^\epsilon x^{-\epsilon}y^\eta) = uy^\eta = \lambda(uy^\eta) = \lambda(uv)$. Se $u = wy^{-\eta}$ temos $\lambda(ux^\epsilon x^{-\epsilon}v) = w = \lambda(uy^\eta) = \lambda(uv)$. Podemos afirmar então que vale para $|v| = 1$.
Suponhamos que vale para todo v tal que $|v| = n$. Se temos $|w| = n + 1$, temos que $ux^\epsilon x^{-\epsilon}w = ux^\epsilon x^{-\epsilon}vy^\eta$ onde $|v| = n$. Por hipotese temos $\lambda(ux^\epsilon x^{-\epsilon}v) = \lambda(uv)$. Se $\lambda(uv)$ não termina por $y^{-\eta}$ temos $\lambda(ux^\epsilon x^{-\epsilon}w) = \lambda(ux^\epsilon x^{-\epsilon}vy^\eta) = \lambda(ux^\epsilon x^{-\epsilon}v)y^\eta = \lambda(uv)y^\eta = \lambda(uvy^\eta) = \lambda(uw)$. Se $\lambda(uv) = sy^{-\eta}$ teremos que $\lambda(ux^\epsilon x^{-\epsilon}v) = \lambda(uv) = sy^{-\eta}$ e logo $\lambda(ux^\epsilon x^{-\epsilon}w) = \lambda(ux^\epsilon x^{-\epsilon}vy^\eta) = s = \lambda(uvy^\eta) = \lambda(uw)$.
Concluimos então que para todo $x \in X$ e $u, v \in M$ com u sendo uma palavra reduzida que não termina por $x^{-\epsilon}$, $\lambda(ux^\epsilon x^{-\epsilon}v) = \lambda(uv)$.

Tomemos agora duas palavras w_1, w_2 em X tais que $w_1 \sim w_2$. Temos que uma das palavras é obtida da outra por reduções finitas de elementos do tipo $x_i^\epsilon x_i^{-\epsilon}$. Suponhamos sem perda de generalidade que w_2 é obtida de w_1 por redução e que w_2 seja uma palavra reduzida. Se $w_1 = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$, tomaremos o maior indice j tal que $x_{i_1}^{\epsilon_1}...x_{i_j}^{\epsilon_j}$ seja uma palavra reduzida. Então pela maximilidade de j temos que $x_{i_1}^{\epsilon_1}...x_{i_j}^{\epsilon_j}x_{i_{j+1}}^{\epsilon_{j+1}}$ não é uma palavra reduzida, isto é, $x_{i_{j+1}} = x_{i_j}$ e $\epsilon_j = -\epsilon_{j+1}$. Assim $w_1 = ux_{i_j}^{\epsilon_j}x_{i_j}^{-\epsilon_j}v$ onde $u = x_{i_1}^{\epsilon_1}...x_{i_{j-1}}^{\epsilon_{j-1}}$ é uma palavra reduzida que nao termina por $x_{i_j}^{-\epsilon_j}$, pois caso contrário $x_{i_1}^{\epsilon_1}...x_{i_j}^{\epsilon_j}$ não seria uma palavra reduzida, e $v = x_{i_{j+2}}^{\epsilon_{j+2}}...x_{i_n}^{\epsilon_n}$. Pelo que já mostramos teremos

$$\lambda(w_1) = \lambda(ux_{i_j}^{\epsilon_j}x_{i_j}^{-\epsilon_j}v) = \lambda(uv)$$

onde uv vem de w_1 por redução. Se uv já estiver reduzida entao $uv = w_2$ e não há mais nada a demonstrar, se não, podemos repetir o processo um numero finito de vezes até que a palavra fique na sua forma reduzida w_2.

Se w_2 não for reduzida, podemos encontrar uma palavra $\bar{w}$ reduzida tal que $\bar{w}$ é obtida de w_2 por reduções. Logo $\bar{w}$ também pode ser obtida de w_1 por reduções. Desta maneira teremos $\lambda(w_1) = \lambda(\bar{w}) = \lambda(w_2)$

A demonstração da proprosição é consequência direta das propriedades de λ. Dadas duas palavras reduzidas w_1 e w_2 tais que $w_1 \sim w_2$ temos que

$$w_1 = \lambda(w_1) = \lambda(w_2) = w_2.$$

■

A Proposição 2.7 nos dá uma maneira melhor para definir os elementos de F(X). Como cada classe de equivalência só tem uma palavra reduzida, utilizaremos a palavra reduzida de cada classe para representa-las como elemento do grupo. O produto de duas palavras reduzidas u e v será a palavra obtida pela redução de uv

Proposição 2.8. *Grupos livres são residualmente finitos. Isto é, se F é um grupo livre e $w \neq 1$ é um elemento de F, então existe um subgrupo normal N de F tal que $w \notin N$ e F/N é finito.*

Demonstração. Vamos mostrar que se $w \neq 1$ existe um grupo G finito e um homomorfismo $\phi : F \to G$ tal que e $\phi(w) \neq 1$. Seja $1 \neq w \in F$. Como já caracterizamos os elementos de F sabemos que w é uma palavra reduzida em X, isto é, $w = x_1^{\epsilon_1}...x_n^{\epsilon_n}$. Consideremos então o grupo finito S_{n+1} das permutações de $\{1, ..., n+1\}$ e definiremos uma função $\phi : X \to S_{n+1}$ que satisfaça as seguintes condições:

$$\phi(x) = \begin{cases} \text{f } \in S_{n+1} \text{ tal que } f(i+1) = i, & \text{se } x = x_i \text{ e } \epsilon_i = 1 \\ \text{f } \in S_{n+1} \text{ tal que } f(i) = i+1, & \text{se } x = x_i \text{ e } \epsilon_i = -1 \end{cases}$$

De fato, podemos encontrar uma função $\phi : X \to S_{n+1}$ que satisfaça essas condiçoes, de maneira que f esteja bem definida, isto é, nao manda um elemento em duas imagens

distintas. Se $f(i+1)=i$ e $f(i+1)=i+2$ (pois nossa condição só exige que mande esses elementos em seus antecessores ou sucessores) teriamos que $x=x_i$ e $\epsilon_i=1$ e ao mesmo tempo $x=x_{i+1}$ e $\epsilon_{i+1}=-1$. Neste caso, w não seria reduzida. Estas condições também não permitem que f não seja injetiva. Se f não fosse injetiva teriamos $f(i+1)=i=f(i-1)$ e neste caso teriamos que $x=x_i$ e $\epsilon_i=1$ e ao mesmo tempo $x=x_{i-1}$ e $\epsilon_{i-1}=-1$, o que também implicaria que w não é reduzida.
Podemos então definir uma função $\phi: X \to S_{n+1}$ satisfazendo as condições necessarias. Como F é um grupo livre, existe um homomorfismo $\varphi: F \to S_{n+1}$ que extende ϕ. Temos então que

$$\varphi(w)=\varphi(x_1^{\epsilon_1}...x_n^{\epsilon_n})=\varphi(x_1)^{\epsilon_1}...\varphi(x_n)^{\epsilon_n}=\phi(x_1)^{\epsilon_1}...\phi(x_n)^{\epsilon_n}.$$

Observe que $\phi(x_i)^{-\epsilon_i}(i)=i+1$ para todo i, pois se $\epsilon_i=1$ temos $\phi(x_i)(i+1)=i$ e logo $\phi(x_i)^{-\epsilon_i}=\phi(x_i)^{-1}(i)=i+1$. Se $\epsilon_i=-1$ temos que $\phi(x_i)(i)=i+1$ e logo $\phi^{-\epsilon}(x_i)(i)=\phi^{-(-1)}(x_i)(i)=\phi(x_i)(i)=i+1$

Então temos que $\varphi^{-1}(w)(1)=\phi(x_n)^{-\epsilon_n}...\phi(x_1)^{-\epsilon_1}(1)=\phi(x_n)^{-\epsilon_n}(...(\phi(x_1)^{-\epsilon_1}(1))..)=n+1$, pois a primeira função levara 1 em 2, a segunda levara 2 em 3, e assim sucessivamente ate chegar em n+1. Desta maneira temos que $\varphi(w)(n+1)=1$ logo $\varphi(w)\neq 1$.

Pelo primeiro teorema de isomorfismo, temos que $ker\varphi$ é normal em F e $F/ker\varphi \cong Im(F) \leq S_{n+1}$. Logo temos que $w \notin ker\varphi$, $ker\varphi$ é subgrupo normal de F e $F/ker\varphi$ é finito pois é isomorfo a um subgrupo do grupo finito S_{n+1}. Tomando $N=ker\varphi$, podemos concluir que F é residualmente finito. ∎

Corolário 2.9. *Seja F um grupo livre finitamente gerado. Todo endomorfismo sobrejetivo de F é um automorfismo.*

Demonstração. Suponha por contradição que existe um endomorfismo sobrejetivo $\varphi: F \to F$ que não é um automorfismo. Como φ é sobrejetivo, temos então que não pode ser injetiva, isto é, existe $1 \neq w \in F$ tal que $\varphi(w)=1$. Pela proposição anterior já vimos que como $w \neq 1$ então existe um homomorfismo $\alpha: F \to S$ onde S é um grupo finito, tal que $\alpha(w)\neq 1$. Sejam $n,m \in \mathbb{N}$ tal que $n>m$. Como φ é sobrejetivo, φ^m também é. Logo, existe $v \in F$ tal que $\varphi^m(v)=w$ o que nos dá $\alpha\varphi^m(v)=\alpha(\varphi^m(v))=\alpha(w)\neq 1$. Por outro lado, como $n>m$ temos $n=m+k$ para algum $k \in \mathbb{N}$. Logo $\alpha\varphi^n(v)=\alpha\varphi^k\varphi^m(v)=\alpha(\varphi^k(\varphi^m(v)))=\alpha(\varphi^k(w))=\alpha(1)=1$. Então para cada $n \in \mathbb{N}$ temos que $\alpha\varphi^n$ são homomorfismos distintos, isto é, existem infinitos homomorfismos de F em S. Por outro lado, como F é finitamente gerado, temos que só existe uma quantidade finita de homomorfismos de F em S. Pois seja X o conjunto finito de geradores de F, então existem exatamente $|S|^{|X|}$ homomorfismos de F em S, que dá uma contradição. Concluimos então que φ tem que ser injetivo, e logo um automorfismo. ∎

Proposição 2.10. *F(X) é isomorfo a F(Y) se e somente se $|X|=|Y|$.*

Demonstração. Suponhamos que $|X| = |Y|$. Então existe uma bijeção $f : X \to Y$. Pela Proposição 2.4, se (F_1, i_1), e (F_2, i_2) são livres sobre um mesmo conjunto X então são isomorfos. Vamos mostrar então que se $(F(X), i)$ é livre sobre X então $(F(X), if)$ é livre sobre Y. Desta maneira teremos que $F(X)$ e $F(Y)$ são livres sobre Y e logo $F(X) \cong F(Y)$.

De fato, seja G um grupo qualquer e $\varphi : Y \to G$ uma função. Temos $\varphi f^{-1} : X \to G$. Como (F(X),i) é livre sobre X, existe um único homomorfismo ϕ tal que $\phi i = \varphi f^{-1} \Rightarrow \phi if = \varphi$. Logo, $(F(X), if)$ é livre sobre Y, como queriamos mostrar.

Suponha que $F(X) \cong F(Y)$, isto é, existe um isomorfismo $\varphi : F(Y) \to F(X)$. Suponha que X e Y são conjuntos infinitos. Então $|X| = |F(X)|$, pois os elementos de $F(X)$ são palavras de comprimento finito. Similarmente $|Y| = |F(Y)|$, e por isso, $|X| = |Y|$. Agora suponha que X seja um conjunto finito. Seja $\mathcal{A}$ o conjunto de todos os homomorfismos de F(X) em $\mathbb{Z}_2$, e $\mathcal{H}$ o conjunto de todos os homomorfismos de F(Y) em $\mathbb{Z}_2$. Defina $\phi : \mathcal{A} \to \mathcal{H}$ por $\phi(f) = f\varphi$. Vamos mostrar que ϕ é uma bijeção. Se $\phi(f) = \phi(g)$ então $f\varphi = g\varphi$. Como φ é uma bijeção, tem inversa e logo $f\varphi\varphi^{-1} = g\varphi\varphi^{-1} \Rightarrow f = g$. Se $g \in \mathcal{H}$ temos que $g\varphi^{-1} \in \mathcal{A}$ e $\phi(g\varphi^{-1}) = g\varphi^{-1}\varphi = g$. Logo ϕ é uma bijeção, o que implica $|\mathcal{A}| = |\mathcal{H}|$.

Por outro lado temos para cada homomorfismo de F(X) em $\mathbb{Z}_2$ uma função de X em $\mathbb{Z}_2$, apenas restringindo o homomorfismo em X. E também para cada função de X em $\mathbb{Z}_2$ temos um homomorfismo de F(X) em $\mathbb{Z}_2$. Logo o número de homomorfismos de F(X) em $\mathbb{Z}_2$ é o mesmo número de funções de X em $\mathbb{Z}_2$, isto é, $|\mathcal{A}| = 2^{|X|}$. Analogamente temos $|\mathcal{H}| = 2^{|Y|}$ e logo

$$2^{|X|} = |\mathcal{A}| = |\mathcal{H}| = 2^{|Y|} \Rightarrow |X| = |Y|.$$

■

Definição 2.11. *Um grupo G é chamado de grupo livre se é isomorfo a F(X) para algum X. Se $i : F(X) \to G$ é um isomorfismo, dizemos que $i(X)$ é uma base de G. Também dizemos que G é livre sobre $i(X)$*

É facil verificar que se A é uma base de G e φ é um automorfismo de G então $\varphi(A)$ também é uma base de G. Pela Proposicão 2.10, se A e B são bases de G então $|A| = |B|$. Chamamos a cardinalidade da base de um grupo livre G de posto de G.

Exemplo 2.12. *Seja $F = F(x, y)$ um grupo livre. Então $\{x^{-1}, xy\}$ também é uma base de F. Seja $\varphi : F \to F$ tal que $\varphi(x) = x^{-1}$ e $\varphi(y) = xy$. A função φ induz um homomorfismo de F em F que é sobrejetivo, pois $\varphi(x^{-1}) = \varphi(x)^{-1} = x$ e $\varphi(xy) = \varphi(x)\varphi(y) = x^{-1}xy = y$. Logo, temos que φ é um endomorfismo sobrejetivo. Pelo Corolário 2.9 temos que φ é um automorfismo, pois F é finitamente gerado. Analogamente podemos verificar que $\{xy, xy^2\}$ também é uma base.*

Por outro lado temos que $\{yx, xy^2\}$ não é uma base. Suponhamos que houvesse um homomorfismo φ tal que $\varphi(x) = yx$ e $\varphi(y) = xy^2$. Então φ não pode ser sobrejetivo, pois se fosse, existiria uma palavra reduzida w tal que $\varphi(w) = x$. Porém é facil verificar que $\varphi(w)$ também é reduzida. Logo se $|w| \geq 2$ então $|\varphi(w)| \geq 4$, o que é uma contradição de que $\varphi(w) = x$. Logo $\{yx, xy^2\}$ não é uma base de F. Outro conjunto que também não é uma base é $\{xy, x^2y^3\}$. Se fosse, teriamos que $\{xy, x^2y^3(xy)^{-1}\} = \{xy, x^2y^2x^{-1}\}$ também seria, pois $x^2y^3(xy)^{-1}xy = x^2y^3$. Neste caso, tomando o automorfismo $\varphi : F \to F$ dada pela conjugação por x, isto é, $\varphi(w) = x^{-1}wx$ teriamos que $\varphi(\{xy, x^2y^2x^{-1}\}) = \{yx, xy^2\}$ seria uma base.

Proposição 2.13. *Seja G um grupo e seja X um subconjunto de G. Então as seguintes afirmações são equivalentes:*

1. *G é livre com a base X.*

2. *Todo elemento de G pode ser escrito de maneira única por $x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$ para algum $n \geq 0$, $x_{i_r} \in X$ e $\epsilon_r = \pm 1$, onde $\epsilon_r \neq -\epsilon_{r+1}$ se $i_r = i_{r+1}$.*

3. *X gera G e nenhum produto $x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$ para $n > 0$, $x_{i_r} \in X$ e $\epsilon_r = \pm 1$, onde $\epsilon_r \neq -\epsilon_{r+1}$ se $i_r = i_{r+1}$, é igual a 1.*

Demonstração. $2 \Rightarrow 3$ é trivial. $3 \Rightarrow 2$ também é direto, sendo necessário apenas mostrar parte da unicidade. De fato, se um elemento $w \in G$ pode ser escrito por $w = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n} = x_{j_1}^{\eta_1}...x_{j_m}^{\eta_m}$ então $x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}x_{j_m}^{-\eta_m}...x_{j_1}^{-\eta_1} = 1$. Porém, pela hipotese temos que 1 não pode ser escrito por nenhum produto se estiver na forma reduzida. Logo, esse produto tem que poder ser reduzido a palavra vazia. Como $x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$ e $x_{j_1}^{\eta_1}...x_{j_m}^{\eta_m}$ estão na forma reduzida, a única alternativa é que $x_{i_n}^{\epsilon_n} = x_{j_m}^{\eta_m}$, ... ,$x_{i_1}^{\epsilon_n} = x_{j_m}^{\eta_1}$. Concluimos que a maneira de escrever w é única.

Se G é livre sobre X, as propriedades 2 e 3 seguem diretamente da construção de F(X). Logo $1 \Rightarrow 2$ e $1 \Rightarrow 3$ também é trivial.

Suponhamos que G tem as propriedades 2 e 3. Considere o homomorfismo $\phi : F(X) \to G$ induzido por $\varphi : X \to G$ definido pela função identidade. Temos ϕ é sobrejetiva, pois X gera G. Além disso, ϕ é injetiva, pois se $w \neq 1$, pela hipotese 3, $\phi(w) \neq 1$. Logo ϕ é um isomorfismo e G é livre sobre X. Concluimos que $2, 3 \to 1$. ∎

Corolário 2.14. *Seja X um conjunto de geradores de G e seja $\varphi : G \to H$ um homomorfismo injetivo em X tal que $\varphi(G)$ é livre sobre $\varphi(X)$. Então G é livre sobre X*

Demonstração. A condição (3) da Proposição 2.13 vale para X e G já que vale para $\varphi(X)$ e $\varphi(G)$. ∎

Corolário 2.15. *Seja G livre sobre X e $Y \subset X$. Então o subgrupo $< Y >$ é livre sobre Y.*

Demonstração. Também segue direto da condição (3) da Proposição 2.13 que vale para $< Y >$ e Y. ■

Corolário 2.16. *Seja F livre sobre a base $\{x, y\}$. Seja $\varphi : F \to \mathbb{Z}$ tal que $\varphi(x) = 1$ e $\varphi(y) = 0$. Então $ker\varphi$ é livre sobre a base $\{x^{-i}yx^i;\ i \in \mathbb{Z}\}$*

Demonstração. Temos que qualquer elemento de $ker\varphi$ é produto dos elementos da base $\{x^{-i}yx^i;\ i \in \mathbb{Z}\}$, e qualquer palavra reduzida dessa base é diferente de 1. Assim o corolário segue pela Proposição 2.13. ■

Definição 2.17. *Seja $w = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$ uma palavra reduzida. Dizemos que w é ciclicamente reduzida se $i_1 \neq i_n$ ou se $i_1 = i_n$ mas $\epsilon_1 \neq -\epsilon_n$. Por convenção 1 é ciclicamente reduzida.*

Claramente se w é uma palavra ciclicamente reduzida, então w^n é também ciclicamente reduzida e logo $|w^n| = n|w|$. E também se $w = u^{-1}vu$ é uma palava reduzida e v uma palavra ciclicamente reduzida, temos $w^n = u^{-1}v^nu$

Definição 2.18. *Uma permutação cíclica de $w = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$ é qualquer palavra da forma $x_{i_r}^{\epsilon_r}...x_{i_n}^{\epsilon_n}x_{i_1}^{\epsilon_1}...x_{i_{r-1}}^{\epsilon_{r-1}}$*

Proposição 2.19.

1. *Todo elemento de $F(X)$ é conjugado de uma palavra ciclicamente reduzida, isto é, para todo $w \in F(X)$ temos $w = u^{-1}vu$ onde v é ciclicamente reduzida.*

2. *Qualquer permutação cíclica de uma palavra ciclicamente reduzida é ciclicamente reduzida.*

Demonstração.

1. Faremos a demonstração por indução. Como toda palavra reduzida em F de comprimento 2 claramente é ciclicamente reduzida, começaremos mostrando para $|w| = 3$. Seja w tal que $|w| = 3$, isto é, $w = x_{i_1}^{\epsilon_1}x_{i_2}^{\epsilon_2}x_{i_3}^{\epsilon_3}$. Se w já é ciclicamente reduzida então podemos escrever $w = 1w1$. Se w não for ciclicamente reduzida então $i_1 = i_3$ e $\epsilon_1 = -\epsilon_3$. Logo temos $w = x_{i_1}^{\epsilon_1}x_{i_2}^{\epsilon_2}x_{i_1}^{-\epsilon_1}$. Chamando $u = x_{i_1}^{-\epsilon_1}$ e $v = x_{i_2}^{\epsilon_2}$ temos $w = u^{-1}vu$, e claramente v é ciclicamente reduzida, pois tem comprimento 1.

   Suponha que vale para todo $w \in F(X)$ tal que $|w| < n$. Seja $w \in F(X)$ tal que $|w| = n$, isto é, $w = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$. Se w é ciclicamente reduzida, novamente é direto que $w = 1w1$. Se w não for ciclicamente reduzida entao $i_1 = i_n$ e $\epsilon_1 = -\epsilon_n$ e temos então que $w = x_{i_1}^{\epsilon_1}x_{i_2}^{\epsilon_2}...x_{i_{n-1}}^{\epsilon_{n-1}}x_{i_1}^{-\epsilon_1} = x_{i_1}^{\epsilon_1}\bar{w}x_{i_1}^{-\epsilon_1}$. Como $|\bar{w}| < n$, por hipotese $\bar{w} = u^{-1}vu$, onde v é ciclicamente reduzida. Logo temos $w = x_{i_1}^{\epsilon_1}u^{-1}vux_{i_1}^{-\epsilon_1}$. Tomando $\bar{u} = ux_{i_1}^{-\epsilon_1}$ temos $\bar{u}^{-1} = x_{i_1}^{\epsilon_1}u^{-1}$. Logo temos $w = \bar{u}^{-1}v\bar{u}$ e v é uma palavra ciclicamente reduzida. Concluimos que vale para todo $w \in F(X)$.

2. Seja $w = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$ uma palavra ciclicamente reduzida. Qualquer permutação ciclica $x_{i_r}^{\epsilon_r}...x_{i_n}^{\epsilon_n}x_{i_1}^{\epsilon_1}...x_{i_{r-1}}^{\epsilon_{r-1}}$ é reduzida pois w é ciclicamente reduzida então $x_{i_1}^{\epsilon_1} \neq x_{i_n}^{-\epsilon_n}$. Além disso será ciclicamente reduzida pois para qualquer r temos $x_{i_r}^{\epsilon_r} \neq x_{i_{r-1}}^{-\epsilon_{r-1}}$.

■

Proposição 2.20. *Grupos livres são livres de torção. Isto é, se $w \neq 1$ então $w^n \neq 1$ para todo inteiro n diferente de 0.*

Demonstração. Seja $w \neq 1$. Pela Proposição 2.19 temos $w = u^{-1}vu$, onde v é ciclicamente reduzida diferente de 1. Logo $|v| \geq 1$. Então $w^n = u^{-1}v^n u$, o que implica que $|w^n| \geq |v^n| = n|v| \geq 1$. Logo w^n não pode ser 1, pois $|1| = 0$. ■

Corolário 2.21. *Seja F um grupo livre e sejam $g, h \in F$. Se $g^k = h^k$ para algum $k \neq 0$ então $g = h$.*

Demonstração. Suponha $g^k = h^k$. Então $g^k h^{-k} = 1 \Rightarrow g^k(h^{-1})^k = 1$. Como $g, h \neq 1$, pela Proposição 2.20 temos $g^k \neq 1$ e $h^{-k} \neq 1$. Logo, para que $g^k(h^{-1})^k = 1$ precisamos de $gh^{-1} = 1$, que implica que $g = h$. ■

2.2 Elementos Primitivos

Definição 2.22. *Seja F um grupo livre. Dizemos que $w \in F$ é um elemento primitivo se w é parte de uma base livre, isto é, se $w \in X$ para algum conjunto X que seja base de F.*

Exemplo 2.23. *Seja $F(x, y)$ um grupo livre. Vimos no Exemplo 2.12 que x^{-1} e xy são elementos primitivos, pois $\{x^{-1}, xy\}$ é uma base. O elemento xy^2 também é primitivo, pois $\{xy, xy^2\}$ também é uma base.*

Proposição 2.24. *Seja F um grupo livre. Se w é um elemento primitivo então para todo grupo G e elemento $g \in G$ existe um homomorfismo $\varphi : F \to G$ tal que $\varphi(w) = g$*

Demonstração. Seja F um grupo livre e w um elemento primitivo. Então existe uma base X tal que $w \in X$.
Afirmação: F é livre sobre X com a função inclusão $i : X \to F$.

De fato, como F é um grupo livre com a base X temos que F é isomorfo a $F(\bar{X})$ para algum conjunto $\bar{X}$. Em particular, existe um isomorfismo $f : F(\bar{X}) \to F$ com $f(\bar{X}) = X$. Basta considerarmos uma função bijetiva de $\bar{X}$ em X, que existe, pois pela Proposição 2.10 $|X| = |\bar{X}|$. Pela definição de grupo livre, tem que existir um homomorfismo de $F(\bar{X})$ em F que extenda esta função bijetiva. E como é um homomorfismo que leva base em base do forma bijetiva, temos que é um isomorfismo.

Agora seja G um grupo qualquer e $\varphi : X \to G$ uma função. Temos $\varphi \circ f : \bar{X} \to G$. Por definição de grupo livre existe um único homomorfismo $\phi : F(\bar{X}) \to G$ tal que $\phi\,|_{\bar{X}} = \varphi \circ f$. Logo o homomorfismo $\phi \circ f^{-1}$ satisfaz $\phi \circ f^{-1}|_X = \varphi$, pois $f^{-1}(X) = \bar{X}$. A unicidade vem direto da unicidade de ϕ.

Dado então um grupo G e um elemento $g \in G$, considere uma função $\varphi : X \to G$ tal que $\varphi(w) = g$. Por definição de grupo livre, existe um homomorfismo $\phi : F \to G$ tal que $\phi \circ i = \varphi$. Como i é a função inclusão, temos $\phi(w) = \phi \circ i(w) = \varphi(w) = g$.

■

Corolário 2.25. *Seja F um grupo livre e $x \in F$. Então para todo $n \geq 2$, x^n não é um elemento primitivo.*

Demonstração. Suponha por contradição que x^n é um elemento primitivo. Tomemos $G = \mathbb{Z}$ e $g = 1$. Então existe um homomorfismo $\varphi : F \to \mathbb{Z}$ tal que

$$\varphi(x^n) = 1 \Rightarrow \varphi(x)^n = 1 \Rightarrow n\varphi(x) = 1 \Rightarrow \varphi(x) = \frac{1}{n},$$

que é uma contradição, pois como $n \geq 2$ teremos que $\varphi(x)$ não é inteiro. ■

Corolário 2.26. *Seja F um grupo livre e sejam $x, y \in F$. O elemento $[x, y] = xyx^{-1}y^{-1}$ não é primitivo.*

Demonstração. Seja $G = \mathbb{Z}$. Para qualquer homomorfismo $\varphi : F \to \mathbb{Z}$ temos $\varphi([x, y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x) + \varphi(y) - \varphi(x) - \varphi(y) = 0$ pois $\mathbb{Z}$ é abeliano. Logo nao existe homomorfismo de F em $\mathbb{Z}$ que mande $[x, y]$ em outro elemento de $\mathbb{Z}$ que não seja o 0. ■

3 Grafos

3.1 Definições e Propriedades

Definição 3.1. *Um grafo é um par de dois conjuntos (V,E), onde V é o conjunto de vértices e E é o conjunto de arestas, que é formado por pares de vértices. O conjunto E é um multiconjunto, isto é, seus elementos podem aparecer mais de uma vez, o que faz com que cada elemento tenha multiplicidade.*

Observação 3.2. *Os pares de arestas não são ordenados, isto é, os pares (u,v) e (v,u) são o mesmo.*

Definição 3.3.

1. *Os vértices u e v são vértices finais da aresta (u,v).*
2. *Arestas que tem os mesmos vértices finais são paralelas.*
3. *Uma aresta da forma (v,v) é um loop.*
4. *Um grafo é dito simples se não tem vertices paralelos ou loops.*
5. *Um grafo sem arestas, isto é, com $E = \emptyset$ é dito vazio.*
6. *Um grafo sem vértices, isto é, com $V = \emptyset$ é dito nulo.*
7. *Duas arestas são adjacentes se compartilham um mesmo vértice final.*
8. *Dois vértices são adjacentes se são conectados por uma aresta*
9. *O grau do vértice v, denotado por d(v), é o número de arestas que tem v como vértice final. Por convenção contamos o loop duas vezes e as arestas paralelas são contadas separadamente.*

Teorema 3.4. *O grafo G=(V,E), onde $V = \{v_1, ..., v_n\}$ e $E = \{e_1, ..., e_m\}$ satisfaz*

$$\sum_{i=1}^{n} d(v_i) = 2m$$

Demonstração. Podemos fazer a demonstração por indução em m. Para m=1, temos que $E = \{e_1\}$. Seja $e_1 = (v_1, v_2)$ temos que os únicos vértices com grau maior que zero são v_1 e v_2, pois do contrário teriamos que ter outra aresta além de e_1. Além disso, o grau de cada um deles deve ser 1, pois do contrário também teriamos que ter mais arestas além de e_1. Logo temos $\sum_{i=1}^{n} d(v_i) = d(v_1) + d(v_2) = 1 + 1 = 2 = 2.1$.

Agora suponhamos que vale para $|E| = m$. Seja G=(V,E) com $|E| = m + 1$. Considere $G^* = (V, E^*)$, onde $E^* = E \setminus \{e_{m+1}\}$. Por hipotese temos $\sum_{i=1}^{n} d^*(v_i) = 2m$. Agora, acrescentando a aresta e_{m+1}. Seja $e_{m+1} = (v_i, v_k)$ então temos que $d(v_i) = d^*(v_i)+1$, $d(v_k) = d^*(v_k) + 1$ e $d^*(v_j) = d(v_j)$ para todo $j \neq i, k$. Logo

$$\sum_{i=1}^{n} d(v_i) = 2m + 2 = 2(m + 1)$$

■

Corolário 3.5. *Todo grafo tem um número par de vértices com grau ímpar.*

Demonstração. Podemos nomear os vértices do grafos de modo que $v_1, ..., v_k$ sejam os vértices com graus ímpares e $v_{k+1}, ..., v_n$ sejam os vertices com graus pares. Pelo teorema anterior temos que

$$\begin{aligned}
d(v_1) + ... + d(v_k) + d(v_{k+1}) + ... + d(v_n) &= 2m \\
d(v_1) + ... + d(v_k) &= 2m - d(v_{k+1}) - ... - d(v_n) \\
2j_1 + 1 + ... + 2j_k + 1 &= 2m - 2j_{k+1} - ... - 2j_n \\
2(j_1 + ... + j_k) + k &= 2(m - j_{k+1} - ... - j_n) \\
k &= 2(m - j_{k+1} - ... - j_n) - 2(j_1 + ... + j_k) \\
k &= 2(m - j_{k+1} - ... - j_n - j_1 - ... - j_k)
\end{aligned}$$

Logo k é par. ■

Definição 3.6. *Um grafo simples em que todos os vértices são adjacentes é chamado completo. Isto é, um grafo é completo se para todo par de vértices existe uma aresta conectando-os.*

Observação 3.7. *Um grafo completo com n vértices é denotado por K_n*

Definição 3.8. *O grafo $G_1 = (V_1, E_1)$ é um subgrafo do grafo $G_2 = (V_2, E_2)$ se $V_1 \subset V_2$ e $E_1 \subset E_2$.*

Definição 3.9. *Um grafo direcionado é um grafo onde o conjunto E de pares $V \times V$ é ordenado. Isto é, agora os pares (u,v) e (v,u) são diferentes.*

Usamos basicamente as mesmas noções para os grafos direcionados, com algumas adaptações.

Definição 3.10.

1. *O vértice v é chamado vertice inicial e o vértice u é chamado vértice final da aresta (v,u)*
2. *O grau de saída do vértice v, denotados por $d^+(v)$, é o número de arestas que estão saindo de v. Isto é, $d^+(v) = |\{(v, u) \in E \ ; \ u \in V\}|$.*

3. *O grau de entrada do vértice v, denotados por $d^-(v)$, é o número de arestas que estão chegando em v. Isto é, $d^-(v) = |\{(u,v) \in E \ ; \ u \in V\}|$.*

Observação 3.11. *Em um grafo direcionado a direção de um loop é irrelevante.*

3.2 Grafos Conexos

Definição 3.12. *Seja $G(V,E)$ um grafo. Um caminho em G é uma sequência de vértices que são conectados por uma sequência de arestas.*

Exemplo 3.13. *Seja $G = K_4$. A sequência $\{(v_1,v_2),(v_2,v_3),(v_3,v_4)\}$ é um caminho em G que liga os vertices v_1 e v_4.*

Definição 3.14. *Seja $G(V,E)$ um grafo. Dizemos que dois vertices $v_1, v_2 \in V$ são conectos se existe um caminho em G ligando os vertices v_1 e v_2*

Definição 3.15. *Um grafo $G(V,E)$ é dito conecto, se todo par de vertices em V são conectos.*

Definição 3.16. *Seja $G(V,E)$ um grafo. Um vertice de corte é um vertice $v \in V$ tal que se retirarmos v e todas as suas arestas adjacentes, obtemos um grafo não conecto*

Proposição 3.17. *Seja $G(V,E)$ um grafo com $|V| \geq 3$. Se G não é conecto então G tem um vértice de corte.*

Demonstração. Por hipotese G não é conecto, logo existem vertices $a, b \in V$ tal que não existe um caminho que ligue a e b.

Se ambos os vértices forem isolados, isto é, ambos não têm nenhuma aresta adjacente a eles. Então qualquer um dos vertices pode ser um vertice de corte. De fato, como $|V| \geq 3$ existe um outro vértice $c \in V$ e temos que c não é conecto com nenhum dos vértices a ou b. Logo se retirarmos qualquer um deles, c ainda não será conecto com o outro, fazendo com que o grafo resultante não seja conecto.

Caso um dos vértices não seja isolado, suponha sem perda de generalidade que seja o vértice a. Então existe uma aresta (a,c) para algum vértice c. Afirmamos então que a é um vértice de corte. De fato temos que no grafo resultante os vértices c e b não são conectos. Caso contrário, existiria um caminho $\{(c,x_1),(x_1,x_2),...,(x_n,b)\}$ e neste caso teriamos que no grafo G teriamos o caminho $\{(a,c),(c,x_1),(x_1,x_2),...,(x_n,b)\}$ ligando os vértices a e b. ■

Proposição 3.18. *O grafo K_n não possui vértice de corte.*

Demonstração. De fato, seja a um vértice de K_n e seja G o grafo que obtemos retirando o vértice a e suas arestas adjacentes do grafo K_n. Dados quaisquer dois vertices x, y em VG temos que x e y são diferentes de a. Logo a aresta (x, y) de K_n não foi retirada para obter G. Então o caminho $\{(x, y)\}$ conecta x e y. ■

4 Análise de Matrizes

Definição 4.1. *Uma função* $|||.|||$: $M_n \to \mathbb{R}$ *é uma norma de matriz, se para todo* $A, B \in M_n$ *satisfaz os seguintes axiomas:*

1. $|||A||| \geq 0$ *e* $|||A||| = 0$ *se e somente se* $A = 0$
2. $|||cA||| = |c| |||A|||$, *para todo* $c \in \mathbb{R}$
3. $|||A + B||| \leq |||A||| + |||B|||$
4. $|||AB||| \leq |||A||| \; |||B|||$

Exemplo 4.2. *A* $l_1 -$ *norma definida para* $A \in M_n$ *por*

$$\|A\|_1 = \sum_{i,j=1}^{n} |a_{ij}|$$

é uma norma de matriz, pois satisfaz $\|AB\| \leq \|A\| \; \|B\|$.

Já a $l_\infty -$ *norma definida para* $A \in M_n$ *por*

$$|||A|||_\infty = \max_{1 \leq i,j \leq n} |a_{ij}|$$

é uma norma do espaço M_n, *porém não é uma norma de matriz pois se tomarmos* $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ *temos* $\|A.A\| = \|2A\| = 2\|A\| = 2$ *e* $\|A\| \; \|A\| = 1.1 = 1$. *Logo não satisfaz o axioma 4 para norma de matrizes.*

Definição 4.3. *Seja A uma matriz de ordem n. Definimos o raio espectral da matriz A, denotado por* $\rho(A)$, *por* $\max\{|\lambda|;\ \lambda$ *é autovalor de* $A\}$.

Propriedades 4.4.

1. *Se* λ *é autovalor da matriz A, então* $c\lambda$ *é autovalor da matriz* cA. *De fato, temos que* $Ax = \lambda x \Rightarrow cAx = c\lambda x$
2. *Se c>0, então* $\rho(cA) = c\rho(A)$. *Direto do item 1, temos que o conjunto de autovalores de cA é o conjunto* $\{c\lambda;\ \lambda$ *é autovalor de* $A\}$. *Logo temos* $\rho(cA) = \max\{|\lambda|;\ \lambda$ *é autovalor de* $cA\} = \max\{|c\lambda|;\ \lambda$ *é autovalor de* $A\} = |c| \max\{|\lambda|;\ \lambda$ *é autovalor de* $A\} = c\rho(A)$.
3. *Se* λ *é autovalor de A, então* λ^k *é autovalor de* A^k *para qualquer* $k \in \mathbb{N}$. *Por indução em k, suponha que vale para todo inteiro menor ou igual a k. Temos então* $A^{k+1}x = AA^kx = A(\lambda^k x) = \lambda^k(Ax) = \lambda^k \lambda x = \lambda^{k+1}x$. *Desta mesma maneira é trivial mostrar que vale para k=2. Logo, vale para todo inteiro positivo k.*

4. $\rho(A^k) = \rho(A)^k$. *De fato, pelo item anterior temos que o conjunto de autovalores de* A^k *é o conjunto* $\{\lambda^k;\ \lambda$ *é autovalor de* $A\}$. *Logo,* $\rho(A^k) = \max\{|\lambda|^k;\ \lambda$ *é autovalor de* $A\} = (\max\{|\lambda|;\ \lambda$ *é autovalor de* $A\})^k = \rho(A)^k$

Teorema 4.5. *Sejam* $|||.|||$ *uma norma de matriz em* M_n*,* $A \in M_n$ *e* λ *um autovalor de* A*. Então* $|\lambda| \leq \rho(A) \leq |||A|||$.

Demonstração. A primeira desigualdade é direto da definição de $\rho(A)$. Agora, se λ é um autovalor de A, então existe $x \in \mathbb{R}^n$ tal que $x \neq 0$ e $Ax = \lambda x$. Tomemos então $X \in M_n$ definidido por $X = (x, x..., x)$. Temos que $AX = (Ax, Ax, ..., Ax) = (\lambda x, \lambda x, ..., \lambda x) = \lambda X$. Logo, temos $|\lambda|\ |||X||| = |||\lambda X||| = |||AX||| \leq |||A|||\ |||X||| \Rightarrow |\lambda| \leq |||A|||$. Como $\rho(A) = |\lambda|$ para algum autovalor λ de A, temos $\rho(A) \leq |||A|||$. ■

Lema 4.6. *Seja* $A \in M_n$*. Dado* $\epsilon > 0$*, existe uma norma de matriz* $|||.|||$ *tal que* $\rho(A) \leq |||A||| \leq \rho(A) + \epsilon$.

Lema 4.7. *Seja* $A \in M_n$*. Se existe uma norma de matriz* $|||.|||$ *tal que* $|||A||| < 1$*, então* $\lim_{k\to\infty} A^k = 0$*. Isto é, cada entrada de* A^k *tende a zero quando* $k \to \infty$.

Demonstração. Temos $|||A^k||| \leq |||A|||^k$. Como $|||A||| < 1$ então

$$\lim_{k\to\infty} |||A^k||| \leq \lim_{k\to\infty} |||A|||^k = 0$$

. ■

Teorema 4.8. *Seja* $A \in M_n$*. Então* $\lim_{k\to\infty} A^k = 0$ *se e somente se* $\rho(A) < 1$.

Demonstração. Supondo que $A^k \to 0$ e seja $x \neq 0$ um vetor tal que $Ax = \lambda x$, então $A^k x = \lambda^k x$. Logo, como $A^k x \to 0$ temos $\lambda^k x \to 0$, e isso só ocorre se $|\lambda| < 1$. Como a desigualdade vale para qualquer autovalor de A, temos $\rho(A) < 1$.

Supondo que $\rho(A) < 1$. Pelo Lema 4.6 podemos tomar uma norma de matriz tal que $|||A||| < 1$. Logo, pelo Lema 4.7 $A^k \to 0$. ■

Corolário 4.9. *Sejam* $|||.|||$ *uma norma de matriz em* M_n *e* $A \in M_n$*. Então*

$$\lim_{k\to\infty} |||A^k|||^{\frac{1}{k}} = \rho(A)$$

Demonstração. Como $\rho(A)^k = \rho(A^k) \leq |||A^k|||$, temos $\rho(A) \leq |||A^k|||^{\frac{1}{k}}$ para todo $k \in \mathbb{N}$. Dado $\epsilon > 0$, a matriz $\bar{A} = \dfrac{1}{\rho(A)+\epsilon} A$ tem raio espectral $\rho(\bar{A}) = \dfrac{1}{\rho(A)+\epsilon}\rho(A) < 1$. Pelo Teorema 4.8 temos $\bar{A}^k \to 0$, logo existe k_0 tal que, se $k \geq k_0$ temos $|||\bar{A}^k||| < 1 \Rightarrow \left|\left|\left|\left(\dfrac{1}{\rho(A)+\epsilon} A\right)^k\right|\right|\right| < 1 \Rightarrow \dfrac{1}{(\rho(A)+\epsilon)^k} |||A^k||| < 1 \Rightarrow |||A^k||| < (\rho(A)+\epsilon)^k \Rightarrow |||A^k|||^{\frac{1}{k}} < \rho(A) + \epsilon$. Então

$$\rho(A) \leq |||A^k|||^{\frac{1}{k}} < \rho(A) + \epsilon.$$

Como ϵ foi dado arbitrariamente, temos $\lim_{k\to\infty} |||A^k|||^{\frac{1}{k}} = \rho(A)$.

■

Definição 4.10. *Sejam $A = [a_{ij}]$ e $B = [b_{ij}]$ matrizes de ordem n. Dizemos que $A \leq B$ se $a_{ij} \leq b_{ij}$ para todo $i, j \in \{1, ..., n\}$. A primeira desigualdade é estrita quando a segunda desigualdade é estrita .*

Proposição 4.11. *Sejam A e B matrizes não negativas, isto é, $A, B \geq 0$. Se $A \leq B$ então:*
(a) $A^m \leq B^m$
(b) $\|A\|_1 \leq \|B\|_1$

Demonstração. (a) Para m=2 temos que Se $A \leq B$ então $a_{ij} \leq b_{ij}$ para todo $i, j \in \{1, ..., n\}$. Logo $a_{ik}a_{kj} \leq b_{ik}b_{kj}$ para todo $k \in \{1, ..., n\}$. Então $a^2_{ij} = a_{i1}a_{1j} + a_{i2}a_{2j} + ... + a_{in}a_{nj} \leq b_{i1}b_{1j} + b_{i2}b_{2j} + ... + b_{in}b_{nj} = b^2_{ij} \Rightarrow A^2 \leq B^2$.
Por indução em m, suponhamos que vale para m. Então $A^{m+1} = A^m A$ e $B^{m+1} = B^m B$ e temos que $a^{m+1}_{ij} = a^m_{i1}a_{1j} + ... + a^m_{n1}a_{nj} \leq b^m_{i1}b_{1j} + ... + b^m_{n1}b_{nj} = b^{m+1}_{ij} \Rightarrow A^{m+1} \leq B^{m+1}$.
(b) Como $a_{ij} \leq b_{ij}$ para todo $i, j \in \{1, ..., n\}$ e A,B são matrizes não negativas, todas as entradas são não negativas. Logo, a norma $\|.\|_1$ é a soma das entradas da matriz. Então $\|A\|_1 = \sum_{i,j=1}^n a_{ij} \leq \sum_{i,j=1}^n = \|B\|$ ■

Teorema 4.12. ***(Perron-Frobenius)*** *Seja A uma matriz não negativa. Então $\rho(A)$ é um autovalor de A, associado a um autovetor v não negativo. Isto é, existe $v > 0$ tal que $Av = \rho(A)v$.*

Proposição 4.13. *Sejam A, B matrizes simetricas positivas tal que $A < B$. Então $\rho(A) < \rho(B)$*

Demonstração. Primeiro observe que como B é simétrica, seus autovetores formam uma base de $\mathbb{R}^n$ e logo para todo $x \in \mathbb{R}^n$, se $\{v_1, ...v_n\}$ é a base de autovetores temos

$$\begin{aligned} Bx &= B(x_1v_1 + ... + x_nv_n) \\ &= x_1Bv_1 + ...x_nBv_n \\ &= x_1\lambda_1v_1 + ... + x_n\lambda_nv_n \\ &\leq x_1\rho(B)v_1 + ...x_n\rho(B)v_n \\ &= \rho(B)(x_1v_1 + ... + x_nv_n) \\ &= \rho(B)x \end{aligned}$$

E temos também que A=B+(A-B)

Usando o Teorema de Perron-Frobenius existe um vetor positivo v tal que $Av = \rho(A)v$. E como $A < B$ temos $(A - B) < 0$ e logo $(A - B)v < 0$ pois v é positivo. Então

$$\begin{aligned} \rho(A)v &= Av \\ &= [B + (A - B)]v \\ &= Bv + (A - B)v \\ &\leq \rho(B)v + (A - B)v \\ &\leq \rho(B)v \end{aligned}$$

Como v é positivo, temos $\rho(A) \leq \rho(B)$

■

Teorema 4.14. ***(Teorema Espectral)*** *Seja A uma matriz simétrica de ordem n com coeficientes reais. Então:*

1. *Todos os autovalores de A são reais.*
2. *autovetores associados a autovalores distintos são ortogonais.*
3. *a dimensão do autoespaço associado a um autovalor é igual a multiplicidade deste autovalor como raiz do polinomio caracteristico de A.*
4. *Existe uma base ortonormal de $\mathbb{R}^n$ formada por autovetores de A.*
5. *A é diagonalizável por uma matriz de mudança de coordenadas ortonormal P. A matriz P cujas colunas são os autovetores (ortonormais) de A é tal que*

$$P^T AP = P^{-1}AP = D,$$

onde D é a matriz diagonal com sua diagonal principal sendo os autovalores de A.

Proposição 4.15. *Seja A uma matriz simétrica de ordem n. Para todo vetor $v \in \mathbb{R}^n$ temos que*

$$\frac{vAv^T}{vv^T} \leq \rho(A)$$

.

Demonstração. Como A é uma matriz simétrica, pelo Teorema Espectral temos que existe uma base ortonormal de $\mathbb{R}^n$ formada por autovetores de A. Seja $\{u_1, ..., u_n\}$ a base ortonormal de $\mathbb{R}^n$ formada por autovetores de A. Logo $v = a_1u_1 + ... + a_nu_n$ e como a base é formada por autovetores de A e é ortonormal, temos

$$\begin{aligned} vAv^T &= < v, Av > \\ &= < (a_1u_1 + ... + a_nu_n), A(a_1u_1 + ... + a_nu_n) > \\ &= < (a_1u_1 + ... + a_nu_n), a_1Au_1 + ... + a_nAu_n > \\ &= < (a_1u_1 + ... + a_nu_n), a_1\lambda_1u_1 + ... + a_n\lambda_nu_n > \\ &= a_1^2\lambda_1 < u_1, u_1 > +... + a_n^2\lambda_n < u_n, u_n > \\ &= a_1^2\lambda_1 + ... + a_n^2\lambda_n \\ &\leq a_1^2\rho(A) + ... + a_n^2\rho(A) = \rho(A)(a_1^2 + ... + a_n^2) \end{aligned}$$

e também,

$$\begin{aligned} vv^T &= < v, v > \\ &= < (a_1u_1 + ... + a_nu_n), (a_1u_1 + ... + a_nu_n) > \\ &= a_1^2 < u_1, u_1 > +... + a_n^2 < u_n, u_n > \\ &= a_1^2 + ... + a_n^2. \end{aligned}$$

Logo, temos

$$\begin{aligned} \frac{vAv^T}{vv^T} &= \frac{vAv^T}{(a_1^2 + ...a_n^2)} \\ &\leq \frac{\rho(A)(a_1^2 + ... + a_n^2)}{(a_1^2 + ...a_n^2)} \\ &= \rho(A) \end{aligned}$$

■

Definição 4.16. *Duas matrizes de A e B, de ordem n, são semelhantes se existir uma matriz invertível M tal que*

$$A = M^{-1}BM$$

Observação 4.17. *É facil observar que a semelhança de matrizes define uma relação de equivalência*

Proposição 4.18. *Sejam A e B são matrizes semelhantes. Então*

- $det(A) = det(B)$
- $Tr(A) = Tr(B)$

Demonstração. Como $A = M^{-1}BM$, usando a propriedade $det(AB) = det(A)det(B)$ do determinante do produto matrizes, temos

$$det(A) = det(M^{-1}BM) = det(M^{-1})det(B)det(M) = \frac{1}{det(M)}det(B)det(M) = det(B)$$

Usando a propriedade $Tr(AB) = Tr(BA)$ do Traço do produto de matrizes, temos

$$tr(A) = Tr(M^{-1}BM) = Tr(BMM^{-1}) = Tr(B)$$

■

Corolário 4.19. *Seja A é uma matriz simétrica. O determinante de A é dado pelo produto de seus autovalores elevados a suas multiplicidades. E o traço de A é a soma dos seus autovalores contados pela multiplicidade.*

Demonstração. Pelo Teorema Espectral temos que A é diagonalizavel e que $A = PDP^{-1}$, onde D é a matriz diagonal com diagonal igual aos autovalores de A. Podemos observar também que neste caso A e D são semelhantes, logo tem o mesmo determinante e o mesmo traço. Como D é uma matriz diagonal, seu determinante é o produto da diagonal principal. Logo

$$det(A) = det(D) = \prod \lambda_i^{m_i}$$

e

$$Tr(A) = Tr(D) = \sum m_i \lambda_i$$

onde λ_i é autovalor de A e m_i é a multiplicidade do autovalor λ_i. ■

Proposição 4.20. *Seja A uma matriz simétrica. Se $\chi A(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ é o polinomio caracteristico de A, então temos*

$$\begin{gathered} a_0 = det(A) \\ a_1 = -\sum det(A_{ii}) \\ a_{n-1} = (-1)^{n-1}Tr(A) \end{gathered}$$

Demonstração. Pelo Teorema Espectral todos os autovalores de A são reais. Podemos então escrever o polinômio caracteristico como

$$\chi A(x) = (-1)^n (x - \lambda_1)(x - \lambda_2)...(x - \lambda_n)$$

Desenvolvendo a expressão apenas para os termos de x^{n-1}, x e x^0 e usando o corolário 4.19 teremos

$$\begin{gathered} x^{n-1}(-1)^n(-\lambda_1 - \lambda_2 - ... - \lambda_n) = (-1)^n[-(\lambda_1 + \lambda_2 + ... + \lambda_n)] = x^{n-1}(-1)^{n-1}Tr(A) \\ x(-1)^n[(-1)^{n-1}\prod_{i\neq 1}\lambda_i + (-1)^{n-1}\prod_{i\neq 2}\lambda_i + ... + (-1)^{n-1}\prod_{i\neq n}\lambda_i] = x[-\sum det(A_{ii})] \\ x^0(-1)^n[(-1)^n \prod \lambda_i] = x_0[det(A)] \end{gathered}$$

e concluimos que $a_{n-1} = (-1)^{n-1}Tr(A)$, $a_1 = -\sum det(A_{ii})$ e $a_0 = det(A)$.

Obs: Para a igualdade do coeficiente a_1 usamos que a matriz A_{ii} ainda é uma matriz simetrica e a matriz diagonal a qual ela é semelhante é a matriz dos com a diagonal principal sendo os autovalores, exceto o autovalor λ_i. ■

5 Densidades

Neste capítulo iremos definir as primeiras noções de densidades, algumas de suas propriedades básicas e daremos alguns exemplos de subconjuntos com comportamentos estranhos.

5.1 Introdução a Densidades

Definição 5.1. *Seja G um grupo finitamente gerado e X o conjunto finito de geradores de G. A bola de raio n, centrada na identidade, com respeito a X, denotada por $B_X(n)$, é o conjunto de elementos de G que podem ser escritos como uma palavra em X tendo comprimento no maximo n.*

Definição 5.2. *Seja G um grupo finitamente gerado e X o conjunto finito de geradores de G. A esfera de raio n, centrada na identidade, com respeito a X, denotada por $S_X(n)$ é exatamente $\{1\}$ para $n = 0$ e $B_X(n) \setminus B_X(n-1)$ se $n \neq 0$*

Lema 5.3. *Seja a_n uma sequência de números reais maiores que 1. Se a_n é submultiplicativa, então $\sqrt[n]{a_n}$ converge.*

Demonstração. Primeiro vamos mostrar que se c_n é uma sequência de números reais positivos subaditiva, então

$$\lim \frac{c_n}{n} = \inf \frac{c_n}{n}$$

Dado $m \in \mathbb{N}$. Para todo $n \in \mathbb{N}$, temos $n = mq + r$, com $r < m$. Se $a = \max\{c_1, ..., c_m\}$ temos $c_r \leq a$. Logo

$$\begin{aligned} c_n &= c_{mq+r} \\ &\leq qc_m + c_r \\ &\leq qc_m + a \end{aligned}$$

$$\frac{c_n}{n} \leq \frac{q}{n}c_m + \frac{a}{n}$$

Note que quando $n \to \infty$ temos $q \to \infty$ e $\lim \frac{q}{n} = \lim \frac{q}{mq+r} = \lim \frac{1}{m + \frac{r}{q}} = \frac{1}{m}$.
Como m foi dado arbirariamente, temos que

$$\limsup_{n\to\infty} \frac{c_n}{n} \leq \inf \frac{c_m}{m}$$

Por outro lado temos que $\frac{c_n}{n} \geq \inf \frac{c_m}{m}$ e logo $\liminf \frac{c_n}{n} \geq \inf \frac{a_m}{m}$.

Concluimos então que

$$\inf \frac{c_m}{m} \leq \liminf \frac{c_n}{n} \leq \limsup \frac{c_n}{n} \leq \inf \frac{c_m}{m}$$

$$\lim_{n\to\infty} \frac{c_n}{n} = \inf \frac{c_n}{n}$$

.

Agora seja a_n uma sequência de números reais maiores que 1, submultiplicativa. Então $c_n = \ln(a_n)$ é uma sequência de números reais positivos, aditiva. De fato temos $c_{n+m} = \ln(a_{n+m}) \leq \ln(a_n a_m) = \ln(a_n) + \ln(a_m) = c_n + c_m$. Vimos então que existe o limite

$$l = \lim \frac{c_n}{n} = \lim \frac{1}{n} \ln(a_n) = \lim \ln(\sqrt[n]{a_n})$$

■

Proposição 5.4. *O limite* $\lim_{n\to\infty} |B_X(n)|^{1/n}$ *sempre existe. Chamamos esse limite de taxa de crescimento exponencial de G com respeito a X. Em geral, esse limite depende de X, mas o fato de ser 1 ou maior que 1 não depende de X.*

Demonstração. Considere o conjunto

$$S = B_X(n) \times B_X(m) = \{w \in F_p \ ; \ w = uv, \ com \ u \in B_X(n) \ e \ v \in B_X(m)\}$$

Note que $|B_X(n) \times B_X(m)| < |B_X(n)|.|B_X(m)|$. Pois dois pares distintos de palavras podem resultar na mesma palavra reduzida em S

Seja $w \in B_X(n+m)$ uma palavra reduzida. Então $|w| \leq n+m$. Se $|w| \leq n$ temos que $w \in B_X(n)$ e logo $w = w.1 \in B_X(n) \times B(m)$. Se $|w| > n$, então $w = uv$ com $|u| = n$ e $|v| < m$ e neste caso também temos $w = u.v \in B_X(n) \times B(m)$ Logo $B_X(n+m) \subseteq S$ e consequentemente

$$|B_X(n+m)| \leq |S| \leq |B_X(n)|.|B_X(m)|$$

Logo, a sequência de números reais $B_n = |B_X(n)|$ é submultiplicativa.
Pelo Lema 5.3 temos que existe $\lim \sqrt[n]{|B_X(n)|}$. ■

Definição 5.5. *Dizemos que um grupo tem crescimento exponencial quando a taxa de crescimento exponencial é maior que 1, e subexponencial quando a taxa de crescimento é igual a 1.*

Definição 5.6. *Seja G um grupo finitamente gerado com conjunto finito de geradores X. Para qualquer subconjunto de $S \subseteq G$ nós definimos a desnsidade natural do conjunto S com respeito a X, denotado por $\delta_X(S)$ como*

$$\delta_X(S) = \limsup_{n\to\infty} \frac{|S \bigcap B_X(n)|}{|B_X(n)|}.$$

E a densidade exponencial de S com respeito a X, denotado por $d_X(S)$ como

$$d_X(S) = \limsup_{n\to\infty} \left(\frac{|S \bigcap B_X(n)|}{|B_X(n)|} \right)^{1/n}.$$

Observação 5.7. *De acordo com a proposição 3.3, se 'a' é a taxa de crescimento de G podemos escrever*

$$d_X(S) = \frac{1}{a} \limsup_{n\to\infty} |S \bigcap B_X(n)|^{1/n}.$$

Propriedades 5.8.

1. *Tanto a densidade natural quando a densidade exponencial são numeros reais entre 0 e 1. Pois $\dfrac{|S \bigcap B_X(n)|}{|B_X(n)|}$ está sempre entre 0 e 1.*

2. *Se $|G| = \infty$ então subconjuntos finitos de G terão densidade natural 0. Pois para n suficientemente grande, $|S \bigcap B_X(n)|$ será constante e $|B_X(n)|$ vai para infinito.*

3. *O próprio G tem densidade natural e exponencial 1. Pois neste caso temos $|S \bigcap B_X(n)| = |B_X(n)|$.*

4. *O conjunto vazio é o unico com densidade exponencial zero. Isso decorre de que $d_X(S) = \dfrac{1}{a} \limsup_{n\to\infty} |S \bigcap B_X(n)|^{1/n}$. Se $S \neq \emptyset$ teremos $|S \bigcap B_X(n)| \geq 1$. O que implica $|S \bigcap B_X(n)|^{1/n} \geq 1$. Logo $\limsup_{n\to\infty} |S \bigcap B_X(n)|^{1/n} \geq 1 > 0$.*

5. *Conjuntos finitos tem densidade exponencial $\frac{1}{a}$. Pois para n suficientemente grande, $|S \bigcap B_X(n)|$ será uma constante C e $\lim_{n\to\infty} C^{1/n} = 1$.*

6. *Se G é um grupo com crescimento subexponencial, isto é, com taxa de crescimento exponencial igual a 1, então para todo conjunto $S \subseteq G$ não vazio*

$$d_X(S) = \limsup_{n\to\infty} |S \bigcap B_X(n)|^{1/n} = 1.$$

   Pois neste caso

$$|S \bigcap B_X(n)| \geq 1.$$

   Então temos $d_X(S) \geq 1$ e $d_X(S) \leq 1$. Logo $d_X(S) = 1$.

   Neste caso a desnsidade exponencial não mede nada. Desta maneira apenas a densidade natural é relevante.

7. *Se G é um grupo com crescimento exponencial $a > 1$ e S um subconjunto de G com densitade exponencial menor que 1, então existe $\epsilon > 0$ tal que $|S \bigcap B_X(n)| < (a-\epsilon)^n$ para n sufucientemente grande. Como $\lim |B_X(n)|^{1/2} = a$ temos que para n suficientemente grande $|B_X(n)|^{1/n} > a - \frac{\epsilon}{2} \Rightarrow |B_X(n)| > (a - \frac{\epsilon}{2})^n$. Logo temos $\dfrac{|S \bigcap B_X(n)|}{|B_X(n)|} < \left(\dfrac{a-\epsilon}{a-\frac{\epsilon}{2}} \right)^n$. O que implica que a densidade natural de S é zero*

   Neste caso a densidade natural so é sensivel entre conjuntos com densidade exponencial igual a 1.

8. *Conjuntos com densidade natural positiva tem densidade exponencial 1. De fato como vimos anteriormente, se a densidade exponencial fosse menor que 1 a densidade natural teria que ser 0.*

Em geral, a densidade natural e exponencial de um conjunto $S \subseteq G$ depende do conjunto de geradores X, como veremos no exemplo a seguir.

Exemplo 5.9. *Considere $G = \mathbb{Z}^2$, os pontos de coordenadas inteiras no plano, e os conjuntos de geradores $X = \{(1,0),(0,1)\}$ e $Y = \{(1,0),(1,1)\}$. Seja S o conjuntos de pontos de coordenadas positivas, isto é, $S = \{(x,y); x, y > 0\}$.*

Observe que $|B_X(n)| = |B_X(n-1)| + 4 + 4(n-1)$ pois é composta dos pontos da bola de raio $n-1$ mais os pontos a^n, b^n, a^{-n}, b^{-n} e os pontos da forma

$$a^{n-1}b, a^{n-2}b^2, ..., a^2b^{n-2}, ab^{n-1}, a^{-(n-1)}b, a^{-(n-2)}b^2, ..., a^{-2}b^{n-2}, a^{-1}b^{n-1}$$

e seus inversos, onde $a = (1,0)$ e $b = (0,1)$. (Veja a figura 1). Desta maneira temos:

$$\begin{aligned}
|B_X(0)| &= 1 \\
|B_X(1)| &= 1+4 \\
|B_X(2)| &= 1+4+4+4(1) \\
|B_X(3)| &= 1+4+4+4.(1)+4+4.(2) \\
&\vdots \\
|B_X(n)| &= 1+4n+4(1+2+...+(n-1)) \\
&= 1+4n+4(\frac{n(n-1)}{2}) \\
&= 1+4n+2n^2-2n \\
&= 2n^2+2n+1
\end{aligned}$$

Analogamente, temos que $|B_Y(n)| = |B_Y(n-1)| + 2(n+1) + 2(n-1)$ pois é composta da bola de raio $n-1$ mais os pontos

$$a^nb^0, a^{n-1}b, ..., a^1b^{n-1}, a^0b^n, a^{-1}b^{n-1}, a^{-2}b^{n-2}, ..., a^{n-1}b$$

e seus inversos, onde $a = (1,0)$ e $b = (1,1)$. (Veja figura 1). Desta maneira temos:

$$
\begin{aligned}
|B_Y(0)| &= 1 \\
|B_Y(1)| &= 1 + 2(2) + 2(0) \\
|B_Y(2)| &= 1 + 2(2) + 2(3) + 2(1) \\
|B_Y(3)| &= 1 + 2(2) + 2(3) + 2(1) + 2(4) + 2(2) \\
|B_Y(4)| &= 1 + 2(2) + 2(3) + 2(1) + 2(4) + 2(2) + 2(5) + 2(3) \\
&\vdots \\
|B_Y(n)| &= 1 + 2(1 + 2 + ... + (n+1)) + 2(2 + 3 + ... + (n-1)) \\
&= 1 + 2(1 + 2 + ... + (n+1)) + 2(1 + 2 + 3 + ... + (n-1) - 1) \\
&= 1 + 2\left(\frac{(n+1)(n+2)}{2}\right) + 2\left(\frac{n(n-1)}{2} - 1\right) \\
&= 1 + 2\left(\frac{(n+1)(n+2)}{2}\right) + 2\left(\frac{n(n-1)-2}{2}\right) \\
&= 1 + (n+1)(n+2) + n(n-1) - 2 \\
&= 1 + n^2 + 2n + n + 2 + n^2 - n - 2 \\
&= 2n^2 + 2n + 1
\end{aligned}
$$

Logo temos $|B_X(n)| = |B_Y(n)| = 2n^2 + 2n + 1$.

Agora, note que $|S \bigcap B_X(n)| = |S \bigcap B_X(n-1)| + (n-1)$.
Logo $|S \bigcap B_X(n)| = 1 + 2 + ... + (n-1) = \dfrac{n^2 - n}{2}$. Temos então

$$\delta_X(S) = \limsup \frac{|S \bigcap B_X(n)|}{|B_X(n)|} = \lim \frac{n^2 - n}{4n^2 + 4n + 2} = \frac{1}{4}$$

Já para $|S \cap B_Y(n)|$ *temos*

$$\begin{aligned}
|S \bigcap B_Y(1)| &= 1 \\
|S \bigcap B_Y(2)| &= 1+2 \\
|S \bigcap B_Y(3)| &= 1+2+3+1 \\
|S \bigcap B_Y(4)| &= 1+2+3+1+4+1 \\
|S \bigcap B_Y(5)| &= 1+2+3+1+4+1+5+2 \\
|S \bigcap B_Y(6)| &= 1+2+3+1+4+1+5+2+6+2 \\
&\vdots \\
|S \bigcap B_Y(2n)| &= 1+2+3+1+4+1+...+(2n-1)+(n-1)+2n+(n-1) \\
&= (1+2+...+2n)+2(1+2+...+(n-1)) \\
&= n(2n+1)+n(n-1) \\
&= 2n^2+n+n^2-n \\
&= 3n^2 \\
|S \bigcap B_Y(2n+1)| &= 3n^2+(2n+1)+n \\
&= 3n^2+3n+1
\end{aligned}$$

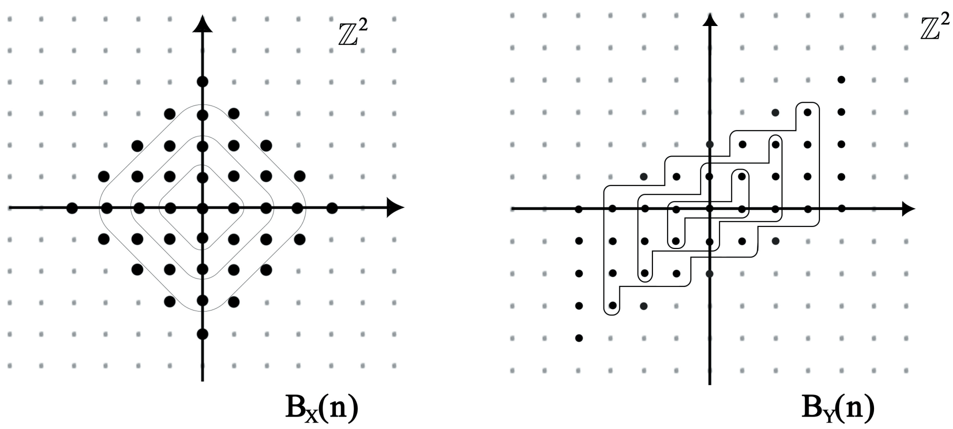

Figura 1 –

E teremos então que

$$\delta_X(S) = \limsup \frac{|S \cap B_Y(n)|}{|B_Y(n)|} = \lim \frac{|S \cap B_Y(2n)|}{|B_Y(2n)|} = \lim \frac{3n^3}{4n^3+4n^2+2n} = \frac{3}{2}.$$

Logo, as densidades naturais dependem do conjunto de geradores.

Exemplo 5.10. *Consideremos agora um grupo livre de classe 2* $F_2 =< a, b >$ *e* $X = \{a, b\}$. *Seja* S *o conjunto das palavras positivas em* X, *isto é,* $S = \{x_1...x_r \ ; \ x_i = a, b\}$.

Como F_2 é um grupo livre, só tem relatores triviais. Logo, pelo principio fundamental da contagem temos $4 \times 3^{n-1}$ possibilidades para escrever uma palavra em X de comprimento n. Pois só não podemos escolher o elemento inverso para cada letra seguinte. Logo temos $|S_X(n)| = 4 \times 3^{n-1}$. Então

$$\begin{aligned} |B_X(n)| &= 1 + \sum_{i=1}^{n} |S_X(i)| \\ &= 1 + 4\sum_{i=0}^{n-1} 3^i \\ &= 1 + 4\left(\frac{1-3^n}{1-3}\right) \\ &= 1 + 2(3^n - 1) \\ &= 2(3)^n - 1 \end{aligned}$$

Logo, F_2 tem crescimento exponencial, e temos $a = \lim(2.3^n - 1)^{1/n} = \lim(2.3^n)^{1/n} = 3$. Analogamente temos que existem 2^n palavras positivas de comprimento n. Então

$$\begin{aligned} |S \bigcap B_X(n)| &= 1 + \sum_{i=1}^{n} |S \bigcap S_X(i)| \\ &= 1 + \sum_{i=1}^{n} 2^i \\ &= \sum_{i=0}^{n} 2^i \\ &= \left(\frac{1-2^{n+1}}{1-2}\right) \\ &= 2^{n+1} - 1. \end{aligned}$$

Temos então

$$d_X(S) = \frac{1}{3}\lim(2^{n+1} - 1)^{1/n} = \frac{2}{3}$$

Proposição 5.11. *Seja G um grupo infinito, finitamente gerado por um conjunto de geradores X. Existe um subconjunto $S \subset G$ tal que $\delta_X(S) = 1$ e também $\delta_X(G \setminus S) = 1$*

Demonstração. Para construirmos este conjunto, encontraremos duas sequencias $(n_i)_{i\in\mathbb{N}}$ e $(m_i)_{i\in\mathbb{N}}$, tais que $n_1 = 1$ e $n_i < m_i < n_{i+1}$ e definiremos o conjunto S da seguinte maneira

$$S = \bigcup_{i\geq 1}\left(\bigcup_{n_i<j\leq m_i} S_X(j)\right)$$

Escolheremos nossas sequencias da seguinte maneira: $n_1 = 1, m_1 > 1$ e a partir dai escolheremos n_2 tal que $|B_X(n_2)| > 2(|B_X(m_1)| - |B_X(n_1)|)$. Assim temos n_2 que satisfaça (Veja figura 2)

$$\begin{aligned} \frac{|S \bigcap B_X(n_2)|}{|B_X(n_2)|} &= \frac{|B_X(m_1)| - |B_X(n_1)|}{|B_X(n_2)|} \\ &< \frac{1}{2}. \end{aligned}$$

Agora, tomemos m_2 tal que $|B_X(m_2)| > 2|B_X(n_2)|$. O que implica $\frac{1}{2} > \frac{|B_X(n_2)|}{|B_X(m_2)|}$. Logo (Veja figura 2)

$$\begin{aligned}
\frac{|S \bigcap B_X(m_2)|}{|B_X(m_2)|} &> \frac{|B_X(m_2)| - |B_X(n_2)|}{|B_X(m_2)|} \\
&= 1 - \frac{|B_X(n_2)|}{|B_X(m_2)|} \\
&> 1 - \frac{1}{2}
\end{aligned}$$

Analogamente, tomemos n_3 tal que $|B_X(n_3)| > 3(|B_X(m_2)| - |B_X(n_2)| + |B_X(m_1)| - |B_X(n_1)|)$ e teremos assim n_3 que satisfaça

$$\begin{aligned}
\frac{|S \bigcap B_X(n_3)|}{|B_X(n_3)|} &= \frac{|B_X(m_2)| - |B_X(n_2)| + |B_X(m_1)| - |B_X(n_1)|}{|B_X(n_3)|} \\
&< \frac{1}{3}
\end{aligned}$$

Tomemos m_3 tal que $|B_X(m_3)| > 3|B_X(n_3)|$, o que implica $\frac{1}{3} > \frac{|B_X(n_3)|}{|B_X(m_3)|}$. Logo

$$\begin{aligned}
\frac{|S \bigcap B_X(m_3)|}{|B_X(m_3)|} &> \frac{|B_X(m_3)| - |B_X(n_3)|}{|B_X(m_3)|} \\
&= 1 - \frac{|B_X(n_3)|}{|B_X(m_3)|} \\
&> 1 - \frac{1}{3}
\end{aligned}$$

Continuando analogamente a construção dessas sequências, teremos

$$\frac{|S \bigcap B_X(n_i)|}{|B_X(n_i)|} < \frac{1}{i} \quad \text{e} \quad \frac{|S \bigcap B_X(m_i)|}{|B_X(m_i)|} > 1 - \frac{1}{i}$$

E consequentemente

$$\begin{aligned}
1 &= \frac{|B_X(n_i)|}{|B_X(n_i)|} \\
&= \frac{|S \bigcap B_X(n_i)| + |(G \setminus S) \bigcap B_X(n_i)}{|B_X(n_i)|} \\
&= \frac{|S \bigcap B_X(n_i)|}{|B_X(n_i)|} + \frac{|(G \setminus S) \bigcap B_X(n_i)|}{|B_X(n_i)|} \\
&< \frac{1}{i} + \frac{|(G \setminus S) \bigcap B_X(n_i)|}{|B_X(n_i)|}
\end{aligned}$$

Com calculos analogos temos

$$\frac{|(G \setminus S) \bigcap B_X(n_i)|}{|B_X(n_i)|} > 1 - \frac{1}{i} \quad \text{e} \quad \frac{|(G \setminus S) \bigcap B_X(m_i)|}{|B_X(m_i)|} < \frac{1}{i}$$

Podemos então concluir que $\delta_X(S) = \delta_X(G \setminus S) = 1$

■

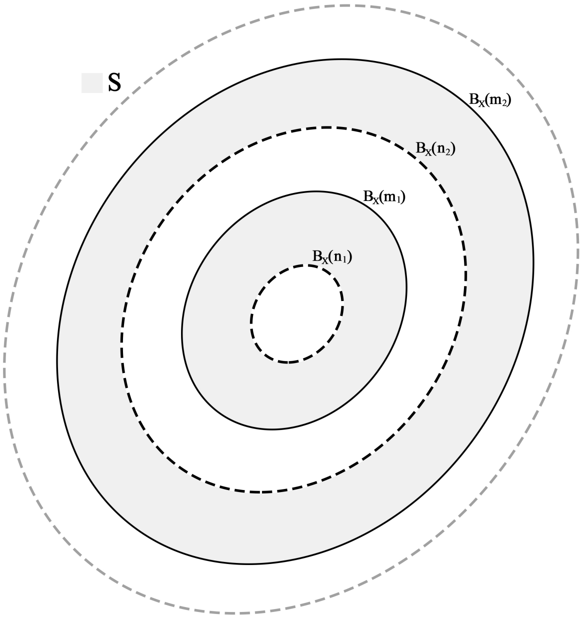

Figura 2 –

A proposicão 3.10 mostra que, em geral, a densidade natural não é aditiva mesmo em conjuntos disjuntos. Isto é, podemos ter conjuntos disjuntos S_1 e S_2 tais que $\delta_X(S_1 \bigcup S_2) \neq \delta_X(S_1) + \delta_X(S_2)$. Daremos um exemplo importante a disto a seguir.

Exemplo 5.12. *Considere o grupo livre F_p de classe $p \geq 2$ e a base livre X. Tomemos os seguintes conjuntos disjuntos*

$$S_1 = \bigcup_{n\ impar} S_X(n) \qquad e \qquad S_2 = \bigcup_{n\ par} S_X(n)$$

Temos $|S_X(n)| = 2p(2p-1)^{n-1}$. Logo

$$\begin{aligned}
|S_1 \bigcap B_X(2n+1)| &= |S_X(1)| + |S_X(3)| + ... + |S_X(2n+1)| \\
&= 2p + 2p(2p-1)^2 + 2p(2p-1)^4 + ... + 2p(2p-1)^{2n} \\
&= 2p \sum_{j=0}^{n} (2p-1)^{2j} \\
&= 2p \left(\frac{[(2p-1)^2]^{n+1} - 1}{(2p-1)^2 - 1} \right) \\
&= \frac{2p[(2p-1)^{2n+2} - 1]}{(2p-1)^2 - 1}
\end{aligned}$$

E também

$$\begin{aligned}
|B_X(2n+1)| &= 1 + |S_X(1)| + |S_X(2)| + |S_X(3)| + ... + |S_X(2n+1)| \\
&= 1 + 2p + 2p(2p-1) + 2p(2p-1)^2 + ... + 2p(2p-1)^{2n} \\
&= 1 + 2p\sum_{j=0}^{2n}(2p-1)^j \\
&= 1 + 2p\frac{(2p-1)^{2n+1}-1}{(2p-1)-1} \\
&= 1 + 2p\frac{(2p-1)^{2n+1}-1}{2p-2} \\
&= \frac{2p-2+2p[(2p-1)^{2n+1}-1]}{2p-2} \\
&= \frac{2p(2p-1)^{2n+1}-2}{2p-2}
\end{aligned}$$

O que nos dá

$$\begin{aligned}
\frac{|S_1 \bigcap B_X(2n+1)|}{|B_X(2n+1)|} &= \frac{\frac{2p[(2p-1)^{2n+2}-1]}{(2p-1)^2-1}}{\frac{2p(2p-1)^{2n+1}-2}{2p-2}} \\
&= \frac{(2p-2)2p[(2p-1)^{2n+2}-1]}{[(2p-1)^2-1][2p(2p-1)^{2n+1}-2]} \\
&= \frac{(2p-2)}{(2p-1)^2-1}.\frac{2p[(2p-1)^{2n+2}-1]}{2p[(2p-1)^{2n+1}-\frac{1}{p}]} \\
&= \frac{(2p-2)}{(2p-1)^2-1}.\frac{(2p-1)^{2n+2}-1}{(2p-1)^{2n+1}-\frac{1}{p}} \\
&= \frac{(2p-2)}{(2p-1)^2-1}.\frac{(2p-1)[(2p-1)^{2n+1}-\frac{1}{2p-1}]}{(2p-1)^{2n+1}-\frac{1}{p}} \\
&= \frac{(2p-2)(2p-1)}{(2p-1)^2-1}.\frac{(2p-1)^{2n+1}-\frac{1}{2p-1}}{(2p-1)^{2n+1}-\frac{1}{p}}
\end{aligned}$$

Como $\lim_{n\to\infty} \dfrac{(2p-1)^{2n+1}-\frac{1}{2p-1}}{(2p-1)^{2n+1}-\frac{1}{p}} = 1$ *temos*

$$\delta_X(S_1) = \lim_{n\to\infty}\frac{|S_1 \bigcap B_X(2n+1)|}{|B_X(2n+1)|} = \frac{(2p-2)(2p-1)}{(2p-1)^2-1}$$

Analogamente temos

$$\begin{aligned}
|S_2 \bigcap B_X(2n+2)| &= 1 + |S_X(2)| + |S_X(4)| + ... + |S_X(2n+2)| \\
&= 1 + 2p(2p-1) + 2p(2p-1)^3 + ... + 2p(2p-1)^{2n+1} \\
&= 1 + 2p(2p-1)\sum_{j=0}^{n}(2p-1)^{2j} \\
&= 1 + \frac{2p(2p-1)[(2p-1)^{2n+2}-1]}{(2p-1)^2-1} \\
&= \frac{(2p-1)^2 - 1 + 2p(2p-1)[(2p-1)^{2n+2}-1]}{(2p-1)^2-1}
\end{aligned}$$

E também

$$\begin{aligned}
|B_X(2n+2)| &= 1 + |S_X(1)| + |S_X(2)| + |S_X(3)| + ... + |S_X(2n+2)| \\
&= 1 + 2p + 2p(2p-1) + 2p(2p-1)^2 + ... + 2p(2p-1)^{2n+1} \\
&= 1 + 2p\sum_{j=0}^{2n+1}(2p-1)^j \\
&= 1 + 2p\frac{(2p-1)^{2n+2}-1}{(2p-1)-1} \\
&= 1 + 2p\frac{(2p-1)^{2n+2}-1}{2p-2} \\
&= \frac{2p-2+2p[(2p-1)^{2n+2}-1]}{2p-2} \\
&= \frac{2p(2p-1)^{2n+2}-2}{2p-2}
\end{aligned}$$

O que também nos dará

$$
\begin{aligned}
\frac{|S_2 \bigcap B_X(2n+2)|}{|B_X(2n+2)|} &= \frac{\frac{(2p-2)^2-1+2p(2p-1)[(2p-1)^{2n+2}-1]}{(2p-1)^2-1}}{\frac{2p(2p-1)^{2n+2}-2}{2p-2}} \\
&= \frac{[2p-2][(2p-1)^2-1+2p(2p-1)(2p-1)^{2n+2}-2p(2p-1)]}{[(2p-1)^2-1][2p(2p-1)^{2n+2}-2]} \\
&= \frac{(2p-2)}{(2p-1)^2-1}.\frac{(2p-1)^2-1+2p(2p-1)(2p-1)^{2n+2}-2p(2p-1)}{2p(2p-1)^{2n+2}-2} \\
&= \frac{(2p-2)}{(2p-1)^2-1}.\frac{(2p-1)[(2p-1)-\frac{1}{2p-1}+2p(2p-1)^{2n+2}-2p]}{2p(2p-1)^{2n+2}-2} \\
&= \frac{(2p-2)(2p-1)}{(2p-1)^2-1}.\frac{-1-\frac{1}{2p-1}+2p(2p-1)^{2n+2}}{2p(2p-1)^{2n+2}-2} \\
&= \frac{(2p-2)(2p-1)}{(2p-1)^2-1}.\frac{2p[-\frac{1}{2p}-\frac{1}{2p(2p-1)}+(2p-1)^{2n+2}]}{2p[(2p-1)^{2n+2}-\frac{1}{p}]} \\
&= \frac{(2p-2)(2p-1)}{(2p-1)^2-1}.\frac{-\frac{1}{2p}-\frac{1}{2p(2p-1)}+(2p-1)^{2n+2}}{(2p-1)^{2n+2}-\frac{1}{p}} \\
&= \frac{(2p-2)(2p-1)}{(2p-1)^2-1}.\frac{(2p-1)^{2n+2}-\frac{2p}{2p-1}}{(2p-1)^{2n+2}-\frac{1}{p}}
\end{aligned}
$$

Novamente, como $\lim_{n\to\infty} \dfrac{(2p-1)^{2n+2}-\frac{2p}{2p-1}}{(2p-1)^{2n+2}-\frac{1}{p}} = 1$ *temos*

$$\delta_X(S_2) = \lim_{n\to\infty} \frac{|S_2 \bigcap B_X(2n+2)|}{|B_X(2n+2)|} = \frac{(2p-2)(2p-1)}{(2p-1)^2-1}$$

Logo

$$\delta_X(S_1) = \delta_X(S_2) = \frac{(2p-2)(2p-1)}{(2p-1)^2-1}$$

Temos então que $S_1 \bigcap S_2 = \emptyset$, $S_1 \bigcup S_2 = F_p$, *porém* $\delta_X(S_1) + \delta_X(S_2) \neq 1 = \delta_X(F_p)$ *pois* $p \neq 1$

5.2 Propriedades de Densidades

Nesta seção nossa proposta é mostrar que os comportamentos patologicos mostrados anteriormente não ocorrem se olharmos conjuntos distribuidos razoavelmente uniformemente dentro de G.

Proposição 5.13. *Seja G um grupo e X um conjunto de geradores de G. Dado $g \in G$ defina $|g|_X = min\{n \in \mathbb{N}\ ;\ g = x_1...x_n,\ com\ x_i \in X \bigcup X^{-1}\}$ se $g \neq 1$ e $|g|_X = 0$ se $g = 1$. A função $d : G \times G \to \mathbb{N}$ definida por $d(s, g) = |g^{-1}s|_X$ é uma métrica em G.*

Demonstração. De fato, temos que

1. $d(g, g) = |g^{-1}g|_X = |1|_X = 0$.

2. Seja g tal que $|g|_X = n$. Então $g = x_1...x_n \Rightarrow g^{-1} = x_n^{-1}...x_1^{-1}$. Logo $|g^{-1}|_X \leq n = |g|_X$. De maneira anologa, temos $|g|_X \leq |g^{-1}|_X$. Concluimos então que $|g|_X = |g^{-1}|_X$. Logo, $d(s, g) = |g^{-1}s|_X = |(g^{-1}s)^{-1}|_X = |s^{-1}g|_X = d(g, s)$.

3. Sejam $u, v \in G$ tais que $|u|_X = n$ e $|v|_X = m$. Então $u = x_1...x_n$ e $v = y_1...y_m$, o que nos dá $uv = x_1...x_ny_1...y_m$. Logo $|uv|_X \leq n + m = |u|_X + |v|_X$. Temos então $d(s, g) = |g^{-1}s|_X = |g^{-1}rr^{-1}s|_X \leq |g^{-1}r|_X + |r^{-1}s|_X = d(s, r) + d(r, g)$.

■

Definição 5.14. *Um subconjunto $S \subseteq G$ é chamado net se existe uma constante $C > 0$ tal que, todo elemento de g está a uma X-distância no máximo C de algum elemento de S. Isto é, para todo elemento $g \in G$ existe $s \in S$ com $|g^{-1}s|_X \leq C$*

Proposição 5.15. *A noção de um conjunto net não depende do conjunto de geradores de G. Isto é, um conjunto que é net com respeito ao conjunto de geradores X de G também é net com respeito a qualquer outro conjunto de geradores Y de G.*

Demonstração. Seja G um grupo finitamente gerado e X um conjunto de geradores de G. Suponha que $S \subseteq G$ é um subconjunto net de G com respeito a X, isto é, existe $C > 0$ talque, para todo $g \in G$ existe $s \in S$ com $|g^{-1}s|_X \leq C$. Seja Y um outro conjunto finito de geradores de G. Escrevendo cada elemento de X com os elementos geradores de Y temos um número finito de elementos para escrever. Tomemos então M como o máximo de $\{|y_{i1}...y_{im}|_Y;$ onde $y_{i1}...y_{im} = x_i \in X\}$. Agora, seja $g \in G$. Por hipotese existe $s \in S$ com $|g^{-1}s| \leq C$, seja $g^{-1}s = w$ temos

$$\begin{aligned} |w|_X &= |x_1...x_q| \\ &= |y_{11}...y_{1m_1}y_{21}...y_{2m_2}...y_{q1}...y_{qm_q}| \\ &\leq M|x_1...x_q| \end{aligned}$$

logo temos

$$\begin{aligned} |g^{-1}s|_Y &= |y_{11}...y_{1m_1}y_{21}...y_{2m_2}...y_{q1}...y_{qm_q}| \\ &\leq M|g^{-1}s|_X \\ &\leq MC \end{aligned}$$

Logo S também é net com respeito ao conjunto de geradores Y, porém com a constante MC. ■

Proposição 5.16. *Seja G um grupo finitamente gerado e $S \subseteq G$ um subconjunto de G. Se S é um conjunto net então $\delta_X(S) > 0$, independente do conjunto de geradores X.*

Demonstração. Seja X um conjunto de geradores de G e S um subconjunto net de G com constante C com respeito a X. Se $g \in G$, denotaremos $B_{X,g}(n)$ a bola de raio n centrada em g, isto é $B_{X,g}(n) = \{h \in G; |h^{-1}g|_X \leq n\}$.

Afirmação: $B_X(n-C) \subset \bigcup_{a \in S \bigcap B_X(n)} B_{X,a}(C)$
De fato, se $g \in B_X(n-C)$ então $|g| \leq n - C \Rightarrow |g| + C \leq n$. Por hipotese, existe $a \in S$ tal que $|g^{-1}a| \leq C$. Então

$$|a| = |gg^{-1}a| \leq |g| + |g^{-1}a| \leq |g| + C \leq n$$

Logo $g \in B_{X,a}(C)$ e $a \in S \bigcap B_X(n)$.

Observe também que $|B_X(C)| = |B_{X,a}(C)|$. Basta tomar a bijeção $g \mapsto ag^{-1}$. De fato, se $g \in B_X(C)$ temos $|g| \leq C$ e logo $|(ag^{-1})^{-1}a| = |ga^{-1}a| = |g| \leq C \Rightarrow ag^{-1} \in B_{X,a}(C)$. Claramente é uma função injetiva. Para todo $g \in B_{X,a}(C)$ temos $|g^{-1}a| \leq C \Rightarrow g^{-1}a \in B_X(C)$ e $a(g^{-1}a)^{-1} = aa^{-1}g = g$. Logo a função também é sobrejetiva. Concluimos que $|B_X(C)| = |B_{X,a}(C)|$.

Temos então

$$\begin{aligned}
|B_X(n-C)| &\leq |S \bigcap B_X(n)||B_{X,a}(C)| \\
&= |S \bigcap B_X(n)||B_X(C)| \\
\frac{|B_X(n-C)|}{|B_X(n)|} &\leq \frac{|S \cap B_X(n)||B_X(C)|}{|B_X(n)|} \\
\frac{|B_X(n-C)|}{|B_X(n)||B_X(C)|} &\leq \frac{|S \cap B_X(n)|}{|B_X(n)|}
\end{aligned}$$

Logo

$$\begin{aligned}
\liminf \frac{|S \cap B_X(n)|}{|B_X(n)|} &\geq \liminf \frac{|B_X(n-C)|}{|B_X(n)||B_X(C)|} \\
&= \frac{1}{|B_X(C)|} \liminf \frac{|B_X(n-C)|}{|B_X(n)|}
\end{aligned}$$

Observe que, se $g \in B_X(n)$ então $g = x_1...x_n$, podendo ter $x_i = 1$. Podemos então escrever $g = (x_1...x_C)(x_{C+1}...x_n) = g_1 g_2$, onde temos $g_1 \in B_X(C)$ e $g_2 \in B_X(n-C)$. Desta maneira, concluimos que $B_X(n) \subset B_X(C).B_X(n-C)$, que nós dá a desigualdade $|B_X(n) \leq |B_X(n-C)||B_X(C)|$.

Usando que $|B_X(n) \leq |B_X(n-C)||B_X(C)|$, temos

$$\begin{aligned}
\delta_X(S) &\geq \liminf \frac{|S \bigcap B_X(n)|}{|B_X(n)|} \\
&\geq \frac{1}{|B_X(C)|} \liminf \frac{|B_X(n-C)|}{|B_X(n)|} \\
&\geq \frac{1}{|B_X(C)|^2} > 0
\end{aligned}$$

Logo, mesmo que a densidade natural dependa do conjunto de geradores X, o fato de ser positivo é independente do conjunto de geradores. ■

Observação 5.17. *A reciproca não é verdadeira. Tomemos o exemplo 3.8 do grupo* $G = \mathbb{Z}^2$*, o conjunto de geradores* $X = \{a, b\}$*, onde* $a = (1, 0), b = (0, 1)$ *e* $S = \{(x, y);\ x, y > 0\}$*. Vimos que a densidade natural de* S *é positiva, porém* S *não é net. Pois para todo* $C > 0$ *tomando* $g = (-C, -C)$ *temos que qualquer elemento* $s \in S$ *satisfaz* $|g^{-1}s| = |(C, C)(x, y)| = |(C + x, C + y)| = |a^{C+x}b^{C+y}| = 2C + x + y > C$*, pois* $x, y > 0$*.*

Proposição 5.18. *Seja* G *um grupo finitamente gerado, e seja* X *o conjunto finito de geradores de* G*, satisfazendo*

$$\lim_{n\to\infty} \frac{|B_X(n+1)|}{|B_X(n)|} = 1.$$

Então a densidade natural com respeito a X *é invariante pela esquerda e pela direita. Isto é, dado* $S \subseteq G$ *temos* $\delta_X(xS) = \delta_X(S)$ *e* $\delta_X(Sx) = \delta_X(S)$ *para todo* $x \in X^{\pm}$*.*

Demonstração. **Afirmação 1**: $|S \bigcap B_X(n)| = |x(S \bigcap B_X(n))|$.
De fato, a função $\varphi : S \bigcap B_X(n) \to x(S \bigcap B_X(n))$ dada por $\varphi(g) = xg$ é injetiva, pois $xg_1 = xg_2 \Rightarrow g_1 = g_2$. Além disso se $w \in x(S \bigcap B_X(n))$ então $w = xg$ com $g \in (S \bigcap B_X(n))$, logo temos $\varphi(g) = xg = w$, o que significa que φ é uma bijeção.

Afirmação 2: $x(S \bigcap B_X(n)) \subseteq xS \bigcap B_X(n+1)$.
Se $w \in x(S \bigcap B_X(n))$ então $w = xg$ onde $g \in S \bigcap B_X(n)$. Como $g \in S$, temos $xg \in xS$. Além disso, como $g \in B_X(n)$ temos $|g| \leq n$ e logo $|xg| \leq n + 1$. Concluimos então que $w = xg \in xS \bigcap B_X(n+1)$.

Usando as afirmações 1 e 2 temos

$$|S \bigcap B_X(n)| = |x(S \bigcap B_X(n))| \leq |xS \bigcap B_X(n+1)|$$

Consequentemente,

$$\begin{aligned}
\delta_X(S) = \limsup \frac{|S \bigcap B_X(n)|}{|B_X(n)|} &\leq \limsup \frac{|xS \bigcap B_X(n+1)|}{|B_X(n)|} \\
&= \limsup \frac{|xS \bigcap B_X(n+1)||B_X(n+1)|}{|B_X(n)||B_X(n+1)|} \\
&= \limsup \frac{|xS \bigcap B_X(n+1)|}{|B_X(n+1)|} \limsup \frac{|B_X(n+1)|}{|B_X(n)|} \\
&= \delta_X(xS)
\end{aligned}$$

Afirmação 3: $xS \bigcap B_X(n) \subseteq x(S \bigcap B_X(n+1))$.
Se $w \in xS \bigcap B_X(n)$ então $w = xg$, onde $g \in S$. Como $|w| = |xg| \leq n$ temos que $|g| \leq n+1$, pois como g é uma palavra reduzida, temos que ou $w = xg$ também é reduzida e $|w| = |g|+1$, ou $w = h$, onde $g = x^{-1}h$ e $|h| = |g| - 1$. Logo, supondo por contradição que $|g| > n+1$ teriamos $|w| > n+2$ ou $|w| > n$ que é uma contradição.
Concluimos que $g \in S \bigcap B_X(n+1)$ e $w \in x(S \bigcap B_X(n+1))$

Usando a afirmação 3 e novamente a afirmação 1 temos

$$|xS \bigcap B_X(n)| \leq |x(S \bigcap B_X(n+1))| = |S \bigcap B_X(n+1)|$$

Consequentemente,

$$\begin{aligned} \delta_X(xS) = \limsup \frac{|xS \bigcap B_X(n)|}{|B_X(n)|} &\leq \limsup \frac{|S \bigcap B_X(n+1)|}{|B_X(n)|} \\ &= \limsup \frac{|S \bigcap B_X(n+1)||B_X(n+1)|}{|B_X(n)||B_X(n+1)|} \\ &= \limsup \frac{|S \bigcap B_X(n+1)|}{|B_X(n+1)|} \limsup \frac{|B_X(n+1)|}{|B_X(n)|} \\ &= \delta_X(S) \end{aligned}$$

Logo temos $\delta_X(S) \leq \delta_X(xS)$ e $\delta_X(xS) \leq \delta_X(S)$. Concluimos que $\delta_X(xS) = \delta_X(S)$

A demonstração para $\delta_X(Sx) \leq \delta_X(S)$ é análoga ■

Proposição 5.19. *Sejam G um grupo finitamente gerado e $H \leq G$ um subgrupo de índice finito de G. Para todo conjunto finito de geradores X de G satisfazendo*

$$\lim_{n\to\infty} \frac{|B_X(n+1)|}{|B_X(n)|} = 1,$$

a densidade natural de H com respeito a X é $\delta_X(H) = \dfrac{1}{[G:H]}$.

Demonstração. ainda nao sei ■

Exemplo 5.20. *O exemplo 4.11 é um contra exemplo da proposição anterior caso a hipotese sobre o limite fosse retirada. De fato, temos que o conjunto das palavras em F_p que tem comprimento par é um subgrupo de F_p de índice 2, porém se $p > 1$ temos $\delta_X(H) = \dfrac{(2p-2)(2p-1)}{(2p-1)^2-1} \neq \dfrac{1}{2}$*

Lema 5.21. *Seja G um grupo com um conjunto finito de geradores X, e seja S_i, $i = 1, ..., k$, uma coleção finita de subconjuntos de G. Então,*

$$d_X(\bigcup_{i=1}^{k} S_i) = \max_i\{d_X(S_i)\}$$

Demonstração. Seja $d_X(S_i) = \alpha_i$ e vamos assumir sem perda de generalidade que $\max_i \alpha_i = \alpha_1$. Para facilitar os calculos, vamos chamar de $\beta_i = a\alpha_i$, onde a é a taxa de crescimento exponencial de G. Como a>0, temos $\max_i \beta = a \max_i \alpha = a\alpha_1$. Então

$$d_X(S_i) = \frac{1}{a} \limsup |S_i \bigcap B_X(n)|^{1/n} = \alpha_i$$

$$\limsup |S_i \bigcap B_X(n)|^{1/n} = a\alpha_i = \beta_i.$$

Dado $\epsilon > 0$. Pela definição de limsup, para n suficientemente grande, teremos

$$\begin{aligned} |S_i \bigcap B_X(n)|^{1/n} &< \beta_i + \epsilon \\ |S_i \bigcap B_X(n)| &< (\beta_i + \epsilon)^n \\ &< (\beta_1 + \epsilon)^n \end{aligned}$$

Agora note que

$$\left| \left(\bigcup_{i=1}^{k} S_i \right) \bigcap B_X(n) \right| \leq \sum_{i=1}^{k} |S_i \bigcap B_X(n)| \leq k(\beta_1 + \epsilon)^n$$

$$\left| \left(\bigcup_{i=1}^{k} S_i \right) \bigcap B_X(n) \right|^{1/n} \leq k^{1/n}(\beta_1 + \epsilon)$$

$$\limsup \left| \left(\bigcup_{i=1}^{k} S_i \right) \bigcap B_X(n) \right|^{1/n} \leq \limsup k^{1/n}(\beta_1 + \epsilon) = (\beta_1 + \epsilon)$$

Como ϵ foi dado arbitrariamente, podemos concluir que

$$\limsup \left| \left(\bigcup_{i=1}^{k} S_i \right) \bigcap B_X(n) \right|^{1/n} \leq \beta_1 = a\alpha_1$$

$$\frac{1}{a} \limsup \left| \left(\bigcup_{i=1}^{k} S_i \right) \bigcap B_X(n) \right|^{1/n} \leq \alpha_1$$

$$d_X \left(\bigcup_{i=1}^{k} S_i \right) \leq \alpha_1.$$

A outra desigualdade é direta, pois $S_1 \subseteq \bigcup_{i=1}^{k} S_i$ implica que $|S_1 \cap B_X(n)| \leq \left| \left(\bigcup_{i=1}^{k} S_i \right) \cap B_X(n) \right|$. ■

Proposição 5.22. *Sejam G um grupo com um conjunto finito de geradores X e $S \subseteq G$ um subconjunto de G. Então, se $|S| = \infty$ nos temos*

$$\limsup |S \bigcap B_X(n)|^{1/n} = \limsup |S \bigcap S_X(n)|^{1/n}$$

6 Densidade de Conjuntos Gráficos em Grupos Livres

A partir de agora iremos calcular a densidade exponencial de alguns subconjuntos de grupos livres

Observação 6.1. *É importante lembrar que um grupo livre F_p, de classe p, tem taxa de crescimento exponencial 2p-1. De fato*

$$\begin{aligned}
|B_X(n)| &= 1+\sum_{i=1}^{n}|S_X(i)| \\
&= 1+\sum_{i=1}^{n}2p(2p-1)^{i-1} \\
&= 1+\sum_{i=0}^{n-1}2p(2p-1)^{i} \\
&= 1+2p\sum_{i=0}^{n-1}(2p-1)^{i} \\
&= 1+2p\frac{1-(2p-1)^n}{1-(2p-1)} \\
&= 1+p\frac{1-(2p-1)^n}{1-p} \\
&= \frac{1-p(2p-1)^n}{1-p}.
\end{aligned}$$

Desta maneira temos

$$\begin{aligned}
\lim|B_X(n)|^{1/n} &= \lim\left(\frac{1-p(2p-1)^n}{1-p}\right)^{1/n} \\
&= 2p-1
\end{aligned}$$

A partir de agora vamos fixar uma base X do grupo livre F_p, de classe p e considerar grafos direcionados, possivelmente tendo loops, que nao tenham arestas multiplas e que tenham $X^{\pm 1}$ como conjunto de vértices. Além disso também fixaremos uma ordem arbitrára para $X^{\pm 1}$, $a_1 < ... < a_{2p}$. Iremos nos referir a todas essas propriedades apenas com a palavra grafo.

Definição 6.2. *Sejam $a, b \in X^{\pm 1}$, $a \neq b^{-1}$ e $w = x_1...x_n$ uma palavra reduzida em F_p. Dizemos que w contém ab se $ab = x_i x_{i+1}$ para algum $i \in \{1, ..., n-1\}$. Claramente temos que a palavral vazia e as palavras com comprimento igual a 1 não contém nada. E nenhuma palavra contém aa^{-1}.*

Definição 6.3. *Seja Z um grafo. Chamaremos de EZ o conjunto de arestas de Z. A aresta (a,b) é dita redundante quando* $ab = 1$. *Se uma aresta nao é redundante dizemos que ela é irreduntante. Dizemos que Z é irreduntante quando EZ não contém arestas redundantes. Se Z' é outro grafo, dizemos que Z é mais simples que Z' se* $EZ \subseteq EZ'$ *e denotamos por* $Z \leq Z'$.

Definição 6.4. *O grafo inverso de Z é novo grafo* $\bar{Z}$ *com o seguinte conjunto de arestas:*

$$E\bar{Z} = \{(a,b) \in (X^{\pm 1})^2 \mid (ab^{-1}) \in EZ\}$$

Observação 6.5. *Note que, quando invertidos, arestas redundantes se tornam loops e loops se tornam arestas redundantes. Logo, podemos dizer que Z é irreduntante se e somente se* $\bar{Z}$ *não tem loops. Note também que* $\bar{\bar{Z}} = Z$.

Definição 6.6. *Seja Z um grafo. Usando a ordem fixada para* $X^{\pm 1}$ *definimos a matriz adjacente de Z, denotada por ad(Z), como a matriz quadrada de ordem 2p cuja entrada de (i,j) é 1 se* $(a_i, a_j) \in EZ$ *e 0 se não.*

Observação 6.7. *Seja* M_n *o conjunto de matrizes de ordem n. Se considerarmos a seguinte ordem em* M_n: $A \leq B$ *se* $a_{ij} \leq b_{ij}$ *para todo* $i, j \in \{1, ..., n\}$. *Então temos* $Z \leq Z'$ *se e somente se* $ad(Z) \leq ad(Z')$.

Definição 6.8. *O grafo completo, denotado por* K_{2p}, *é o grafo contendo exatamente todos as possiveis arestas que nao sejam loops.*

Observação 6.9. *Note que* $\bar{K_{2p}}$ *é o grafo contendo exatamente todos as arestas irredundantes e agora incluindo os loops. E também, a matriz* $ad(K_{2p})$ *é a matriz quadrada de ordem 2p com todas as entradas 1, exceto a diagonal principal que é 0. Já a matriz* $ad(\bar{K_{2p}})$ *é a matriz com todas as entradas 1 exceto em p pares de entradas simetricas. Ambas as matrizes* $ad(K_{2p})$ *e* $ad(\bar{K_{2p}})$ *são simetricas.*

Exemplo 6.10. *Seja p=2. Fixamos a base* $X^{\pm 1} = \{a_1, a_2, a_3 = a_1^{-1}, a_4 = a_2^{-1}\}$ *e temos:* $EK_4 = \{(a_1, a_2), (a_1, a_3), (a_1, a_4), (a_2, a_1), (a_2, a_3), (a_2, a_4), (a_3, a_1), (a_3, a_2), (a_3, a_4), (a_4, a_1), (a_4, a_2), (a_4, a_3)\}$ *e* $E\bar{K_4} = \{(a_1, a_4), (a_1, a_1), (a_1, a_2), (a_2, a_3), (a_2, a_1), (a_2, a_2), (a_3, a_3), (a_3, a_4), (a_3, a_2), (a_4, a_3), (a_4, a_4), (a_4, a_1)\}$. *Temos então as seguintes matrizes adjacentes:*

$$ad(K_4) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \text{ e } ad(\bar{K_4}) = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Definição 6.11. *Um conjunto grafico é um subconjunto de* F_p *da forma*

$$S(Z) = \{w \in F_p \quad ; \quad \text{se } w \text{ contem } ab, \text{ então } (a,b) \in EZ\}$$

onde Z é um grafo. Por outro lado, seja $w \in F_p$ uma palavra. O grafo local de w, denotado por Z_w, é o grafo Z mais simples tal que $w \in S(Z)$.

Observação 6.12. *O grafo local da palavra $w \in F_p$ localmente descreve w, já que para todo ab contido em w temos que $(a, b) \in EZ_w$. Por exemplo, seja $a_i \in X^{\pm 1}$. Então temos que Z_{a_i} é o grafo sem nenhuma aresta e $Z_{a_i^n}$ é o grafo com apenas um loop em a_i*

Propriedades 6.13. *Seja Z um grafo. Então:*

1. *$X^{\pm 1} \bigcup \{1\} \subset S(Z)$;*

2. *S(Z) é fechado para subpalavras. Isto é, se $w \in S(Z)$ e w contem a palavra u, então $u \in S(Z)$;*

3. *Se $Z = \bigcup_i Z_i$ é a decomposição de Z em componentes conectados, então $S(Z) = \bigcup_i S(Z_i)$;*

4. *S(Z) não muda se deletarmos arestas redundantes de Z. (Por isso chamamos estas arestas de redundantes);*

5. *Seja Z um grafo irredundante. S(Z) é finito se e somente se Z não tem caminhos fechados não triviais;*

6. *Se Z e Z' são irredundantes então, $S(Z) \subseteq S(Z')$ se e somente se $Z \leq Z'$;*

7. *Se Z e Z' são irredundantes então, $S(Z) = S(Z')$ se e somente se $Z = Z'$;*

8. *$S(Z) = F_p$ se e somente se Z comtém todos as arestas irredundantes.*

Demonstração.

1. Por definição a palavra vazia e os elementos de $X^{\pm 1}$ estão em S(Z) já que estas palavras não contem pares de elementos.

2. Sejam $w \in S(Z)$ e u contido em w. Então temos que $w = a_{i_1}...a_{i_j}...a_{i_k}...a_{i_n}$ e $u = a_{i_j}...a_{i_k}$ com $1 \leq j < k \leq n$. Para quaisquer pares ab contido em u, temos que ab está contido em w e logo $(a, b) \in S(Z)$. Concluimos que $u \in S(Z)$.

3. ?

4. Sejam Z um grafo e $(a, b) \in EZ$ uma aresta redundante. Vamos mostrar que se $\bar{Z} = Z \setminus \{(a, b)\}$ então $S(Z) = S(\bar{Z})$. De fato, seja $w \in S(\bar{Z})$ uma palavra reduzida. Temos que $w = a_{i_1}...a_{i_n}$ onde $a_{i_j} \neq a_{i_{j-1}}^{-1}$ para todo $j \in \{2, ..., n\}$. Então para quaisquer pares $a_{i_{j-1}}a_{i_j}$ contidos em w, temos que $(a_{i_{j-1}}, a_{i_j})$ não é redundante e consequentemente $(a_{i_{j-1}}, a_{i_j}) \neq (a, b)$. Logo $(a_{i_{j-1}}, a_{i_j}) \in E\bar{Z} = E(Z \setminus \{(a, b)\})$ e $(a_{i_{j-1}}, a_{i_j}) \neq (a, b)$, o que implica que $(a_{i_{j-1}}, a_{i_j}) \in EZ$. Logo $w \in S(Z)$ e concluimos que $S(\bar{Z}) \subseteq S(Z)$. A outra desigualdade é trivial.

5. ($\Rightarrow$) Seja $S(Z)$ finito. Suponha por contradição que Z tem um caminho fechado não trivial. Logo temos que existem arestas $(a_{i_1}, a_{i_2}), (a_{i_2}, a_{i_3}), ..., (a_{i_{n-1}}, a_{i_n}), (a_{i_n}, a_{i_1})$ em Z. Tomemos $w = a_{i_1}...a_{i_n}$. Como Z é irredundante, temos $a_{i_j} \neq a_{i_{j-1}}^{-1}$ para todo $j \in \{2, ..., n\}$ e também $a_{i_1} \neq a_{in}^{-1}$. Logo w é uma palavra ciclicamente reduzida e $|w^k| = k|w|$. Como $(a_{i_n}, a_{i_1}) \in EZ$ então $w^k \in S(Z)$ para todo $k \in \mathbb{N}$. Logo, para todo $m \in \mathbb{N}$ temos que existe $w \in S(Z)$ tal que $|w| > m$ e consequentemente $S(Z)$ seria infinito, o que nos dá uma contradição.

   ($\Leftarrow$) Seja Z um grafo que não contém caminhos fechados não triviais. Vamos mostrar que se $w \in S(Z)$ então $|w| \leq 2p$. De fato, como $|X^{\pm 1}| = 2p$ então se $|w| > 2p$ teriamos que existe $a_j \in X^{\pm 1}$ que aparece mais de uma vez em w. Teriamos então que $w = v_1 a_j v_2 a_j v_3$, onde $v_{1,2,3}$ são subpalavras de w. Como $S(Z)$ é fechado para subpalavras, teriamos que $a_j v_2 a_j \in S(Z)$. Logo, as arestas $(a_j, a_{i_1}), (a_{i_1}, a_{i_2}), ..., (a_{i_n}, a_j)$, onde $v = a_{i_1}...a_{i_n}$, pertencem a EZ. Teriamos então um caminho fechado não trivial em Z, o que seria uma contradição. Logo temos que se $w \in S(Z)$ entao $|w|/leq2p$ e consequentemente $|S(Z)| \leq B_X(2p) = \dfrac{1 - p(2p-1)^{2p}}{1-p}$. Conluimos então que $S(Z)$ é finito.

6. ($\Rightarrow$) Suponha que $S(Z) \subseteq S(Z')$. Seja $(a, b) \in EZ$ temos que $1 \neq w = ab \in S(Z) \subseteq S(Z')$ e logo $(a, b) \in EZ'$. Concluimos que $Z \leq Z'$. A outra direção é trivial.

7. Direto do item anterior, pois igualdade implica dupla inclusão.

8. Seja Z' um grafo com todas as arestas irredundantes. Então temos $S(Z') = F_p$. Considere $\bar{Z}$ o grafo Z sem arestas reduntantes. Pelo item 4 temos $S(Z) = S(\bar{Z})$ e pelo item 7, se $S(\bar{Z}) = S(Z) = F_p = S(Z')$ então $Z' = \bar{Z} \subseteq Z$.

■

Observação 6.14. *Seja $w \in F_p$. Note que Z_w é irredundante. Pois se $(a, b) \in EZ_w$ é uma aresta redundante, vimos pelo item 4 da propriedade anterior que retirar está aresta nao altera $S(Z_w)$ e logo teriamos um grafo mais simples com o mesmo conjunto $S(Z_w)$, o que contradiz a definição de que Z_w é o grafo mais simples.*

Observação 6.15. *Se Z é um grafo irredundante, existe uma bijeção trivial entre os caminhos em Z e o conjunto $S(Z) \setminus \{1\}$. Palavras em S(Z) de tamanho n, correspondem a caminhos em Z de tamanho n-1.*

Proposição 6.16. *Seja Z um grafo irreduntante. O número de caminhos em Z de tamanho n, que começam com a_i e terminam com a_j é igual a entrada (i, j) da matriz $ad(Z)^n$. Isto é, seja $ad(Z)^n = [a_{ij}]$ então $|\{w \in S(Z)\ ;\ |w| = n+1 \text{ e } w = a_i v a_j \text{para algum } v \in S(Z)\}| = a_{ij}$*

Demonstração. Vamos mostrar por indução em n. Para $n = 1$ o único caminho possivel em Z começando por a_1 e terminando em a_j de tamanho 1 é a aresta (a_i, a_j), caso esta aresta pertença a Z. Neste caso, temos que a entrada (i, j) da matrix $ad(Z)$ é 1, que é o número de caminhos possiveis. Caso a aresta (a_i, a_j) nao pertença a Z, então temos que não existem caminhos em Z de tamanho 1 começando por a_i e terminando por a_j e neste caso também teriamos que a entrada (i, j) de $ad(Z)$ é zero. Logo, a proposição vale para n=1.

Suponhamos que a proposição vale para n. Sejam $ad(Z) = [a_{ij}]$, $ad(Z)^n = [b_{ij}]$ e $ad(Z)^{n+1} = [c_{ij}]$. Temos que $ad(Z)^{n+1} = ad(Z)^n ad(Z)$ e logo $c_{ij} = b_{i1}a_{1j} + b_{i2}a_{2j} + ... + b_{i(2p)}a_{(2p)j}$. Agora observe que um caminho em Z de tamanho n+1 que começa em a_i e termina em a_j pode ser escrito como um caminho de tamanho n que começa em a_i e termina em a_k seguido da aresta (a_k, a_j) para algum $k \in \{1, ..., 2p\}$ como a a aresta (a_k, a_j) está em Z, temos que $a_{kj} = 1$. Para cada $k \in \{1, ..., 2p\}$ o numero de caminhos de tamanho n que começam em a_i e terminam em a_k por hipotese é b_{ik}. Logo os caminhos de tamanho n+1 começados por a_i e terminados por a_j são todos os caminhos de tamanho n que começa em a_i e termina em a_k seguido da aresta (a_k, a_j) para todo k tal que a aresta $(a_k, a_j) \in EZ$. Isto é, a soma de todos os b_{ik} para os quais $a_{kj} = 1$. Para os valores de k tais que $(a_k, a_j) \notin EZ$ temos $a_{kj} = 0$ e logo $b_{ik}a_{kj} = 0$. Logo, a proposição vale para n+1. Concluimos então que vale para todo n. ■

Teorema 6.17. *Seja Z um grafo irredundante. Se Z não tem caminhos fechados não triviais, então a densidade exponencial de S(Z) é* $\dfrac{1}{2p-1}$. *Do contrário,*

$$d_X(S(Z)) = \frac{\rho(ad(Z))}{2p-1},$$

onde $\rho(ad(Z))$ *é o raio espectral da matriz adjacente de Z.*

Demonstração. Se Z não tiver caminhos fechados não triviais, então pelo item 5 da propriedade 6.13 S(Z) é finito. Logo, para algum n_0 suficientemente grande, temos que $|S(Z) \bigcap B_X(n)| = |S(Z)|$ para todo $n \geq n_0$. Teremos então

$$\lim_{n\to\infty} |S(Z) \bigcap B_X(n)|^{\frac{1}{n}} = \lim_{n\to\infty} |S(Z)|^{\frac{1}{n}} = 1.$$

Segue que $d_X(S(Z)) = \dfrac{1}{2p-1} \lim_{n\to\infty} |S(Z) \bigcap B_X(n)|^{\frac{1}{n}} = \dfrac{1}{2p-1}$.

Suponhamos agora que S(Z) é infinito. Seja M a matriz adjacente ad(Z) e denotemos $M^n = [m^n_{i,j}]$, $n \geq 0$. Pela observação 6.15 temos que existe uma bijeção entre as palavras de S(Z) de tamanho n e os caminhos em Z de tamanho n-1. Logo, a cardinalidade do conjunto $|S(Z) \bigcap S_X(n)| = \sum_{i,j=1,...,2p} m^{n-1}_{i,j}$, já que é a união de todas as palavras de tamanho n, isto é, que começam e terminam por todos os $a_i, i \in \{1, ..., 2p\}$. Aplicando o corolário 4.9 temos

$$\lim_{n\to\infty} \Big(\sum_{i,j=1,...,2p} m^{n-1}_{i,j}\Big)^{\frac{1}{n-1}} = \lim_{n\to\infty} \|M^{n-1}\|_1^{\frac{1}{n-1}} = \rho(M)$$

Temos então

$$\begin{aligned}
d_X(S(Z)) &= \frac{1}{2p-1}\lim_{n\to\infty}|S(Z)\bigcap S_X(n)|^{\frac{1}{n}}\\
&= \frac{1}{2p-1}\lim_{n\to\infty}(\sum_{i,j=1,\ldots,2p} m_{i,j}^{n-1})^{\frac{1}{n}}\\
&= \frac{1}{2p-1}\lim_{n\to\infty}(\sum_{i,j=1,\ldots,2p} m_{i,j}^{n-1})^{\frac{1}{n}\frac{n-1}{n-1}}\\
&= \frac{1}{2p-1}\lim_{n\to\infty}(\sum_{i,j=1,\ldots,2p} m_{i,j}^{n-1})^{\frac{1}{n-1}\frac{n-1}{n}}\\
&= \frac{1}{2p-1}\lim_{n\to\infty}(\sum_{i,j=1,\ldots,2p} m_{i,j}^{n-1})^{\frac{1}{n-1}\frac{n-1}{n}}\\
&= \frac{1}{2p-1}\lim_{n\to\infty}(|||M^{n-1}|||_1^{\frac{1}{n-1}})^{\frac{n-1}{n}}\\
&= \frac{1}{2p-1}\lim_{n\to\infty}(\rho(M))^{1-\frac{1}{n}}\\
&= \frac{1}{2p-1}\lim_{n\to\infty}\frac{\rho(M)}{\rho(M)^{\frac{1}{n}}}\\
&= \frac{1}{2p-1}\frac{\rho(M)}{1}\\
&= \frac{\rho(M)}{2p-1}
\end{aligned}$$

■

Corolário 6.18. *Com respeito a uma base livre X, o conjunto de palavras X-positivas em F_p tem densidade exponencial* $\dfrac{p}{2p-1}$

Demonstração. Considere o conjunto $X^{\pm 1} = \{a_1, a_2, ..., a_p, a_{p+1}, ..., a_{2p}\}$ onde a_j é positivo se $1 \leq j \leq p$. Defina o grafo $EZ = \{(a_i, a_j);\ i, j \leq p\}$ e teremos que S(Z) é o conjunto de palavras positivas em X.

Agora, note que $ad(Z) = A = \begin{pmatrix} 1 & 1 & ... & 1 & 0 & 0 & ... & 0\\ 1 & 1 & ... & 1 & 0 & 0 & ... & 0\\ \vdots & \vdots & ... & \vdots & \vdots & \vdots & ... & \vdots\\ 1 & 1 & ... & 1 & 0 & 0 & ... & 0\\ 0 & 0 & ... & 0 & 0 & 0 & ... & 0\\ \vdots & \vdots & ... & \vdots & \vdots & \vdots & ... & \vdots\\ 0 & 0 & ... & 0 & 0 & 0 & ... & 0 \end{pmatrix}$.

Seja $x = (x_1, x_2, ..., x_{2p})$. Temos $Ax = (k, k, ..., k, 0, ..., 0)$, onde $k = x_1 + ... + x_p$. Se $x = (x_1, x_2, ..., -(x_1 + ...x_{p-1}), x_{p+1}, x_{p+2}, ..., x_{2p})$ teremos $Ax = 0 = 0x$. Logo, 0 é um autovalor da matriz A. Como o autoespaço gerado por x tem dimensão $2p-1$, a multiplicidade do autovalor 0 é $2p-1$. Logo, resta apenas um autovalor de A.

Se $\bar{x} = (x, x, ..., x, 0, 0, ..., 0)$ teremos $A\bar{x} = (px, px, ..., px, 0, 0, ...,) = p.x$. Logo p é o outro autovalor de A e temos $\rho(A) = \max\{0, p\} = p$. Pelo teorema anterior $d_X(S(Z)) = \dfrac{p}{2p-1}$ ■

Proposição 6.19. *Sejam Z e Z' dois grafos irredundantes com caminhos fechados não triviais. Se $S(Z) \subseteq S(Z')$ então $d_X(S(Z)) \leq d_X(S(Z'))$, e a inegualdade é estrita sempre que a inclusão for estrita.*

Demonstração. Pelo item 6 da propriedade 6.13 temos que $Z \leq Z'$ e consequentemente $ad(Z) \leq ad(Z')$. Pela proposição 4.11 temos $(ad(Z))^m \leq (ad(Z'))^m \Rightarrow \|(ad(Z))^m\|_1 \leq \|(ad(Z')^m\|_1 \Rightarrow \|(ad(Z))^m\|_1^{\frac{1}{m}} \leq \|(ad(Z')^m\|_1^{\frac{1}{m}}$ para todo inteiro positivo m. Logo, usando o corolário 4.9 e o teorema 6.17 temos

$$\begin{aligned}
\lim_{n\to\infty} \|(ad(Z))^m\|_1^{\frac{1}{m}} &\leq \lim_{n\to\infty} \|(ad(Z')^m\|_1^{\frac{1}{m}} \\
\rho(ad(Z)) &\leq \rho(ad(Z')) \\
\\
\frac{\rho(ad(Z))}{2p-1} &\leq \frac{\rho(ad(Z'))}{2p-1} \\
\\
d_X(S(Z)) &\leq d_X(S(Z'))
\end{aligned}$$

■

Definição 6.20. *Seja Z é um grafo simétrico com 2p vertices. O grau de um vértice $v \in VZ$ é o número de vertices adjacentes a v, isto é, o número de $u \in VZ$ tal que $(u, v) \in EZ$. Denotamos por ∂_{max} o máximo dos graus dos vértices de Z e por $\bar{\partial}$ a média dos graus dos vértices de Z.*

Proposição 6.21. *Sejam Z um grafo simétrico e irredundante com 2p vértices, $VZ = X^{\pm 1}$ e $S(Z) \subseteq F_p$ o conjunto grafico simétrico correspondente. A densidade exponencial de $S(Z)$ com respeito a X satisfaz as seguintes desigualdades.*

1. $\dfrac{\bar{\partial}}{2p-1} \leq d_X(S(Z))$,

2. $\dfrac{\sqrt{\partial_{max}}}{2p-1} \leq d_X(S(Z)) \leq \dfrac{\partial_{max}}{2p-1}$.

Demonstração. 1. Seja $A = ad(Z)$. Como Z é simétrico, A é uma matriz simétrica de ordem 2p e pela proprosição 4.15, para todo vetor $v \in \mathbb{R}^{2p}$ temos

$$\frac{vAv^T}{vv^T} \leq \rho(A)$$

. Tomemos então o vetor $v = (1, 1, ..., 1)$ e temos que $vv^T = 2p$ e

$$\begin{aligned} vAv^T &= < v, Av > \\ &= < (1, ..., 1), A(1, ..., 1) > \\ &= < (1, ..., 1), (a_{11} + a_{12} + ... + a_{1(2p)}, ..., a_{(2p)1} + a_{(2p)2} + ... + a_{(2p)(2p)}) > \\ &= \sum_{i,j=1}^{2p} a_{ij} \end{aligned}$$

Agora note que, a soma dos graus de todos os vertices de Z é $\sum_{i,j=1}^{2p} a_{ij}$, pois seja x_n um vertice de Z, para cada vertice x_m adjacente temos que $(x_m, x_n) \in EZ$ e logo $a_{mn} = 1$. Como temos 2p vertices, a média entre os graus dos vertices é dada por

$$\bar{\partial} = \frac{\sum_{i,j=1}^{2p} a_{ij}}{2p} = \frac{vAv^T}{vv^T} \leq \rho(A)$$

e pelo Teorema 6.17 temos $\dfrac{\bar{\partial}}{2p-1} \leq \dfrac{\rho(A)}{2p-1} = d_X(S(Z))$.

2. Seja x_k o vertice tal que $\partial_{\max} = \partial_{x_k}$ e considere a matriz M de valores iguais a matriz adjacente A na k-ésimá linha e na k-ésima coluna e com 0 em todas as outras entradas. Isto é

$$M = \begin{pmatrix} 0 & ... & 0 & a_{1k} & 0 & ... & 0 \\ 0 & ... & 0 & a_{2k} & 0 & ... & 0 \\ \vdots & ... & \vdots & \vdots & \vdots & ... & \vdots \\ 0 & ... & 0 & a_{(k-1)k} & 0 & ... & 0 \\ a_{k1} & ... & a_{k(k-1)} & 0 & a_{k(k+1)} & ... & a_{kn} \\ 0 & ... & 0 & a_{(k+1)k} & 0 & ... & 0 \\ \vdots & ... & \vdots & \vdots & \vdots & ... & \vdots \\ 0 & ... & 0 & a_{nk} & 0 & ... & 0 \end{pmatrix}$$

Temos que $Mv = (a_{1k}v_k, a_{2k}v_k, ..., a_{(k-1)k}v_k, (a_{k1}v_1 + a_{k2}v_2 + ... + a_{kn}v_n), a_{(k+1)k}v_k, ..., a_{nk}v_k)$. Suponha sem perda de generalidade que $a_{k1} = 1$ e seja $I = \{1 < i \leq n \ ; \ a_{ki} = 1\}$. Tomemos $v = (-\sum_{i \in I} v_i, v_2, ..., v_{k-1}, 0, v_{k+1}, ..., v_n)$ e temos $a_{k1}v_1 + a_{k2}v_2 + ... + a_{kn}v_n = -\sum_{i \in I} v_i + \sum_{i \in I} v_i = 0$. Logo $Mv = 0 = 0v$. Como o autoespaço gerado por v tem dimensao $n - 2$ temos que 0 é um autovalor de multiplicidade $n - 2$ e que restam apenas outros 2 autovalores distintos.
Considere agora o vetor v com $v_k = x\sqrt{m}$ onde $m = \sum_{i=1} a_{ki}$ e as demais coordenadas

$v_i = x$ se $a_{ik} = 1$ e $v_i = 0$ se $a_{ik} = 0$ Como $a_{kk} = 0$ temos

$$\begin{aligned}
Mv &= (a_{1k}v_k, a_{2k}v_k, ..., a_{(k-1)k}v_k, (a_{k1}v_1 + a_{k2}v_2 + ... + a_{kn}v_n), a_{(k+1)k}v_k, ..., a_{nk}v_k) \\
&= (a_{1k}x\sqrt{m}, a_{2k}x\sqrt{m}, ..., a_{(k-1)k}x\sqrt{m}, x(a_{k1} + a_{k2} + ... + a_{kn}), a_{(k+1)k}x\sqrt{m}, ..., a_{nk}x\sqrt{m}) \\
&= (a_{1k}x\sqrt{m}, a_{2k}x\sqrt{m}, ..., a_{(k-1)k}x\sqrt{m}, xm, a_{(k+1)k}x\sqrt{m}, ..., a_{nk}x\sqrt{m}) \\
&= \sqrt{m}(a_{1k}x, a_{2k}x, ..., a_{(k-1)k}x, x\sqrt{m}, a_{(k+1)k}x, ..., a_{nk}x) \\
&= \sqrt{m}v
\end{aligned}$$

De maneira analoga o vetor v com $v_k = x(-\sqrt{m})$ onde $m = \sum_{i=1} a_{ki}$ e as demais coordenadas $v_i = x$ se $a_{ik} = 1$ e $v_i = 0$ se $a_{ik} = 0$ também satisfaz $Mv = -\sqrt{m}v$. Logo, os outros 2 autovalores de M são $\pm\sqrt{m}$. Temos então $\rho(M) = \sqrt{m}$. Note que $m = \sum_{i=1} a_{ki} = \partial_{v_k} = \partial_{\max}$. E como $M < A$, pela proposição 4.13 $\sqrt{\partial_{\max}} = \rho(M) \leq \rho(A)$. Segue do Teorema 6.17 que $\dfrac{\sqrt{\partial_{\max}}}{2p-1} \leq d_X(S(Z))$.

Pelo Teorema de Perron-Frobenius temos que existe um vetor v positivo, tal que $Av = \rho(A)v$. Logo, tomando $u = (1, ..., 1)$ temos $< u, Av >=< u, \rho(A)v >= \rho(A) < u, v >$. Desta forma temos

$$\rho(A)uv^T = uAv^T.$$

Lembrando que o vetor uA é o vetor com os graus de cada vertice de Z, temos que $uA < \partial_{\max}u$, já que $\partial_{\max}u$ é o vetor com todas as coordenadas iguais a $\partial_{\max}$. Como v é positivo temos então $< uA, v >\leq< \partial_{\max}u, v >$. Logo

$$\rho(A)uv^T = uAv^T \leq \partial_{\max}uv^T$$

$$\rho(A) \leq \partial_{\max}.$$

Segue do teorema 6.17 que $d_X(S(Z)) \leq \dfrac{\partial_{\max}}{2p-1}$.

■

Teorema 6.22. *Seja X uma base do grupo livre F_p, de classe $p \geq 2$, e seja S o seguinte conjunto*

$$S = \{w \in F_p \mid Z_w < \bar{K}_{2p}\} \subseteq F_p$$

. Então

$$d_X(S) = \frac{\gamma_p}{2p-1} < 1,$$

onde $\gamma_p \in (2p-2, 2p-1)$ é a maior raiz do polinômio $x^3 - (2p-2)x^2 - (2p-1)x + (2p-2)$. Em particular, $\delta_X(S) = 0$

Demonstração. Primeiro observe que o conjunto S é a união dos conjuntos graficos $S(\bar{K}_{2p} \setminus \{e\})$ onde e varia entre as arestas de $\bar{K}_{2p}$. De fato, se $w \in S$ temos que $Z_w < \bar{K}_{2p}$ e logo Z_w não contém alguma aresta $e = (a, b)$. Consequentemente w não contém ab, logo temos que $w \in S(\bar{K}_{2p} \setminus \{e\})$ pois este grafo possui todas as arestas exceto e. Por outro lado temos que se $w \in \bigcup_{e \in E\bar{K}_{2p}} S(\bar{K}_{2p} \setminus \{e\})$ então para alguma aresta $e = (a, b)$ temos que $w \in S(\bar{K}_{2p} \setminus \{e\})$ e neste caso por definição, como Z_w é o menor grafo satisfazendo essa condição, temos $Z_w \leq S(\bar{K}_{2p} \setminus \{e\}) < \bar{K}_{2p}$. Consequentemente temos $Z_w < \bar{K}_{2p}$ e $w \in S$.

Como o conjunto de arestas de $\bar{K}_{2p}$ é finito, e $\bar{K}_{2p}$ é irredundante, temos pelo Lema 5.21 e o Teorema 6.17 temos que

$$\begin{aligned} d_X(S) = \max_{e \in E\bar{K}_{2p}} \{d_X(S(\bar{K}_{2p} \setminus \{e\}))\} &= \max_{e \in E\bar{K}_{2p}} \{\frac{\rho(ad(\bar{K}_{2p} \setminus \{e\}))}{2p-1}\} \\ &= \frac{1}{2p-1} \max_{e \in E\bar{K}_{2p}} \{\rho(ad(\bar{K}_{2p} \setminus \{e\}))\} \end{aligned}$$

Vamos então calcular o raio espectral da matriz $ad(\bar{K}_{2p} \setminus \{e\})$. Seja $e = (a, b)$ uma aresta de $\bar{K}_{2p}$. Note que temos apenas dois casos para a aresta $e = (a, b)$, o caso $b \neq a$ e o caso $b = a$. Considere a base X reorganizada da seguinte maneira

$$X = \{x_1 = a, x_2 = a^{-1}, x_3 = b, x_4 = b^{-1}, x_5, x_6 = x_5^{-1}, ..., x_{2p} = x_{2p-1}^{-1}\}.$$

No caso em que $b \neq a$ temos

$$A = ad(\bar{K}_{2p} \setminus \{e\}) = \begin{pmatrix} 1 & 0 & \boxed{0} & 1 & 1 & 1 & ... & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & ... & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & ... & 1 & 1 \\ & & & & & & \ddots & & \\ 1 & 1 & 1 & 1 & 1 & 1 & ... & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & ... & 0 & 1 \end{pmatrix}$$

Considere o vetor $u = (-u_1, u_1, 0, 0, -u_2, u_2, -u_3, u_3, ..., -u_{p-1}, u_{p-1})$. Temos que

$$Au = \begin{pmatrix} -u_1 + 0 + 0 + 0 - u_2 + u_2 - u_3 + u_3 - ... - u_{p-1} + u_{p-1} \\ 0 + u_1 + 0 + 0 - u_2 + u_2 - u_3 + u_3 - ... - u_{p-1} + u_{p-1} \\ -u_1 + u_1 + 0 + 0 - u_2 + u_2 - u_3 + u_3 - ... - u_{p-1} + u_{p-1} \\ -u_1 + u_1 + 0 + 0 - u_2 + u_2 - u_3 + u_3 - ... - u_{p-1} + u_{p-1} \\ -u_1 + u_1 + 0 + 0 - u_2 + 0 - u_3 + u_3 - ... - u_{p-1} + u_{p-1} \\ -u_1 + u_1 + 0 + 0 + 0 + u_2 - u_3 + u_3 - ... - u_{p-1} + u_{p-1} \\ \vdots \\ -u_1 + u_1 + 0 + 0 - u_2 + u_2 - u_3 + u_3 - ... + 0 + u_{p-1} \end{pmatrix} = \begin{pmatrix} -u_1 \\ u_1 \\ 0 \\ 0 \\ -u_2 \\ u_2 \\ \vdots \\ u_{p-1} \end{pmatrix} = u$$

Como o autoespaço gerado por u tem dimensão $p-1$ temos que 1 é um autovalor com multiplicidade $p-1$.

Considere o vetor $v = (-(v_1+v_2+...+v_{p-2}), 0, 0, v_1, v_1, v_2, v_2, ..., v_{p-2}, v_{p-2})$. Temos que

$$Av = \begin{pmatrix} -(v_1+v_2+...+v_{p-2})+0+0+0+v_1+v_1+v_2+v_2+...+v_{p-2}+v_{p-2} \\ 0-(v_1+v_2+...+v_{p-2})+0+0+v_1+v_1+v_2+v_2+...+v_{p-2}+v_{p-2} \\ -2(v_1+v_2+...+v_{p-2})+0+0+v_1+v_1+v_2+v_2+...+v_{p-2}+v_{p-2} \\ -2(v_1+v_2+...+v_{p-2})+0+0+v_1+v_1+v_2+v_2+...+v_{p-2}+v_{p-2} \\ -2(v_1+v_2+...+v_{p-2})+0+0+v_1+0+v_2+v_2+...+v_{p-2}+v_{p-2} \\ -2(v_1+v_2+...+v_{p-2})+0+0+0+v_1+v_2+v_2+...+v_{p-2}+v_{p-2} \\ -2(v_1+v_2+...+v_{p-2})+0+0+v_1+v_1+v_2+0+...+v_{p-2}+v_{p-2} \\ -2(v_1+v_2+...+v_{p-2})+0+0+v_1+v_1+0+v_2+...+v_{p-2}+v_{p-2} \\ \vdots \\ -2(v_1+v_2+...+v_{p-2})+0+0+v_1+v_1+v_2+v_2+...+v_{p-2}+0 \\ -2(v_1+v_2+...+v_{p-2})+0+0+v_1+v_1+v_2+v_2+...+0+v_{p-2} \end{pmatrix}$$

$$= \begin{pmatrix} v_1+v_2+...+v_{p-2} \\ v_1+v_2+...+v_{p-2} \\ 0 \\ 0 \\ -v_1 \\ -v_1 \\ -v_2 \\ -v_2 \\ \vdots \\ -v_{p-2} \\ -v_{p-2} \end{pmatrix} = -v$$

Como o autoespaço gerado por v tem dimensão $p-2$ temos que -1 é um autovalor com multiplicidade $p-2$.

Agora considere o polinômio $x^2-(2p-2)x-(2p-2)$. Como $\Delta = (2p-2)^2+4(2p-2) > 0$, o polinômio tem raizes reais. Sejam α_1 e α_2 raizes desse polinômio. Vamos mostrar que o vetor

$$w_1 = \left(-\frac{2p-3}{4p-5}(\alpha_1-1), -\frac{2p-2}{4p-5}(\alpha_1-1), 1, 1, ..., 1\right)$$

é um autovetor de A associado ao autovalor α_2. E analogamente o vetor

$$w_2 = \left(-\frac{2p-3}{4p-5}(\alpha_2-1), -\frac{2p-2}{4p-5}(\alpha_2-1), 1, 1, ..., 1\right)$$

é um autovetor de A associado ao autovalor α_1

Primeiro note que

$$Aw_1 = \begin{pmatrix} -\dfrac{2p-3}{4p-5}(\alpha_1-1)+0+0+1+1+...+1 \\ 0-\dfrac{2p-2}{4p-5}(\alpha_1-1)+1+1+1+...+1 \\ -\dfrac{2p-3}{4p-5}(\alpha_1-1)-\dfrac{2p-2}{4p-5}(\alpha_1-1)+1+0+1+...+1 \\ -\dfrac{2p-3}{4p-5}(\alpha_1-1)-\dfrac{2p-2}{4p-5}(\alpha_1-1)+0+1+1+...+1 \\ \vdots \\ -\dfrac{2p-3}{4p-5}(\alpha_1-1)-\dfrac{2p-2}{4p-5}(\alpha_1-1)+1+1+1+...+0+1 \end{pmatrix}$$

$$= \begin{pmatrix} -\dfrac{2p-3}{4p-5}(\alpha_1-1)+(2p-3) \\ -\dfrac{2p-2}{4p-5}(\alpha_1-1)+(2p-2) \\ -\dfrac{2p-3}{4p-5}(\alpha_1-1)-\dfrac{2p-2}{4p-5}(\alpha_1-1)+(2p-3) \\ -\dfrac{2p-3}{4p-5}(\alpha_1-1)-\dfrac{2p-2}{4p-5}(\alpha_1-1)+(2p-3) \\ \vdots \\ -\dfrac{2p-3}{4p-5}(\alpha_1-1)-\dfrac{2p-2}{4p-5}(\alpha_1-1)+(2p-3) \end{pmatrix}$$

$$= \begin{pmatrix} -\dfrac{2p-3}{4p-5}\left(\alpha_1-1-(4p-5)\right) \\ -\dfrac{2p-2}{4p-5}(\alpha_1-1-(4p-5)) \\ -(\alpha_1-1)\left(\dfrac{2p-3+2p-2}{4p-5}\right)+(2p-3) \\ -(\alpha_1-1)\left(\dfrac{2p-3+2p-2}{4p-5}\right)+(2p-3) \\ \vdots \\ -(\alpha_1-1)\left(\dfrac{2p-3+2p-2}{4p-5}\right)+(2p-3) \end{pmatrix} = \begin{pmatrix} -\dfrac{2p-3}{4p-5}(\alpha_1-4p+4) \\ \\ -\dfrac{2p-2}{4p-5}(\alpha_1-4p+4) \\ \\ -(\alpha_1-1)+(2p-3) \\ -(\alpha_1-1)+(2p-3) \\ \vdots \\ -(\alpha_1-1)+(2p-3) \end{pmatrix}$$

Como α_1 e α_2 são raizes do polinômio $x^2-(2p-2)x-(2p-2)$, usando a regra da soma e do produto temos

$$\begin{cases} \alpha_1+\alpha_2 = 2p-2 \\ \alpha_1\alpha_2 = -(2p-2) \end{cases} \Rightarrow \begin{cases} \alpha_2 = 2p-2-\alpha_1 = \alpha_1+1+2p-3 = -(\alpha_1-1)+(2p-3) \\ (\alpha-1)\alpha_2 = \alpha_1\alpha_2-\alpha_2 = -2p+2+\alpha_1-2p+2 = \alpha_1-4p+4 \end{cases}$$

Logo, podemos concluir que

$$Aw_1 = \begin{pmatrix} -\dfrac{2p-3}{4p-5}(\alpha_1 - 1)\alpha_2 \\ -\dfrac{2p-2}{4p-5}(\alpha_1 - 1)\alpha_2 \\ \alpha_2 \\ \alpha_2 \\ \vdots \\ \alpha_2 \end{pmatrix} = \alpha_2 w_1$$

Os calculos para mostrar que α_1 é autovalor associado ao autovetor w_2 são totalmente analogamos, trocando apenas onde tem α_1 por $\alpha 2$.

Logo, temos que o polinômio caracteristico de A é

$$\chi A(x) = (x-1)^{p-1}(x+1)^{p-2}(x^2 - (2p-2)x - (2p-2))(x-\beta),$$

onde é outro autovalor de A.

Note que mesmo que A não seja simétrica, já mostramos que A possui todos os seus autovalores reais. Como a soma das dimensões dos autoespaços encontrados até agora é $2p-1$, com o autovetor que falta encontrar associado a β teremos que a soma dos autoespaços é $2p$. Podemos concluir então que a matriz A é diagonalizavel e podemos utilizar a proposição 4.20. Então o coeficiente de $\chi A(x)$ que multiplica x^{2p-1} é dado por $-Tr(A)$. Olhando para os termos que tem x^{2p-1} temos

$$x^{2p-1}[-\beta + (p-1).(-1) + (p-2).(1) - (2p-2)].$$

Logo temos $-Tr(A) = -2p = -\beta - 2p + 1$, o que nos dá $\beta = 1$.

Observe que $\alpha_1 = p - 1 - \sqrt{p^2-1}$, logo temos

$$\begin{aligned} -2p &< -2 \\ -2p+1 &< -1 \\ p^2 - 2p + 1 &< p^2 - 1 \\ (p-1)^2 &< p^2 - 1 \\ p - 1 &< \sqrt{p^2-1} \\ p - 1 - \sqrt{p^2-1} &< 0 \end{aligned} \qquad \begin{aligned} p^2 &> p^2 - 1 \\ p &> \sqrt{p^2-1} \\ p - \sqrt{p^2-1} &> 0 \\ p - 1 - \sqrt{p^2-1} &> -1 \end{aligned}$$

O que nos dá $|\alpha_1| < 1$. Logo o raio espectral de A é $w_2 = p - 1 + \sqrt{p^2-1} > 1$

Vamos analisar agora o caso em que $b = a$. Neste caso, usando a mesma base reorganizada X temos

$$B = ad(\bar{K}_{2p} \setminus \{e\}) = \begin{pmatrix} \boxed{0} & 0 & 1 & 1 & 1 & 1 & ... & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & ... & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & ... & 1 & 1 \\ & & & & & & \ddots & & \\ 1 & 1 & 1 & 1 & 1 & 1 & ... & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & ... & 0 & 1 \end{pmatrix}$$

Analogo ao primeiro caso, considere o vetor $u = (0, 0, -u_1, u_1, -u_2, u_2, ..., -u_{p-1}, u_{p-1})$ e temos

$$Au = \begin{pmatrix} 0+0-u_1+u_1-u_2+u_2-....-u_{p-1}+u_{p-1} \\ 0+0-u_1+u_1-u_2+u_2-....-u_{p-1}+u_{p-1} \\ 0+0-u_1+0-u_2+u_2-....-u_{p-1}+u_{p-1} \\ 0+0+0+u_1-u_2+u_2-....-u_{p-1}+u_{p-1} \\ 0+0-u_1+u_1-u_2+0-....-u_{p-1}+u_{p-1} \\ 0+0-u_1+u_1+0+u_2-....-u_{p-1}+u_{p-1} \\ \vdots \\ 0+0-u_1+u_1-u_2+u_2-....-u_{p-1}+0 \\ 0+0-u_1+u_1-u_2+u_2-....0+u_{p-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -u_1 \\ u_1 \\ -u_2 \\ u_2 \\ \vdots \\ -u_{p-1} \\ u_{p-1} \end{pmatrix} = u$$

Como o autoespaço gerado por u tem dimensão $p-1$ temos que 1 é um autovalor com multiplicidade $p-1$.

Considerando agora o vetor

$$v = (0, 0, -(v_1+v_2+...+v_{p-2}), -(v_1+v_2+...+v_{p-2}), v_1, v_1, v_2, v_2, ..., v_{p-2}, v_{p-2})$$

$$Av = \begin{pmatrix} 0+0-2(v_1+v_2+...+v_{p-2})+v_1+v_1+v_2+v_2+...+v_{p-2}+v_{p-2} \\ 0+0-2(v_1+v_2+...+v_{p-2})+v_1+v_1+v_2+v_2+...+v_{p-2}+v_{p-2} \\ 0+0-(v_1+v_2+...+v_{p-2})+0+v_1+v_1+v_2+v_2+...+v_{p-2}+v_{p-2} \\ 0+0+0-(v_1+v_2+...+v_{p-2})+v_1+v_1+v_2+v_2+...+v_{p-2}+v_{p-2} \\ 0+0-2(v_1+v_2+...+v_{p-2})+v_1+0+v_2+v_2+...+v_{p-2}+v_{p-2} \\ 0+0-2(v_1+v_2+...+v_{p-2})+0+v_1+v_2+v_2+...+v_{p-2}+v_{p-2} \\ 0+0-2(v_1+v_2+...+v_{p-2})+v_1+v_1+v_2+0+...+v_{p-2}+v_{p-2} \\ 0+0-2(v_1+v_2+...+v_{p-2})+v_1+v_1+0+v_2+...+v_{p-2}+v_{p-2} \\ \vdots \\ 0+0-2(v_1+v_2+...+v_{p-2})+v_1+v_1+v_2+v_2+...+v_{p-2}+0 \\ 0+0-2(v_1+v_2+...+v_{p-2})+v_1+v_1+v_2+v_2+...+0+v_{p-2} \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 0 \\ v_1 + v_2 + ... + v_{p-2} \\ v_1 + v_2 + ... + v_{p-2} \\ -v_1 \\ -v_1 \\ -v_2 \\ -v_2 \\ \vdots \\ -v_{p-2} \\ -v_{p-2} \end{pmatrix} = -v$$

Como o autoespaço gerado por v tem dimensão $p-2$ temos que -1 é um autovalor com multiplicidade $p-2$.

Logo, temos que o polinômio caracteristico de B é

$$\chi B(x) = (x-1)^{p-1}(x+1)^{p-2}(x^3 + ax^2 + bx + c),$$

onde a, b e c são números reais que podemos encontrar usando ***. Observe que podemos encontrar o determinante da matriz B mais facilmente se fizermos primeiro operações lineares do tipo $l_i = -l_2 + l_i$ para $i = 3, 4, ..., 2p$ e depois operações lineares do tipo $l_1 = l_1 + l_i$ para $i = 3, 4, 5, ...2p$ para obtermos a matriz B'

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

Usando Laplace na primeira linha termos $Det(B) = Det(B') = 2p-2(-1)^2.det(B'_{11})$. Novamente usando Laplace na primeira coluna para encontrar o determinante de B'_{11}

teremos $det(B'_{11}) = 1.(-1)^2.Det(\bar{B}) = Det(\bar{B})$ onde $\bar{B}$ é a matrix

$$\begin{pmatrix} 0 & -1 & 0 & 0 & ... & 0 & 0 \\ -1 & 0 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & -1 & ... & 0 & 0 \\ 0 & 0 & -1 & 0 & ... & 0 & 0 \\ & & & & \ddots & & \\ 0 & 0 & 0 & 0 & ... & 0 & -1 \\ 0 & 0 & 0 & 0 & ... & -1 & 0 \end{pmatrix}$$

Note que se trocarmos as linhas l_{2i-1} e l_{2i} para $i = 1, 2, .., p-1$ teremos uma matriz diagonal onde todos os termos da diagonal principal é -1, logo o determinante dessa matriz diagonal será $(-1)^{2p-2} = 1$. Como para obter a matriz diagonal temos que fazer $p-1$ trocas de linhas em $\bar{B}$, temos que $det(\bar{B}) = (-1)^{p-1}1$.

Logo temos que $det(B) = (2p-2)(-1)^{p-1} = 2(p-1)(-1)^{p-1}$

Agora vamos calcular os determinantes das matrizes reduzidas B_{ii}. Analogo ao calculo anterior, vamos primeiro realizar operações lineares em B_{11} analogas as que fizemos para calcular o determinante de B.

$$det(B_{11}) = det \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & ... & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & ... & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & ... & 1 & 1 \\ & & & & & \ddots & & \\ 1 & 1 & 1 & 1 & 1 & ... & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & ... & 0 & 1 \end{pmatrix} = det \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & ... & 1 & 1 \\ 0 & 0 & -1 & 0 & 0 & ... & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & ... & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & ... & 0 & 0 \\ & & & & & \ddots & & \\ 0 & 0 & 0 & 0 & 0 & ... & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & ... & -1 & 0 \end{pmatrix}$$

Usando Laplace na primeira coluna temos $Det(B_{11}) = 1.(-1)^{p-1}$ pelos mesmos argumentos anteriores.

$$det(B_{22}) = det \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & ... & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & ... & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & ... & 1 & 1 \\ & & & & & \ddots & & \\ 1 & 1 & 1 & 1 & 1 & ... & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & ... & 0 & 1 \end{pmatrix} = det \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 0 & -1 & 0 & 0 & ... & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & ... & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & ... & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & ... & 0 & 0 \\ & & & & & \ddots & & \\ 1 & 0 & 0 & 0 & 0 & ... & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & ... & -1 & 0 \end{pmatrix}$$

$$= det \begin{pmatrix} 2p-2 & 0 & 0 & 0 & 0 & ... & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & ... & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & ... & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & ... & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & ... & 0 & 0 \\ & & & & & \ddots & & \\ 1 & 0 & 0 & 0 & 0 & ... & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & ... & -1 & 0 \end{pmatrix} = (2p-2)(-1)^{p-1}$$

$$det(B_{33}) = det \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & ... & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & \boxed{1} & 1 & 1 & ... & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & ... & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & ... & 1 & 1 \\ & & & & & \ddots & & \\ 1 & 1 & 1 & 1 & 1 & ... & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & ... & 0 & 1 \end{pmatrix} = det \begin{pmatrix} -1 & -1 & 0 & 0 & 0 & ... & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & ... & 0 & 0 \\ 1 & 1 & \boxed{1} & 1 & 1 & ... & 1 & 1 \\ 0 & 0 & 0 & 0 & -1 & ... & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & ... & 0 & 0 \\ & & & & & \ddots & & \\ 0 & 0 & 0 & 0 & 0 & ... & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & ... & -1 & 0 \end{pmatrix}$$

$$= det \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & ... & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & ... & 0 & 0 \\ 1 & 1 & \boxed{1} & 1 & 1 & ... & 1 & 1 \\ 0 & 0 & 0 & 0 & -1 & ... & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & ... & 0 & 0 \\ & & & & & \ddots & & \\ 0 & 0 & 0 & 0 & 0 & ... & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & ... & -1 & 0 \end{pmatrix}$$

Usando Laplace na coluna 3 temos $det(B_{33}) = 1(-1)^{3+3}(-1)^{p=1} = (-1)^{p-1}$

Observe agora que todas as matrizes reduzidas B_{ii} para $i = 3, 4, ..., 2p$ são iguais (Fig 3)

Temos então

$$\begin{aligned} \sum_{i=1}^{2p} det(B_{ii}) &= (-1)^{p-1} + (2p-2)(-1)^{p-1} + (2p-2).(-1)^{p-1} \\ &= (-1)^{p-1}.(4p-3) \end{aligned}$$

$$B = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & \ldots & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & \boxed{1} & 0 & 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & 0 & \boxed{1} & 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & \ldots & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & \ldots & 1 & 1 \\ & & & & & & \ddots & & \\ 1 & 1 & 1 & 1 & 1 & 1 & \ldots & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & \ldots & 0 & 1 \end{pmatrix}$$

Figura 3 –

Como B é uma matriz simétrica de ordem par, podemos usar a proposição 4.20 para determinar os coeficientes do polinômio caracteristico

$$(1) \begin{cases} a_{2p-1} = -Tr(B) = -(2p-1) \\ a_1 = -\sum_{i=1}^{2p} det(B_{ii}) = (-1)(-1)^{p-1}(4p-3) \\ a_0 = det(B) = (2p-2)(-1)^{p-1} \end{cases}$$

Por outro lado, fazendo a distribuitiva no polinômio $\chi B(x)$ temos

$$\begin{cases} a_{2p-1} = a + (p-1)(-1) + (p-2) \\ a_1 = (p-1)(-1)^{p-2}.1^{p-2}.c + (p-2).1^{p-3}(-1)^{p-1}c + (-1)^{p-1}.1^{p-2}b \\ a_0 = (-1)^{p-1}1^{p-2}c \end{cases}$$

$$\begin{cases} a_{2p-1} = a - 1 \\ a_1 = (-1)^{p-1}(-(p-1)c + (p-2)c + b) = (-1)^{p-1}(b-c) \\ a_0 = (-1)^{p-1}c \end{cases}$$

Substituindo em (1) temos

$$\begin{cases} a-1=-(2p-1) \\ (-1)^{p-1}(b-c)=(-1)(-1)^{p-1}(4p-3) \\ (-1)^{p-1}c=(-1)^{p-1}(2p-2) \end{cases} \Rightarrow \begin{cases} a=-(2p-2) \\ b=-(4p-3)+(2p-2)=-(2p-1) \\ c=(2p-2) \end{cases}$$

Então

$$\chi B(x)=(x-1)^{p-1}(x+1)^{p-2}(x^3-(2p-2)x^2-(2p-1)x+(2p-2))$$

Agora note que, seja $h(x)=x^3-(2p-2)x^2-(2p-1)x+(2p-2)$

$$\begin{aligned} h(2p-2) &= (2p-2)^3-(2p-2)^3-(2p-1)(2p-2)+(2p-2) \\ &= (2p-2)(2-2p) \\ &= -(2p-2)^2<0 \qquad e \end{aligned}$$

$$\begin{aligned} h(2p-1) &= (2p-1)^3-(2p-2)(2p-1)^2-(2p-1)^2+(2p-2) \\ &= (2p-1)^2(2p-1-(2p-2)-1)+(2p-2) \\ &= 2p-2>0 \end{aligned}$$

Logo, temos raizes de $h(x)$ em $(2p-2,2p-1)$. Tomemos agora $x>(2p-1)$ temos que $x^2>(2p-1)x$ e logo

$$\begin{aligned} h'(x) &= 3x^2-2(2p-2)x-(2p-1) \\ &> 3x^2-2x^2-(2p-1) \\ &= x^2-(2p-1)>0 \end{aligned}$$

O que implica que $h(x)$ é crescente em $(2p-1,\infty)$. Como $h(2p-1)>0$ concluimos que $h(x)$ não pode ter raizes maiores que $2p-1$ e que a maior raiz γ_p de $h(x)$ está em $(2p-2,2p-1)$.

Agora considere a função $f:[1,\infty)$ definida por $f(p)=p-1+\sqrt{p^2-1}-(2p-2)=\sqrt{p^2-1}-p+1$. Temos $f'(p)=\dfrac{p}{\sqrt{p^2-1}}-1>0$. Logo $f(p)$ é crescente. Como $f(1)=1>0$ temos que $f>0$ e logo temos $p-1+\sqrt{p^2-1}-(2p-2)>0 \Rightarrow p-1+\sqrt{p^2-1}>(2p-2)$.

Lembrando que $\alpha=p-1+\sqrt{p^2-1}$ é raiz do polinômio $x^2-(2p-2)x-(2p-2)$ temos que

$$\begin{aligned} h(\alpha) &= \alpha^3-(2p-2)\alpha^2-(2p-1)\alpha+(2p-2) \\ &= \alpha[\alpha^2-(2p-2)\alpha-(2p-1)]+(2p-2) \\ &= \alpha[\alpha^2-(2p-2)\alpha-(2p-2)-1]+(2p-2) \\ &= \alpha[0-1]+(2p-2) \\ &= (2p-2)-\alpha<0 \end{aligned}$$

Logo, pode os concluir que $\alpha < \gamma_p$. Pois caso contrário teriamos que existe outra raiz de $h(x)$ maior que α e consequentemente maior que γ_p, o que seria uma contradição.

Logo, temos que $\rho(B) = \gamma_p > \rho(A) = \alpha$ e logo

$$\max_{e \in E\bar{K}_{2p}} \{\rho(ad(\bar{K}_{2p} \setminus \{e\}))\} = \gamma_p$$

o que nos dá

$$d_X(S) = \frac{\gamma_p}{2p-1} < 1$$

∎

Corolário 6.23. *Seja S o conjunto de palavras $w \in F_P$ tais que $Z_w = \bar{K}_{2p}$. Então, S tem densidade natural igual a 1.*

Demonstração. Observe que S é o complemento do conjunto do teorema anterior, logo temos $F_p = S \bigcup \bar{S}$ onde $\bar{S}$ é o conjunto do teorema anterior. Pelo teorema anterior $d_X(\bar{S}) < 1$, e pelo item 7 das propriedades 5.8 temos $\delta_X(\bar{S}) = 0$.

Como os conjuntos são disjuntos, temos que

$$\begin{aligned}
|(S \bigcup \bar{S}) \bigcap B_X(n)| &= |S \bigcap B_X(n)| + |\bar{S} \bigcap B_X(n)| \\
\frac{|(S \bigcup \bar{S}) \bigcap B_X(n)|}{|B_X(n)|} &= \frac{|S \bigcap B_X(n)| + |\bar{S} \bigcap B_X(n)|}{|B_X(n)|} \\
&= \frac{|S \bigcap B_X(n)|}{|B_X(n)|} + \frac{|\bar{S} \bigcap B_X(n)|}{|B_X(n)|} \\
\limsup_{n\to\infty} \frac{|(S \bigcup \bar{S}) \bigcap B_X(n)|}{|B_X(n)|} &\leq \limsup_{n\to\infty} \frac{|S \bigcap B_X(n)|}{|B_X(n)|} + \frac{|\bar{S} \bigcap B_X(n)|}{|B_X(n)|} \\
\delta_X(S \bigcup \bar{S}) &\leq \delta_X(S) + \delta_X(\bar{S}) \\
\delta_X(F_p) &\leq \delta_X(S) + 0 \\
1 &\leq \delta_X(S)
\end{aligned}$$

Como $\delta_X(S)$ não pode ser maior que 1, concluimos que $\delta_X(S) = 1$. ∎

7 A densidade das palavras primitivas em F_p

Proposição 7.1. *Seja F_p o grupo livre de classe p, gerado pelo conjunto X. Seja $S' \subseteq F_p$ um subconjunto não vazio de palavras em F_p e seja*

$$S = \{x^{-1}wx \mid w \in S', x \in F_p\}.$$

Se S' contém apenas palavras ciclicamente reduzidas, então

$$d_X(S) = \max\{d_X(S'), (2p-1)^{-\frac{1}{2}}\}$$

Demonstração. Como S' é não vazio, temos $|S| = \infty$ e podemos usar a proposição 5.21 para calcular a densidade de S usando esferas.

Vamos considerar primeiro o caso em que $|S'| = 1$, suponha $S' = \{w\}$ onde w é uma palavra ciclicamente reduzida. Se $|w| = k$ temos $w = x_1x_2...x_k$. Logo para uma palavra do tipo $u^{-1}wu$ com $u \in F_p$ ser de comprimento n temos que ter $|u| = \frac{n-k}{2}$ e u não pode começar nem com a letra x_k^{-1} e nem com a letra x_1, pois $u^{-1}wu = u_{\frac{n-k}{2}}^{-1}...u_1^{-1}x_1...x_ku_1...u_{\frac{n-k}{2}}$. Como w é ciclicamente reduzida, temos que $x_k^{-1} \neq x_1$. Logo as possibilidades para escrever u são

$$(2p-2)(2p-1)^{\frac{n-k}{2}-1} = \frac{2p-2}{2p-1}\sqrt{(2p-1)^{n-k}}$$

Agora observe que podemos também ter em S palavras do tipo $u^{-'}w'u$ onde w' é conjugado de w de comprimento k, isto é, $w' = x_ix_{i+1}...x_kx_1..x_{i-1}$. Obtermos w' fazendo $v^{-1}wv$ onde $v = x_k^{-1}x_{k-1}^{-1}...x_i^{-1}$ e teremos

$$u^{-1}w'u = u^{-1}v^{-1}wvu \in S$$

Temos exatamente k conjugados de w de comprimento k, e para cada um deles vimos que as possibilidades de u para que $|u^{-'}wu|$ é $\frac{2p-2}{2p-1}\sqrt{(2p-1)^{n-k}}$. Logo

$$|S \bigcap S_X(n)| = k\left(\frac{2p-2}{2p-1}\right)\sqrt{(2p-1)^{n-k}}$$

Note que para isso precisamos que $n \equiv k \bmod 2$. No caso em que $n-k$ não for divisivel por 2. temos que não existe $u \in F_p$ com $|u^{-1}wu| = n$. Logo para $n \not\equiv k \bmod 2$ temos $|S \bigcap S_X(n)| = 0$. Podemos então considerar apenas os valores de $n \equiv k \bmod 2$ e temos

$$
\begin{aligned}
d_X(S) &= \frac{1}{2p-1}\limsup|S\bigcap S_X(n)|^{\frac{1}{n}}\\
&= \frac{1}{2p-1}\limsup\left(\frac{k(2p-2)}{2p-1}\sqrt{(2p-1)^{n-k}}\right)^{\frac{1}{n}}\\
&= \frac{1}{2p-1}\limsup\left(\frac{k(2p-2)}{2p-1}\right)^{\frac{1}{n}}\left(\sqrt{(2p-1)^{n-k}}\right)^{\frac{1}{n}}\\
&= \frac{1}{2p-1}\limsup\sqrt{(2p-1)}^{(\frac{n-k}{n})}\\
&= \frac{1}{2p-1}\limsup\sqrt{(2p-1)}^{(1-\frac{k}{n})}\\
&= \frac{1}{2p-1}\sqrt{(2p-1)}\\
&= \frac{1}{\sqrt{2p-1}} = (2p-1)^{-\frac{1}{2}}
\end{aligned}
$$

Como S' é finito, temos $d_X(S') = \frac{1}{2p-1} < \frac{1}{(2p-1)^{\frac{1}{2}}}$. Logo

$$d_X(S) = (2p-1)^{-\frac{1}{2}} = \max\{d_X(S'), (2p-1)^{-\frac{1}{2}}\}$$

Agora suponhamos $|S'| < \infty$. Se $S' = \{w_1, ...w_k\}$, considere os conjuntos $S'_i = \{w_i\}$. Claramente temos que $S = \bigcup S_i$ e logo

$$d_X(S) = \max\{d_X(S_i)\} = \max\{(2p-1)^{-\frac{1}{2}}\} = (2p-1)^{-\frac{1}{2}} = \max\{d_X(S'), (2p-1)^{-\frac{1}{2}}\}.$$

Agora suponha que $|S'| = \infty$. Seja $l = \limsup|S'\bigcap S_X(n)|^{\frac{1}{n}}$ e defina $a = \max\{l, \sqrt{2p-1}\}$. Sabemos que $d_X(S') = \frac{l}{2p-1}$ e também para algum $w_i \in S'$ vimos pelo caso anterior que $S_i = \frac{1}{\sqrt{2p-1}} = \frac{\sqrt{2p-1}}{2p-1}$. Temos que $S' \subseteq S$ e $S_i \subseteq S$, logo $d_X(S') \leq d_X(S)$ e $d_X(S_i) \leq d_X(S)$. Então temos $l \leq d_X(S)(2p-1)$ e $\sqrt{2p-1} \leq d_X(S)(2p-1)$. Logo $a \leq d_X(S)(2p-1)$.

Agora, para a outra desigualdade, seja $w \in S'$ uma palavra ciclicamente reduzida de comprimento k, já vimos que a quantidade de palavras conjugadas de w de tamanho $n > k$ é $k\left(\dfrac{2p-2}{2p-1}\right)\sqrt{(2p-1)^{n-k}}$. Para cada palavra em S' de tamanho k temos essa quantidade de palavras possiveis em S. Logo temos

$$|S\bigcap S_X(n)| \leq \sum_{k=1}^{k=n}|S'\bigcap S_X(k)|k\left(\frac{2p-2}{2p-1}\right)\sqrt{(2p-1)^{n-k}}$$

A desigualdade ocorre pois se w' for uma conjugação de w de tamanho k que também está em S' temos que as palavras conjugadas de w' vão aparecer tanto na contagem de palavras conjugadas de w' quanto na contagem de palavras conjugadas de w.

Dado $\epsilon > 0$. Temos que $\sqrt{2p-1} \leq a < a+\epsilon$. Pela definição de l temos que existe k_0 tal que $|S' \bigcap S_X(k)| \leq (l+\epsilon)^k \leq (a+\epsilon)^k$ para todo $k \geq k_0$. Logo existe uma constante M tal que

$$
\begin{aligned}
|S \bigcap S_X(n)| &\leq \sum_{k=1}^{k=n} |S' \bigcap S_X(k)| k \left(\frac{2p-2}{2p-1}\right) \sqrt{(2p-1)}^{n-k} \\
&\leq \sum_{k=1}^{k=n} k |S' \bigcap S_X(k)| \sqrt{(2p-1)}^{n-k} \\
&= \sum_{k=1}^{k=k_0-1} k |S' \bigcap S_X(k)| \sqrt{(2p-1)}^{n-k} \\
&\quad\quad + \sum_{k=k_0}^{k=n} k |S' \bigcap S_X(k)| \sqrt{(2p-1)}^{n-k} \\
&= M + \sum_{k=k_0}^{k=n} k |S' \bigcap S_X(k)| \sqrt{(2p-1)}^{n-k} \\
&\leq M + \sum_{k=k_0}^{k=n} n (a+\epsilon)^k \sqrt{(2p-1)}^{n-k} \\
&\leq M + \sum_{k=k_0}^{k=n} n (a+\epsilon)^k (a+\epsilon)^{n-k} \\
&= M + n \sum_{k=k_0}^{k=n} (a+\epsilon)^n \\
&= M + n(n-k_0+1)(a+\epsilon)^n \\
&\leq M + n^2 (a+\epsilon)^n
\end{aligned}
$$

Então

$$
\begin{aligned}
(2p-1) d_X(S) &= \limsup |S \bigcap S_X(n)|^{\frac{1}{n}} \\
&\leq \limsup (M + n^2(a+\epsilon)^n)^{\frac{1}{n}} \\
&= a + \epsilon
\end{aligned}
$$

Como vale para todo ϵ temos então $(2p-1)d_X(S) \leq a$. Concluimos então que

$$
\begin{aligned}
(2p-1) d_X(S) &= a \\
d_X(S) &= \max\{\frac{l}{2p-1}, \frac{\sqrt{2p-1}}{2p-1}\} \\
&= \max\{d_X(S'), (2p-1)^{-\frac{1}{2}}\}
\end{aligned}
$$

■

Definição 7.2. *Seja $w = x_1...x_n$ uma palavra em F_p. O grafo Whitehead de w, denotado por W_w, é o grafo com o seguinte conjunto de arestas:*

$$EW_w = \{(a, b^{-1}) \in (X^{\pm 1})^2 \mid w \text{ contém } ab\} \bigcup \{(x_n, x_1^{-1})\}$$

Observação 7.3. *Note que $\bar{Z_w} \subseteq W_w$ e $Z_w \subseteq \bar{W_w}$*

Teorema 7.4. *Seja w uma palavra ciclicamente reduzida do grupo livre F_p. Se w é uma palavra primitiva, então W_w tem um vertice de corte.*

Teorema 7.5. *Seja F_p o grupo livre de classe $p \geq 2$, e seja $S \subseteq F_p$ o conjunto de palavras primitivas de F_p. Para toda base X de F_p, nos temos*

$$\frac{2p-3}{2p-1} \leq d_X(S) \leq \frac{\gamma_p}{2p-1} < 1$$

Consequentemente, temos $\delta_X(S) = 0$

Demonstração. Considere S' o conjunto de palavras primitivas ciclicamente reduzidas. Observe que $S = \{x^{-1}wx \mid w \in S', x \in F_p\}$. De fato, seja $\bar{S} = \{x^{-1}wx \mid w \in S', x \in F_p\}$. Toda palavra reduzida pode ser escrita como $x^{-1}wx$ com w ciclicamente e reduzida. E se $x^{-1}wx$ é primitiva, então w também é pois a função $i_x : F_p \to F_p$ definida por $i_x(w) = x^{-1}wx$ é um isomorfismo e leva base em base. Logo temos $w \in S'$ e $S \subseteq \bar{S}$. A outra inclusião é difeta do isomorfismo i_x. Pela proposição 7.1 temos então

$$d_X(S) = \max\{d_X(S'), (2p-1)^{-\frac{1}{2}}\}$$

Observe que para $p = 2$ temos $\sqrt{2p-1} < 2p-2$. Como a derivada da função $f(p) = 2p - 2 - \sqrt{2p-1}$ é positiva para todo $p \geq 2$ então $\sqrt{2p-1} < 2p-2$ para todo $p \geq 2$. Logo

$$\frac{\sqrt{2p-1}}{2p-1} < \frac{2p-2}{2p-1} < \frac{\gamma_p}{2p-1}$$

Temos então que $(2p-1)^{-\frac{1}{2}} < \frac{\gamma_p}{2p-1}$. Basta mostrar agora que $d_X(S') \leq \frac{\gamma_p}{2p-1}$.

Tomemos $w \in S'$. Pelo teorema 7.4 W_w tem um vértice de corte. Logo temos $W_w < K_{2p}$ e consequentemente $\bar{W_w} < \bar{K}_{2p}$. Então $Z_w \subseteq \bar{W_w} < \bar{K}_2p$. Concluimos então que w pertence ao conjunto do teorema 6.22 e consequentemente S' está contido neste conjunto e temos $d_X(S') \leq \frac{\gamma_p}{2p-1}$. ■

Referências

[1] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, Cambridge, 1993.

[2] R. Grigorchuk and P. de la Harpe, *On problems related to growth, entropy and spectrum in group theory*, J. of Dynamical and Control Systems, **3** 1 (1997), 51-89

[3] R.A. Horn and C.R. Johnson, *Matrix analysis*, Cambridge University Press, Cambridge, 1990.

[4] L. Lovász and J. Pelikán, *On the eigenvalues of trees*, Periodica Math. Hung., **3** (1973), 175-182.

[5] E. Nosal, *Eigenvalues of graphs*, Master's thesis, University of Calgary, 1970.