UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA APLICADA

# Decomposição de Politopos e Aplicações na Fatoração de Polinômios

por

Luiz Emilio Allem

Dissertação submetida como requisito parcial
para a obtenção do grau de

Mestre em Matemática Aplicada

Prof. Dr. Vilmar Trevisan
Orientador

Porto Alegre, Setembro de 2005.

## CIP - CATALOGAÇÃO NA PUBLICAÇÃO

Allem, Luiz Emilio

Decomposição de Politopos e Aplicações na Fatoração de Polinômios / Luiz Emilio Allem.—Porto Alegre: PPGMAp da UFRGS, 2005.

121 p.: il.

Dissertação (mestrado) —Universidade Federal do Rio Grande do Sul, Programa de Pós-Graduação em Matemática Aplicada, Porto Alegre, 2005.
Orientador: Trevisan, Vilmar

Dissertação: Matemática Aplicada
Politopos, Irredutibilidade de polinômios, Fatoração de polinômios

**Decomposição de Politopos e Aplicações na Fatoração de Polinômios**

por

Luiz Emilio Allem

Dissertação submetida ao Programa de Pós-Graduação em Matemática Aplicada do Instituto de Matemática da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de

## Mestre em Matemática Aplicada

Linha de Pesquisa: Algoritmos Numéricos e Algébricos

Orientador: Prof. Dr. Vilmar Trevisan

Banca examinadora:

Prof. Dr. José Plínio de Oliveira Santos
UNICAMP

Prof. Dr. Jaime Bruck Ripoll
PPGMAT/IM/UFRGS

Prof. Dr. José Afonso Barrionuevo
PPGMAp/IM/UFRGS

Dissertação apresentada e aprovada em
26 de Setembro de 2005.

Prof. Dra. Maria Cristina Varriale
Coordenador

# SUMÁRIO

**LISTA DE ABREVIATURAS** . . . . . **VI**

**RESUMO** . . . . . **VII**

**ABSTRACT** . . . . . **VIII**

**1 INTRODUÇÃO** . . . . . **1**

**2 CONVEXIDADE** . . . . . **4**

**2.1 Convexidade** . . . . . 4

**2.2 Hiperplanos e Função Suporte** . . . . . 7

**2.3 Soma de Minkowski** . . . . . 15

2.3.1 Subtração de Minkowski . . . . . 18

**2.4 Politopos** . . . . . 20

**3 FAMÍLIAS IRREDUTÍVEIS** . . . . . **28**

**3.1 Introdução** . . . . . 28

**3.2 Critério de Irredutibilidade** . . . . . 29

**3.3 Construção de Politopos Integralmente Indecomponíveis** . . . 35

**3.4 Projeções** . . . . . 45

**4 DECOMPOSIÇÃO DE POLITOPOS** . . . . . **48**

**4.1 Introdução** . . . . . 48

**4.2 Envoltória Convexa no Plano** . . . . . 49

**4.3 Fatores e Decomposição** . . . . . 53

**4.4 Polígonos** . . . . . 54

**4.5 Politopos de Alta Dimensão** . . . . . 66

**5 FATORANDO POLINÔMIOS VIA POLITOPOS** . . . . . **71**

**5.1 Introdução** . . . . . 71

**5.2 Fatoração Parcial** . . . . . 72

**5.3 Equações do levantamento de Hensel Modificadas** . . . . . 81

**5.4 Lema Geométrico** . . . . . 83

**5.5 O Teorema Principal** . . . . . 86

**6 CONCLUSÃO** . . . . . **98**

**BIBLIOGRAFIA** . . . . . **100**

**APÊNDICE A LEVANTAMENTO DE HENSEL** . . . . . **103**

**APÊNDICE B EXEMPLO DE FATORAÇÃO VIA POLITOPOS 107**

# LISTA DE ABREVIATURAS

| | |
|---|---|
| $[x, y]$ | $\{x + \lambda(y - x) : \lambda \in [0, 1]\}$, segmento de reta entre $x$ e $y$ |
| $\|\| \cdot \|\|$ | norma euclidiana |
| $vert(P)$ | conjunto dos vértices do politopo $P$ |
| $int(P)$ | interior do politopo $P$ |
| $bd(P)$ | fronteira do politopo $P$ |
| $Prob(a)$ | probabilidade de ocorrência do evento $a$ |
| $\log(n)$ | logaritmo na base 2 de $n$ |
| $O(f(n))$ | ordem de complexidade |
| $dim(V)$ | dimensão de $V$ |
| $gerado(u)$ | subespaço gerado por $u$ |

# RESUMO

A presente dissertação aborda pesquisas recentes sobre dois tópicos distintos da Matemática. Não é a primeira vez que as conexões entre geometria e álgebra são frutíferas, mas é somente agora que as idéias geométricas estão sendo aplicadas efetivamente na fatoração de polinômios, um tema puramente algébrico.

Mais especificamente, estudamos a decomposição de politopos e suas aplicações na fatoração de polinômios. Começamos apresentando construções de politopos integralmente indecomponíveis que levam a critérios de irredutibilidade de polinômios. Estudamos detalhadamente algoritmos para a decomposição de politopos, sempre ilustrados com exemplos e comentários sobre suas aplicações.

Terminamos apresentando um algoritmo desenvolvido por Fatima Salem, Shuhong Gao e Alan Lauder, que fatora polinômios bivariados a partir da decomposição do seu politopo de Newton associado. Esse algoritmo é um marco nessa área já que traduz, pela primeira vez, de forma eficiente, idéias geométricas para a fatoração polinomial, usando uma técnica similar ao levantamento de Hensel.

# ABSTRACT

The present work deals with recent research about two distinct mathematical topics. It is not the first time that connections between geometry and algebra are fruitful, but it is only now that geometric ideas are being applied effectively in polynomial factorization, a purely algebraic theme.

More specifically we study the decomposition of polytopes and their applications on polynomial factorization. We begin studying construction of indecomposable polytopes which give many irreducibility criteria polynomial. We study thoroughly algorithms for decomposition of polytopes, always illustrated with examples and comments about their applications.

We finish presenting an algorithm developed by Fatima Salem, Shuhong Gao and Alan Lauder for factoring bivariate polynomials from the decomposition of the Newton polytope associated. This algorithm is a mark land in the field since it translate, for the first time, effectivelly, geometric ideas for polynomial factorization using a technic similar to Hensel lifting.

# AGRADECIMENTOS

Agradeço a meu pai Luiz Costa Allem, a minha mãe Marlei Beatriz Allem e a minha irmã Luciane Beatriz Allem por todos esses anos de amor, compreensão, motivação e ajuda em todos os sentidos. Amo muito vocês.

Agradeço ao Professor e amigo Vilmar Trevisan que, durante todos os anos, desde a graduação até aqui, sempre me motivou e ajudou muito; com certeza, sem o seu auxílio, eu não teria chegado até este ponto.

Agradeço aos queridos amigos e colegas Carlos Hoppen e Clarice Decian que, durante a graduação e o mestrado, nunca me deixaram desistir e sempre me ajudaram muito. Adoro vocês.

Agradeço à Professora e amiga Maria Cristina Varriale pela motivação e pelas conversas engraçadas que tivemos quando eu ia falar com o Professor Vilmar.

Agradecimento especial à Professora Virgínia Maria Rodrigues da PUC-RS por ter sugerido o problema e por ter participado dos seminários que deram origem a este trabalho.

Agradeço ao professor Shuhong Gao, de Clemsom University, a quem conheci através da Professora Virgínia e que, por meio de conversas, deixou muito mais acessíveis e claras as idéias de seus artigos em que esta dissertação está baseada.

Agradeço ao departamento de matemática que sempre me deu ótimas condições de estudar e auxílio financeiro durante estes anos.

Agradeço a Deus por ter me dado saúde e vontade para chegar até aqui.

# 1 INTRODUÇÃO

O tema desta dissertação de mestrado é a conexão entre polinômios multivariados e politopos de Newton. Um dos primeiros resultados conhecidos ligando estes dois assuntos foi feito por Ostrowski em 1921 [16]. Ele associou a cada polinômio multivariado $f$ um politopo, dito politopo de Newton. Observou que se o polinômio multivariado $f$ fosse fatorável, digamos $f = gh$, então o politopo de Newton associado a $f$ seria decomposto como a soma do politopo de Newton associado a $g$ mais o politopo de Newton associado a $h$, sendo esta decomposição em relação à soma de Minkowski.

Motivado por tal resultado Shuhong Gao observa em [4] que cada vez que encontrarmos um politopo integralmente indecomponível este levará a uma família de polinômios absolutamente irredutíveis, ou seja, polinômios sobre um corpo $\mathbb{F}$ que permanecem absolutamente irredutíveis sobre qualquer extensão algébrica de $\mathbb{F}$. Neste trabalho Gao apresenta construções de politopos integralmente indecomponíveis que levam a critérios para irredutibilidade absoluta de polinômios multivariados.

No trabalho feito por Gao e Lauder em [6, 8] são apresentrados dois tipos de algoritmo. Um que decide a indecomponibilidade de politopos em $\mathbb{R}^n$ via projeções. Outro que constrói todos os fatores de um politopo em $\mathbb{R}^2$, polígonos. Ambos algoritmos podem ser usados para encontrarmos famílias de polinômios absolutamente irredutíveis. E o segundo tipo também pode ser usado na fatoração de polinômios bivariados.

No final dos trabalhos feitos por Gao e Lauder fica uma pergunta em aberto: Dado um polinômio $f$, seja $P$ seu politopo de Newton associado integralmente decomponível e seja $K$ um fator integral de $P$, é possível associar $K$ a um fator $g$ de $f$? Esta pergunta foi respondida por Fatima Abu Salem, Shuhong Gao e Alan G. B. Lauder em [18].

Eles responderam esta pergunta para o caso de politopos em $\mathbb{R}^2$, ou seja, para polinômios bivariados. Pois, como pode ser visto na literatura em [5, 12, 13, 15] a fatoração de polinômios em várias variáveis pode ser reduzida ao caso bivariado, que não pode ser reduzido ao caso univariado por métodos polinomialmente eficientes.

Como politopos são conjuntos convexos apresentaremos no capítulo 2 um apanhado de resultados a respeito dessa classe de conjuntos, particularmente politopos. Iremos estudar algumas propriedades de soma e subtração de Minkowski pois quando estivermos tratando da decomposição de politopos, esta sempre será em relação à soma de Minkowski. Gostaríamos de dar atenção especial a dois teoremas que serão apresentados no mesmo capítulo. O teorema de Krein Milmam o qual nos diz que um politopo é a envoltória convexa de seus vértices, ou seja, qualquer elemento do politopo pode ser escrito como uma combinação convexa dos vértices. Este resultado será muito importante quando estivermos estudando os critérios de indecomponibilidade de politopos do capítulo 3. E o teorema 2.4.1 o qual mostra que um fator de um politopo carrega muitas características do politopo. Este resultado será muito importante no capítulo 4 quando estivermos tratando da decomposição de politopos em $\mathbb{R}^2$, ou seja, polígonos. Veremos que cada aresta de um polígono pode ser decomposta, em relação à soma de Minkowski, como a soma de duas arestas ou como a soma de uma aresta a um ponto.

No capítulo seguinte estudaremos os resultados de Shuhong Gao, descritos nos artigos [4, 6]. Apresentaremos o critério de irredutibilidade feito por Gao em [4], o qual observa que se um dado politopo de Newton associado a um polinômio multivariado $f$ é integralmente indecomponível então $f$ é absolutamente irredutível. É importante notar que um dado politopo pode representar inúmeros polinômios, ou seja, podemos mudar os coeficientes dos termos do polinômio ou acrescentar novos termos desde que estes não alterem o formato do politopo. Por isso, a determinação de critérios de indecomponibilidade de politopos levarão a famílias de polinômios absolutamente irredutíveis.

No final do capítulo 3 apresentaremos construções de politopos integralmente indecomponíveis baseadas em projeções que foram feitas em [6]. Por exemplo, se tivermos um quadrado e fizermos a projeção sobre um de seus lados e esta for indecomponível esperamos que o quadrado também o seja.

No capítulo 4 estudaremos os algoritmos feitos por Shuhong Gao e Alan Lauder em [4, 6] que testam a decomponibilidade integral de politopos e constrõem fatores integrais se este for integralmente decomponível. Veremos que o problema de verificar se um politopo é integralmente indecomponível é NP-completo mesmo em dimensão 2, logo não existe, a menos que P=NP, um algoritmo genuinamente eficiente para decompor politopos. Os algoritmos podem ser usados, primeiro, como em [4] que será estudado no capítulo 3, ou seja, cada politopo integralmente indecomponível irá gerar uma família de polinômios absolutamente irredutíveis. Segundo, se um dado politopo é integralmente decomponível então utilizamos o algoritmo para encontrarmos todos os fatores integrais do politopo, o que será útil na fatoração de polinômios.

Como foi explorado em [4] cada politopo integralmente indecomponível gera uma família de polinômios absolutamente irredutíveis. Em [6] foram apresentados algoritmos para decidir a decomponibilidade integral de politopos e construir fatores, no caso deste ser integralmente decomponível. Porém uma pergunta ainda estava em aberto: Dado um polinômio $f$ e seu politopo de Newton associado $P$ integralmente decomponível. Seja $K$ um fator integral de $P$. Será que $K$ corresponde ao politopo de Newton associado de um fator $g$ de $f$? Este problema foi resolvido por Fatima Abu Salem, Shuhong Gao e Alan G. B. Lauder em [18], o qual será estudado no capítulo 5.

Nesta dissertação constam ainda dois apêndices. O primeiro sobre o método de Hensel, que foi primeiramente utilizado por Hans Zassenhauss em 1969 [23] e que é a base para o método de Gao para fatoração via politopos. O segundo com um exemplo explicado detalhadamente no qual fatoramos um polinômio bivariado $f$ via politopos.

# 2 CONVEXIDADE

Neste capítulo estudaremos um apanhado de resultados acerca de conjuntos convexos, particularmente politopos. Veremos algumas propriedades de soma e subtração de Minkowski, já que quando estivermos tratando da decomponibilidade de politopos, esta sempre será em relação à soma de Minkowski. Gostaríamos de enfatizar a importância de dois resultados que estudaremos a seguir. O teorema de Krein-Milman, o qual nos diz que um politopo é a envoltória convexa de seus vértices, ou seja, cada ponto de um politopo pode ser escrito como uma combinação convexa de seus vértices. E, também, o teorema 2.4.1, o qual assegura que um fator $K$ de um politopo $P$ tem muitas das características de $P$. Em particular quando estivermos tratando com politopos em $\mathbb{R}^2$, ou seja, polígonos, veremos que cada aresta poderá ser decomposta em relação à soma de Minkowski apenas como a soma de um ponto e uma aresta ou como a soma de duas arestas, sendo estas paralelas. Os resultados que serão estudados aqui foram retirados, principalmente, de [3, 11, 14, 20, 24].

## 2.1 Convexidade

As formas básicas de geometria que estudaremos nesta seção serão pontos, retas, planos e assim por diante, os quais são chamados de subespaços afins.

**Definição 2.1.1.** *Um conjunto $S \subset \mathbb{R}^n$ é dito convexo se dados $a, b \in S$ e $\lambda \in [0, 1]$, então $a + \lambda(b - a) = (1 - \lambda)a + \lambda b \in S$. Isto é, o segmento de reta entre $a$ e $b$ está em $S$.*

A figura 2.1 mostra à direita um conjunto convexo e à esquerda um conjunto não convexo, pois esta possui um segmento de reta com pontos extremos no conjunto que não está totalmente contido nele.

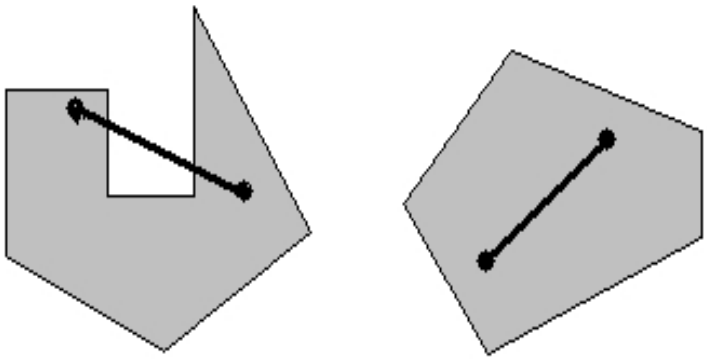

Figura 2.1: exemplo de convexidade

**Lema 2.1.1.** *A intersecção de uma coleção arbitrária de conjuntos convexos é convexa.*

**Dem.:** Se um segmento de reta está contido em todo conjunto da coleção, então ele estará contido na intersecção destes conjuntos. □

**Definição 2.1.2.** *Dizemos que $x$ é uma combinação convexa de $x_1, \ldots, x_r \in \mathbb{R}^n$ se existem $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$ tais que*

1. $x = \lambda_1 x_1 + \cdots + \lambda_r x_r$,
2. $\lambda_1 + \cdots + \lambda_r = 1$,
3. $\lambda_1 \geq 0, \ldots, \lambda_r \geq 0$.

**Definição 2.1.3.** *A envoltória convexa de um conjunto $S \subseteq \mathbb{R}^n$, denotada por $conv(S)$, é o conjunto de todas as combinações convexas de um número finito de elementos de $S$.*

$$conv(S) = \left\{ \lambda_1 x_1 + \cdots + \lambda_k x_k : \{x_1, \ldots, x_k\} \subseteq S, \lambda_i \geq 0, \sum_{i=1}^{k} \lambda_i = 1 \right\}.$$

Uma consequência da definição acima é de que a envoltória convexa de qualquer conjunto $S \subseteq \mathbb{R}^n$ pode ser vista como o menor conjunto convexo contendo $S$, como

provaremos a seguir. Assim, ela pode ser construída como a intersecção de todos os conjuntos convexos contendo $S$:

$$conv\,(S) = \bigcap \Big\{ S^{'} \subseteq \mathbb{R}^d : S \subseteq S^{'}, S^{'} convexo \Big\}.$$

Primeiro note que se $S \subset \mathbb{R}^n$ é convexo, então $conv(S) = S$. Claramente $S \subset conv(S)$. Vamos mostrar por indução que $S$ contém todas as combinações convexas de quaisquer $k$ pontos de $S$. Para $k = 2$ é satisfeito pela definição de convexidade. Suponha sem perda de generalidade que é satisfeito para $k-1$ e que $x = \lambda_1 x_1 + \cdots + \lambda_k x_k$ com $x_1, \cdots, x_k \in S$, $\lambda_1 + \cdots + \lambda_k = 1$ e $\lambda_1, \ldots, \lambda_k > 0$. Note que podemos supor que $x = (1-\lambda_k) \displaystyle\sum_{i=1}^{k-1} \frac{\lambda_i}{1-\lambda_k} x_i + \lambda_k x_k$ e já que $\dfrac{\lambda_i}{1-\lambda_k} > 0$ para $i = 1, \ldots k-1$ e $\displaystyle\sum_{i=1}^{k-1} \frac{\lambda_i}{1-\lambda_k} = 1$ segue que $s = \displaystyle\sum_{i=1}^{k-1} \frac{\lambda_i}{1-\lambda_k} x_i \in S$ por hipótese de indução. Portanto $x = (1-\lambda_k)s + \lambda_k x_k \in S$ por convexidade. Isto prova que $S = conv(S)$.

Consideremos agora um conjunto qualquer $S \subset \mathbb{R}^n$ seja $D(S)$ a intersecção de todos os conjuntos convexos $S^{'} \subset \mathbb{R}^n$ contendo $S$. Já que $S \subset conv(S)$ e $conv(S)$ é convexo, nós temos que $D(S) \subset conv(S)$. Cada conjunto convexo $S^{'}$ com $S \subset S^{'}$ satisfaz $conv(S) \subset conv(S^{'}) = S^{'}$, então $conv(S) \subset D(S)$, o que prova a igualdade.

Observe que se $K = \{x_1, \ldots, x_m\} \subseteq \mathbb{R}^n$ é finito, então é fácil ver que sua envoltória convexa é

$$conv(S) = \left\{ \sum_{i=1}^{m} \lambda_i x_i : \sum_{i=1}^{m} \lambda_i = 1, \lambda_i \geq 0 \right\}$$

O seguinte resultado sobre geração de envoltórias convexas é fundamental. Mas antes vamos definir independência convexa.

**Definição 2.1.4.** *Pontos $x_1, \ldots, x_k \in \mathbb{R}^n$ são convexamente independentes se nenhum deles é uma combinação convexa dos outros, isto é, se*

$$\sum_{i=1}^{k} \lambda_i x_i = 0 \text{ com } \lambda_i \in \mathbb{R} \text{ e } \sum_{i=1}^{k} \lambda_i = 0 \text{ implica que } \lambda_1 = \cdots = \lambda_k = 0.$$

É fácil ver que isto é equivalente à independência linear dos vetores $x_2 - x_1, \ldots, x_k - x_1$.

**Teorema 2.1.1 (Carathéodory).** *Se $A \subset \mathbb{R}^n$ e $x \in conv(A)$, então $x$ é uma combinação convexa de pontos convexamente independentes de $A$. Em particular, $x$ é uma combinação convexa de no máximo $n+1$ pontos de $A$.*

**Dem.:** O ponto $x \in conv(A)$ tem uma representação

$$x = \sum_{i=1}^{k} \lambda_i x_i \text{ com } x_i \in A \ , \ \lambda_i > 0 \ , \ \sum_{i=1}^{k} \lambda_i = 1$$

para algum $k \in \mathbb{N}$, e podemos assumir que $k$ é minimal. Suponha que $x_1, \ldots, x_k$ são convexamente dependentes. Então existem números reais $\alpha_1, \ldots, \alpha_k$, não todos nulos, com

$$\sum_{i=1}^{k} \alpha_i x_i = 0 \text{ e } \sum_{i=1}^{k} \alpha_i = 0.$$

Podemos escolher $m$ tal que $\lambda_m/\alpha_m$ é positivo e, com esta restrição, o menor possível(observe que todo $\lambda_i$ é positivo e que no mínimo um $\alpha_i$ é positivo), ou seja, $0 < \lambda_m/\alpha_m \leq \lambda_i/\alpha_i$ se $\alpha_i > 0$. Então podemos representar $x$ como

$$x = \sum_{i=1}^{k} (\lambda_i - \frac{\lambda_m}{\alpha_m}\alpha_i) x_i$$

com todos os coeficientes não negativos e com no mínimo um deles sendo zero(quando $i = m$). Isto contradiz a minimalidade de $k$. Então $x_1, \ldots, x_k$ são convexamente independentes, que implica $k \leq n+1$. □

## 2.2 Hiperplanos e Função Suporte

Nesta seção estudaremos algumas propriedades de hiperplanos e sua ligação com conjuntos convexos. A principal delas e que será vista posteriormente é de que poderemos representar um politopo como a intersecção de um número finito de semi-espaços definidos por hiperplanos.

A dimensão de um subespaço afim é a dimensão do espaço vetorial linear correspondente. Subespaços afim de dimensão 0, 1, 2, e $n-1$ em $\mathbb{R}^n$ são chamados de pontos, retas, planos, e hiperplanos, respectivamente.

**Proposição 2.2.1.** *Se $\langle\cdot\rangle$ denota o produto interno usual em $\mathbb{R}^n$, então, para $u \in \mathbb{R}^n \setminus \{0\}$ e $\alpha \in \mathbb{R}$ fixos, $H_\alpha(u) = \{x \in \mathbb{R}^n : \langle x, u\rangle = \alpha\}$ é um hiperplano em $\mathbb{R}^n$.*

**Dem.:** Vamos dividir a demonstração em dois casos, $\alpha = 0$ e $\alpha \neq 0$.

1. $\alpha = 0$: Vamos mostrar que $H_0(u) = \{x \in \mathbb{R}^n : \langle x, u\rangle = 0\}$ é um subespaço vetorial de dimensão $n-1$. Começamos mostrando que $H_0(u)$ é um subespaço vetorial de $\mathbb{R}^n$:

   (a) $\langle 0, u\rangle = 0$ então $0 \in H_0(u)$

   (b) Dados $x$,$y \in H_0(u)$ temos que $\langle x+y, u\rangle = \langle x, u\rangle + \langle y, u\rangle = 0$ então $x + y \in H_0(u)$

   (c) Seja $a \in \mathbb{R}$ e $x \in H_0(u)$ então $\langle ax, u\rangle = a\langle x, u\rangle = 0$, logo $ax \in H_0(u)$.

   Portanto $H_0(u)$ é um subespaço vetorial de $\mathbb{R}^n$. Agora vamos mostrar que $dim(H_0(u)) = n-1$. Note que

   $$H_0(u) = \{x \in \mathbb{R}^n : \langle x, u\rangle = 0\} = (gerado(u))^\perp$$

   e $\mathbb{R}^n = (gerado(u)) \oplus ((gerado(u))^\perp)$, e então temos que $dim(\mathbb{R}^n) = dim(gerado(u)) + dim((gerado(u))^\perp)$ e como $dim(gerado(u)) = 1$ e $dim(\mathbb{R}^n) = n$ então $dim((gerado(u))^\perp) = n-1$. Portanto $H_0(u)$ é um subespaço vetorial de $\mathbb{R}^n$ de dimensão $n-1$, um hiperplano em $\mathbb{R}^n$.

2. Para $\alpha \neq 0$ vamos mostrar que $H_\alpha(u)$ é o deslocamento de um subespaço vetorial de $\mathbb{R}^n$ com dimensão $n-1$. Consideremos

   $$H = H_\alpha(u) - \{e_1\} = \{x - e_1 : x \in H_\alpha(u)\} \tag{2.1}$$

   onde $e_1 = \dfrac{\alpha u}{\|u\|}$. Note que $e_1 \in H_\alpha(u)$. Vamos mostrar que $H$ é um subespaço vetorial de dimensão $n-1$ de $\mathbb{R}^n$. Seja $B = \{e_1, \ldots, e_n\}$

uma base ortogonal de $\mathbb{R}^n$. Definamos $v_j = e_j + e_1$ para $j = 2, \ldots, n$ e assim temos que $\langle v_j, u\rangle = \alpha$, logo $v_j \in H_\alpha(u)$ e assim $e_j = v_j - e_1 \in H$ para $j = 2, \ldots, n$. Agora mostraremos que $H$ é um subespaço vetorial de $\mathbb{R}^n$ e que $e_1 \notin H$, logo $H$ terá dimensão $n-1$.

(a) Como $e_1 \in H_\alpha(u)$ então $0 = e_1 - e_1 \in H$ por 2.1.

(b) Dados $v$,$w \in H$ então por 2.1 existem $x$,$y \in H_\alpha(u)$ tais que $v = x - e_1$ e $w = y - e_1$. Para provarmos que $v + w \in H$ basta mostrarmos que $v+w+e_1 \in H_\alpha(u)$ e então por 2.1 $v+w+e_1-e_1 = v+w \in H$. E como $\langle v+w+e_1, u\rangle = \langle x, u\rangle + \langle y, u\rangle - \langle e_1, u\rangle = \alpha$ estamos prontos.

(c) Dados $a \in \mathbb{R}$ e $v \in H$ então existe $x \in H_\alpha(u)$ tal que $v = x - e_1$ e pelo mesmo argumento anterior basta mostrarmos que $av + e_1 \in H_\alpha(u)$ para provarmos que $av \in H$. E como $\langle av + e_1, u\rangle = \langle ax - ae_1 + e_1, u\rangle = \alpha$ estamos prontos.

(d) Vamos mostrar que $e_1 \notin H$. Vamos supor que $e_1 \in H$, então $2e_1 \in H_\alpha(1)$. Mas $\langle 2e_1, u\rangle = 2\alpha$ uma contradição, logo $e_1 \notin H$

Portanto $H$ tem dimensão $n-1$ e $H_\alpha(u)$ é o deslocamento de um subespaço vetorial de $\mathbb{R}^n$ com dimensão $n-1$, logo $H_\alpha(u)$ tem dimensão $n-1$, ou seja, um hiperplano em $\mathbb{R}^n$ □

Dizemos que $u$ é o vetor normal a $H_\alpha(u)$. Então a proposição 2.2.1 caracterizou $H_\alpha(u)$ como um hiperplano em $\mathbb{R}^n$ com vetor normal $u$ e deslocado $\dfrac{\alpha u}{\|u\|}$ da origem.

**Definição 2.2.1.** *Denotaremos por* $H_\alpha^+(u) = \{x \in \mathbb{R}^n : \langle x, u\rangle \geq \alpha\}$ *e* $H_\alpha^-(u) = \{x \in \mathbb{R}^n : \langle x, u\rangle \leq \alpha\}$. *Esses são os semi-espaços limitados por* $H_\alpha(u)$.

Algumas propriedades de um conjunto convexo fechado $K$ podem ser estudadas usando a função que associa a cada ponto do $\mathbb{R}^n$ seu ponto mais próximo em $K$. Começaremos mostrando que esta função está bem definida.

**Lema 2.2.1.** *Seja $K$ um conjunto convexo fechado em $\mathbb{R}^n$. Então, para cada $x \in \mathbb{R}^n$ existe um único $x^{'} \in K$ tal que*

$$\|x - x^{'}\| = \inf_{y \in K} \|x - y\| \tag{2.2}$$

**Dem.:** A existência de $x^{'}$ satisfazendo 2.2 segue de $K$ ser fechado e do fato da função distância $\|\cdot\|$ ser contínua. Agora suponha que existe $x^{''} \in K$, $x^{''} \neq x^{'}$, tal que

$$\|x - x^{'}\| = \|x - x^{''}\| = \inf_{y \in K} \|x - y\|.$$

Considerando o triângulo isósceles com vértices $x$, $x^{'}$ e $x^{''}$, como ilustrado na figura 2.2, podemos notar que o ponto médio $m = \frac{1}{2}(x^{'} - x^{''})$ do segmento de reta que une $x^{'}$ e $x^{''}$ também pertence a $K$ por convexidade, mas $m$ satisfaz

$$\|x - m\| < \|x - x^{'}\| = \inf_{y \in K} \|x - y\|$$

uma contradição. □

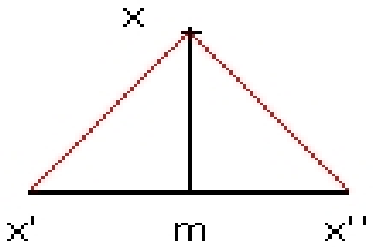


Figura 2.2: triângulo isósceles

O lema 2.2.1 nos leva à definição da seguinte função:

**Definição 2.2.2.** *A função*

$$\begin{aligned} p_K : \ \mathbb{R}^n &\longrightarrow K \\ x &\longrightarrow p_K(x) = x^{'}, \end{aligned}$$

*onde $x^{'}$ é o mesmo do lema 2.2.1, é dita função ponto mais próximo relativa a $K$.*

A definição a seguir generaliza o conceito de hiperplano tangente que está ilustrado na figura 2.3.

**Definição 2.2.3.** *Um hiperplano $H$ é dito um hiperplano de suporte de um conjunto convexo fechado $K \subseteq \mathbb{R}^n$ se $K \cap H \neq \emptyset$ e $K \subset H^-$ ou $K \subset H^+$.*

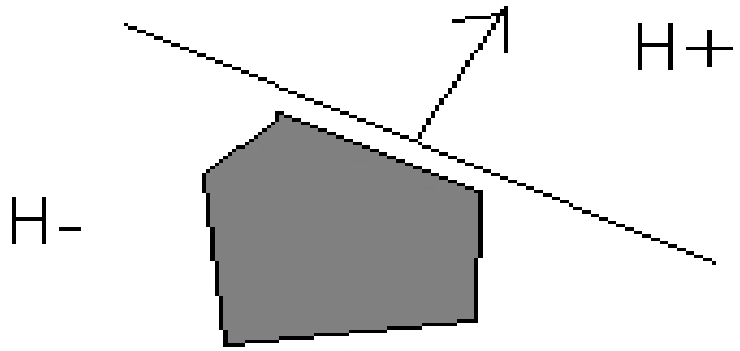


*Figura 2.3: hiperplano de suporte*

**Proposição 2.2.2.** *Seja $K \subseteq \mathbb{R}^n$ fechado, convexo e não vazio. Então, para todo $x \in \mathbb{R}^n \setminus K$, o hiperplano contendo $x^{'} = p_K(x)$ e perpendicular à linha unindo $x$ e $x^{'}$ é um hiperplano de suporte de $K$ e pode ser descrito por $H = \{y \in \mathbb{R}^n : \langle y, u\rangle = 1\}$, onde $u = \dfrac{x - x^{'}}{\langle x^{'}, x - x^{'}\rangle}$ sempre que $0 \notin H$.*

**Dem.:** Note que o hiperplano $H = \{y \in \mathbb{R}^n : \langle y, u\rangle = 1\}$ é perpendicular a $x - x^{'}$ e satisafaz $x^{'} \in H$, pois $H = \left\{y \in \mathbb{R}^n : \langle y, x - x^{'}\rangle = \langle x^{'}, x - x^{'}\rangle\right\}$. Além disso, $\langle x - x^{'}, x - x^{'}\rangle > 0$ implica $\langle x, x - x^{'}\rangle > \langle x^{'}, x - x^{'}\rangle$ então $x \in H^+$. Vamos supor que $H$ não é um hiperplano de suporte de $K$. Então existe algum $y \in K \cap (H^+ \setminus H)$. Vamos considerar o círculo de centro $x$ e raio $\left\|x - x^{'}\right\|$, como ilustrado na figura 2.4, assim $H$ é um hiperplano tangente ao círculo no ponto $x^{'}$. Deste modo o segmento de reta $\left[x^{'}, y\right]$ possui um ponto $z$ interior ao círculo sendo que $z \in K$ por convexidade. Então, $\|x - z\| < \|x - x^{'}\|$, uma contradição. □

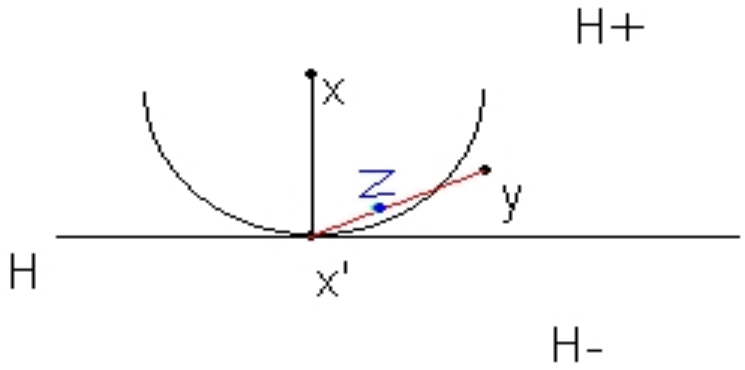


Figura 2.4: hiperplano tangente ao círculo

**Definição 2.2.4.** *Seja $K \subset \mathbb{R}^n$ um conjunto convexo não vazio. A função*

$$\begin{aligned} h_K : \ \mathbb{R}^n &\longrightarrow \mathbb{R} \text{ definida por} \\ u &\longmapsto h_K(u) = sup_{x \in K} \langle x, u \rangle \end{aligned}$$

*é a função suporte de $K$.*

A figura 2.5 ilustra a definição 2.2.4.

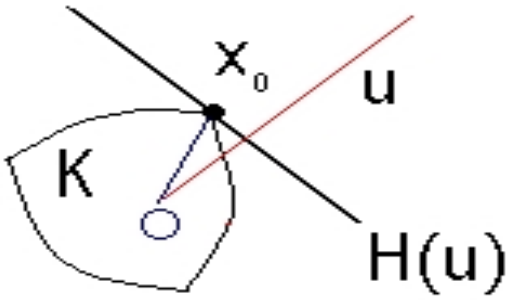


Figura 2.5: função suporte

A próxima afirmação é uma consequência da definição.

**Lema 2.2.2.** *Se $K + a$ é uma translação do conjunto convexo $K$, então,*

$$h_{K+a}(u) = h_k(u) + \langle a, u \rangle$$

*para todo $u \in \mathbb{R}^n$.*

**Proposição 2.2.3.**

1. *Para todo* $u \in \mathbb{R}^n \setminus \{0\}$*, o hiperplano*

$$H_K(u) = \{x \in \mathbb{R}^n : \langle x, u\rangle = h_K(u)\}, \tag{2.3}$$

*é um hiperplano de suporte de* $K$*.*

2. *Se* $H$ *é um hiperplano de suporte de* $K$*, ele tem uma representação na forma 2.3.*

**Dem.:**

1. Já que $K$ é fechado e $\langle \cdot, u\rangle$ é contínua, então existe $x_0 \in K$ tal que

$$\langle x_0, u\rangle = h_K(u) = sup_{x\in K}\langle x, u\rangle.$$

Agora dado $y \in K$, segue que $\langle y, u\rangle \leq \langle x_0, u\rangle$, então $K \subset H_K^-(u)$.

2. Seja $H = \{x \in \mathbb{R}^n : \langle x, u\rangle = \langle x_0, u\rangle\}$ um hiperplano de suporte de K em $x_0$. Escolhemos $u \neq 0$ tal que $K \subset H^-$. Então, $\langle x_0, u\rangle = sup_{x\in K}\langle x, u\rangle = h_K(u)$.

□

**Definição 2.2.5.** *Um cone convexo com um vértice* $v$ *é definido como um conjunto convexo* $S$ *em* $\mathbb{R}^n$ *tal que* $v$ *é um ponto extremo de* $S$ *e, para qualquer* $a \in S$*,* $v + \lambda(a - v) \in S$ *para todo número real* $\lambda \geq 0$*.*

**Lema 2.2.3.** *Seja* $C$ *um cone convexo com vértice* $v$ *e seja* $H$ *um hiperplano em* $\mathbb{R}^n$ *com* $v \notin H$*.Suponha que* $Q = C \cap H$ *é não vazio e limitado. Então, para* $r \in \mathbb{R}^n$*,* $C \cap (r + H)$ *é vazio ou existe um número real* $t \geq 0$ *tal que*

$$C \cap (r + H) = v + t(Q - v) = \{v + t(a - v) : a \in Q\}$$

**Dem.:** Sejam $\alpha \in \mathbb{R}^n$ e $\beta \in \mathbb{R}$ tais que

$$H = \{x \in \mathbb{R}^n : \langle \alpha, x\rangle = \beta\}$$

e podemos assumir sem perda de generalidade que $v \in H^+$ e assim, temos que

$$\langle \alpha, v \rangle > \beta.$$

Vamos mostrar que para todo ponto $a \in C$ com $a \neq v$, temos que

$$\langle \alpha, a \rangle < \langle \alpha, v \rangle. \tag{2.4}$$

Suponhamos o contrário, ou seja, que existe um ponto $a_0 \in C$ tal que $\langle \alpha, a_0 \rangle \geq \langle \alpha, v \rangle$. Seja $b \in Q = C \cap H$. Então

$$\langle \alpha, b \rangle = \beta < \langle \alpha, v \rangle \leq \langle \alpha, a_0 \rangle.$$

Seja $a_1 = \lambda_1 a_0 + (1 - \lambda_1)\, b$ onde $\lambda_1 = \dfrac{\langle \alpha, v \rangle - \beta}{\langle \alpha, a_0 \rangle - \beta} > 0$. Já que $\lambda_1 \leq 1$ e $C$ é convexo, então $a_1 \in C$ e

$$\langle \alpha, a_1 \rangle = \langle \alpha, v \rangle. \tag{2.5}$$

Dado $t \geq 0$, então

$$b + t\,(a_1 - v) = v + (t+1)\left(\left(\frac{b}{t+1} + \frac{t a_1}{t+1}\right) - v\right)$$

pertence a $C$, pois $a_1$,$b \in C$ e $C$ é cone convexo com vértice $v$. Por 2.5 temos que $\langle \alpha, b + t\,(a_1 - v) \rangle = \langle \alpha, b \rangle + t\langle \alpha, a_1 \rangle - t\langle \alpha, v \rangle = \langle \alpha, b \rangle = \beta$. Então $b + t\,(a_1 - v) \in H$ e assim $b + t\,(a_1 - v) \in H \cap C$ para todo $t \geq 0$, contradizendo o fato de $Q$ ser limitado. Portanto 2.4 é verdade.

Dado $r \in \mathbb{R}^n$ e $a \in C$ com $a \neq v$, considere a intersecção do raio

$$\{v + \lambda\,(a - v) : \lambda \geq 0\} \tag{2.6}$$

com o hiperplano

$$r + H = \{r + x \in \mathbb{R}^n : \langle \alpha, x \rangle = \beta\} = \{x \in \mathbb{R}^n : \langle \alpha, x \rangle = \langle \alpha, r \rangle + \beta\}. \tag{2.7}$$

Então se um ponto está nesta intersecção ele satisfaz (2.6) e (2.7). Assim $\langle \alpha, v + \lambda\,(a - v) \rangle = \langle \alpha, r \rangle + \beta$ que implica $\lambda = \dfrac{\langle \alpha, v \rangle - \beta - \langle \alpha, r \rangle}{\langle \alpha, v \rangle - \langle \alpha, a \rangle}$. Já que $\langle \alpha, v \rangle > \langle \alpha, a \rangle$, Então $\lambda \geq 0$ se e somente se $\langle \alpha, v \rangle - \beta \geq \langle \alpha, r \rangle$. Quando esta condição é satisfeita, $r + H$ intercepta todo raio (2.6) em um único ponto determinado pelo $\lambda$ acima. Para

$r = 0$ temos que $\langle \alpha, v \rangle - \beta \geq 0 = \langle \alpha, r \rangle$ e então cada raio 2.6 intercepta $H$, e então $Q$, em um único ponto. Logo, podemos indexar todos os raios (2.6) pelos $a \in Q$. Agora suponha que $\langle \alpha, r \rangle \leq \langle \alpha, v \rangle - \beta$. Então para cada $a \in Q$, o raio 2.6 intercepta $r + H$ no ponto $b = v + \lambda_0 (a - v)$ onde

$$\lambda_0 = \frac{\langle \alpha, v \rangle - \beta - \langle \alpha, r \rangle}{\langle \alpha, v \rangle - \beta}.$$

Seja $t = \lambda_0$, logo, o lema está provado. □

## 2.3 Soma de Minkowski

O objetivo desta seção será o estudo de uma operação fundamental para conjuntos convexos a qual pode ser definida para conjuntos arbitrários em $\mathbb{R}^n$ chamada soma de Minkowski. Nosso interesse é estudar algumas propriedades dessa soma, pois nos capítulos seguintes estaremos interessados na decomposição de politopos em função da soma de Minkowski.

**Definição 2.3.1.** *Sejam $K, L \subseteq \mathbb{R}^n$. A soma de Minkowski de $K$ e $L$ é o conjunto $K + L = \{k + l : k \in K, l \in L\}$.*

Uma observação importante a respeito desta soma e que será útil para o entendimento de alguns resultados diz respeito à soma de retas e pontos. Por exemplo, quando somamos um ponto e uma reta, teremos uma reta conforme ilustrado na figura 2.6a. Porém, note que, quando somamos duas retas, teremos uma reta se elas forem paralelas conforme ilustardo na figura 2.6b, caso contrário teremos uma figura retangular conforme ilustrado na figura 2.6c. No capítulo 4 veremos que está observação é a chave para o algoritmo de decomposição de politopos em $\mathbb{R}^2$, ou seja, polígonos.

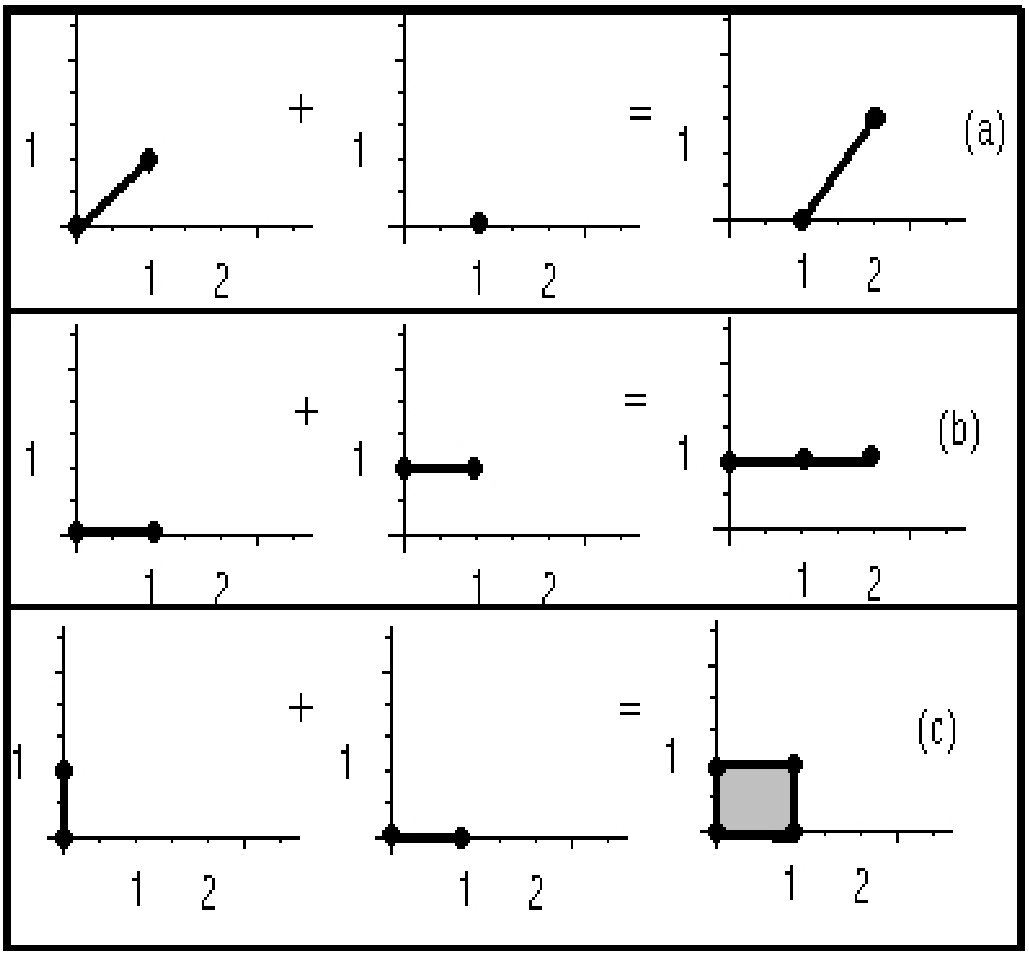


Figura 2.6: soma de retas

A soma de Minkowski de dois triângulos $K, L$ no plano pode ser um triângulo(figura 2.7a), um retângulo(figura 2.7b), um pentágono(figura 2.7c), ou um hexágono(figura 2.7d).

**Lema 2.3.1.**

1. *Se $\tau$ denota uma translação, então, para quaisquer conjuntos $K, L$ em $\mathbb{R}^n$,*

$$\tau(K) + L = \tau(K + L) = K + \tau(L).$$

2. *Se $K, L$ são ambos conjuntos convexos, fechados, limitados, então, $K + L$ é um conjunto convexo, fechado, limitado, respectivamente.*

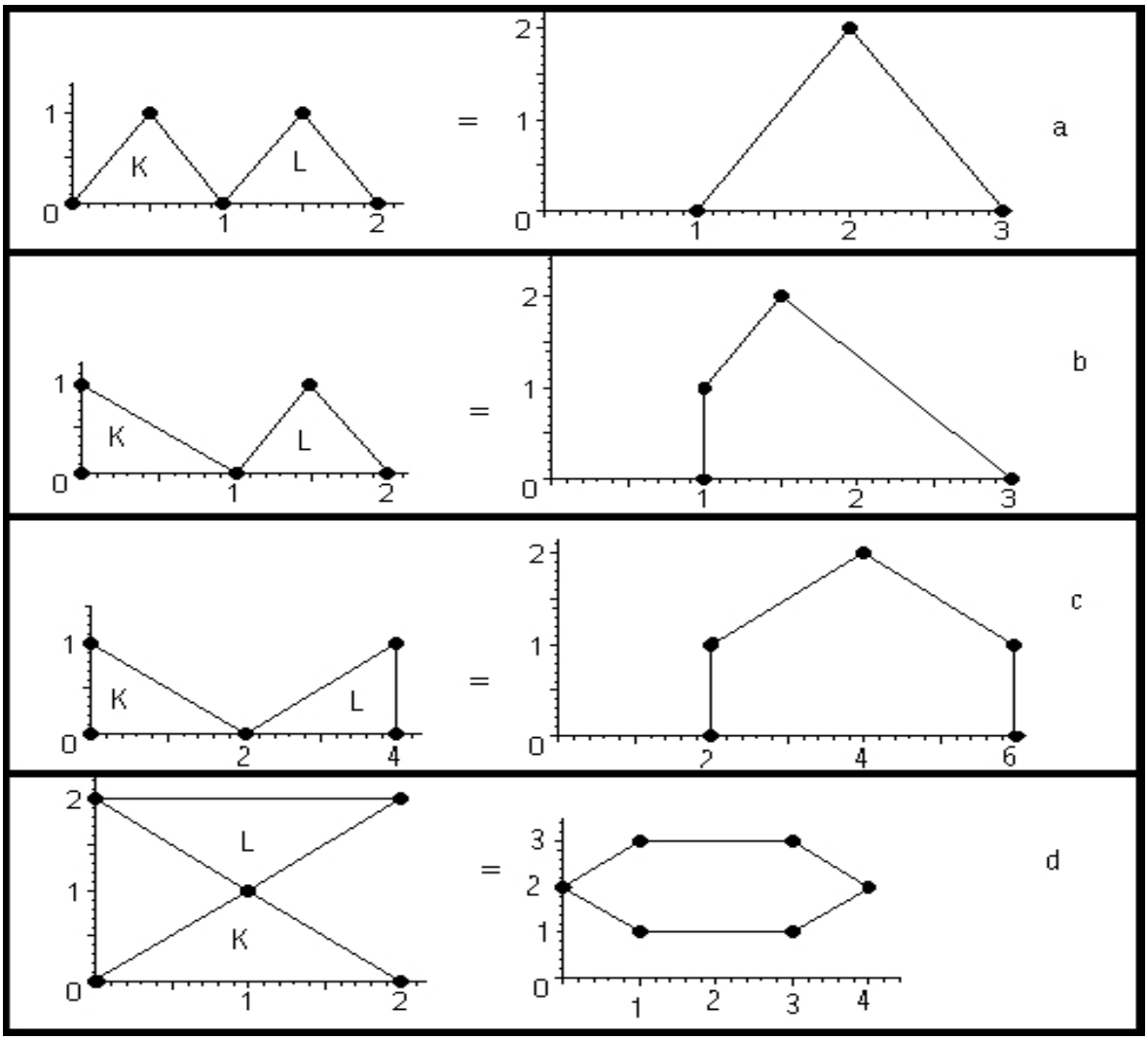


Figura 2.7: somando politopos

**Dem.:**

1. $\tau$ é dado por um vetor de translação $t$. Logo a afirmação segue de

$$(t + K) + L = t + (K + L) = K + (t + L)$$

2. Sejam $x, x^{'} \in K$ e $y, y^{'} \in L$. Então, para $0 \leq \lambda \leq 1$,

$$\lambda\,(x + y) + (1 - \lambda)\left(x^{'} + y^{'}\right) = \lambda x + (1 - \lambda)\,x^{'} + \lambda y + (1 - \lambda)\,y^{'} \in K + L,$$

se $K$ e $L$ são convexos. As propriedades fechado e limitado seguem de $K$ e $L$ para $K + L$ já que soma é uma operação contínua e leva pares de conjuntos limitados para um conjunto limitado.

□

A maioria das considerações sobre soma de Minkowski são invariantes sob translações, devido ao lema 2.3.1. Podemos visualizar a soma de $K + L$ fixando $L$ e movê-lo por translação por todos os pontos $p$ tal que $p$ esteja em $K$. Então a translação de $L$ cobre $K + L$, que é, $K + L = \bigcup_{p \in K} (p + L)$.

**Definição 2.3.2.** *Se $\lambda$ é um número real e $K \subset \mathbb{R}^n$ é um conjunto, então, dizemos que $\lambda K = \{\lambda x : x \in K\}$ é um múltiplo de $K$. Se $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$ e $K_1, \ldots, K_r$ são conjuntos em $\mathbb{R}^n$, dizemos que $\lambda_1 K_1 + \cdots + \lambda_r K_r$ é uma combinação linear de $K_1, \ldots, K_r$.*

Observamos que $\lambda$ pode ser negativo. Entretanto, $(-1)\, K = -K$ não é o negativo de $K$ com respeito a soma de Minkowski. Na figura 2.7d, $L = -K$, mas $K + L = K + (-K)$ é um hexágono.

Da definição de combinação linear e do lema anterior, temos o seguinte:

**Lema 2.3.2.** *Se $K_1, \ldots, K_r$ são convexos e $\lambda_1, \ldots, \lambda_r$ são números reais quaisquer, então, $\lambda_1 K_1 + \cdots + \lambda_r K_r$ é convexo.*

### 2.3.1 Subtração de Minkowski

Como já estudamos algumas propriedades de soma de Minkowski, agora podemos introduzir uma operação complementar chamada subtração de Minkowski. Enquanto a soma de Minkowski de dois conjuntos $A$, $B \subset \mathbb{R}^n$ pode ser definida por

$$A + B = \bigcup_{b \in B} (A + b),$$

a diferença de Minkowski de $A$ e $B$ pode ser definida da seguinte maneira

**Definição 2.3.3.** $A \sim B = \bigcap_{b \in B} (A - b)$

Se $B$ é vazio, $A \sim B$ é, por convenção, igual a $\mathbb{R}^n$. Também podemos escrever

$$A \sim B = \{x \in \mathbb{R}^n : B + x \subset A\},$$

ou seja, são todos os deslocamentos do conjunto $B$ que o levam a estar contido no conjunto $A$.

**Exemplo 2.3.1.** *Considere o retângulo* $A = conv((0,0),(2,0),(2,1),(0,1))$ *e o segmento de reta* $B = conv((0,0),(1,0))$ *como ilustrados na figura 2.8. Note que* $A \sim B = conv((0,0),(1,0),(1,1),(0,1))$*, ou seja, se somarmos* $B$ *a qualquer elemento* $x$ *do conjunto* $A \sim B$ *então* $x + B \subset A$.

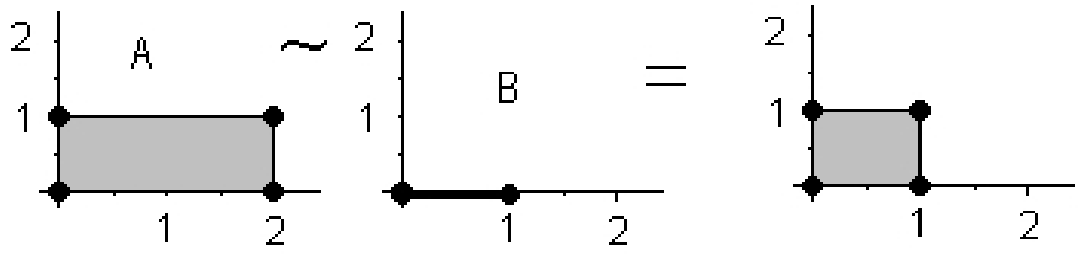


*Figura 2.8: subtração de Minkowski*

Existem algumas propriedades simples ligando soma e subtração de Minkowski

$$(A + B) \sim B \supset A \tag{2.8}$$

$$(A \sim B) + B \subset A, (B \neq \emptyset) \tag{2.9}$$

$$(A \sim B) + C \subset (A + C) \sim B \tag{2.10}$$

$$(A \sim B) \sim C = A \sim (B + C) \tag{2.11}$$

$$A + B \subset C \Leftrightarrow A \subset C \sim B \tag{2.12}$$

As verificações são imediatas das definições. Se trabalharmos com conjuntos convexos, um pouco mais é verdade. Como, por exemplo, se $A$ é convexo, então $A \sim B$ é uma intersecção de conjuntos convexos e então convexo.

**Definição 2.3.4.** *Para conjuntos convexos* $K$,$L \in \mathbb{R}^n$ *dizemos que* $L$ *é um fator de* $K$ *se existe um conjunto convexo* $M$ *tal que* $K = M + L$.

**Lema 2.3.3.** *Sejam $K$,$L \in \mathbb{R}^n$ conjuntos convexos. Então $(K + L) \sim L = K$. A relação $(K \sim L) + L = K$ é satisfeita se, e somente se, $L$ é um fator de $K$.*

**Dem.:** Seja $x \in (K+L) \sim L$, então $L+x \subset K+L$ e, além disso, $h_L+h_{\{x\}} \leq h_K+h_L$. Subtraindo $h_L$, obtemos $x \in K$. Então $(K+L) \sim L \subset K$, que junto com 2.8 prova a primeira afirmação. Se $(K \sim L)+L = K$, então $L$ é um fator de $K$. Reciprocamente, suponha que $K = M + L$ para algum $M \in \mathbb{R}^n$. Então $K \sim L = (M + L) \sim L = M$, que prova a segunda afirmação □

## 2.4 Politopos

Nesta seção estudaremos algumas propriedades de politopos, pois como será visto no capítulo 3, a cada polinômio associaremos uma figura geométrica que será um politopo. Assim, informações a respeito de politopos nos levarão a informações sobre polinômios.

**Definição 2.4.1.** *Se $S$ é um conjunto finito, então $conv(S)$ é denominado politopo de $S$.*

Se $S = ((0,0),(1,2),(2,2),(3,2),(2,4),(4,2))$. Então $conv(S)$ é um politopo, conforme ilustrado na figura 2.9.

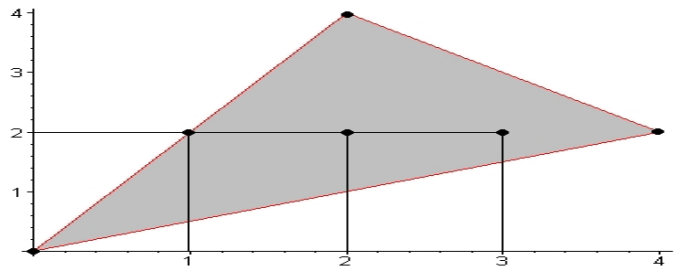


Figura 2.9: Politopo

**Definição 2.4.2.** *Um ponto de um politopo é dito um vértice(ou um ponto extremo) se ele não está no segmento de reta que liga quaisquer outros dois pontos do politopo.*

Note que o ponto $v = (4, 2)$ é um vértice do politopo $conv(S)$, como pode ser observado na figura 2.9.

Se $P = conv\{x_1, \ldots, x_k\}$, então claramente os pontos extremos de $P$ estão entre $x_1, \ldots, x_k$. Se $H$ é um hiperplano de suporte de $P$, então

$$H \cap P = conv(H \cap \{x_1, \ldots, x_k\}),$$

que nos leva a definir uma face de um politopo.

**Definição 2.4.3.** *Se $H$ é um hiperplano de suporte de um conjunto convexo fechado $P$, chamamos $F = P \cap H$ uma face de $P$.*

Então cada face de um politopo é também um politopo. Como já foi definido os pontos extremos de um politopo são ditos seus vértices. O conjunto de vértices de $P$ é também denotado por $vert(P)$. A definição a seguir ajuda a caracterizar o politopo.

**Definição 2.4.4.** *Dado um politopo $P$ em $\mathbb{R}^n$. Diremos que $F$:*

1. *é vértice de $P$, se $F$ é face de dimensão 0.*
2. *é aresta de $P$, se $F$ é face de dimensão 1.*
3. *é faceta $P$, se $F$ é face de dimensão $k - 1$.*

Os ítens 1 e 2 do teorema a seguir dizem respeito a qualquer conjunto convexo. Porém preferimos apresentá-los apenas agora e explicarmos sua importância para politopos.

**Teorema 2.4.1.** *Sejam $K$ e $L$ conjuntos convexos. Então,*

1. *Se $h_K, h_L$ são as funções suporte de $K$ e $L$, então $h_K + h_L$ é a função suporte de $K + L$,*

$$h_{K+L} = h_K + h_L.$$

2. *Se $F$ é uma face de $K+L$, então existem únicas faces $F_K, F_L$ de $K$ e $L$, respectivamente, tais que $F = F_K + F_L$.*
   *Em particular, para cada vértice $v$ de $K+L$ existem únicos vértices $v_1$ e $v_2$ de $K$ e $L$, respectivamente, tais que $v = v_1 + v_2$.*

3. *Se $K, L$ são politopos, então $K+L$ é um politopo.*

**Dem.:**

1. Seja $u \in \mathbb{R}^n \setminus \{0\}$, então $h_{K+L}(u) = sup_{x\in K+L}\langle x, u\rangle = sup_{y\in K, z\in L}\langle y + z, u\rangle = sup_{y\in K}\langle y, u\rangle + sup_{z\in L}\langle z, u\rangle = h_K(u) + h_L(u)$.

2. Como $F$ é uma face de $K+L$ então existe um hiperplano de suporte $H$ tal que $F = (K+L)\cap H$ e por 2.2.3 $H$ tem uma representação na forma $H_{K+L}(u) = \{x \in \mathbb{R}^n : \langle x, u\rangle = h_{k+l}(u)\}$ para um certo $u \in \mathbb{R}^n \setminus \{0\}$. Definamos $F_K = K \cap H_K(u)$ e $F_L = L \cap H_L(u)$, onde $H_K(u) = \{x \in \mathbb{R}^n : \langle x, u\rangle = h_k(u)\}$ e $H_L(u) = \{x \in \mathbb{R}^n : \langle x, u\rangle = h_l(u)\}$. Note que $H_{K+L} = H_K + H_L$, pois dados $x \in H_K$ e $y \in H_L$ temos que $\langle x+y, u\rangle = \langle x, u\rangle + \langle y, u\rangle = h_K + h_L = h_{K+L}$. Logo, $x + y \in H_{K+L}$ e como $H_K, H_L$ e $H_{K+L}$ são hiperplanos paralelos, temos a igualdade. Segue que

$$F = (K+L)\cap H_{K+L}(u) = (K+L)\cap (H_K(u) + H_L(u))$$

$$= (K\cap H_K(u)) + (L\cap H_L(u)) = F_K + F_L.$$

   Onde a igualdade acima é satisfeita pois dado $z \in (K+L)\cap H_{K+L}$ temos que $z = x + y = x_1 + y_1$ com $x \in K$, $y \in L$, $x_1 \in H_K$ e $y_1 \in H_L$. Queremos mostrar que $x \in H_k$ e $y \in H_L$. Como $x \in K \subset H_K^-$ então $\langle x, u\rangle \leq h_K = \langle x_1, u\rangle$ e do mesmo modo $\langle y, u\rangle \leq h_L = \langle y_1, u\rangle$. Temos que $\langle z, u\rangle = h_{K+L}$, ou seja, $\langle x, u\rangle + \langle y, u\rangle = \langle x_1, u\rangle + \langle y_1, u\rangle$. Então $\langle x, u\rangle = h_K$ e $\langle y, u\rangle = h_L$ e a igualdade é satisfeita.

3. é uma consequência do ítem 2 , já que a soma de dois vértices é um vértice e cada vértice de $K+L$ é obtido deste modo.

A prova da unicidade dos primeiros dois ítens será feita no capítulo seguinte. □

O ítem 2 do teorema acima é muito importante pois nos diz que um fator de uma face possui o mesmo vetor normal que a face. Isto fica evidente no corolário a seguir quando tratamos especificamente de polígonos.

O corolário a seguir nos leva a enxergar como decompor as arestas de um polígono.

**Corolário 2.4.1.** *Sejam $P, Q$ e $R$ polígonos convexos em $\mathbb{R}^n$ com $P = Q+R$. Então toda aresta de $P$ decompõe-se unicamente como a soma de uma aresta de $Q$ e uma aresta de $R$, possivelmente uma delas sendo um ponto.*

Como já foi observado na seção 2.3 toda aresta de $P$ decompõe-se como a soma de duas arestas paralelas a ela ou como a soma de uma aresta e um ponto. A importância deste resultado ficará evidente no capítulo 4 da presente dissertação, quando estivermos buscando fatores de um polígono.

**Teorema 2.4.2.** *Todo politopo possui um número finito de faces, que também são politopos.*

**Dem.:** Seja o politopo $P = conv\,(x_1, \ldots, x_n)$, e $F = P \cap H$ uma face de $P$ onde $H = \{x \in \mathbb{R}^n : \langle x, a\rangle = \alpha\}$ é um hiperplano de suporte de $P$ tal que $P \subset H^-$. Podemos assumir que $x_1, \ldots, x_s \in H$ e $x_{s+1}, \ldots, x_n \in H^- \setminus H$ e assim:

$$\langle x_i, a\rangle = \alpha \quad \text{para} \quad i = 1, \ldots, s$$

$$\langle x_i, a\rangle = \alpha - \beta_i, \beta_i > 0 \quad \text{para} \quad i = s+1, \ldots, n.$$

Seja $x \in P$, logo, $x = \sum_{i=1}^{n} \lambda_i x_i, \sum_{i=1}^{n} \lambda_i = 1,\ \lambda_i \geq 0, i = 1, \ldots, n.$ Assim $\langle x, a\rangle = \langle \sum_{i=1}^{n} \lambda_i x_i, a\rangle = \sum_{i=1}^{n} \lambda_i \langle x_i, a\rangle = \sum_{i=1}^{s} \lambda_i \alpha + \sum_{i=s+1}^{n} \lambda_i\,(\alpha - \beta_i) = \alpha \sum_{i=1}^{n} \lambda_i - \sum_{i=s+1}^{n} \lambda_i \beta_i = \alpha - \sum_{i=s+1}^{n} \lambda_i \beta_i$. Portanto

$$x \in H \Leftrightarrow \sum_{i=s+1}^{n} \lambda_i \beta_i = 0 \Leftrightarrow \sum_{s+1}^{n} \lambda_i = 0$$

assim $x$ é uma combinação convexa de $x_1, \ldots, x_s$ então $H \cap P = conv\,(x_1, \ldots, x_s)$. $\square$

O teorema a seguir mostra que para politopos a distinção entre faces é desnecessária.

**Teorema 2.4.3.** *Seja $P \subset \mathbb{R}^n$ um politopo, $F_1$ uma face de $P$ e $F$ uma face de $F_1$. Então $F$ é uma face de $P$.*

**Dem.:** Podemos assumir que $0 \in F$. Então existe um hiperplano de suporte $H_{u,0}$ para $P$ tal que $H_{u,0} \cap P = F_1$ e $P \subset H^-_{u,0}$. Em $H_{u,0}$ existe um hiperplano de suporte $H$ para $F_1$ tal que $H \cap F_1 = F$, diremos

$$H = \{x \in H_{u,0} : \langle x, v\rangle = 0\},$$

$$F_1 \subset \{x \in H_{u,0} : \langle x, v\rangle \leq 0\}.$$

Definimos

$$\eta_0 := max\,\{-\langle x, v\rangle / \langle x, u\rangle : x \in ext(P) \setminus ext(F_1)\} \text{ e}$$

$H(\eta) := H_{\eta u+v,0}$ com $\eta > \eta_0$. Temos que $\langle x, u\rangle < 0$ para $x \in ext(P) \setminus ext(F_1)$, então

$$\langle x, \eta u + v\rangle < \eta_0 \langle x, u\rangle + \langle x, v\rangle \leq 0$$

pela definição de $\eta_0$. Para $x \in ext(F_1) \setminus ext(F)$ obtemos

$$\langle x, \eta + v\rangle = \langle x, v\rangle < 0,$$

e para $x \in ext(F)$, $\langle x, \eta u + v\rangle = 0$. Então $ext(F) \subset H(\eta)$, enquanto $ext(P) \setminus ext(F) \subset intH^-_{\eta u+v,0}$. Vemos que $H(\eta)$ é um hiperplano de suporte para $P$ com $H(\eta) \cap P = F$ e além disso $F$ é uma face de $P$. $\square$

Um politopo foi definido como a envoltória convexa de um conjunto finito de pontos. Alternativamente podemos representá-lo como a intersecção de um número finito de semi espaços. Antes vamos denotar, para um politopo $P$, $int(P)$ como seu interior e $bd(P)$ como sua fronteira.

**Teorema 2.4.4.** *Todo politopo é a intersecção de um conjunto finito de semi espaços limitados por hiperplanos.*

**Dem.:** Seja $P \subset \mathbb{R}^n$ um politopo. Podemos assumir que $dim(P) = n$. Sejam $F_1, \ldots, F_k$ as facetas de $P(dim(F_i) = n-1)$. Então $F_i = H_i \cap P$ onde $H_i$ é um hiperplano de suporte único de $P$. Seja $H_i^-$ o semi espaço limitado por $H_i$ e contendo P para $i = 1, \ldots, k$. Afirmamos que

$$P = H_1^- \cap \ldots \cap H_k^- . \tag{2.13}$$

A inclusão $P \subset H_1^- \cap \ldots \cap H_k^-$ é trivial. Seja $x \in \mathbb{R}^n \setminus P$. Seja $A$ a união de envoltórias convexas de $x$ e quaisquer $n-1$ vértices de $P$. Podemos escolher um ponto $y \in (int(P)) \setminus A$. Existe um ponto $z \in bd(P) \cap [x, y]$, o qual pertence a algum hiperplano de suporte de $P$ e assim a alguma face $F$ de $P$. Vamos supor por absurdo que $dim(F) = j \leq n-2$ . Pelo teorema 2.1.1, $z$ pertence à envoltória convexa de $j+1 \leq n-1$ vértices de $P$ e assim a $A$. Mas então $y \in A$, uma contradição. Isto mostra que $F$ é uma faceta, e assim $F = F_i$ para algum $i \in \{1, \ldots, k\}$. De $y \in int(P) \subset int(H_i^-)$ deduzimos que $x \notin H_i^-$. Isto prova 2.13. □

**Teorema 2.4.5 (Krein-Milman).** *Todo politopo $P$ é a envoltória convexa de seus vértices, isto é,*

$$P = conv\,(vert(P)) .$$

**Dem.:** Como $vert(P) \subset P$ então $conv\,(vert(P)) \subset conv(P) = P$. Para a outra inclusão podemos assumir que $P = conv\,(x_1, \ldots, x_n)$ e considerar os elementos $x_i$ tais que $x_i \notin P_i = conv\,(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ para $1 \leq i \leq n$ (a idéia é mostrar que cada um desses $x_i$'s é um vértice de $P$). Seja $q_i = p_{p_i}(x_i)$ a imagem de $x_i$ sob a função ponto mais próximo. Por 2.2.2 o hiperplano passando por $q_i$ e perpendicular a $x_i - q_i$ é um hiperplano de suporte $H_i$ para $P_i$. Mostraremos que $H_i' = H_i + \{x_i - q_i\}$ é um hiperplano de suporte para $P$ tal que $H_i' \cap P = \{x_i\}$, isto é, uma face de dimensão zero, portanto, um vértice de $P$.(Observe a figura 2.10)

1. Primeiramente vamos mostrar que $H_i'$ é um hiperplano de suporte para $P$ em $x_i$. Temos que $x_i \in H_i'$, pois $x_i = q_i + x_i - q_i$ e $q_i \in H_i$. $H_i'$ e $H_i$ possuem o mesmo vetor normal $x_i - q_i$ que denotaremos por $u$. Deste modo podemos definir $H_i = \{x \in \mathbb{R}^n : \langle x, u\rangle = \langle q_i, u\rangle\}$ e

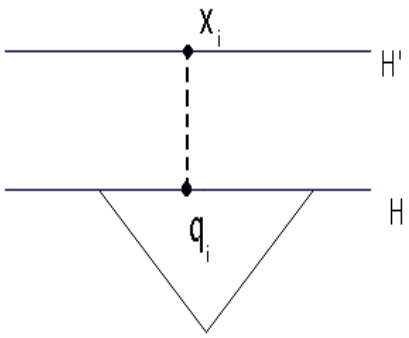


Figura 2.10: hiperplano deslocado

$H_i^{'} = \{x \in \mathbb{R}^n : \langle x, u\rangle = \langle x_i, u\rangle\}$. Vamos mostrar que $P \subset (H_i^{'})^{-}$. Para isso podemos supor que $P_i \subset H_i^{'}$, ou seja, dado $z \in P_i$ segue que $\langle z, u\rangle \leq \langle q_i, u\rangle$. Seja $x \in P$, então $x = \lambda x_i + (1-\lambda)z$ pois $P = conv(\{x_i\} \cup P_i)$. Precisamos mostrar que $\langle x, u\rangle \leq \langle x_i, u\rangle$. Temos que

$$\begin{aligned} \langle x, u\rangle &= \lambda\langle x_i, u\rangle + (1-\lambda)\langle z, u\rangle \\ &\leq \lambda\langle x_i, u\rangle + (1-\lambda)\langle q_i, u\rangle \\ &= \langle x_i, u\rangle - (1-\lambda)\langle x_i - q_i, u\rangle \end{aligned}$$

e como $x_i \in H_i^{+}$ segue que $\langle x_i, u\rangle \geq \langle q_i, u\rangle$ e assim $\langle x_i - q_i, u\rangle \geq 0$. Isto nos leva a $\langle x, u\rangle \geq \langle x_i, u\rangle$,isto é, $P \subset (H_i^{'})^{-}$.

2. Agora vamos mostrar que $H_i^{'} \cap P = \{x_i\}$. Suponha, por absurdo, que exista $y \in H_i^{'} \cap P$ tal que $y \neq x_i$, mas $H_i^{'} \cap P$ é uma face de $P$ então teríamos $x_j \neq x_i$ tal que $x_j \in H_i^{'} \cap P$ pois todas as faces de $P$ são geradas por subconjuntos de $\{x_1, \ldots, x_n\}$, onde $x_j \in P_i$. Temos que $\langle x_j, u\rangle \leq \langle q_i, u\rangle$ pois $P_i \subset H_i^{-}$ e assim $\langle x_j, u\rangle < \langle q_i, u\rangle + \langle x_i - q_i\rangle$ que nos leva a $\langle x_j, u\rangle < \langle x_i, u\rangle = \langle x_j, u\rangle$,absurdo. Portanto $H_i^{'} \cap P = \{x_i\}$

Concluimos que $x_i$ é um vértice de $P$. Isto implica que $P \subseteq conv(vert(P))$ □

Note que, como consequência do teorema de Krein-Milman, quando estivermos interessados na soma de Minkowski de politopos, podemos apenas somar os vértices dos politopos, ou seja,

$$K + L = conv\left(vert\left(K\right) + vert\left(L\right)\right).$$

Como está ilustrado na figura 2.7. Com o teorema 2.4.5 em mãos também podemos observar que se $x_1, \ldots, x_k$ são os vértices do politopo $P$ e $F$ é uma face de P, então existe um hiperplano $H$ tal que

$$F = H \cap P = conv(H \cap \{x_1, \ldots, x_k\}).$$

Portanto, cada face de $P$ é a envoltória convexa de um subconjunto dos vértices de $P$.

Agora que estudamos algumas propriedades de politopos, vamos associar os polinômios às suas respectivas figuras geométricas. Nos capítulos seguintes da dissertação estudaremos propriedades geométricas dos politopos que levarão a propriedades algébricas como fatoração e irredutibilidade dos seus polinômios associados.

# 3 FAMÍLIAS IRREDUTÍVEIS

Neste capítulo associaremos a cada polinômio multivariado um politopo, dito seu politopo de Newton. Apresentaremos o critério de Gao que diz que um polinômio é absolutamente irredutível se seu politopo de Newton associado é integralmente indecomponível. Veremos alguns critérios para indecomponibilidade de politopos que levam a critérios para irredutibilidade de polinômios. Observaremos que os polinômios que satisfazem esses critérios poderão ter seus coeficientes alterados ou serem acrescentados novos termos a eles e ainda assim permanecerão absolutamente irredutíveis.

## 3.1 Introdução

Neste capítulo associaremos a cada polinômio $f \in \mathbb{F}[x_1, \ldots, x_n]$ um politopo chamado politopo de Newton da $f$. Apresentaremos o critério de irredutibilidade de Gao que diz que um polinômio é absolutamente irredutível se seu politopo de Newton associado é integralmente indecomponível em relação à soma de Minkowski.

Na seção 3.3 apresentaremos as construções feitas por Gao em [4] de politopos integralmente indecomponíveis e, como veremos, um único politopo poderá representar inúmeros polinômios pois poderemos mudar os coeficientes dos termos de $f$ ou acrescentar novos termos desde que o politopo de Newton associado não seja alterado. Isto levará a famílias de polinômios absolutamente irredutíveis.

Na seção 3.4 apresentaremos construções de politopos integralmente indecomponíveis baseadas em projeções. Por exemplo, se tivermos um quadrado e fizermos a projeção sobre um de seus lados e esta for indecomponível, então espera-se que o quadrado também o seja.

## 3.2 Critério de Irredutibilidade

Polinômios multivariados necessitam de algumas definições específicas como por exemplo a respeito de seu grau, enquanto a definição de irredutibilidade usada para polinômios univariados é a mesma para multivariados.

**Definição 3.2.1.** *Consideremos um polinômio* $f(x_1, \ldots, x_n) = \sum f_{i_1 i_2 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n} \in \mathbb{F}[X_1, \ldots, X_n]$ *com* $(i_1, \ldots, i_n) \in \mathbb{N}^n$, *onde* $\mathbb{F}$ *é um corpo qualquer.*

1. *Para um termo* $t = X_1^{i_1} \ldots X_n^{i_n}$ *de* $f$, *chamado monômio, o número* $grau(t) = i_1 + \cdots + i_n$ *é dito o grau de* $t$.

2. *Para cada termo de* $f$ *com* $f_{i_1 i_2 \ldots i_n} \neq 0$, *o correspondente expoente vetorial* $(i_1, \ldots, i_n)$, *visto em* $\mathbb{R}^n$, *é dito um vetor suporte de* $f$.

3. $Supp(f)$ *será o conjunto de todos os vetores suporte de* $f$, *isto é,*

$$Supp(f) = \{(i_1, \ldots, i_n) : f_{i_1 i_2 \ldots i_n} \neq 0\}.$$

   *Note que* $Supp(f)$ *é vazio se* $f = 0$.

4. *Se* $f \neq 0$, *diremos que o grau da f é o maior grau entre os seus termos, isto é*

$$grau(f) = max\{grau(t) : t \text{ é um termo de } f\}.$$

   *Também podemos dizer que o* $grau(f)$ *é o grau total da* $f$.

O exemplo a seguir ilustra a definição dada.

**Exemplo 3.2.1.** *Seja* $f(x_1, x_2, x_3) := x_1^{11} x_2^7 x_3 - \frac{8}{13} x_1^9 x_2^3 x_3^3 - x_1^5 x_2^5 x_3 - 7 x_1^3 x_2^5 x_3 - \frac{3}{7} x_1 x_2^5 x_3 + x_1^4 x_2 + 5 x_2^2 x_3^3 \in \mathbb{Q}[x_1, x_2, x_3]$ *então a sequência de seus graus é* 19, 15, 11, 9, 7, 5, 5 *e assim* $grau(f) = 19$ *que é o grau máximo entre os seus termos. De acordo com a definição* $Supp(f) = \{(11, 7, 1), (9, 3, 3), (5, 5, 1), (3, 5, 1), (1, 5, 1), (4, 1, 0), (0, 2, 3)\}$.

**Definição 3.2.2.** *Um polinômio* $f \in \mathbb{F}[x_1, \ldots, x_n]$, $\mathbb{F}$ *corpo, é dito redutível se este é um produto de dois polinômios* $f = g \cdot h$, $g$,$h \in \mathbb{F}[x_1, \ldots, x_n]$ *com* $f$ *e* $g$ *não constantes. Caso contrário ele é dito irredutível.*

**Exemplo 3.2.2.**

1. *Todos polinômios univariados de grau* 0 *ou* 1 *são irredutíveis. Já que eles certamente não podem ser expressos como um produto de polinômios de grau menor.*

2. *O polinômio* $x^2 - 2$ *é irredutível sobre* $\mathbb{Q}[x]$*. Para mostrarmos isto supomos uma contradição. Vamos supor que ele é redutível. Então*

$$x^2 - 2 = (ax + b)(cx + d)$$

*onde a,b,c,d* $\in \mathbb{Q}$*. Dividindo se necessário podemos assumir que* $a = c = 1$*. Então* $b + d = 0$ *e* $bd = -2$*, logo* $b^2 = 2$*. Mas nenhum número racional tem seu quadrado igual a* 2*. Portanto* $x^2 - 2$ *é irredutível sobre o corpo dos números racionais.*

3. *Entretanto,* $x^2 - 2$ *é redutível sobre os racionais adjunção com* $\sqrt{2}$*,* $\mathbb{Q}(\sqrt{2})$*, pois*

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

4. *O mesmo vale para polinômios multivariados.O polinômio multivariado* $x_1^2 - 2x_2^2$ *é irredutível sobre o corpo dos números racionais, mas ele torna-se redutível sobre* $\mathbb{Q}(\sqrt{2})$*, pois*

$$x_1^2 - 2x_2^2 = (x_1 - \sqrt{2}x_2)(x_1 + \sqrt{2}x_2).$$

Isto mostra que um polinômio $f \in \mathbb{F}$ irredutível pode tornar-se redutível sobre uma extensão algébrica de $\mathbb{F}$.

**Definição 3.2.3.** *Um polinômio multivariado sobre um corpo* $\mathbb{F}$ *é dito absolutamente irredutível se ele permanece irredutível sobre toda extensão algébrica de* $\mathbb{F}$*.*

Agora podemos definir a figura geométrica associada a um polinômio $f$, a qual veremos será um politopo.

**Definição 3.2.4.** *O politopo de Newton associado ao polinômio* $f(x_1, \ldots, x_n)$ *é a envoltória convexa do conjunto* $Supp(f) = \{(i_1, \ldots, i_n) \in \mathbb{N}^n : f_{i_1,\ldots,i_n} \neq 0\}$*, que denotaremos por* $P_f$*.*

**Exemplo 3.2.3.** *Seja* $f = \underbrace{x^4y^2}_{(4,2)} + 3\underbrace{x^2y^4}_{(2,4)} + \underbrace{x^2y^2}_{(2,2)} + \underbrace{10}_{(0,0)} \in \mathbb{R}[x, y]$*. Então*

$$Supp(f) = \{(4, 2), (2, 4), (2, 2), (0, 0)\}$$

*e assim*

$$P_f = conv(Supp(f)) = conv\{(4, 2), (2, 4), (2, 2), (0, 0)\}.$$

*Como ilustrado na figura 3.1*

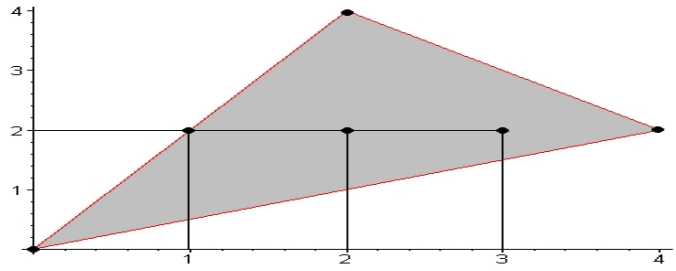


*Figura 3.1: Politopo de Newton associado ao polinômio bivariado f*

Note que o polinômio

$$5\underbrace{x^4y^2}_{(4,2)} + 7\underbrace{x^2y^4}_{(2,4)} + 20\underbrace{x^2y^2}_{(2,2)} + \underbrace{17}_{(0,0)}$$

possui o mesmo politopo de Newton associado que o polinômio $f$ do exemplo 3.2.3, ou seja, podemos mudar arbitrariamente os coeficientes dos termos de $f$ desde que os coeficientes dos termos cujos expoentes vetoriais, que correspondem aos vértices do politopo, permaneçam não nulos e deste modo o politopo permanece o mesmo.

Observe também que o polinômio

$$f = 5\underbrace{x^4y^2}_{(4,2)} + 3\underbrace{x^2y^4}_{(2,4)} + 7\underbrace{x^2y^3}_{(2,3)} + 20\underbrace{x^2y^2}_{(2,2)} + \underbrace{xy^2}_{(1,2)} + \underbrace{17}_{(0,0)}$$

possui o mesmo politopo de Newton associado que o polinômio do exemplo 3.2.3, ou seja, podemos acrescentar monômios a $f$ desde que os expoentes vetoriais que correspondem a estes termos estejam no interior do politopo.

O lema seguinte é devido a Ostrowski [16] e data de 1921.

**Lema 3.2.1.** *Sejam $f, g, h \in \mathbb{F}[x_1, \ldots, x_n]$ tais que $f = gh$. Então $P_f = P_g + P_h$.*

**Dem.:** Começamos mostrando que $P_f \subseteq P_g + P_h$. Para tal observe que $Supp(f) \subseteq Supp(g) + Supp(h)$ e assim $P_f = conv(Supp(f)) \subseteq conv(Supp(g) + Supp(h)) \subseteq conv(Supp(g)) + conv(Supp(h)) = P_g + P_h$.

Para mostrar que $P_g + P_h \subseteq P_f$ precisamos observar que de acordo com o teorema 2.4.1 $P_g + P_h$ é um politopo e pelo teorema de Krein-Milman cada politopo é a envoltória convexa dos seus vértices. Então para provarmos a inclusão precisamos mostrar que para cada vértice $v$ de $P_g + P_h$ existem únicos vértices $v_1$ e $v_2$ de $P_g$ e $P_h$, respectivamente, tais que $v = v_1 + v_2$ e assim poderemos concluir que existe um único termo na expansão de $g \cdot h$ que tem $v$ como seu expoente vetorial(ou seja, não tem como este termo se anular na expansão $g \cdot h$). Logo $v \in P_f$. De acordo com o teorema 2.4.1, cada vértice $v$ de $P_g + P_h$ vem da soma de um vértice $v_1$ de $P_g$ e um vértive $v_2$ de $P_h$. Suponha que exista um outro par tal que $v_1^{'} \in P_g$ e $v_2^{'} \in P_h$

$$v = v_1 + v_2 = v_1^{'} + v_2^{'}. \tag{3.1}$$

Então

$$v = \frac{1}{2}(v_1 + v_2^{'}) + \frac{1}{2}(v_1^{'} + v_2).$$

Observe que $v_1 + v_2^{'}$,$v_1^{'} + v_2 \in P_g + P_h$ e como $v$ é um vértice de $P_g + P_h$, temos que $v$ não pode estar no segmento de reta que une quaisquer outros pontos do politopo. Isso nos leva a

$$v_1 + v_2^{'} = v_1^{'} + v_2. \tag{3.2}$$

Subtraindo 3.2 de 3.1 temos que

$$v_2 - v_2^{'} = v_2^{'} - v_2, \text{ isto é, } 2(v_2 - v_2^{'}) = 0.$$

Segue que $v_2 = v_2'$ e $v_1 = v_1'$.

Mostramos que todos os vértices de $P_g + P_h$ estão em $P_f$. Como dito antes, isto mostra que $P_g + P_h \subseteq P_f$ pelo 2.4.5. □

Acabamos de mostrar que para cada vértice $v$ de $P_g + P_h$ existem únicos vértices $v_1$ e $v_2$ de $P_g$ e $P_h$, respectivamente, tais que $v = v_1 + v_2$. Sabemos que cada face $F$ do politopo $P_f$ vem da soma de uma face $F_1$ de $P_g$ e uma face $F_2$ de $P_h$ e como toda face de $P_f$ é a envoltória convexa de um subconjunto dos vértices de $P_f$ podemos garantir a unicidade das faces $F_1$ e $F_2$. Assim a prova do teorema 2.4.1 está completa.

**Exemplo 3.2.4.** *Seja* $f = \overbrace{(1+x+xy)}^{g}\overbrace{\left(xy+x^2y^2\right)}^{h} \in \mathbb{R}[x,y]$. *Então* $P_g = conv\{(0,0),(1,0),(1,1)\}$ *e* $P_h = \{(1,1),(2,2)\}$, *logo*

$$P_f = P_g + P_h = conv\{(1,3),(2,2),(1,2),(0,2),(3,1),(2,1),(1,1),(2,0)\}.$$

*Conforme ilustrado na figura 3.2.*

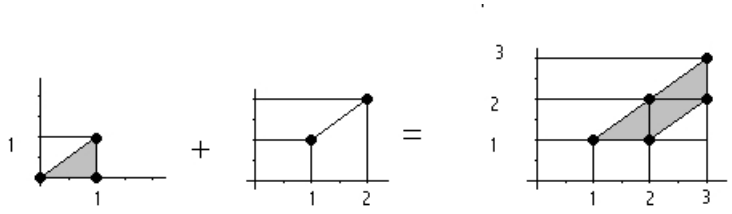


*Figura 3.2: lema de Ostrowski*

**Definição 3.2.5.** *Um ponto em* $\mathbb{R}^n$ *é dito integral se suas coordenadas são inteiras.*

**Definição 3.2.6.** *Um politopo em* $\mathbb{R}^n$ *é dito integral se todos seus vértices são integrais.*

**Definição 3.2.7.** *Um politopo integral* $C$ *é dito integralmente decomponível se existirem politopos integrais* $A$ *e* $B$ *tais que* $C = A + B$ *onde ambos* $A$ *e* $B$ *possuem no mínimo dois pontos cada. Caso contrário,* $C$ *é dito integralmente indecomponível.*

Note que o conceito de indecomponibilidade usado aqui é diferente do que é usado nos livros [11, 20].

Motivado pelo lema 3.2.1, Gao em [4] fez a seguinte observação.

**Corolário 3.2.1 (Critério de Irredutibilidade).** *Seja* $\mathbb{F}$ *um corpo e* $f \in \mathbb{F}[X_1, \ldots, X_n]$ *um polinômio não nulo, não divisível por nenhum* $X_i$*. Se o politopo de Newton de* $f$ *é integralmente indecomponível então* $f$ *é absolutamente irredutível sobre* $\mathbb{F}$*.*

**Dem.:** $f$ não possui fatores com apenas um termo. Suponha $f = gh$ onde $g, h$ possuem dois termos não nulos no mínimo. Então os politopos de Newton de $g$ e $h$ possuem dois pontos ou mais cada e pelo lema 3.2.1 $P_f = P_g + P_h$, contradizendo nossa hipótese de $P_f$ ser indecomponível. □

É importante notar que quando o $Newt(f)$ é integralmente decomponível, então $f$ pode ser redutível ou irredutível. Por exemplo, se $f = 1 + y + xy + x^2 + y^2$, então o $Newt(f)$ é decomposto como a soma do triângulo de vértices $(0,0)$, $(1,0)$ e $(0,1)$ com ele mesmo. Porém $f$ é absolutamente irredutível sob qualquer corpo de característica diferente de 2. Sob um corpo de característica 2 temos que

$$f = (1 + x + wy)\left(1 + x + w^2 y\right),$$

onde $w$ é um elemento de ordem 3.

Se o politopo de Newton da $f$ é indecomponível então $f$ é absolutamente irredutível e permanecerá absolutamente irredutível se mudarmos os coeficientes dos seus termos ou acrescentarmos termos cujos expoentes vetoriais correspondam a pontos que pertençam ao politopo de Newton mas sempre mantendo os coeficientes dos termos que correspondem aos vértices do politopo não nulo. Podemos notar que esta observação nos dá uma grande liberdade na escolha de polinômios para aplicações.

Como já foi comentado, um único politopo pode representar inúmeros polinômios e de acordo com o critério 3.2.1, se este dado politopo for integralmente

indecomponível então todos os polinômios que são representados por este politopo serão absolutamente irredutíveis, ou seja, podemos observar que cada vez que tivermos um politopo integralmente indecomponível teremos uma família de polinômios absolutamente irredutíveis, polinômios estes que são representados por tal politopo.

## 3.3 Construção de Politopos Integralmente Indecomponíveis

Contruiremos agora politopos indecomponíveis em $\mathbb{R}^n$. Como observado na seção anterior, cada tipo de politopo indecomponível dará uma família de polinômios absolutamente irredutíveis. Quando um politopo tem somente um ponto diremos que este é trivial. Examinaremos vários tipos de politopos não triviais simples como segmentos de reta, triângulos, tetraedros, pirâmides e outros. Também mostraremos como construir politopos indecomponíveis a partir de um politopo dado.

Um segmento de reta, $conv\,(v_1, v_2)$, será simplesmente denotado por $v_1v_2$. Para um ponto integral ou vetor $v = (a_1, \ldots, a_n)$ escreveremos $mdc\,(v)$ para significar $mdc\,(a_1, \ldots, a_n)$, isto é, o máximo divisor comum das componentes em v. Similarmente, para vários pontos $v_1, \ldots, v_k$, $mdc\,(v_1, \ldots, v_k)$ significa o $mdc$ de todas componentes em $v_1, \ldots, v_k$ juntas.

**Exemplo 3.3.1.** *Seja* $v_1 = (n, 0)$, $v_2 = (0, m)$ *e* $v_3 = (u, u)$, *então* $mdc\,(v_1, v_2, v_3) = mdc\,(n, 0, 0, m, u, u) = mdc\,(n, m, u)$.

**Lema 3.3.1.** *Sejam* $v_0$ *e* $v_1$ *dois pontos integrais distintos em* $\mathbb{R}^n$. *Então o número de pontos integrais no segmento de reta* $v_0v_1$, *incluindo* $v_0$ *e* $v_1$ *é igual ao* $mdc\,(v_1 - v_0)+1$. *Além disso, se* $v_2$ *é outro ponto integral sobre* $v_0v_1$, *então*

$$\frac{|v_2 - v_0|}{|v_1 - v_0|} = \frac{mdc\,(v_2 - v_0)}{mdc\,(v_1 - v_0)}, \tag{3.3}$$

*onde* $|v|$ *denota o comprimento euclidiano de um vetor* $v$.

**Dem.:** Os pontos no segmento de reta unindo $v_0$ e $v_1$ são da forma

$$v = v_0 + t\,(v_1 - v_0)\,, 0 \leq t \leq 1$$

como $v_0$ é integral, então $v$ é integral se, e somente se, $t\,(v_1 - v_0)$ for integral. Mas $v_1 - v_0$ é integral, logo $t$ deve ser um número racional da forma

$$t = \frac{i}{k},\ \text{com } 0 \leq i < k \text{ e } mdc\,(i,k) = 1.$$

Então $t\,(v_1 - v_0)$ é integral se, e somente se, $k$ divide $mdc\,(v_1 - v_0)$. Logo, $k = mdc\,(v_1 - v_0) \geq 1$. Pois se $k < mdc\,(v_1 - v_0)$ não contaríamos todos os pontos integrais sobre $v_0v_1$. Assim todos os pontos integrais no segmento de reta $v_0v_1$ diferentes de $v_0$ e $v_1$ tem $t$ da forma

$$t = \frac{i}{mdc\,(v_1 - v_0)}, \text{ para } 0 < i < mdc\,(v_1 - v_0).$$

Logo, o número de escolhas para $i$ é $mdc\,(v_1 - v_0) - 1$ e assim o número de pontos integrais sobre $v_0v_1$ incluindo $v_0$ e $v_1$ é $mdc\,(v_1 - v_0) - 1 + 2 = mdc\,(v_1 - v_0) + 1$. Agora vamos provar a equação 3.3. Seja $d = mdc\,(v_1 - v_0)$ e suponha que $v_2 = v_0 + i/d\,(v_1 - v_0)$ é um ponto integral sobre $v_0v_1$ com $0 \leq i \leq d$. Note que $(v_1 - v_0)/d$ é integral e $mdc\,((v_1 - v_0)/d) = 1$ então

$$mdc\,(v_2 - v_0) = mdc\left(i\left(\frac{v_1 - v_0}{d}\right)\right) = i \cdot mdc\left(\frac{v_1 - v_0}{d}\right) = i.$$

E também

$$|v_2 - v_0| = i\frac{|v_1 - v_0|}{d}, |v_1 - v_0| = d\frac{|v_1 - v_0|}{d}$$

e assim

$$\frac{|v_2 - v_0|}{|v_1 - v_0|} = \frac{i}{d} = \frac{mdc\,(v_2 - v_0)}{mdc\,(v_1 - v_0)}.$$

□

O teorema a seguir é muito importante pois mostra como construir politopos integralmente indecomponíveis a partir de um dado politopo.

**Teorema 3.3.1.** *Seja $Q$ um politopo integral em $\mathbb{R}^n$ contido em um hiperplano $H$ e seja $v \in \mathbb{R}^n$ um ponto integral fora de $H$. Suponha que $v_1, \ldots, v_k$ são todos os vértices de $Q$. Então o politopo $conv\,(v, Q)$ é integralmente indecomponível se, e somente se,*

$$mdc\,(v - v_1, v - v_2, \cdots, v - v_k) = 1.$$

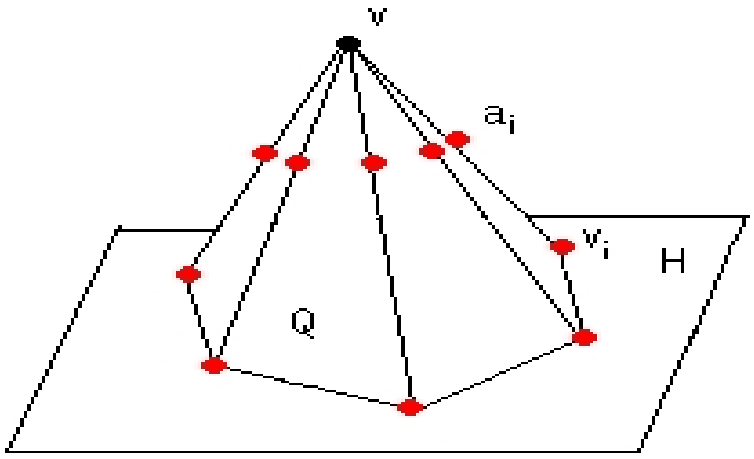


Figura 3.3: piramide indecomponível

**Dem.:** Seja $C = conv\,(v, Q)$ como descrito na figura 3.3 e suponha que $C = A + B$ onde $A$ e $B$ são politopos integrais em $\mathbb{R}^n$. Deslocando adequadamente $A$ e $B$ podemos supor $v \in A$ e $0 \in B$. Como $v, v_1, \ldots, v_k$ são todos os vértices de $C$, pelo lema 2.4.1 existem vértices $a_i$ do $A$ e $b_i$ do $B$ ,únicos, tais que

$$v_i = a_i + b_i \text{ para } 1 \leq i \leq k$$

e

$$vv_i = va_i + 0b_i \text{ para } 1 \leq i \leq k.$$

Já que $0 \in 0b_i$, então por soma de Minkowski $va_i + 0 \subseteq vv_i$, logo o segmento de reta $va_i$ coincide com uma parte de $vv_i$ começando em $v$ (observe a figura 3.3).Dados $v_1, v_2$ vértices de Q, então $v_1v_2$ é uma aresta de $C$, logo pelo teorema 2.4.1

$$v_1v_2 = a_1a_2 + b_1b_2.$$

Então o segmento de reta $a_1a_2$ é paralelo a aresta $v_1v_2$. Isto significa que o triângulo $conv\,(v, a_1, a_2)$ é semelhante ao triângulo maior $conv\,(v, v_1, v_2)$. Então

$$\frac{|a_1 - v|}{|v_1 - v|} = \frac{|a_2 - v|}{|v_2 - v|}$$

e pelo lema 3.3.1, temos

$$\frac{mdc\,(a_1 - v)}{mdc\,(v_1 - v)} = \frac{mdc\,(a_2 - v)}{mdc\,(v_2 - v)} \tag{3.4}$$

e como 3.4 vale para quaisquer dois vértices adjacentes, temos

$$\frac{|a_i - v|}{|v_i - v|} = \frac{mdc\,(a_i - v)}{mdc\,(v_i - v)} = t \text{ para } 1 \leq i \leq k, \tag{3.5}$$

onde $t$ é uma constante tal que $0 \leq t \leq 1$. O número $t$ deve ser racional, digamos $t = m/d$ onde $0 \leq m \leq d$, $d \geq 1$ e $mdc\,(m,d) = 1$. Então $d \mid mdc\,(v_i - v)$ para $1 \leq i \leq k$. Suponha que $mdc\,(v - v_1, v - v_2, \cdots, v - v_k) = 1$ e já que

$$mdc\,(v - v_1, v - v_2, \ldots, v - v_k) =$$

$$mdc\,(mdc\,(v - v_1)\,, mdc\,(v - v_2)\,, \ldots, mdc\,(v - v_k)) = 1$$

então vemos que $d = 1$, assim $m = 0$ ou $m = 1$, logo $t = 0$ ou $t = 1$. Se $t = 0$ então por 3.5 $a_i = v$ para $1 \leq i \leq k$, logo $A = \{v\}$. Se $t = 1$ então 3.5 implica que $a_i = v_i$ para $1 \leq i \leq k$, logo $A = C$ e $B = \{0\}$. Portanto $C$ é integralmente indecomponível.

Para a reciproca, suponhamos $mdc\,(v - v_1, v - v_2, \cdots, v - v_k) = d > 1$. Seja $u_i = \frac{1}{d}\,(v_i - v)$ para $1 \leq i \leq k$. Assim os $u_i$'s são pontos integrais em $\mathbb{R}^n$. Definamos

$$A = conv\,(v, v_1 - u_1, \cdots, v_k - u_k) \text{ e } B = conv\,(0, u_1, \ldots, u_k)\,.$$

Vamos mostrar que $C = A + B$. Começaremos mostrando que $A + B \subseteq C$. Sejam $a \in A$ e $b \in B$, então $a + b = \sum_{i=0}^{k} \lambda_i\,(v_i - u_i) + \sum_{i=0}^{k} \tau_i u_i$ onde $v_0 = v$, $u_0 = 0$ e $\sum_{i=0}^{k} \lambda_i = \sum_{i=0}^{k} \tau_i = 1$. Assim $a + b = \sum_{i=0}^{k} \lambda_i\,(v_i - u_i) + \sum_{i=0}^{k} \tau_i u_i = \sum_{i=0}^{k} v_i \left(\lambda_i + \frac{1}{d}\,(\tau_i - \lambda_i)\right)$ $\in$ $conv\,(v, Q)$ $=$ $C$ pois $\sum_{i=0}^{k} \lambda_i + \frac{1}{d}\,(\tau_i - \lambda_i) = \sum_{i=0}^{k} \lambda_i = 1$. Agora vamos provar a outra inclusão, que $C \subseteq A + B$:

$$\sum_{i=0}^{k} \lambda_i v_i = \sum_{i=0}^{k} \lambda_i\,(v_i + u_i - u_i) = \sum_{i=0}^{k} \lambda_i\,(v_i - u_i) + \sum_{i=0}^{k} \lambda_i u_i \in A + B \text{ pois } \sum_{i=0}^{k} \lambda_i = 1.$$

Já que $d > 1$ e $u_i \neq 0$ e $v_i - u_i \neq v$ para $1 \leq i \leq k$. Então $A$ e $B$ tem no mínimo dois pontos cada, logo $C$ é decomponível. □

**Exemplo 3.3.2.** *Seja $f$ o polinômio $1 + x^n + y^m + x^n y^m + x^i y^j z^k \in \mathbb{F}\,[x, y, z]$ onde n,m,k $> 0$ e i,j $\geq 0$. Então o politopo de Newton da $f$ é a pirâmide com*

*vértices* $(0,0,0)$,$(n,0,0)$,$(n,m,0)$,$(0,m,0)$ *e* $(i,j,k)$. *Se* $mdc\,(n,m,i,j,k)=1$ *então a pirâmide é indecomponível e assim, de acordo com o critério de irredutibilidade 3.2.1,* $f$ *é absolutamente irredutível sobre* $\mathbb{F}$.

Note que no exemplo 3.3.2 $f$ permanece absolutamente irredutível se acrescentarmos a ela termos cujos expoentes vetoriais permaneçam na pirâmide. Também os coeficientes do polinômio são todos 1, mas observe que poderíamos mudá-los para qualquer elemento não nulo do corpo em que estivéssemos trabalhando e isso não mudaria o politopo de Newton associado a $f$ e assim $f$ continuaria absolutamente irredutível.

Os corolários seguintes especializam os casos simples como quando $Q$ é um ponto integral, um segmento de linha ou um triângulo.

**Corolário 3.3.1.** *Sejam* $v_0$ *e* $v_1$ *dois pontos integrais distintos em* $\mathbb{R}^n$. *Então o segmento de reta* $v_0v_1$ *é integralmente indecomponível sse* $mdc\,(v_0-v_1)=1$.

**Dem.:** Construímos o hiperplano $H$ passando por $v_0$ e perpendicular à reta unindo $v_0$ e $v_1$, então $v_0 \in H$ e $v_1 \notin H$, assim, pelo teorema 3.3.1 $v_0v_1$ é integralmente indecomponível sse $mdc\,(v_1-v_0)=1$ □

O corolário 3.3.1 nos leva à seguinte aplicação:

**Corolário 3.3.2.** *Um polinômio com dois termos*

$$aX_1^{i_1}\dots X_k^{i_k}+bX_{k+1}^{i_{k+1}}\dots X_n^{i_n}\in\mathbb{F}\,[X_1,\dots,X_n] \tag{3.6}$$

$a,b\in\mathbb{F}\setminus 0$ *é absolutamente irredutível sobre* $\mathbb{F}$ *sse* $mdc\,(i_1,\dots,i_n)=1$

**Dem.:** A demonstração da recíproca deste corolário é imediata da aplicação do corolário 3.3.1. Porém a ida será feita agora. Começamos dividindo 3.6 pelo seu primeiro termo, e assim ficamos com

$$f:=1+cx_1^{-i_1}\dots x_k^{-i_k}x_{k+1}^{i_{k+1}}\dots x_n^{i_n} \tag{3.7}$$

agora, vamos supor que $mdc\,(i_1,\ldots,i_n)=d>1$. Assim, $i_k=d\alpha_k$ para $k=1,\ldots,n$. Podemos colocar $\omega=x_1^{-\alpha_1}\ldots x_k^{-\alpha_k}x_{k+1}^{\alpha_{k+1}}\ldots x_n^{\alpha_n}$ e assim $f=1+c\omega^d$ com $d>1$. Logo, $f$ é redutivel quando adjuntarmos o elemento $c^{1/d}$, a $d$-ésima raíz de $-1$, ao corpo $F$. Contradizendo nossa afirmação de o polinômio 3.6 ser absolutamente irredutível. □

**Exemplo 3.3.3.** *De acordo com o corolário 3.3.2 temos que:*

1. $x^n+y^m$ *é absolutamente irredutível sobre um corpo* $\mathbb{F}$ *se, e somente se,* $mdc(n,m)=1$.
2. $y^i+x^jz^k$ *é absolutamente irredutível sobre um corpo* $\mathbb{F}$ *se, e somente se,* $mdc(i,j,k)=1$.

**Corolário 3.3.3.** *Sejam* $v_0,v_1,v_2$ *três pontos integrais em* $\mathbb{R}^n$*, nem todos na mesma reta. Então o triângulo* $conv\,(v_0,v_1,v_2)$ *é integralmentre indecomponível sse*

$$mdc\,(v_0-v_1,v_0-v_2)=1$$

**Dem.:** Aplicando o teorema 3.3.1 com $v_1v_2=Q\subset H=\{v_0+\lambda\,(v_2-v_1):\lambda\in\mathbb{R}\}$ e $v_0\notin H$, temos que $conv\,(v_0,Q)=conv\,(v_0,v_1,v_2)$ é integralmente indecomponível sse $mdc\,(v_0-v_1,v_0-v_2)$ □

O próximo resultado mostra uma aplicação do corolário 3.3.3.

**Corolário 3.3.4.** *Seja* $f=aX^n+bY^m+cX^uY^v+\sum c_{ij}X^iY^j\in F\,[X,Y]$ *com* $a,b,c$ *não nulos. Suponha que o politopo de Newton da* $f$ *é o triângulo com vértices* $(n,0)$*,* $(0,m)$ *e* $(u,v)$*. Se* $mdc\,(m,n,u,v)=1$ *então* $f$ *é absolutamente irredutível sobre* $F$*.*

**Dem.:** Sejam $v_0=(u,v)$, $v_1=(n,0)$ e $v_2=(0,m)$. Pelo corolário 3.3.3 se $mdc\,(v_0-v_1,v_0-v_2)$ $=mdc\,(u-n,v,u,v-m)=1$ então $conv\,(v_0,v_1,v_2)$ é integralmente indecomponível e assim $f$ será absolutamente irredutível. Então devemos mostrar que $mdc\,(u-n,v,u,v-m)=1$. Por hipótese $mdc(m,n,u,v)=1$. Seja $d=mdc(u-n,v,u,v-m)$ então $d\mid(u-n-u)=-n$, logo, $d\mid n$. Da mesma maneira $d\mid(v-m-v)=-m$, logo, $d\mid m$. Então $d\mid(m,n,v,u)$ logo $d\mid mdc\,(m,n,u,v)=1$ que nos leva a $d=1$. □

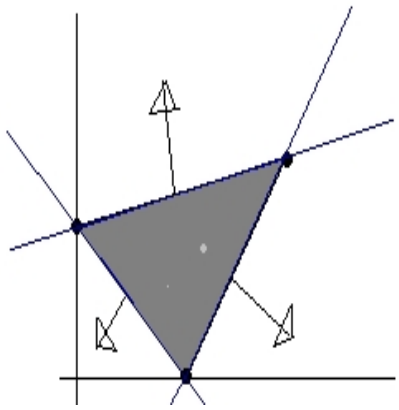

Figura 3.4: hiperplanos de suporte

Para que o polinômio no corolário 3.3.4 permaneça absolutamente irredutível devemos tomar cuidado para que os expoentes vetoriais $(i, j)$ referentes aos termos $x^i y^j$ permaneçam no politopo. Conforme foi estudado no capítulo 2 cada aresta do triângulo é a intersecção do politopo com um hiperplano(observe a figura 3.4). Então

1. se $a_1$ é a aresta que une os pontos $(0, m)$ e $(n, 0)$ temos que $a_1 := P \cap H_1 = P \cap \{(x, y) \in \mathbb{R}^2 : (x, y)(m, n) = nm\}$
2. se $a_2$ é a aresta que une os pontos $(n, 0)$ e $(u, v)$ temos que $a_2 := P \cap H_2 = P \cap \{(x, y) \in \mathbb{R}^2 : (x, y)(-v, u - n) = -vn\}$
3. se $a_3$ é a aresta que une os pontos $(u, v)$ e $(0, m)$ temos que $a_3 := P \cap H_3 = P \cap \{(x, y) \in \mathbb{R}^2 : (x, y)(v - m, -u) = -mu\}$

e de acordo com 2.4.4 temos que $P = H_1^- \cap H_2^- \cap H_3^-$. Assim, $(i, j)$ está em $P$ se, e somente se, ele satisfizer:

1. $mi + nj - mn \geq 0$
2. $-vi + j(u - n) + vn \geq 0$

3. $i(v-m) - ju + mu \geq 0$.

**Corolário 3.3.5.** *Sejam $v_0, v_1, v_2, v_3$ quatro pontos integrais em $\mathbb{R}^n$, nem todos contidos no mesmo plano. Então o tetraedro $conv\,(v_0, v_1, v_2, v_3)$ é integralmente indecomponível sse $mdc\,(v_0 - v_1, v_0 - v_2, v_0 - v_3) = 1$.*

**Dem.:** Sejam $Q = conv\,(v_1, v_2, v_3)$, $v_0 \notin Q$, $C = conv\,(v_0, v_1, v_2, v_3) = conv\,(v_0, Q)$ é integralmente indecomponível sse $mdc\,(v_0 - v_1, v_0 - v_2, v_0 - v_3) = 1$. □

O próximo resultado é uma aplicação do corolário 3.3.5.

**Corolário 3.3.6.** *Suponha que o politopo de Newton da $f = a_1X^l + a_2Y^m + a_3Z^n + a_4X^uY^vZ^w + \sum c_{ijk}X^iY^jZ^k \in \mathbb{F}[X, Y, Z]$ seja o tetraedro com vértices $(l, 0, 0)$, $(0, m, 0)$, $(0, 0, n)$ e $(u, v, w)$. Se $mdc\,(l, m, n, u, v, w) = 1$ então $f$ é absolutamente irredutível sobre $\mathbb{F}$.*

**Dem.:** Sejam $v_0 = (u, v, w)$, $v_1 = (l, 0, 0)$, $v_2 = (0, m, 0)$ e $v_3 = (0, 0, n)$, se $mdc\,(v_0 - v_1, v_0 - v_2, v_0 - v_3) = mdc\,(u - l, v, w, u, v - w, w - n) = 1$ então $P_f$ será integralmente indecomponível, logo, $f$ será absolutamente irredutível. Por hipótese $mdc\,(l, m, n, u, v, w) = 1$. Seja $d = mdc\,(u - l, v - m, w - n, u, v, w)$ então $d \mid (u - l - u) = -l$, logo $d \mid l$ e do mesmo modo $d \mid m$, $d \mid n$ e assim $d \mid mdc\,(l, m, n, u, v, w) = 1$. O que leva a $d = 1$. □

O corolário seguinte nos diz que se, por exemplo em $\mathbb{R}^3$, tivermos uma pirâmide com uma aresta lateral ou uma aresta da base indecomponível então a pirâmide será indecomponível.

**Corolário 3.3.7.** *Seja $Q$ um politopo integral em $\mathbb{R}^n$ contido em um hiperplano $H$ e seja $v \in \mathbb{R}^n$ um ponto integral fora de $H$. Se $Q$ tem uma aresta $v_1v_2$ tal que $mdc\,(v_1 - v_2) = 1$ ou um vértice $v_1$ tal que $mdc\,(v - v_1) = 1$ então o politopo $conv\,(v, Q)$ é integralmente indecomponível.*

**Dem.:** Sejam $v_1, \ldots, v_k$ todos os vértices de $Q$. Se $mdc\,(v - v_1) = 1$ então $mdc\,(v - v_1, v - v_2, \cdots, v - v_k) = mdc\,(mdc\,(v - v_1), \cdots, (v - v_k)) = 1$ e pelo teo-

rema 3.3.1 $conv\,(v, Q)$ é integralmente indecomponível. Se $mdc\,(v_1 - v_2) = 1$ e $d = mdc\,(v - v_1, v - v_2, \cdots, v - v_k)$ então $d \mid (v_1 - v)$ e $d \mid (v - v_2)$, logo $d \mid (v_1 - v + v - v_2) = (v_1 - v_2)$, assim $d \mid mdc\,(v_1 - v_2) = 1$ e isso implica que $d = 1$. Pelo teorema 3.3.1 $conv\,(v, Q)$ é integralmente indecomponível. □

**Corolário 3.3.8.** *Seja* $f = g\,(X) + h\,(X_1, \ldots, X_n)$ *onde* $g \in \mathbb{F}\,[X]$ *de grau* $r$ *e* $h \in \mathbb{F}\,[X_1, \ldots, X_n]$ *de grau total* $m$. *Se* $mdc\,(r, m) = 1$ *então* $f$ *é absolutamente irredutível sobre* $\mathbb{F}$.

**Dem.:** Se necessário, podemos fazer uma translação na variável $X$ para que a constante de $f$ seja não nula e assim o politopo de Newton de $h$ que fica sendo a base da nossa pirâmide. Como $h$ continua tendo grau total m, existe um termo $c_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$ em $h$ tal que $i_1 + \cdots + i_n = m$ cujo expoente vetorial $(i_1, \ldots, i_n)$ é o vértice $v_1$ de $P_h$. E como $g$ tem grau $r$, teremos um termo $aX^r$ em $g$ cujo expoente vetorial $(r, 0, \ldots, 0)$ determina num vértice $v$ da pirâmide fora da base. Seja $d = mdc(v - v_1) = mdc(r, i_1, \ldots, i_n)$. Então $d \mid i_1 + \cdots + i_n = m$, logo $d \mid (m, r)$, ou seja, $d \mid mdc(m, r)$. Isso implica que $d = 1$ e pelo corolário 3.3.7 temos que $P_f$ é integralmente indecomponível e assim, pelo teorema 3.2.1, $f$ é absolutamente irredutível. □

**Teorema 3.3.2.** *Seja* $Q$ *um politopo integralmente indecomponível em* $\mathbb{R}^n$ *que está contido no hiperplano* $H$ *e tem no mínimo dois pontos, e seja* $v \in \mathbb{R}^n$ *um ponto(não necessariamente integral) fora de* $H$. *Seja* $S$ *um conjunto qualquer de pontos integrais no politopo* $conv\,(v, Q)$. *Então o politopo* $conv\,(S, Q)$ *é integralmente indecomponível.*

**Dem.:** Seja $C = conv\,(S, Q)$ e como $Q = C \cap H$ então $Q$ é uma face de $C$. Se $C = A + B$, então pelo lema 2.4.1 $A, B$ tem faces únicas $A_1$ e $B_1$, respectivamente, tais que $Q = A_1 + B_1$. Como $Q$ é integralmente indecomponível então $A_1$ ou $B_1$ deve ter apenas um ponto, digamos $A_1$. Fazendo um deslocamento adequado de $A$ e $B$, podemos assumir que $A_1 = \{0\}$ e $B_1 = Q$. Queremos mostrar que $A = A_1 = \{0\}$. Seja $r \in A$. Então $r + Q \subseteq r + B \subseteq C = conv\,(S, Q)$ e como $Q \subset H$ temos que

$r + Q \subseteq r + H$ e assim

$$r + Q \subseteq C \cap (r + H). \tag{3.8}$$

Seja $C_1$ o cone gerado por $v$ e $Q$. Então

$$C \subseteq conv(v, Q) \subseteq C_1 \text{ e } C_1 \cap H = Q \tag{3.9}$$

e por 3.8 temos que

$$r + Q \subseteq C_1 \cap (r + H) \tag{3.10}$$

e pelo lema 2.2.3 existe um número real $t \geq 0$ tal que

$$C_1 \cap (r + H) = v + t(Q - v) \tag{3.11}$$

Vamos mostrar que $t \leq 1$. Seja $a \in Q$, então $r + a \in C_1 \cap (r + H)$ e por 3.11 existe $b \in Q$ tal que $r + a = v + t(b - v)$. E também, $r + a \in C \subseteq conv(v, Q)$ então existe $b_1 \in Q$ tal que $r + a = v + t_1(b_1 - v)$ para um certo $0 \leq t_1 \leq 1$. Então

$$t(b - v) = t_1(b_1 - v) \tag{3.12}$$

Seja $H = \{x \in \mathbb{R}^n : \langle \alpha, x \rangle = \beta\}$ onde $\alpha \in \mathbb{R}^n$, $\beta \in \mathbb{R}$. Como $b, b_1 \in Q$, então $\langle \alpha, b \rangle = \langle \alpha, b_1 \rangle$ e a equação 3.12 implica que $\langle \alpha, v + t(b - v) \rangle = \langle \alpha, v + t_1(b_1 - v) \rangle$ e assim $t(\beta - \langle \alpha, v \rangle) = t_1(\beta - \langle \alpha, v \rangle)$ , logo $t = t_1$. E como $0 \leq t_1 \leq 1$ segue que $0 \leq t \leq 1$. De 3.8 e 3.11 temos $r + Q \subseteq v + t(Q - v)$, isto é

$$Q \subseteq tQ + d \tag{3.13}$$

onde $d = (1 - t)v - r \in \mathbb{R}^n$. Para $k > 0$ inteiro aplicamos (3.13) $k$ vezes

$$Q \subseteq t^k Q + \left(t^{k-1} + \cdots + t + 1\right) d \tag{3.14}$$

Se $0 \leq t < 1$ então 3.14 pode ser escrita como

$$Q \subseteq t^k Q + \frac{t^k - 1}{t - 1} d.$$

E como $Q$ é limitado quando $k \to \infty$, temos

$$Q \subseteq \{0\} + \frac{-1}{t - 1} a = \left\{ \frac{-1}{t - 1} a \right\}$$

e assim $Q$ tem apenas um ponto contradizendo a hipótese de $Q$ ter no mínimo dois pontos. Portanto $t = 1$ e assim 3.13 fica

$$r + Q \subseteq Q. \tag{3.15}$$

Para $k > 0$ inteiro, aplicando (3.15) $k$ vezes temos que

$$kr + Q \subseteq Q$$

e como Q é limitado quando $k \to \infty$ então $r = 0$ e $A = A_1 = \{0\}$. □

**Exemplo 3.3.4.** *Considere o tetraedro com vértices* $(0,0,0)$, $(n,0,0)$, $(0,m,0)$ *e* $(0,0,u)$. *Note que o tetraedro é indecomponível se* $mdc(m,n) = 1$. *Dado o polinômio* $f = 1 + x^n + y^m + x^w y^v + y^i z^j + z^k$, *se* $(w,v,0)$, $(0,i,j)$ *e* $(0,0,k)$ *estiverem no tetraedro então de acordo com o teorema 3.3.2* $P_f$ *será integralmente indecomponível pois estará contido no tetraedro e os dois com a mesma base no plano xy. Logo, f será absolutamente irredutível.*

**Corolário 3.3.9.** *Seja* $f = aX^m + bY^n + \sum c_{ij} X^i Y^j \in \mathbb{F}[X,Y]$ *com* $a, b$ *não nulos e* $(i,j)$ *diferente de* $(m,0)$, $(0,n)$. *Suponha que o politopo de Newton de f esteja contido no triângulo* $(m,0)$, $(0,n)$ *e* $(u,v)$ *para algum ponto* $(u,v) \in \mathbb{R}^2$. *Se* $mdc(m,n) = 1$ *então f é absolutamente irredutível sobre* $\mathbb{F}$.

## 3.4 Projeções

Agora veremos novas construções de politopos integralmente indecomponíveis baseadas em projeções. Intuitivamente esperamos que, por exemplo, se tivermos um quadrado e fizermos a projeção sobre um de seus lados e esta for integralmente indecomponível, então o quadrado será também, porém veremos que isto nem sempre é verdade.

**Definição 3.4.1.** *Dizemos que uma transformada linear* $\pi : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ *é integral se ela leva pontos integrais de* $\mathbb{R}^n$ *para pontos integrais em* $\mathbb{R}^m$.

**Lema 3.4.1.** *Seja $P$ um politopo integral em $\mathbb{R}^n$ e $\pi : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ uma transformada linear integral. Se $\pi(P)$ é integralmente indecomponível e cada vértice de $\pi(P)$ tem somente uma pré imagem em $P$ então $P$ deve ser integralmente indecomponível.*

Antes de provarmos o lema 3.4.1, vamos observar que um politopo integral $P$ sob qualquer transformada linear integral continua sendo um politopo integral e que cada vértice de $\pi(P)$ vem de um vértice de P.

Seja $P$ um politopo em $\mathbb{R}^n$. Então pelo teorema de Krein-Milman temos que $P = conv(vert(P))$. Logo, $P = conv(v_1, \ldots, v_l)$. Dado $w \in \pi(P)$ temos que $w = \pi\left(\sum_{i=1}^{l} \lambda_i v_i\right) = \sum_{i=1}^{l} \lambda_i \pi(v_i)$ com $\sum_{i=1}^{l} \lambda_i = 1$ então $\pi(P) \subseteq conv(\pi(v_1), \ldots, \pi(v_l))$.

Agora, seja $w \in conv(\pi(v_1), \ldots, \pi(v_l))$ então $w = \sum_{i=1}^{l} \alpha_i \pi(v_i) = \pi\left(\sum_{i=1}^{l} \alpha_i v_i\right)$ com $\sum_{i=1}^{l} \alpha_i = 1$, logo $w \in \pi(P)$. Portanto $\pi(P) = conv(\pi(v_1), \ldots, \pi(v_l))$,logo $\pi(P)$ é um politopo integral em $\mathbb{R}^n$.

Então $\pi(P) = conv(\pi(vert(P)))$, ou seja, cada vértice $w$ de $\pi(P)$ vem de $w = \pi(v_j)$ e assim, cada vértice de $\pi(P)$ vem de um vértice de $P$. Agora estamos prontos para provar o lema 3.4.1.

**Dem.:** Iremos mostrar que se $P$ é decomponível então $\pi(P)$ também o será. Suponha $P = A + B$ onde $A, B$ são politopos integrais em $\mathbb{R}^n$ com no mínimo dois pontos cada. Então $\pi(P) = \pi(A) + \pi(B)$ e precisamos mostrar que $\pi(A)$ e $\pi(B)$ tem no mínimo dois pontos cada, vamos supor que $\pi(A)$ tem apenas um ponto. Seja $w_0$ um vértice de $P$ tal que $\pi(w_0)$ seja um vértice de $\pi(P)$. Já que $P = A + B$, pelo teorema 2.4.1 existem vértices únicos $a_0$ de $A$ e $b_0$ de $B$ tais que $w_0 = a_0 + b_0$. Como $A$ tem no mínimo dois pontos, seja $a_1$ outro vértice de $A$ tal que $a_0a_1$ seja uma aresta de $A$. Pelo teorema 2.4.1, $a_0a_1$ será fator de uma aresta $w_0w_1$, com $w_0 \neq w_1$. Note que $w_0w_1$ é paralelo a $a_0a_1$, ou seja, elas tem o mesmo vetor direção. Então podemos escrever $w_1 = w_0 + t(a_1 - a_0)$, logo, $w_1 - w_0 = t(a_1 - a_0)$ para algum t

real. Então

$$\pi\left(w_1 - w_0\right) = \pi\left(t\left(a_1 - a_0\right)\right) = t\left(\pi\left(a_1\right) - \pi\left(a_0\right)\right) = 0$$

pois $\pi\left(A\right)$ tem apenas um ponto. Logo $\pi\left(w_1\right) = \pi\left(w_0\right)$ e assim dois vértices de $P$ vão para um vértice de $\pi\left(P\right)$, contradizendo nossa hipótese. □

**Corolário 3.4.1.** *Seja $P$ um politopo integral em $\mathbb{R}^n$ e $\pi : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ uma transformada linear integral que é injetora sobre os vértices de $P$. Se $\pi\left(P\right)$ é integralmente indecomponível então $P$ também deve ser.*

**Teorema 3.4.1.** *Seja $Q$ um politopo integralmente indecomponível em $\mathbb{R}^m$ e $\pi : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ uma transformada linear integral. Seja $S$ um conjunto de pontos integrais em $\pi^{-1}\left(Q\right)$ tendo exatamente um ponto em $S$ para cada vértice $v$ de $Q$. Então o politopo $conv\left(S\right)$ em $\mathbb{R}^n$ é integralmente indecomponível.*

**Dem.:** Basta notar que $\pi\left(conv\left(S\right)\right) = Q$ e aplicar o lema 3.4.1. □

**Exemplo 3.4.1.** *Dado o polinômio $f(x,y,z) = y^5z + x^2y^4z^3 + x^3z^2 + x^3y^7z^7 + x^4y^6z^5 + x^6y^{10}z^{12} + x^7y^{13}$ então temos que o politopo de Newton associado a $f$ é $P = conv((0,5,1),(2,4,3),(3,0,2),(3,7,7),(4,6,5),(6,10,12),(7,13,0))$. Vamos definir $\pi$ como a projeção no plano $xy$.*

*Então $\pi(P) = conv((0,5),(2,4),(3,0),(3,7),(4,6),(6,10),(7,13))$. Mas $\pi(P)$ é o triângulo com vértices $v_0 = (0,5)$,$v_1 = (3,0)$ e $v_2 = (7,13)$ e cada um deles possui apenas uma pré-imagem em $P$. Usando o corolário 3.3.3 concluímos que $\pi(P)$ é integralmente indecomponível pois $mdc(v_0 - v_1, v_0 - v_2) = mdc(3,5,7,8) = 1$. Como as condições do lema 3.4.1 são satisfeitas podemos afirmar que $P$ é integralmente indecomponível. Deste modo, segue que $f$ é absolutamente irredutível.*

# 4 DECOMPOSIÇÃO DE POLITOPOS

Neste capítulo estudaremos os algoritmos desenvolvidos por Shuhong Gao e Alan Lauder em [6, 8]. Começaremos com um algoritmo que testa a indecomponibilidade de politopos e sua aplicação será importante na construção de novas famílias de polinômios absolutamente irredutíveis. Depois veremos um algoritmo que constrói todos os fatores integrais de um politopo e que pode ser útil na fatoração de polinômios como será visto no capítulo seguinte. Terminamos estudando um algoritmo que testa indecomponibilidade via projeções para politopos de dimensão maior do que 2.

## 4.1 Introdução

Neste capítulo e como feito no anterior, associaremos a cada polinômio multivariado um politopo, dito seu politopo de Newton. Como foi observado por Ostrowski em 1921, se um polinômio $f$ é redutível, então seu politopo de Newton é decomponível em relação a soma de minkowski em politopos de Newton associados aos fatores de $f$. Este resultado nos leva a dois problemas que serão estudados neste capítulo:

**Problema 1**:

Dado um politopo integral, decidir se este é integralmente indecomponível.

Aqui o politopo representará a envoltória convexa de um conjunto finito de pontos integrais. Este é um caminho difícil pois mostraremos que decidir indecomponibilidade de politopos é NP-completo. O interesse neste procedimento é que cada vez que descobrimos um politopo integralmente indecomponível este nos leva a uma família de polinômios absolutamente irredutíveis que podem ser representados por tal politopo.

**Problema 2**:

Dado um politopo integral , encontrar todos os seus fatores integrais.

Dado um polinômio $f$ o interesse em sabermos os fatores de seu politopo de Newton associado poderá ser útil na fatoração de $f$. Como será visto no capítulo 5 tentaremos fatorar um polinômio $f$ em fatores cujos politopos de Newton associados foram encontrados quando decompomos o politopo de Newton associado a $f$.

Na seção 4.2 apresentaremos o algoritmo de Grahan que também pode ser encontrado com mais detalhes em [10, 17] que fornece os vértices da envoltória convexa de $n$ pontos no plano em $O(n \log n)$. O algoritmo de Grahan poderá ser usado para encontrar os vértices de um dado polígono. Na seção 4.4 iremos apresentar os algoritmos de Gao e Lauder feitos em [6, 8]. O primeiro algoritmo dirá se um polígono integral é integralmente indecomponível ou não. Enquanto o segundo algoritmo retornará todos os fatores integrais de um polígono integral, inclusive os triviais. Na seção 4.5 apresentaremos o algoritmo feito por Gao e Lauder em [6, 8] que decidirá indecomponibilidade de politopos em $\mathbb{R}^n$ fazendo sua projeção no plano.

## 4.2 Envoltória Convexa no Plano

Nosso objetivo nesta seção é apresentar o algoritmo de Grahan que fornece os vértices no sentido anti-horário da envoltória convexa de $n$ pontos no plano em $O(n \log n)$. Este algoritmo poderá ser usado para calcular os vértices do politopo de Newton associado de um polinômio bivariado.

Começaremos apresentando um exemplo com algumas hipóteses, para facilitar o entendimento, que mais tarde serão removidas.

Seja $P = conv((2,5),(1,0),(0,2),(1,1),(4,4),(4,5),(5,0))$. Vamos assumir que tenhamos um ponto extremo $a = (5,0)$ sendo que este é o ponto extremo com coordenada $x$ de mais alto valor e com coordenada $y$ de mais baixo valor. Agora vamos classificar os outros pontos de acordo com a sua inclinação em relação

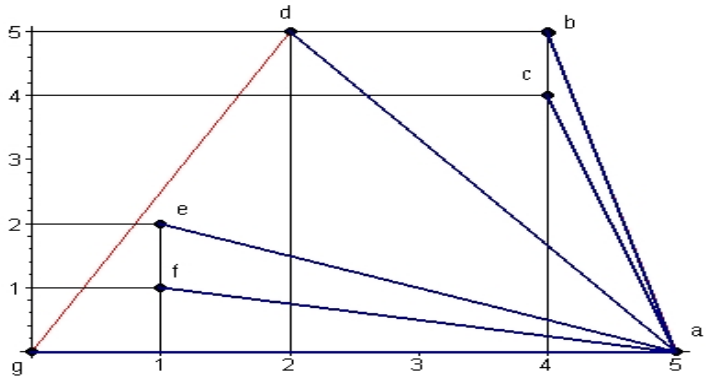


Figura 4.1: ordenação no sentido anti-horário

ao ponto $a$ no sentido anti-horário: $b = (4, 5)$, $c = (4, 4)$, $d = (2, 5)$, $e = (1, 2)$, $f = (1, 1)$ e $g = (0, 0)$ (observe a figura 4.1). Estamos assumindo que temos sempre somente dois pontos sobre cada segmento de reta que liga o ponto $a$ a qualquer outro ponto de $S$. Uma condição que será facilmente removida.

Iremos armazenar os pontos sobre a envoltória convexa em uma pilha $S$. Inicialmente a pilha contém os dois primeiros pontos : $S = (b, a)$. Em nosso exemplo, com $b$ no topo da pilha. Cada elemento que for adicionado à pilha ficará na posição mais a esquerda dela, ou seja, no topo da pilha.

Vamos verificar se $c$ será adicionado a pilha. Para isso vamos calcular o valor da área formada pelos pontos $a$, $b$ e $c$. Note que $(a, b, c)$ formam um triângulo no sentido anti horário em $b$ e por consequência disso $A(a, b, c) > 0$, e assim adicionamos $c$ a pilha. $S = (c, b, a)$. Agora vamos verificar se $d$ será adicionado à pilha. Note que $(b, c, d)$ forma um triângulo no sentido horário em $c$, logo $A(b, c, d) < 0$. Isso quer dizer que $c \in int(P)$, pois $c \in H^-$, onde $H$ é o hiperplano de suporte da aresta que liga os pontos $b$ e $d$ que está ilustrado na figura 4.2. Logo, retiramos $c$ da pilha $S$. $S = (b, a)$ e verificamos se $d$ entra na pilha. Agora adicionamos $d$ à pilha, pois $a, b, d$ forma um triângulo no sentido anti horário em $b$. $S = (d, b, a)$.

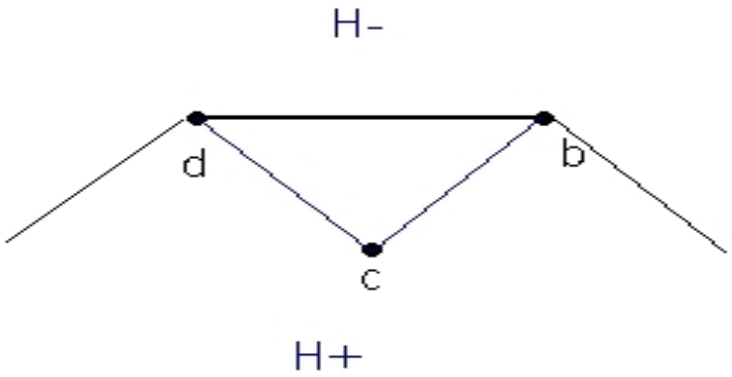


Figura 4.2: ponto interior

Continuando desta maneira notamos que $e$ e $f$ são adicionados à pilha, assim $S = (f, e, d, b, a)$. O ponto $g$ nos leva a tirar $e$ e $f$ da pilha, pois $e, f, g$ formam um triângulo no sentido horário em $f$. Logo, $f \in int(P)$. Assim como, $d, e, g$ támbem formam um triângulo no sentido horário em $e$, logo, $e \in int(P)$. Deste modo adicionamos $g$ à pilha e ficamos com $S = (g, d, b, a)$.

Antes de prosseguirmos vamos apresentar os comandos coloca($p$,$S$) e retira($S$), que coloca $p$ no topo da lista $S$, e retira o elemento que está no topo da lista $S$, respectivamente.

**Escolhendo $p_0$, o vértice inicial.** Escollheremos o ponto com a ordenada $y$ de menor valor e no caso de existirem muitos pontos com a mesma ordenada, procuramos entre estes o de abscissa de valor mais alto. Ponto que certamente será um vértice. Considerando $p_0$ como a origem, calculamos as inclinações dos outros pontos e enumeramos como $p_0$, $p_1$,...,$p_{n-1}$ com $p_{n-1}$ sendo o ponto de maior angulação anti-horário conforme ilustrado na figura 4.3.

É importante notar que quando ordenamos os pontos deste modo então $p_1 \in bd(P)$, assim inicializamos $S = (p_1, p_0)$.

**Colinearidade**

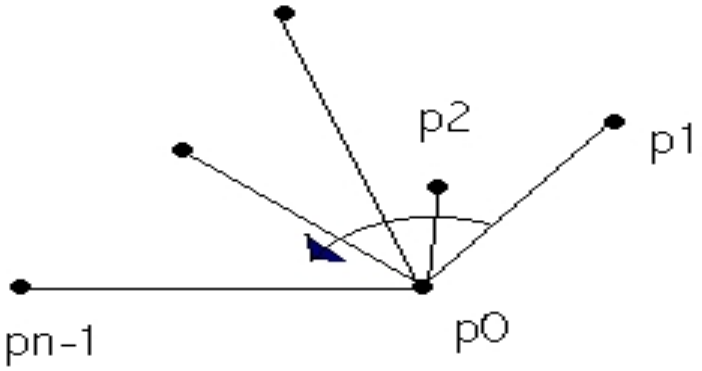


Figura 4.3: ordenação dos pontos

No caso de termos três pontos ou mais colineares com um deles sendo o $p_0$, ou seja, três pontos ou mais sobre um segmento de reta que liga $p_0$ a outros pontos, então ficamos com o ponto mais distante de $p_0$ e descartamos os outros.

No caso de a área entre três pontos classificados for zero, $A(p_i, p_{i+1}, p_{i+2}) = 0$ então estes pontos são colineares e por isso o algoritmo que apresentaremos segue adiante apenas se $A(a, b, c) > 0$ que é o mesmo que dizer: formar um triângulo no sentido anti horário.

**Algoritmo 4.2.1 (Grahan).**

***Entrada***: *Um conjunto $S$ de pontos no plano.*
***Saída***: *Os vértices da conv$(S)$ ordenados no sentido anti-horário.*

1. *Encontre o ponto com coordenada y de menor valor e entre estes o de coordenada x de maior valor. Chame-o de $p_0$.*

2. *Ordene todos os outros pontos de acordo com sua angularidade ao redor de $p_0$. No caso de um ou mais pontos com a mesma angularidade, fique com o mais distante de $p_0$ e descarte os demais.*

3. *Pilha $S = (p_1, p_0) = (p_t, p_{t-1})$; $t$ é o índice do ponto no topo da pilha.*

$i \leftarrow 2$

***enquanto*** $i < n$ ***faça***

***se*** $p_i$ *forma um triângulo no sentido anti- horário com* $p_{t-1}$,$p_t$

***então*** *coloca(*$p_i$*,S) e* $i \leftarrow i + 1$

***senão*** *retire(S).*

**Teorema 4.2.1.** *A envoltória convexa de n pontos no plano pode ser encontrada utilizando o algoritmo de Graham em* $O(n \log n)$.

**Dem.:** Na linha 2 o algoritmo precisa ordenar uma lista com $n - 1$ elementos. É sabido que os algoritmos de ordenação trabalham em $O(n \log n)$ que pode ser visto com maiores detalhes em [1, 2]. Nos demais passos há $O(n)$ operações, logo o algoritmo trabalha em $O(n \log n)$. □

## 4.3 Fatores e Decomposição

Como foi definido anteriormente o ente convexo $L$ é um fator de $K$ se existe um ente convexo $M \in \mathbb{R}^n$ tal que $K = L + M$. Veremos que um fator de um politopo tem a estrutura fortemente relatada pelo politopo. Essa observação ficará clara quando estivermos tratando de politopos em $\mathbb{R}^2$, ou seja polígonos.

**Definição 4.3.1.** *Para entes convexos* $K$,$L \in \mathbb{R}^n$ *diremos que L pode ser deslocado para dentro de K se para cada ponto x da fronteira de K existe um vetor translação* $t \in \mathbb{R}^n$ *tal que* $x \in L + t \subset K$.

**Teorema 4.3.1.** *Sejam* $K$,$L \in \mathbb{R}^n$. *Então L é um fator de K se, e somente se, L pode ser deslocado para dentro de K.*

**Dem.:** Se $K = L + M$ e $x \in K$, existe $y \in L$ e $t \in M$ tal que $x = y + t$, assim $x \in L + t \subset K$. Suponha que $L$ desliza livremente para $K$. Seja $x$ na fronteira de $K$. Por hipótese, existe $t \in \mathbb{R}^n$ tal que $x \in L + t \subset K$. Então $t \in K \sim L$ e $x \in L + (K \sim L)$. Pelo lema 2.3.3, $L$ é um fator de $K$. □

Os possíveis fatores de um politopo têm a estrututa muito parecida com a do próprio politopo. Sejam $P$, $Q$, $R \in \mathbb{R}^n$ tais que $P = Q + R$, então como foi feito no teorema 2.4.1 se $F$ é uma face de $P$, então existem faces $F_Q$ de $Q$ e $F_R$ de $R$ tais que $F = F_Q + F_R$, todas as faces com o vetor normal em comum. Esta observação é para notarmos que os vetores normais das faces de um fator $Q$ de $P$ estão entre os vetores normais das faces de $P$. Particularmente fácil é descrever os fatores de um polígono em $\mathbb{R}^2$, o qual será feito na seção seguinte.

## 4.4 Polígonos

Dado um polígono $P$ podemos representá-lo por sua sequência de arestas. Sejam $v_0, v_1, \ldots, v_{m-1}$ os vértices do polígono ordenados ciclicamente na direção horária. As arestas de $P$ são representadas pelos vetores $E_i = v_i - v_{i-1} = (a_i, b_i)$ para $1 \leq i \leq m$, onde $a_i, b_i \in \mathbb{N}$ e os índices são feitos módulo m. Chamamos cada $E_i$ um vetor aresta.

**Definição 4.4.1.** *Um vetor $v = (a, b) \in \mathbb{Z}^2$ é dito um vetor primitivo se $mdc\,(a, b) = 1$.*

Seja $n_i = mdc\,(a_i, b_i)$ e defina $e_i = (a_i/n_i, b_i/n_i)$. Então $E_i = n_i e_i$ onde $e_i$ é um vetor primitivo para $1 \leq i \leq m$.

A sequência de vetores $\{n_i e_i\}_{1 \leq i \leq m}$, que chamamos sequência de arestas ou sequência poligonal, identifica unicamente o polígono sob translação determinada pelo vetor $v_0$, e esta será a entrada para o algoritmo de decomposição. Como a região do polígono é fechada, temos que $\sum_{1 \leq i \leq m} n_i e_i = (0, 0)$.

O lema a seguir é a motivação para o algoritmo de decomposição de polígonos, pois ele diz exatamente como serão os fatores de uma possível decomposição do polígono dado.

**Lema 4.4.1.** *Seja $P$ um polígono com sequência de arestas $\{n_i e_i\}_{1\leq i\leq m}$ onde $e_i \in \mathbb{Z}^2$ são vetores primitivos. Então um polígono integral é um fator de $P$ sse sua sequência de arestas é da forma $\{k_i e_i\}_{1\leq i\leq m}$, $0 \leq k_i \leq n_i$, com $\sum_{1\leq i\leq m} k_i e_i = (0,0)$.*

**Dem.:** Seja $\left\{e_i^{'}\right\}_{1\leq i\leq m}$ a sequência de arestas de um fator $Q$ de $P$. Sabemos que cada aresta $ne$ de P pode ser decomposta, em relação à soma de Minkowski, pela soma de duas arestas paralelas a $e$ ou pela soma de uma aresta paralela a $e$ e um ponto. Assim $e^{'}$ deve ser da forma $ke$ com $0 \leq k \leq n$, logo $\left\{e_i^{'}\right\}_{1\leq i\leq m} = \{k_i e_i\}_{1\leq i\leq m}$ onde $1 \leq k_i \leq n_i$. A sequência de arestas $\{k_i e_i\}_{1\leq i\leq m}$ define um polígono fechado e será um fator de $P$, com o outro fator tendo sequência de arestas da forma $\{(n_i - k_i)\, e_i\}_{1\leq i\leq m}$. □

Dada uma sequência de arestas $\{n_i e_i\}_{1\leq i\leq m}$ o algoritmo de decomposição checará a existência de uma sequência de inteiros $k_i$, com $0 \leq k_i \leq n_i$ para $1 \leq i \leq m$, tal que $\sum_{1\leq i\leq m} k_i e_i = (0,0)$, com $k_m \neq n_m$ e algum $k_i \neq 0$.

**Exemplo 4.4.1.** *Seja $P$ o polígono da figura 4.4. Então seus vértices ordenados ciclicamente no sentido anti-horário são $v_0 = (0,0)$, $v_1 = (2,0)$, $v_3 = (2,2)$ e $v_4 = (0,2)$. Deste modo as arestas de $P$ são representadas pelos vetores $E_1 = (2,0)$, $E_2 = (0,2)$, $E_3 = (-2,0)$ e $E_4 = (0,-2)$. Os quais nos levam à seguinte sequência de arestas : $n_1 = 2$ e $e_1 = (1,0)$, $n_2 = 2$ e $e_2 = (0,1)$, $n_3 = 2$ e $e_3 = (-1,0)$, $n_4 = 2$ e $e_4 = (0,-1)$. Note que $\sum_{i=1}^{4} n_i e_i = (0,0)$. De acordo com o lema 4.4.1 para encontrarmos um fator do polígono $P$ precisaremos resolver a seguinte equação:*

$$k_1 e_1 + k_2 e_2 + k_3 e_3 + k_4 e_4 = (0,0) \text{ com } 0 \leq k_i \leq n_i \text{ para } 1 \leq i \leq 4. \tag{4.1}$$

*Note que $k_1 = \cdots = k_4 = 1$ satisfaz 4.1, então acabamos encontrando um fator $L = v_0 + \sum_{i=1}^{4} k_i e_i$ de $P$ representado na figura 4.4. Observe que o outro fator $M$ de $P$ tal que $P = M + L$ também é $M = v_0 + \sum_{i=1}^{4} k_i e_i$.*

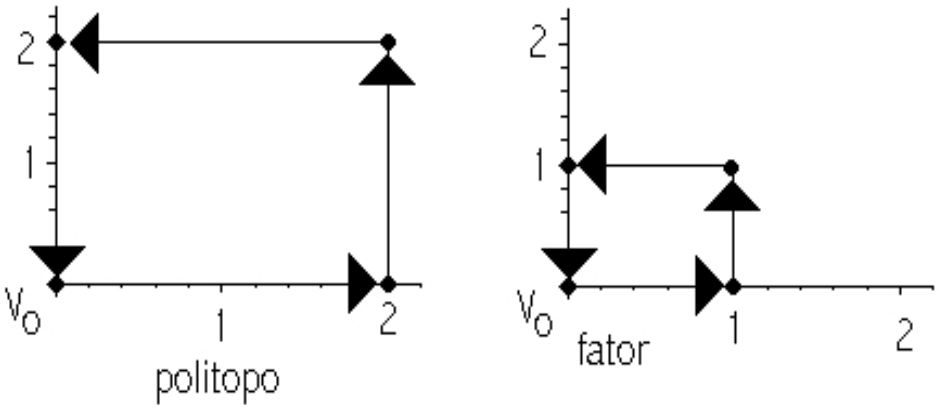


Figura 4.4: decomposição de politopos

**Observações**

1. Note que de acordo com o teorema 4.3.1 $L$ pode ser deslocado para dentro de $P$.

2. Note que cada aresta $a_P$ de $P$ vem da soma de uma aresta $a_L$ de $L$ com uma aresta $a_M$ de $M$ onde as arestas $a_P$,$a_L$ e $a_M$ são paralelas.

3. Note que $P$ é o politopo de Newton associado do polinômio $f = 1 + x^2 + y^2 + x^2y^2$. A pergunta que será respondida no capítulo 5 é: O fator $L$ do politopo $P$ corresponde ao politopo de Newton associado de um fator $g$ do polinômio $f$ ?

O problema que o algoritmo de decomposição irá resolver é

**Decomponibilidade do polígono**(POLIDECOMP)

**Entrada**: A sequência de arestas $\{n_i e_i\}_{1 \leq i \leq m}$ de um polígono convexo integral $P$.

**Questão**: $P$ tem uma decomposição integral ?

O tamanho da entrada deste problema é $O\left(m\left(logN + logE\right)\right)$ onde $N = max\left\{n_1, \ldots, n_m\right\}$ e $E$ o valor absoluto máximo das coordenadas de $e_i$, $1 \leq i \leq m$.

A proposição a seguir mostra a dificuldade deste problema.

**Proposição 4.4.1.** *POLIDECOMP é NP-completo*

**Dem.:** Certamente POLIDECOMP está em NP,pois dada uma decomposição própria $\{k_i e_i\}_{i=1}^{m}$ do polígono podemos verificá-la em tempo polinomial.

Para mostrarmos que POLIDECOMP é NP-completo, faremos uma redução polinomial do problema da Partição, que é sabido ser NP-completo, para POLIDECOMP. Vale lembrar que a entrada para Partição é uma sequência $\{s_i\}_{i=1}^{m}$ de inteiros positivos que podemos pegá-los em ordem não-decrescente, ou seja, $s_1 \leq s_2 \leq \ldots \leq s_m$. Seja $t = \sum_{i=1}^{m} s_i$, a questão em Partição é se existe uma subsequência de $\{s_i\}$ cuja soma dê $t/2$. Aqui assumimos que $t$ é par, para caso contrário a questão é facilmente respondida. Dada a sequência $\{s_i\}_{i=1}^{m}$ para partição, podemos transformá-la na seguinte sequência de arestas:

$$(s_1, 1), (s_2, 1), \ldots, (s_m, 1), m\,(0, -1), (-t/2, -1), (-t/2, 1)$$

onde verificamos que esta sequência dá um polígono, pois $\sum_{i=1}^{m+3} n_i e_i = (0, 0)$ com $n_{m+1} = m$ e $n_i = 1$ para o restante. Assim, o polígono associado a essa sequência de arestas possui decomposição própria se, e somente se, a sequência $\{s_i\}_{i=1}^{m}$ possui uma subseqência com soma $t/2$. Então temos uma redução polinomial, logo POLIDECOMP é NP-completo. □

A seguir apresentaremos um algoritmo que procura todos os fatores de um polígono $P \subset \mathbb{R}^2$ para verificar se $P$ é integralmente decomponível ou não. Usaremos a figura 4.4 como exemplo para explicarmos o que o algoritmo fará. Uma observação muito importante que deve ser feita é a de que o algoritmo irá procurar fatores de $P$ da forma $v_0 + \sum k_i e_i$, ou seja, se encontrarmos um fator $Q$ de $P$ então $Q \subseteq P$.

**Exemplo 4.4.2.** *Dado o polígono $P$ e sua sequência de arestas como no exemplo 4.4.1. Começaremos listando todos pontos integrais em $P$ e armazenando no conjunto $PI$. Então $PI = \{(0,0), (0,1), (0,2)(1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}$.*

*Começamos calculando todos os pontos integrais que são obtidos via* $e_1$ *saindo de* $v_0 = (0, 0)$*:*

- $v_0 + 0e_1 = (0, 0) \in PI$*;*
- $v_0 + 1e_1 = (1, 0) \in PI$*;*
- $v_0 + 2e_1 = (2, 0) \in PI$*.*

*Então, temos* $A_1 = \{(0, 0), (1, 0),(2, 0)\}$ *o conjunto de pontos integrais alcançados via* $e_1$*. Agora veremos que pontos integrais são alcançados via* $e_1$ *e* $e_2$*.*

- $(0, 0) + 0e_2 = (0, 0) \in PI$*;*
- $(0, 0) + 1e_2 = (0, 1) \in PI$*;*
- $(0, 0) + 2e_2 = (0, 2) \in PI$*;*
- $(1, 0) + 0e_2 = (1, 0) \in PI$*;*
- $(1, 0) + 1e_2 = (1, 1) \in PI$*;*
- $(1, 0) + 2e_2 = (1, 2) \in PI$*;*
- $(2, 0) + 0e_2 = (2, 0) \in PI$*;*
- $(2, 0) + 1e_2 = (2, 1) \in PI$*;*
- $(2, 0) + 2e_2 = (2, 2) \in PI$*;*

*Então os pontos integrais alcançados via* $e_1$ *e* $e_2$ *são:*

$$A_2 = \{(0, 0), (0, 1), (0, 2)(1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)\}.$$

*(Note que* $A_1 \subset A_2$*). Agora vamos para os pontos integrais que são alcançados via* $e_1$*,* $e_2$ *e* $e_3$*.*

- $(0,0) + 0e_3 = (0,0) \in PI$

  $(0,0) + 1e_3 = (-1,0) \notin PI$. *Este ponto integral é então descartado pois estamos procurando decomposições de* $P$ *contidas em* $P$.

*Prosseguindo como anteriormente temos que os pontos integrais alcançados via* $e_1$,$e_2$ *e* $e_3$ *são:*

$$A_3 = \{(0,0),(0,1),(0,2)(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}.$$

*(Note que* $A_2 \subset A_3$*). Do mesmo modo, os pontos integrais alcançados via* $e_1$,$e_2$,$e_3$ *e* $e_4$ *são:*

$$A_4 = \{(0,0),(0,1),(0,2)(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}.$$

*(Note que* $A_3 \subset A_4$*).*

*Podemos ver que* $v_0 = (0,0) \in A_4$. *Mas os pontos* $v$ *que estão em* $A_4$ *são da forma*

$$v = v_0 + k_1e_1 + k_2e_2 + k_3e_3 + k_4e_4.$$

*Então encontramos uma sequência* $\{k_ie_i\}$ *tal que* $v_0 = v_0 + k_1e_1 + k_2e_2 + k_3e_3 + k_4e_4$, *logo* $k_1e_1 + k_2e_2 + k_3e_3 + k_4e_4 = (0,0)$ *que pelo lema 4.4.1 sabemos que é um fator de* $P$. *Logo,* $P$ *é integralmente decomponível.*

**Algoritmo 4.4.1 (PoliDecomp).**
***Entrada****: A sequência de arestas* $\{n_ie_i\}_{1\leq i\leq m}$ *de um polígono convexo integral* $P$ *começando em um vértice* $v_0$ *onde* $e_i \in \mathbb{Z}^2$ *são vetores primitivos.*
***Saída****:* $P$ ***Decomponível*** *ou* ***Indecomponível****.*

1. *Calcular o conjunto* $PI$ *de todos os pontos integrais em* $P$, *e inicializar* $A_0 = \emptyset$.
2. ***Para cada*** $i$ ***de*** $1$ ***até*** $m-1$, *calcular o conjunto* $A_i$ *de pontos em* $PI$ *que são obtidos via os vetores* $e_1, \ldots, e_i$*:*

   ***Para cada*** $0 < k \leq n_i$ ***faça***

   ***Se*** $v_0 + ke_i \in PI$ ***então***

*acrescente-o a* $A_i$

***Para cada*** $u \in A_{i-1}$ ***e*** $0 \leq k \leq n_i$ ***faça***

***Se*** $u + ke_i \in PI$ ***então***

*acrescente-o a* $A_i$

*3. Calcular o último conjunto* $A_m$*:*

***Para cada*** $u \in A_{m-1}$ ***e*** $0 \leq k < n_m$ ***faça***

***Se*** $u + ke_m \in PI$ ***então***

*acrescente-o a* $A_m$

*4. Retorne* ***Indecomponível*** *se* $v_0 \notin A_m$ *e* ***Decomponível*** *caso contrário.*

**Teorema 4.4.1.** *O algoritmo acima decide corretamente decomponibilidade em* $O(tmN)$ *operações vetoriais onde* $t$ *é o número de pontos integrais em* $P$*,* $m$ *o número de arestas e* $N$ *o número máximo de pontos integrais em uma aresta.*

**Dem.:** Para provar que o algoritmo funciona observe que todos os pontos em $A_m$ são da forma $v_0 + \sum_{i=1}^{m} k_i e_i$ com $0 \leq k_i \leq n_i$. O passo 2.1 garante $k_i > 0$ para algum $i < m$(para eliminarmos a decomposição trivial nula) e o passo 3 assegura que $k_m < n_m$, isso pode ser feito pois se algum fator $M$ de $P$ possuir uma aresta $n_m e_m$ o outro fator $L$ de $P$, tal que $P = L + M$, não terá nenhum pedaço da aresta $e_m$ e este fator também será encontrado no algoritmo(note que $v_0 + ke_m \notin PI$ para $k > 0$). Se um dos pontos em $A_m$ é igual a $v_0$ então

$$v_0 = \sum_{i=1}^{m} k_i e_i + v_0 \text{ e assim } \sum_{i=1}^{m} k_i e_i = (0,0),$$

logo a sequência $k_i e_i$ forma uma sequência de arestas de um fator integral próprio de $P$. Seja $Q$ um fator integral próprio de $P$, então podemos transladar $Q$ para o vértice $v_0$ e assim colocá-lo em $P$, logo todos os pontos integrais de $Q$ estarão em $P$ e assim sua sequência de arestas será detectada pelo algoritmo.

O pior caso ocorre quando cada aresta alcança todos os pontos do politopo. Como o politopo tem $t$ pontos integrais e cada um deles pode ser alcançado $O(Nm)$ vezes, então o número de passos do algoritmo é $O(tmN)$. □

Observe que $t = O(N^m)$, logo, o número de passos do algoritmo 4.4.1 é exponencial. O exemplo a seguir mostra como o número de decomposições de um polígono pode ser exponencial.

**Exemplo 4.4.3.** *Considere o polígono com sequência de arestas*

$$(1,1),(2,1),\ldots,(m,1),m(0,-1),t(-1,0)$$

*onde* $t = (m+1)m/2$. *Para encontrarmos o número de decomposições, primeiro devemos observar que:* $e_1 = (1,1) \Rightarrow n_1 = 1$, $e_2 = (2,1) \Rightarrow n_2 = 1$,..., $e_m = (m,1) \Rightarrow n_1 = 1$ *e assim para termos um polígono fechado devemos ter:* $e_{m+1} = (0,-1) \Rightarrow n_{m+1} = m$ $e_{m+2} = (-1,0) \Rightarrow n_{m+2} = (m+1)m/2$, *e assim satisfazendo* $\sum_{i=1}^{m+2} n_i e_i = (0,0)$.

*Logo, nosso problema é: De quantas maneiras podemos resolver a seguinte equação?*

$$k_1(1,1)+k_2(2,1)+\cdots+k_m(m,1)+k_{m+1}(0,-1)+k_{m+2}(-1,0)=(0,0)$$

*onde* $0 \leq k_i \leq n_i$ *para* $1 \leq i \leq m+2$.

*Observe que:*

$$\underbrace{\underbrace{k_1(1,1)}_{2escolhas}+\cdots+\underbrace{k_m(m,1)}_{2escolhas}}_{2^m escolhas}+(0,-m)+(-t,0)=(0,0)$$

*Temos exatamente* $2^m$ *fatores integrais do polígono.*

Enquanto o algoritmo 4.4.1 retorna como resposta apenas se o polígono é decomponível ou não, o algoritmo que apresentaremos a seguir é uma generalização deste, no qual dado um polígono sua saída não será apenas um sim ou não e sim um array contendo o número de decomposições próprias do polígono e informações suficientes para contruir tais decomposições.

**Algoritmo 4.4.2.**

***Entrada***: *A sequência de arestas* $\{n_i e_i\}_{1 \leq i \leq m}$ *de um polígono convexo integral* $P$ *começando em um vértice* $v_0$ *onde* $e_i \in \mathbb{Z}^2$ *são vetores primitivos.*
***Saída***: *O número de fatores integrais de* $P$ *incluindo os triviais, e um array* $A$. *Cada célula em* $A$ *contém um par* $(u, S)$ *onde* $u$ *é um inteiro não negativo e* $S$ *é um subconjunto de* $\{(k, i) : 1 \leq k \leq n_i, 1 \leq i \leq m\}$.

1. *Calcular o conjunto* $PI$ *de todos os pontos integrais em* $P$ *(logo* $v_0 \in PI$*); digamos que* $PI$ *tem* $t$ *pontos. Inicialize um* $t$*-array* $A_0$ *indexado pelos pontos em* $PI$. *Inicialize* $A_0[v] := (0, \emptyset)$ *para todo* $v \in PI$ *exceto a célula* $A_0[v_0]$ *que é inicializada com* $(1, \emptyset)$.

2. ***Para*** $i$ ***de*** $1$ ***até*** $m$ ***faça***, *calcular o* $t$*-array* $A_i$ *de* $A_{i-1}$

   *Primeiro copie o conteúdo de todas as células de* $A_{i-1}$ *para* $A_i$ *(este passo é para* $k = 0$*).*

   ***Para cada*** $v \in PI$ *com o primeiro número da célula* $A_{i-1}[v]$ *não nulo* ***faça***

   ***Para cada*** $0 < k \leq n_i$ ***faça***

   ***Se*** $v' = v + ke_i \in PI$ ***então***

   *reescreva a célula* $A_i[v']$ *como segue:*

   ***Se*** $(u_1, S_1)$ *é o valor de* $A_{i-1}[v]$ *e* $(u_2, S_2)$ *é o valor atual de* $A_i[v']$ ***então***

   *o novo valor de* $A_i[v']$ *é* $(u_1 + u_2, S_2 \cup \{(k, i)\})$.

3. *Retorne o número* $u$ *e o array* $A = A_m$, *onde* $(u, S)$ *é o conteúdo da célula* $A_m[v_0]$.

**Teorema 4.4.2.** *O inteiro na saída do algoritmo acima é o número total de fatores integrais do polígono P.*

**Dem.:** Note que no final da $i$-ésima iteração $v = v_0 + k_1e_1 + \cdots + k_ie_i$ onde $0 \leq k_i \leq n_i$, ou seja, descrevemos um caminho de $v_0$ até $v$ usando as arestas $e_1, \ldots, e_i$. Na célula $A_i[v]$ armazenamos o número inteiro positivo $u$ que nos diz de quantas maneiras diferentes saimos de $v_0$ e chegamos até $v$. Enquanto o conjunto $S$ armazena pares $(k, j)$,$0 < k \leq n_j$, com $j \leq i$ que nos dizem que em um dos caminhos que unem $v$ e $v_0$ a última aresta usada foi $ke_j$.

No final do algoritmo o inteiro $u$ na célula $A_m[v_0]$ nos diz o número de caminhos fechados da forma $v_0 + \sum_{i=1}^{m} k_ie_i = v_0$, incluindo os triviais, e pelo lema 4.4.1 este é o número de fatores integrais de $P$. □

**Como encontrar a decomposição a partir do array $A$?**

Quando o algoritmo retorna o array $A$, a célula $A[v_0]$ contém o par $(u, S)$. Para recuperarmos uma decomposição do polígono, escolhemos um par $(k, i)$ do conjunto $S$ e este nos leva ao segmento de linha $ke_i$ que será a última aresta de nossa decomposição de $P$. Para encontrarmos a penúltima aresta, vamos até a célula $A[v_0 - ke_i] = \left(u', S'\right)$ e pegamos um par $\left(k', i'\right)$ de $S'$ tal que $i' < i$ e assim o segmento de linha $k'e_{i'}$ será nossa penúltima aresta na decomposição. Continuando este processo criaremos uma sequência $i > i' > i'' > \cdots$ decrescente que nos levará até a célula $A[v_0]$ novamente. Então teremos uma decomposição do polígono $P$.

**Exemplo 4.4.4.** *Seja $P$ o polígono com sequência de arestas*

$$n_1 = 2, e_1 = (0, 2), n_2 = 1, e_1 = (2, 1), n_3 = 2, e_3 = (0, -1), n_4 = 1, e_4 = (-2, -1)$$

*com $v_0 = (0, 0)$. Após aplicarmos o algoritmo a este polígono, nossa saída será a seguinte:*

$A = [A[(0,0)] = (6; (1,3) \cup (2,3) \cup (1,4))$; $A[(0,1)] = (4; (1,1) \cup (1,3) \cup (1,4))$; $A[(1,1)] = (0, \emptyset)$; $A[(2,1)] = (3; (1,2) \cup (1,3) \cup (2,3))$; $A[(0,2)] = (2; (2,1) \cup (1,4))$; $A[(1,2)] = (0, \emptyset)$; $A[(2,2)] = (2; (1,2) \cup (1,3))$; $A[(2,3)] = [(1; (1,2))]$.

*Para recuperarmos uma decomposição própria do Polígono $P$ vamos até a célula:*

$$A\left[(0,0)\right] = (6; (1,3) \cup (2,3) \cup (1,4))$$

*agora escolhemos um par $(k,i)$, que pode ser o par $(1,4)$. Este par diz que para chegarmos no ponto $(0,0)$, o último segmento de aresta usado foi o $1e_4$, ou seja que nós estavamos no ponto $(0,0) - 1e_4 = (2,1)$. Então, vamos para a célula $A\,(2,1)$:*

$$A\left((0,0) - 1e_4\right) = A\,(2,1) = (3; (1,2) \cup (1,3) \cup (2,3))$$

*Agora escolhemos um par $(k,i)$ tal que $i < 4$, pois já usamos a aresta $e_4$. Seja o par $(1,3)$, ele diz que para chegarmos no ponto $(2,1)$ usamos o segmento de aresta $1e_3$, ou seja, que estavamos no ponto $(2,1) - 1e_3 = (2,2)$. Então, vamos para a célula $A\,(2,2)$:*

$$A\left[(2,2)\right] = (2; (1,2) \cup (1,3))$$

*Agora escolhemos um par $(k,i)$ tal que $i < 3$, pois já usamos a aresta $e_3$. Seja o par $(1,2)$, ele diz que para chegarmos no ponto $(2,2)$ usamos o segmento de aresta $1e_2$, ou seja, que estavamos no ponto $(2,2) - 1e_2 = (0,1)$. Então, vamos para a célula $A\,(0,1)$:*

$$A\left[(0,1)\right] = (4; (1,1) \cup (1,3) \cup (1,4))$$

*Agora escolhemos um par $(k,i)$ tal que $i < 2$, pois já usamos a aresta $e_2$. Seja o par $(1,1)$, ele diz que para chegarmos no ponto $(0,1)$ usamos o segmento de aresta $1e_1$, ou seja, que estavamos no ponto $(0,1) - 1e_1 = (0,0)$. Assim, acabamos recuperando a seguinte decomposiçã própria do polígono:*

$$(0,0) - 1e_4 - 1e_3 - 1e_2 - 1e_1 = (0,0)\,.$$

*Deste modo podemos recuperar todas as decomposições próprias do polígono $P$, fazendo todas as combinações possíveis dos pares $(k,i)$, respeitando as condições necessárias.*

Gostaríamos de mencionar que quando encontramos algum fator integral $P_g$ de $P_f$, ele não necessariamente corresponde a um fator $g$ de $f$. Por Exemplo:

**Exemplo 4.4.5.** *Seja*

$$f := (a + bx^n) + y^m (c + dx^n) \in \mathbb{K}[x, y].$$

*Seu politopo de Newton é o retângulo definido pelos vértices* $(0,0)$,$(n,0)$,$(n,m)$, *e* $(0,m)$. *Para decompor este retângulo estamos interessados em resolver a seguinte equação*

$$k_1 (1,0) + k_2 (0,1) + k_3 (-1,0) + k_4 (0,-1) = (0,0) \text{ com}$$

$$0 \leq k_1 \leq n,$$

$$0 \leq k_2 \leq m,$$

$$0 \leq k_3 \leq n \text{ e}$$

$$0 \leq k_4 \leq m.$$

*ou seja, resolvermos* $\left( \underbrace{k_1 - k_3}_{n+1}, \underbrace{k_2 - k_4}_{m+1} \right) = (0,0)$.

*Logo, teremos* $(n+1)(m+1)$ *fatores integrais de* $P_f$. *Porém* $f$ *é quase sempre irredutível, salvo alguns poucos casos.*

Faremos agora um exemplo utilizando os resultados até agora vistos o qual nos motivará para a seção seguinte.

**Exemplo 4.4.6.** *Seja* $f = (x^{10}y^4 + x) z^5 + x^7y^2z^3 + x^2y^2z^2 + y^3z + x^2y^3 \in \mathbb{R}$, *assim o*

$$Newt(f) = conv((10,4,5), (1,0,5), (7,2,3), (2,2,2), (0,3,1), (2,3,0)).$$

*Definamos* $\pi$ *sendo a projeção no plano* $xy$ *e assim*

$$\pi(Newt(f)) = conv((10,4), (1,0), (7,2), (2,2), (0,3), (2,3)).$$

*Utilizando o algoritmo 4.2.1 encontramos que os vértices do* $\pi(Newt(f))$ *ordenados no sentido anti-horário são* $(10,4)$,$(0,3)$,$(1,0)$,$(7,2)$. *Os quais têm somente uma pré-imagem no* $Newt(f)$. *Aplicando o algoritmo 4.4.1 no* $\pi(Newt(f))$ *descobrimos*

*que este é integralmente indecomponível. Logo, as condições do lema 3.4.1 são satisfeitas e podemos concluir que o* $Newt\,(f)$ *é integralmente indecomponível. Deste modo, segue que* $f$ *é absolutamente irredutível.*

## 4.5 Politopos de Alta Dimensão

Nesta seção será apresentado um algoritmo, para politopos em $\mathbb{R}^n$, motivado pelo lema 3.4.1. A idéia será escolher uma transformada linear integral que leve o politopo $P$ de $\mathbb{R}^n$ para um polígono $\pi(P)$ no plano e então verificar se as condições do lema são satisfeitas. Isto é, checar se o polígono $\pi(P)$ é integralmente indecomponível e se cada vértice de $\pi(P)$ tem somente uma pré imagem em $P$, se as condições forem satisfeitas então podemos dizer que $P$ é integralmente indecomponível.

Representaremos pontos em $\mathbb{R}^n$ como vetores coluna:

$x \in \mathbb{R}^n$ então $x = \begin{pmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_n \end{pmatrix}$ com $x_1, \ldots, x_n \in \mathbb{R}$. Assim, um conjunto $S$ de $l$ pontos em $\mathbb{R}^n$ pode ser representado por uma matriz $n \times l$ onde cada coluna representa um ponto.

Sejam $u, v \in \mathbb{R}^n$ dois pontos integrais. Então dado um ponto $w \in \mathbb{R}^n$, o produto $(u, v)^t w$ pode ser visto como um ponto em $\mathbb{R}^2$. Isto define uma transformação integral

$$\pi : \mathbb{R}^n \longrightarrow \mathbb{R}^2$$

e

$$(u, v)^t \, S \tag{4.2}$$

é a imagem de $S$ sob $\pi$ em $\mathbb{R}^2$. O polígono definido pela envoltória convexa dos pontos em 4.2 é dito polígono sombra, ou simplesmente sombra, de $P$ transformado por $u$ e $v$.

Pelo lema 3.4.1 notamos que a condição de que cada vértice de $\pi(S) \subset \mathbb{R}^2$ tenha somente uma pré imagem em $S$ é necessária, por isso o lema a seguir dá uma idéia da probabilidade de escolhermos aleatoriamente pontos $u$ e $v$ em $\mathbb{R}^n$ que levem a uma transformada injetiva.

**Lema 4.5.1.** *Seja $S$ uma matriz $n \times l$ sobre um corpo sem colunas repetidas e seja $K$ qualquer subconjunto de cardinalidade $k$ do mesmo corpo. Pegue $u_i \in K$ aleatoriamente e independentemente, $1 \leq i \leq n$, e seja*

$$(a_1, \ldots, a_l) = (u_1, \ldots, u_n)\, S.$$

*Então com probabilidade de no mínimo $1 - \dfrac{l(l-1)}{2k}$ as entradas $a_1, \ldots, a_l$ são distintas.*

**Dem.:** Diremos que um vetor é distinto se todas suas entradas são distintas, e um vetor é constante se todas suas entradas são iguais. Provaremos o lema por indução sobre $l$. Quando $l = 1$, o lema é trivial. Seja $l > 1$. Assuma que o lema é satisfeito para todas matrizes com menos que $l$ colunas. Já que $l > 1$, nem todas as linhas de $S$ são constantes. Também, linhas constantes podem ser descartadas. Logo a primeira linha de $S$ pode ser assumida não constante. Particionamos as colunas de $S$ por seus valores das entradas na primeira linha. Permutando as colunas de $S$, podemos assumir que $S$ é da forma

$$\begin{pmatrix} r_1 \ldots r_1 & \cdots & r_t \ldots r_t \\ S_1 & \cdots & S_t \end{pmatrix}$$

onde $t \geq 2$. $S_i$ tem $l_i$ colunas com $l_1 + \cdots + l_t = m$, e $(r_1, \ldots, r_t)$ é distinto. Já que $S$ não tem colunas repetidas, $S_i$ também não tem para $1 \leq i \leq t$. Observe que $(a_1, \ldots, a_l)$ é distinto sse

1. para cada $1 \leq i \leq t$, $(u_2, \ldots, u_n)\, S_i$ é distinto; e

2. para cada par $1 \leq i < j \leq t$, cada entrada de $u_1(r_i, \ldots, r_i) + (u_2, \ldots, u_n)S_i$ é distinta de toda entrada de $u_1(r_j, \ldots, r_j) + (u_2, \ldots, u_n)S_j$.

Pela hipótese de indução, temos

$$Prob((u_2, \ldots, u_n)\, S_i \text{ é distinto}) \geq 1 - \frac{l_i\,(l_i - 1)}{2k} \text{ para } 1 \leq i \leq t,$$

logo

$$Prob((1) \text{ ser satisfeito }) \geq 1 - \sum_{i=1}^{t} \frac{l_i\,(l_i - 1)}{2k}.$$

Agora, calculamos a probabilidade do ítem 2 ser satisfeito sobre as condições do ítem 1 satisfeitas. Precisamos encontrar a probabilidade do ítem 2 ser satisfeito dada qualquer escolha de $u_2, \ldots, u_n$. Para qualquer par $1 \leq i < j \leq t$, qualquer coluna $w_1$ de $S_i$ e qualquer coluna $w_2$ de $S_j$, se

$$u_1 r_i + (u_2, \ldots, u_n)\, w_1 = u_1 r_j + (u_2, \ldots, u_n)\, w_2,$$

então

$$u_1 = (u_2, \ldots, u_n)\,(w_2 - w_1)\,/\,(r_i - r_j)\,,$$

como $r_i \neq r_j$. Logo $u_1$ deve evitar estes valores quando pertencer a $S_1$. O número desses valores possíveis é no máximo

$$l = \sum_{1 \leq i < j \leq t} l_i l_j.$$

Então, para qualquer escolha de $u_2, \ldots, u_n$, a probabilidade do ítem 2 ser satisfeito é no mínimo $1 - l/k$,i.é.,

$$Prob(\ (2) \text{ ser satisfeito} : (1) \text{ é satisfeito }) \geq 1 - \frac{l}{k}.$$

Além disso

$$Prob((a_1, \ldots, a_m) \text{ ser distinto })$$

$$= Prob((1) \text{ e } (2) \text{ serem satisfeitos})$$

$$= Prob((1) \text{ ser satisfeito}).Prob((2) \text{ ser satisfeito} : (1) \text{ é satisfeito})$$

$$\geq \left( \geq 1 - \sum_{i=1}^{t} \frac{l_i\,(l_i - 1)}{2k} \right) \left( 1 - \frac{l}{k} \right)$$

$$1- \geq 1 - \sum_{i=1}^{t} \frac{l_i\,(l_i-1)}{2k} - \frac{l}{c} = 1 - \frac{m\,(m-1)}{2k}$$

como $l_1 + \cdots + l_t = m$. Isto completa a prova. □

Por exemplo, $K = \{-l^2, \ldots, -1, 0, 1, \ldots, l^2\}$ tem $k = 2l^2+1$ inteiros. Se escolhermos as componentes de $u$ e $v$ de $K$ aleatoriamente. Então com probabilidade de no mínimo 3/4 os pontos em 4.2 são distintos, logo a condição do lema 3.4.1 é satisfeita, isto é, cada vértice da sombra tem somente uma pré imagem em $S$. Esta probabilidade pode ser aumentada arbitrariamente para perto de 1 se aumentarmos o tamanho do conjunto $K$.

**Algoritmo 4.5.1.**

***Entrada****: Um conjunto finito $S$ de pontos integrais de $\mathbb{R}^n$.*

***Saída****: **Indecomponível** ou **Falhou**. O primeiro caso significa que o politopo $P = conv\,(S)$ é provado ser indecomponível, enquanto o último significa que a decomponibilidade de $P$ não está decidida.*

1. ***Passo****: Organize os pontos em $S$ como uma matriz $n \times l$, ainda denotado por $S$, onde $l$ representa o número de linhas de $S$ e cada coluna representa um ponto. Fixe um conjunto $K$ de inteiros pequenos.*

2. ***Passo****: Escolha dois vetores $u, v \in K^n$ aleatoriamente e calcule a projeção $(u, v)^t\, S = (a_1, \ldots, a_l)$ onde $a_i \in \mathbb{Z}^2$.*

3. ***Passo****: Calcular os vértices, digamos $v_1, \ldots, v_m$ na direção anti-horário, do polígono convexo definido pelos pontos $a_1, \ldots, a_l$. Se mais que dois pontos de $S$ são transformados em um dos vértices $v_i's$, então retorne **Falhou** e pare aqui.*

4. ***Passo****: Calcular $E_i = v_i - v_{i-1} = n_i e_i$ onde $n_i$ é um inteiro positivo e $e_i$ é um vetor primitivo, $1 \leq i \leq m$.*

5. ***Passo****: Entre com a sequência de arestas $\{n_i e_i\}$ no Algoritmo **PoliDecomp**. Se o último diz **Indecomponível** então retorne **Indecomponível**, caso contrário retorne **Falhou**.*

Mesmo que o politopo seja integralmente indecomponível o algoritmo 4.5.1 pode falhar, embora com probabilidade pequena de acordo com o lema 4.5.1. Se o politopo for decomponível então o algoritmo sempre retornará falhou. De fato a questão de decidir a decomponibilidade de politopos é um problema difícil, como pode ser visto no trabalho [21], onde é apresentado um politopo indecomponível cujas faces são todas decomponíveis. Portanto, é possível que exista algum politopo indecomponível cujos polígonos sombra sempre serão decomponíveis e então o algoritmo nunca obterá êxito.

# 5 FATORANDO POLINÔMIOS VIA POLITOPOS

Neste capítulo final, vamos aplicar todos os resultados até aqui estudados em um problema clássico da álgebra: a fatoração de polinômios. Mais especificamente, estudaremos o algoritmo desenvolvido por Fatima Abu Salem, Shuhong Gao e Alan G. B. Lauder em [18, 19] que fatora um dado polinômio bivariado $f$ a partir da decomposição do seu politopo de Newton associado.

## 5.1 Introdução

Neste capítulo estudaremos um método para fatorar um polinômio bivariado a partir de informações a respeito do seu politopo de Newton associado, como feito por Fatima Abu Salem, Shuhong Gao e Alan G. B. Lauder em [18].

Como foi estudado no capítulo 3, o politopo de Newton associado ao polinômio multivariado $f$ carrega muitas informações a respeito de $f$. Por exemplo, quando o politopo de Newton associado ao polinômio $f$ é integralmente indecomponível então $f$ é absolutamente irredutível. Porém não sabíamos responder se quando o politopo de Newton associado a $f$ fosse integralmente decomponível se $f$ seria redutível ou não.

No artigo [6] que foi estudado no capítulo 4 é apresentado um algoritmo que encontra todas as decomposições integrais de um politopo em $\mathbb{R}^2$. A pergunta que ficara em aberto e que foi respondida em [18], e que será estudada no presente capítulo, é se um dado fator integral do politopo de newton associado a $f$ corresponde a um fator do polinômio bivariado $f$.

Estudaremos o algoritmo feito em [18] que é uma modificação do levantamento de Hensel. Este algoritmo procura um fator $g$ de um polinômio bivariado $f$ a partir de um fator do politopo de Newton associado a $f$. Como será visto, o

algoritmo não funcionará para todos os polinômios, e sim para aqueles que são livre de quadrados sobre certos subconjuntos das arestas de seus politopos de Newton.

Na seção 5.2 estudaremos o problema central do capítulo e na seção 5.3 poderemos notar a similaridade do problema que estamos estudando com o levantamento de Hensel padrão. Na seção 5.4 estudaremos um lema chave para o algoritmo de fatoração via politopos, o qual será apresentado na seção 5.5.

## 5.2 Fatoração Parcial

De agora em diante estaremos trabalhando apenas com polinômios bivariados, e assim $f$ sempre representará um polinômio em $\mathbb{F}[x, y]$. Para $e = (e_1, e_2) \in \mathbb{N}^2$, o termo $x^{e_1}y^{e_2}$ será representado por $x^e$ e o politopo de Newton associado a $f$ será denotado por $P_f$ ou $Newt(f)$.

Dado $f$ um polinômio em $\mathbb{F}[x, y]$ podemos encontrar uma decomposição integral para seu politopo de Newton associado usando o algoritmo 4.4.2, ou seja, $Newt(f) = Q + R$ com $Q$ e $R$ polígonos integrais no primeiro quadrante. Como estamos interessados em saber se $Q$ e $R$ representam politopos de Newton de fatores de $f$ podemos associar a cada ponto integral $q$ de $Q$ e $r$ de $R$ as indeterminadas $g_q$ e $h_r$. Isso nos leva a definir

$$g := \sum_{q \in Q} g_q X^q$$
$$h := \sum_{r \in R} h_r X^r.$$

Diremos que $g$ e $h$ são os polinômios genéricos associados à decomposição $Newt(f) = Q + R$. Nosso objetivo será determinar os valores de $g_q$ e $h_r$ para que $f = gh$.

**Exemplo 5.2.1.** *Seja* $f := x^2 + y^2 + x^3 + x^3y^2 \in \mathbb{R}[x, y]$.

*Então usando o algoritmo 4.4.2 encontramos uma decomposição integral do polígono* $Newt(f) = Q + R$ *onde* $Q$ *e* $R$ *estão ilustrados na figura 5.1. Logo, os polinômios genéricos dados pela decomposição integral são:* $g := g_{20}x^2 + g_{11}xy + g_{12}xy^2 + g_{02}y^2 + g_{12}xy^2 + g_{22}x^2y^2$ *e* $h := h_{00} + h_{10}x$.

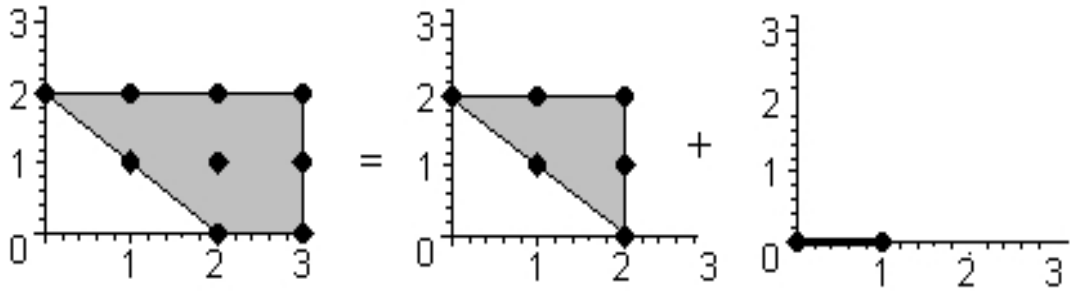


*Figura 5.1: polinômios genéricos*

Seja $\#Newt(f)$ o número de pontos integrais no $Newt(f)$. Para descobrirmos se a decomposição leva a fatores de $f$ poderíamos multiplicar os polinômios genéricos $g$ e $h$ e igualarmos a $f$. A igualdade $f = gh$ nos leva a um sistema de $\#Newt(f)$ equações nas indeterminadas $g_q$ e $h_r$, obtidas quando igualamos os coeficientes de cada monômio $x^e$ com $e \in Newt(f)$ em ambos os lados da igualdade.

Mas o objetivo de agora em diante não será apenas o de resolver este sistema e sim, apresentar um modo eficiente de resolvê-lo.

Antes de prosseguirmos gostaríamos de dar uma idéia de como será feita a fatoração via politopos. Como pode ser visto no apêndice A o levantamento de Hensel de um polinômio $f = \sum f_i(x)y^i \in \mathbb{F}[x, y]$ constrói uma fatoração $f = gh$, onde $g = \sum g_i(x)y^i$ e $h = \sum h_i(x)y^i$, a partir de uma fatoração inicial $f_0(x) = g_0(x)h_0(x)$ e depois vai encontrando os termos dos fatores $g$ e $h$ do tipo $g_1(x)y^1$ e $h_1(x)y^1$,$g_2(x)y^2$ e $g_2(x)y^2$ e assim por diante. Ou seja, é feito um levantamento horizontal e os termos em $y$ vão aparecendo sucessivamente como ilustrado na esquerda da figura 5.2. Na fatoração via politopos já temos o formato dos possíveis fatores $g$ e $h$ de $f$, ou seja, já sabemos quais são seus possíveis termos usando os polinômios genéricos dados pela decomposição do $Newt(f)$. Então motivado pelo levantamento de Hensel estudaremos uma mudança de variável que levará a começarmos a determinar os coeficientes dos termos de $g$ e $h$ que correspondem a expoentes vetoriais que estão sobre as arestas e vamos subindo ao longo do politopo como está ilustrado na figura 5.2, à direita.

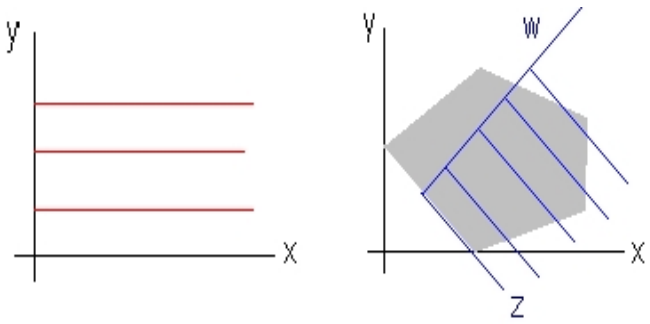


Figura 5.2: levantamento

Como foi descrito acima, os coeficientes dos termos dos possíveis fatores $g$ e $h$ da $f$ serão determinados gradativamente a partir de um conjunto de arestas, isso nos leva à seguinte definição.

**Definição 5.2.1.** *Seja $S$ um subconjunto do $Newt(f)$. Uma $S$-fatoração parcial da $f$ é uma determinação de um subconjunto das indeterminadas $g_q$ e $h_r$ tal que para cada ponto integral $s \in S$ os coeficientes dos monômios $X^s$ nos polinômios $gh$ e $f$ são iguais.*

**Exemplo 5.2.2.** *Referindo-se ao exemplo 5.2.1, seja $S = \{(2,0),(1,1),(1,2)\}$. Então quando igualamos os coeficientes dos monômios $x^s$ tal que $s \in S$ obtemos*

$$\begin{aligned} x^2 = h_{00}g_{20}x^2 \quad & logo \quad h_{00}g_{20} = 1 \\ x^2y = h_{00}g_{21}x^2y + h_{10}xg_{11}xy \quad & logo \quad h_{00}g_{21} + h_{10}g_{11} = 1 \\ x^2y^2 = h_{00}g_{22}x^2y_2 + h_{10}xg_{12}xy^2 \quad & logo \quad h_{00}g_{22} + h_{10}g_{12} = 1 \end{aligned}$$

O caso $S =$ pontos integrais do $Newt(f)$ é equivalente a uma fatoração da $f$ no sentido tradicional, e nos referiremos a ela como uma fatoração completa. Agora suponha que tenhamos uma $S$-fatoração parcial e uma $S'$-fatoração parcial e que além disso $S \subset S'$ e que as indeterminadas determinadas na $S$-fatoração parcial foram determinadas no mesmo corpo de elementos da $S'$-fatoração parcial.

Então diremos que a $S'$-fatoração parcial estende a $S$-fatoração parcial. Chamaremos de extensão própria se $S'$ tiver estritamente mais pontos integrais que $S$.

Denotaremos o conjunto de todas as arestas do $newt\,(f)$ por $Edge\,(f)$. Cada aresta $\delta \in Edge\,(f)$ será vista como um segmento de reta de um vértice $(u_1, v_1)$ para um vértice $(u_2, v_2)$, onde $(u_1, v_1)$ é dito o vértice inicial da aresta.

Sejam $d = mdc\,(u_2 - u_1, v_2 - v_1)$, $u_0 = (u_2 - u_1)\,/d$, e $v_0 = (v_2 - v_1)\,/d$. Então $(u_0, v_0)$ representa a direção de $\delta$ e os pontos integrais sobre $\delta$ são da forma

$$(u_1, v_1) + i\,(u_0, v_0) \text{ para } 0 \leq i \leq d,$$

de acordo com o lema 3.3.1. Sejam $(\gamma_1, \gamma_2) = (-v_0, u_0)$, uma rotação de 90 graus do vetor $(u_0, v_0)$ no sentido anti-horário, pois assim $(\gamma_1, \gamma_2)$ apontará para dentro do politopo como ilustrado na figura 5.3.

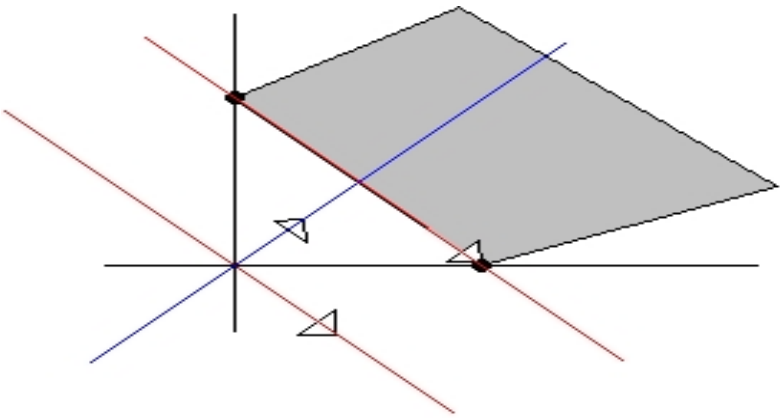

Figura 5.3: vetores

Seja $h_\delta = \langle (u_1, v_1), (\gamma_1, \gamma_2) \rangle$, onde $h_\delta$ é a função suporte de $\delta$. Definimos

$$\ell\,(e) = \gamma_1 e_1 + \gamma_2 e_2 - h_\delta \text{ para } e = (e_1, e_2) \in \mathbb{R}^2.$$

**Exemplo 5.2.3.** *Referindo-se ao exemplo 5.2.1, seja $\delta \in Edge(f)$ tal que $\delta$ vai de $(0,2)$ a $(2,0)$ então $\ell_\delta = e_1 + e_2 - 2$. Note que $\ell_\delta \geq 0$ para todo $e \in Newt(f)$:*

$$\ell_\delta(1,2) = 1 + 2 - 2 = 1, \quad \ell_\delta(3,2) = 3 + 2 - 2 = 3, \quad \text{e } \ell_\delta(2,0) = 2 + 0 - 2 = 0.$$

*E que* $\ell_\delta = 0$ *para* $e \in \delta$.

Deste modo podemos observar que $\ell$ tem a seguinte propriedade.

**Proposição 5.2.1.** *Seja* $Newt(f)$ *o polígono construído no sentido anti-horário, então* $\ell(e) \geq 0$ *para cada ponto* $e \in Newt(f)$*, valendo a igualdade se* $e \in \delta$

**Dem.:** Note que $(\gamma_1, \gamma_2)$ aponta para dentro do $Newt(f)$, logo $Newt(f) \subset H^+$, assim, dado $e \in Newt(f)$,

$$\langle (\gamma_1, \gamma_2), (e_1, e_2) \rangle \geq h_\delta,$$

logo, $\langle (\gamma_1, \gamma_2), (e_1, e_2) \rangle = h_\delta + r$ para algum $r \geq 0$, assim $\ell(e) = \langle (\gamma_1, \gamma_2), (e_1, e_2) \rangle - h_\delta = r \geq 0$. Agora se $e \in \delta$ então $\langle (\gamma_1, \gamma_2), (e_1, e_2) \rangle = h_\delta$,logo $\ell(e) = 0$. □

**Definição 5.2.2.** *Com a notação acima dizemos que* $\ell$ *é a função primitiva afim associada com* $\delta$ *, denotada por* $\ell_\delta$.

A função $\ell_\delta$ também tem a seguinte propriedade. Como $mdc(\gamma_1, \gamma_2) = 1$ então pelo algoritmo de Euclides existem únicos $\sigma_1$ e $\sigma_2$ tais que

$$\sigma_1\gamma_1 + \sigma_2\gamma_2 = 1 \tag{5.1}$$

sob a condição de que $0 \leq \sigma_2 < \gamma_1$.

Como pode ser visto na figura 5.4 o $Newt(f)$ é cortado pelas retas $\ell_\delta = i$ onde $i$ é um inteiro não negativo. Além disso, podemos observar que todos os pontos integrais do politopo estarão sobre estas retas.

Conforme a figura 5.5 cada ponto integral $(e_1, e_2)$ do $Newt(f)$ pode ser escrito em função dos vetores $(u_0, v_0)$ e $(\gamma_1, \gamma_2)$ de uma aresta qualquer do $Edge(f)$. Então

$$(e_1, e_2) := w(u_0, v_0) + \frac{\alpha(\gamma_1, \gamma_2)}{\|(\gamma_1, \gamma_2)\|} \tag{5.2}$$

onde $\alpha = e_1\gamma_1 + e_2\gamma_2$. De acordo com 5.1 temos que $\gamma_1\sigma_1 + \gamma_2\sigma_2 = 1$, ou seja, $(-v_0)\sigma_1 + u_0\sigma_2 = 1$. Multiplicando 5.2 por $(\sigma_2, -\sigma_1)$ temos que

$$e_1\sigma_2 - e_2\sigma_1 = w + \underbrace{\alpha(\gamma_1, \gamma_2)(\sigma_2, -\sigma_1)/\|(\gamma_1, \gamma_2)\|}_{\text{termo constante sobre cada reta paralela a } (u_0, v_0)}.$$

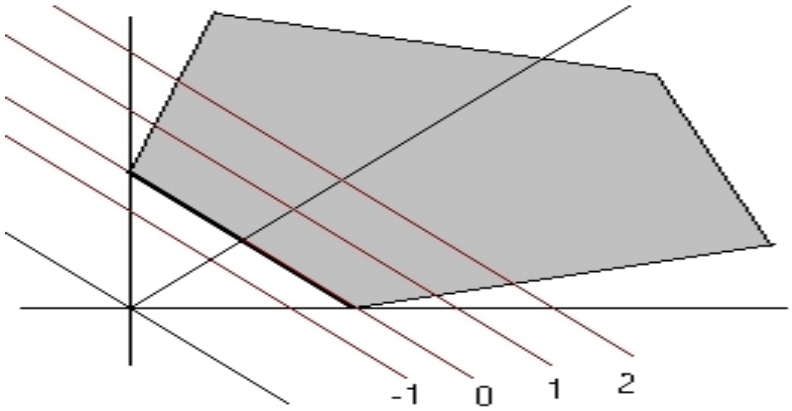


Figura 5.4: arestas

Então $w = e_1\sigma_2 - e_2\sigma_1 + constante$ em cada reta paralela a $(u_0, v_0)$. Deste modo qualquer monômio da forma $x^{e_1}y^{e_2}$ pode ser escrito como $x^{e_1}y^{e_2} = z^{i_1}w^{i_2}$, onde

$$\begin{pmatrix} i_1 \\ i_2 \end{pmatrix} = \begin{pmatrix} \sigma_2 & -\sigma_1 \\ \gamma_1 & \gamma_2 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

cuja transformada inversa é

$$\begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} \gamma_2 & \sigma_1 \\ -\gamma_1 & \sigma_2 \end{pmatrix} \begin{pmatrix} i_1 \\ i_2 \end{pmatrix}$$

Esta mudança de variável tem as seguintes propriedades:

Quando $e \in \delta$, então $e = (u_1, v_1) + i(u_0, v_0)$. Note que $i_2 = \gamma_1 e_1 + \gamma_2 e_2 = \ell_\delta(e) + h_\delta$ permanece constante ($i_2 = h_\delta$). Enquanto $i_1 = \sigma_2 e_1 - \sigma_1 e_2 = \sigma_2 u_1 \sigma_1 v_1 + i(\underbrace{\sigma_2 u_0 - \sigma_1 v_0}_{=1})$, ou seja, o expoente de $z$ aumenta para cada incremento de $(u_0, v_0)$. Observe que a mudança de variável funciona do mesmo jeito para as arestas paralelas a $\delta$.

**Exemplo 5.2.4.** *Referindo-se ao exemplo 5.2.1. Seja $\delta$ a aresta do $Newt(f)$ que vai do vértice $(0, 2)$ ao vértice $(2, 0)$. Então $\ell_\delta(e) = e_1 + e_2 - 2$, $i_1 = -e_2$ e $i_2 = e_1 + e_2$. Fazendo a mudança de variável em $f$ chegamos a*

$$f = w^2 + z^{-2}w^2 + w^3 + z^{-2}w^5$$

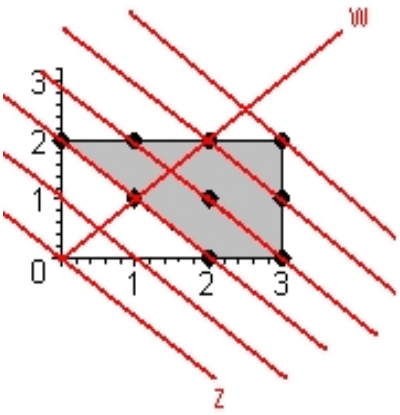


*Figura 5.5: mudança de variável*

Pelo teorema 2.4.1 sabemos que para cada $\delta \in Newt(f)$ existe um único par de faces(sendo arestas ou vértices) $\delta' \in Q$ e $\delta'' \in R$ tal que $\delta = \delta' + \delta''$. Pela propriedade 5.2.1 podemos definir $\delta$ da seguinte maneira

$$\delta = \{e \in Newt(f) : \ell_\delta(e) = 0\}$$

pelo teorema 2.4.1 sabemos que $h_\delta = h_{\delta'} + h_{\delta''}$ e assim

$$\delta' = \{e \in Q : \ell_\delta(e) = h_{\delta'} - h_\delta\}$$

e

$$\delta'' = \{e \in R : \ell_\delta(e) = -h_{\delta'}\}.$$

**Exemplo 5.2.5.** *Referindo-se ao exemplo 5.2.1, seja $\delta$ a aresta do $Newt(f)$ que vai do vértice $(0,2)$ ao vértice $(2,0)$. Então*

$$\delta' = \{e \in Q : \ell_\delta(e) = 0\}$$

*e*

$$\delta'' = \{e \in R : \ell_\delta(e) = -2\}.$$

Seja $\Gamma \subseteq Edge(f)$, e seja $K = (k_\gamma)_{\gamma\in\Gamma}$ um vetor de inteiros positivos, um para cada $\gamma \in \Gamma$. Defina

$$Newt(f)|_{\Gamma,K} := \{e \in Newt(f) | \, 0 \leq \ell_\gamma(e) < k_\gamma \text{ para } \gamma \in \Gamma\}.$$

$$Q\left|_{\Gamma,K}\right. := \{e \in Q |\, 0 \leq \ell_\gamma(e) < k_\gamma - h_{\gamma''} \text{ para } \gamma \in \Gamma\}$$

$$R\left|_{\Gamma,K}\right. := \{e \in R |\, 0 \leq \ell_\gamma(e) < k_\gamma + h_{\gamma''} \text{ para } \gamma \in \Gamma\}.$$

Note que $Newt(f)\ |_{\Gamma,K}$, $Q\ |_{\Gamma,K}$ e $R\ |_{\Gamma,K}$ representam faixas nos seus respectivos politopos, conforme pode ser observado na figura 5.6.

**Exemplo 5.2.6.** *Referindo-se ao exemplo 5.2.1. Seja* $\delta_1$ *a aresta do* $Newt(f)$ *que vai do vértice* $(0,2)$ *ao vértice* $(2,0)$ *e* $\delta_2$ *a aresta do* $Newt(f)$ *que vai do vértice* $(2,0)$ *ao vértice* $(3,0)$. *Sejam* $\Gamma = \{\delta_1, \delta_2\}$ *e* $K = (1,1)$. *Então os pontos integrais no* $Newt(f)\ |_{\Gamma,K}$ *são* $\{(0,2),(1,1),(2,0),(3,0)\}$, *os pontos integrais no* $Q\ |_{\Gamma,K}$ *são* $\{(0,2),(1,1),(2,0)\}$ *e os pontos integrais no* $R\ |_{\Gamma,K}$ *são* $\{(0,0)\}$. *Conforme representado na figura 5.6.*

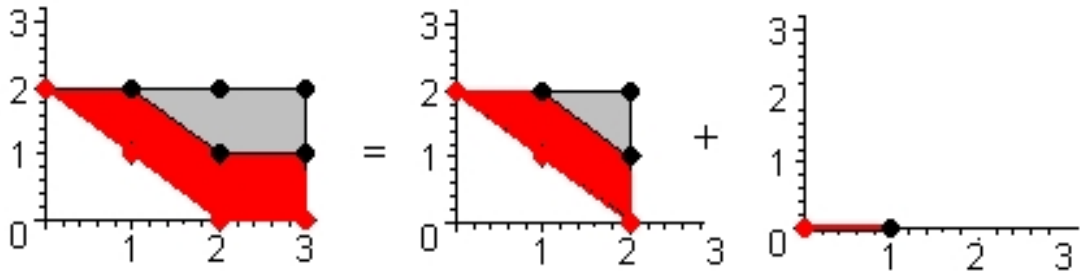


*Figura 5.6: faixas*

**Definição 5.2.3.** *Uma* $Newt(f) \mid \Gamma, K$*- fatoração é dita uma* $(\Gamma, K; Q, R)$*- fatoração se as seguintes duas propriedades forem satisfeitas:*

- *Exatamente os coeficientes indeterminados de* $g$ *e* $h$ *indexados pelos pontos inteiros em* $Q\ |_{\Gamma,K}$ *e* $R\ |_{\Gamma,K}$, *respectivamente, foram determinados.*

- *Seja* $K' = \left(k'_\gamma\right)_{\gamma\in\Gamma}$ *um vetor de inteiros positivos com* $k'_\gamma \geq k_\gamma$ *para todo* $\gamma \in \Gamma$, *com a desigualdade estrita para no mínimo um* $\gamma$. *Então nem todos coeficientes indeterminados de* $g$ *indexados por pontos inteiros em* $Q\ |_{\Gamma,K'}$ *foram determinados.*

**Exemplo 5.2.7.** *Continuando o exemlo 5.2.6, onde* $K = (1,1)$. *Conforme a definição 5.2.3, teríamos uma* $(\Gamma, K; Q, R)$*- fatoração se os coeficientes* $g_{02}, g_{11}, g_{20}, g_{30}$ *e* $h_{00}, h_{10}$ *indexados por pontos integrais em* $Q\mid_{\Gamma,K}$ *e* $R\mid_{\Gamma,K}$ *estivessem determinados. E os coeficientes,* $g_{20}$ *e* $g_{02}$*, indexados por pontos integrais em* $Q\mid_{\Gamma,K'}$ *não foram determinados onde* $K^{'} = (1,2)$.

Se o vetor $K$ é unitário, denotado por $K = (\underline{1})$, diremos uma $(\Gamma; Q, R)$-fatoração parcial.

**O problema central deste capítulo é**:

**Problema 5.2.1.** *Seja* $f \in \mathbb{F}[x,y]$ *com seu polígono de Newton ,*$Newt(f)$*, e uma decomposição de Minkowski fixa* $Newt(f) = Q + R$ *onde* $Q$ *e* $R$ *são polígonos integrais no primeiro quadrante. Suponha que seja dada uma* $(\Gamma; Q, R)$*- fatoração parcial de* $f$ *para algum conjunto* $\Gamma \subseteq Edge(f)$. *Construa uma fatoração completa de* $f$ *que a estenda, ou mostre que não pode ser estendida.*

O algoritmo que será apresentado no final do capítulo começa com $K = (\underline{1})$, ou seja, teremos uma $K$-fatoração(fatoração parcial) na qual os coeficientes que correspondem aos elementos dos conjuntos $Q\mid_{\Gamma,K}$ e $R\mid_{\Gamma,K}$ foram determinados. A idéia do algoritmo é de que a cada passo possamos estender a fatoração parcial, ou mostrar que ela não pode ser estendida, usando um novo $K^{'} = (k^{'}_{\delta})$ tal que

$$\sum_{\delta\in\Gamma} k^{'}_{\delta} > \sum_{\delta\in\Gamma} k_{\delta}.$$

Este processo é feito até encontrarmos uma fatoração parcial que não pode ser estendida ou quando chegarmos até um $K$ tal que $Q \subseteq Q\mid_{\Gamma,K}$, neste caso checamos por divisão se encontramos um fator de $f$.

## 5.3 Equações do levantamento de Hensel Modificadas

Neste momento estudaremos as equações básicas que serão usadas no algoritmo as quais foram derivadas das equações que são usadas no levantamento de Hensel padrão que pode ser visto no apêndice A.

Para qualquer $\delta \in Edge\,(f)$, temos $\ell_\delta$. Para $i \geq 0$ definimos

$$f_i^\delta := \sum_{\ell_\delta(e)=i} a_e X^e.$$

Note que $f_i^\delta$ é obtida de $f$ após retirarmos todos os pontos cujos expoentes não estão sobre o hiperplano de suporte deslocado $i$ para dentro do $Newt\,(f)$, conforme figura 5.7. Chamaremos o polinômio $f_0^\delta$ de polinômio aresta.

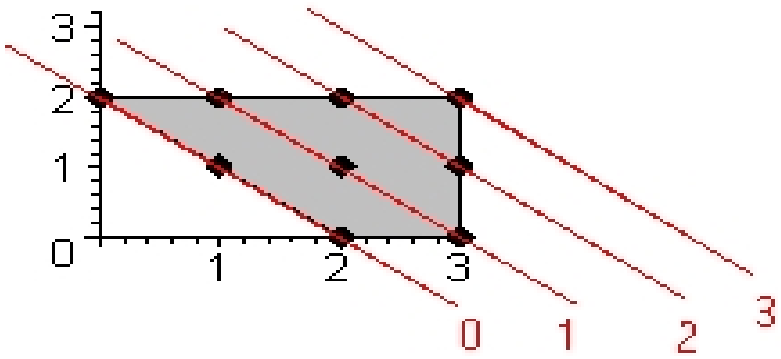


Figura 5.7: polinômios aresta

Dada a decomposição $Newt\,(f) = Q + R$, sejam $\delta^{'}$ e $\delta^{''}$ as únicas arestas de $Q$ e $R$ respectivamente, cuja soma dá $\delta$. Como antes vamos assumir que $\ell_\delta\left(\delta^{'}\right) = h_{\delta'} - h_\delta$ e $\ell_\delta\left(\delta^{''}\right) = -h_{\delta'}$. Para $i \geq 0$ definimos

$$g_i^\delta := \sum_{q\in Q, \ell_\delta(q)=h_{\delta'}-h_\delta+i} g_q X^q$$

$$h_i^\delta := \sum_{r\in R, \ell_\delta(r)=-h_{\delta'}+i} h_r X^r.$$

**Exemplo 5.3.1.** *Referindo-se ao exemplo 5.2.1. Seja $\delta$ a aresta do Newt(f) que vai de $(0,2)$ a $(2,0)$. Então $\ell_\delta(e) = e_1 + e_2 - 2$. Assim*

$$f_0^\delta = \sum_{\ell_\delta(e)=i} a_e x^e = x^2 + xy + y^2$$

$$f_1^\delta = \sum_{\ell_\delta(e)=i} a_e x^e = x^3 + x^2y + xy^2$$

*como ilustrado em 5.7. Assim como para*

$$g_0^\delta = g_{20}x^2 + g_{11}xy + g_{02}y^2$$

$$g_1^\delta = g_{21}x^2y + g_{12}xy^2$$

*e para*

$$h_0^\delta = h_{00}$$

$$h_1^\delta = h_{10}x$$

**Lema 5.3.1.** *Sejam $f \in \mathbb{F}[x,y]$ e $Newt(f) = Q + R$ uma decomposição integral com polinômios genéricos correspondentes $g$ e $h$. Seja $\delta \in Edge(f)$. O sistema de equações nos coeficientes indeterminados de $g$ e $h$ que são definidos quando igualamos os monômios em ambos os lados da igualdade $f = gh$ tem as mesmas soluções que o sistema de equações definido a seguir:*

$$f_0^\delta = g_0^\delta h_0^\delta \text{ e } g_0^\delta h_k^\delta + h_0^\delta g_k^\delta = f_k^\delta - \sum_{k-1}^{j=1} g_j^\delta h_{k-j}^\delta \text{ para } k \geq 1. \tag{5.3}$$

*Então qualquer determinação dos coeficientes indeterminados que é uma solução das equações 5.3 dará uma fatoração completa de f.*

**Dem.:** Na equação $f = gh$ basta igualar em ambos os lados todos os monômios cujos expoentes vetoriais estão sobre o mesmo deslocamento da reta suporte $\delta$. □

Estas são as equações que serão usadas no algoritmo de fatoração via politopos. Começamos com uma determinação dos coeficientes de $g_0^\delta$ e $h_0^\delta$ que dá uma fatoração do polinômio $f_0^\delta$, neste momento obtemos uma fatoração parcial. A equação 5.3 com $k = 1$ dá um sistema linear nos coeficientes indeterminados de $g_1^\delta$

e $h_1^\delta$, a idéia é resolver este sistema para estender a fatoração parcial original. Este processo é iterado para $k > 1$ até que todos os coeficientes indeterminados em um dos polinômios genéricos tenham sido determinados, neste momento checamos se encontramos um fator por divisão.

## 5.4 Lema Geométrico

**Definição 5.4.1.** *Seja $\Lambda$ um conjunto de arestas de um polígono $P$ em $\mathbb{R}^2$ e $r$ um vetor em $\mathbb{R}^2$. Dizemos que $\Lambda$ domina $P$ na direção $r$ se as seguintes duas condições são satisfeitas:*

- *$P$ está contido na soma de Minkowski do conjunto $\Lambda$ e o segmento de reta infinito $r\mathbb{R}_{\geq 0}$(A envoltória positiva de $r$). Chamaremos esta soma de $Mink\,(\Lambda, r)$.*

- *Cada uma das duas arestas infinitas de $Mink\,(\Lambda, r)$ contém exatamente um ponto de $P$.*

**Definição 5.4.2.** *Diremos que $\Lambda$ é um conjunto dominante irredundante na direção $r$ se $\Lambda$ é um conjunto dominante na direção $r$ que não contem estritamente qualquer outro conjunto dominante na direção $r$.*

**Exemplo 5.4.1.** *Como podemos observar na figura 5.8. $\Gamma = \{\delta_1, \delta_2\}$, onde $\delta_1$ vai do vértice $(0, 2)$ ao $(2, 0)$ e $\delta_2$ vai do vértice $(2, 0)$ ao $(3, 0)$, é um conjunto dominante irredundante do politopo na direção $r = (1, 1)$.*

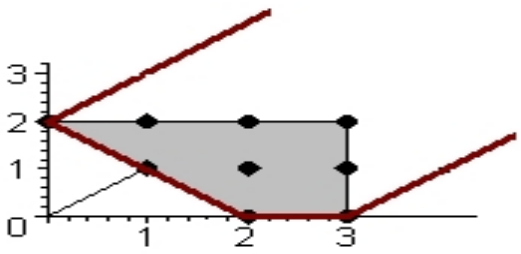


*Figura 5.8: conjunto dominante de arestas*

**Proposição 5.4.1.** *As aresta em um conjunto dominante irredundante são adjacentes.*

Vamos definir a transformada $\pi_r$.

**Definição 5.4.3.**

$$\pi_r : \mathbb{R}^2 \longrightarrow \langle r \rangle^{\perp} := \{s \in \mathbb{R}^2 \mid \langle s, r \rangle = 0\}.$$

Assim, dado $v \in \mathbb{R}^2$ então $v = w + \lambda r$ com $w \in \langle r \rangle^{\perp}$ e $\lambda \in \mathbb{R}$. Logo, $v = w + \lambda r$. Fazendo produto interno com $r$ obtemos: $\langle v, r \rangle = \langle w, r \rangle + \lambda \langle r, r \rangle = \lambda \langle r, r \rangle$(pois $w \perp r$). Logo, $\lambda = \frac{\langle v,r \rangle}{\langle r,r \rangle}$ e definimos $\pi_r(v) = v - \left(\frac{\langle v,r \rangle}{\langle r,r \rangle}\right) r$.

Segue desta definição que $\pi_r(P) = \pi_r(\Lambda)$ se $\Lambda$ domina $P$ na direção $r$.

**Proposição 5.4.2.** *Se $e_1$ e $e_2$ são arestas adjacentes em um conjunto dominante irredundante $\Lambda$ na direção $r$, então $\pi_r(e_1 e_2) = \pi_r(e_1) + \pi_r(e_2)$.*

**Dem.:** Note que, como $\Lambda$ domina $P$ na direção $r$, então $r$ não pode ser paralelo a qualquer aresta do $P$, pois o segundo ítem da definição 5.4.1 não seria satisfeito.

Vamos supor que não seja verdade. Então $\pi_r(e_1) \subseteq \pi_r(e_2)$ ou vice-versa, conforme a figura 5.9.

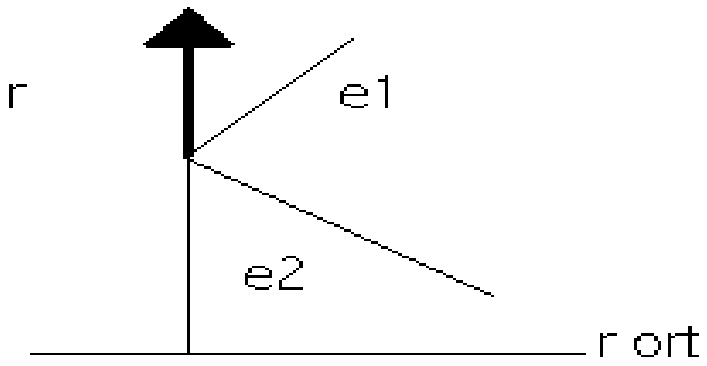


Figura 5.9: projeção

Logo, $r\mathbb{R}_{\geq 0} + e_1 \subseteq r\mathbb{R}_{\geq 0} + e_2$ e assim $\Lambda$ seria redundante, uma contradição. □

A propriedade 5.4.2 continua valendo se repassarmos $e_1$ e $e_2$ por quaisquer segmentos de reta paralelos a eles. Ainda obteremos uma aditividade nos comprimentos.

O lema a seguir é a chave do algoritmo, pois garante que a fatoração parcial pode ser estendida.

**Lema 5.4.1.** *Seja $P$ um polígono integral e $\Lambda$ um conjunto dominante irredundante de arestas de $P$. Suponha $\Lambda_1$ um segmento de reta poligonal em $P$ tal que cada aresta de $\Lambda_1$ é paralela a alguma aresta de $\Lambda$. Se $\Lambda_1$ é diferente de $\Lambda$ então $\Lambda$ tem no mínimo uma aresta que tem estritamente mais pontos inteiros que a correspondente aresta em $\Lambda_1$.*

A figura 5.10 ilustra o lema 5.4.1.

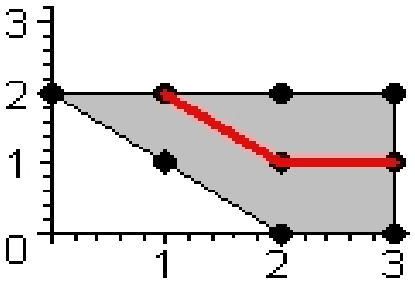


Figura 5.10: segmento de reta poligonal

**Dem.:** Assumimos que $\Lambda$ domina $P$ na direção $r$. Sejam $\delta_1, \ldots, \delta_k$ as arestas em $\Lambda$ paralelas às arestas $\delta_1', \ldots, \delta_k'$ de $\Lambda_1$. Seja $n_i$ o número de pontos inteiros sobre $\delta_i$ e $m_i$ o número de pontos inteiros sobre $\delta_i'$, para $1 \leq i \leq k$. Dado $\Lambda \neq \Lambda_1$, queremos mostrar que $n_i > m_i$ para no mínimo um $i$ entre 1 e $k$. Vamos supor o contrário, que

$$n_i \leq m_i \text{ para } 1 \leq i \leq k. \tag{5.4}$$

Note que se $m_i = 0$ para algum $i$, então estamos prontos, pois cada $\delta_i$ possui no mínimo dois pontos inteiros($n_i \geq 2$ para $1 \leq i \leq k$). Assim, podemos assumir que $m_i \geq 1$ para $1 \leq i \leq k$.

Como $\Lambda$ é dominante, então $\pi(P) = \pi(\Lambda)$ e $\pi(\Lambda_1) \subset \pi(P)$, logo $\pi(\Lambda_1) \subset \pi(\Lambda)$. Note que como $\Lambda_1$ é diferente de $\Lambda$, seus pontos finais não podem coincidir, pois o único modo de $\Lambda_1$ e $\Lambda$ terem seus pontos finais e iniciais coincidindo é se $\Lambda_1 = \Lambda$. Assim, pelo menos um dos pontos finais de $\Lambda_1$ não estará sobre as arestas infinitas de $Mink(\Lambda, r)$. Então $\pi(\Lambda_1)$ estará totalmente contido no $\pi(\Lambda)$. Logo

$$\|\pi(\Lambda_1)\| < \|\pi(\Lambda)\|. \tag{5.5}$$

Agora, vamos considerar o vetor direção de $\delta_i$ o $v_i^0$ e $\|\pi(v_i^0)\| = \epsilon_i$ , o qual será o mesmo para $\delta_i^{'}$, então $\|\pi(\delta_i)\| = (n_i - 1)\epsilon_i$ e pela propriedade 5.4.2 $\|\pi(\Lambda)\| = \sum_{i=1}^{k}(n_i - 1)\epsilon_i$. E como $\delta_i \| \delta_i^{'}$, então

$$\|\pi(\Lambda_1)\| = \sum_{i=1}^{k}(m_i - 1)\epsilon_i.$$

Assim, 5.4 nos leva a

$$\sum_{i=1}^{k}(n_i)\epsilon_i \leq \sum_{i=1}^{k}(m_i)\epsilon_i,$$

ou seja, que $\|\pi(\Lambda)\| \leq \|\pi(\Lambda_1)\|$. Contradizendo 5.5, a qual nos diz que $\pi(\Lambda_1)$ é estritamente menor que $\pi(\Lambda)$. O lema está provado. □

## 5.5 O Teorema Principal

Seja $\Gamma$ um conjunto dominante irredundante do $Newt(f)$ na direção de $r$. Chamaremos uma $(\Gamma; Q, R)$-fatoração parcial de $f$ de uma fatoração de arestas dominante relativa a $\Gamma$, $Q$ e $R$.

**Definição 5.5.1.** *Uma fatoração de arestas dominante coprima é uma* $(\Gamma; Q, R)$*-fatoração parcial com a propriedade que para cada* $\delta \in \Gamma$ *os polinômios aresta* $g_0^\delta$ *e* $h_0^\delta$ *são coprimos, sob fatores monomiais.*

**Teorema 5.5.1.** *Seja* $f \in \mathbb{F}[x,y]$ *e* $Newt(f) = Q + R$ *uma decomposição de Minkowski fixa, onde* $Q$ *e* $R$ *são polígonos integrais no primeiro quadrante. Seja* $\Gamma$ *um conjunto dominante irredundante do* $Newt(f)$ *na direção* $r$*, e assuma que* $Q$ *não é apenas um ponto nem um segmento de reta paralelo a* $r\mathbb{R}_{\geq 0}$*. Para qualquer fatoração de arestas dominante coprima de* $f$ *relativa a* $\Gamma$*,* $Q$ *e* $R$*, existe no máximo uma fatoração completa de* $f$ *que a estende, e além disso esta fatoração completa pode ser encontrada ou mostrar que não existe em tempo polinomial em* $\neq Newt(f)$*.*

A prova do teorema seguirá facilmente após a prova dos próximos dois lemas.

Algumas propriedades de conjuntos dominantes

$$\Lambda := \{\delta \in \Gamma \subset Edge(f) : \delta^{'} \text{ é uma aresta e não apenas um vértice }\}.$$

**Proposição 5.5.1.** $\Lambda \neq \emptyset$*.*

**Dem.:** Vamos supor que $\Lambda = \emptyset$. Então com um deslocamento adequado vemos que $\Gamma \subset R$ e $\pi(R) = \pi(\Gamma)$ que é a $\pi(P)$ conforme a figura 5.11. Assim, se $Q$ for apenas um ponto, podemos ter $\Lambda = \emptyset$. Mas assim não respeitamos nossas hipóteses. Agora, se $Q$ tiver pelo menos uma aresta $\vartheta$, essa aresta deverá ser paralela a $r$ ou $\Lambda$ não dominará o $Newt(f)$. Pois, $\Gamma + \vartheta$ não estará contido no $Mink(\Lambda, r)$. Logo $\Lambda \neq \emptyset$.

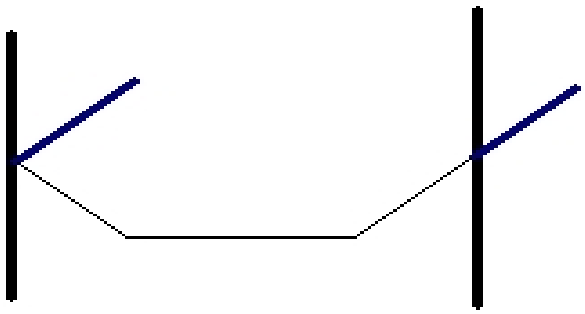

Figura 5.11: conjuntos dominantes

□

**Proposição 5.5.2.** *Seja* $\Gamma$ *um conjunto dominante irredundante para* $Newt\,(f)$ *na direção* $r$*. Então o conjunto* $\Gamma^{'} = \left\{\delta^{'}\right\}_{\delta\in\Lambda}$ *é um conjunto dominante irredundante para* $Q$ *na direção* $r$*.*

**Dem.:** Começamos mostrando que $\Gamma^{'}$ domina $Q$ na direção $r$ , para então mostrarmos que $\Gamma^{'}$ é irredundante. Vamos supor que exista $\delta_j^{'}$ aresta de $Q$ que não está totalmente contida no $Mink\left(\Gamma^{'}, r\right)$, então $\delta_j$ não estará totalmente contida no $Mink\,(\Gamma, r)$, contradição.Assim $Q \subset Mink\left(\Gamma^{'}, r\right)$.

Agora vamos supor que pelo menos uma das arestas infinitas de $Mink\left(\Gamma^{'}, r\right)$ contém dois pontos ou mais de $Q$, ou seja, $Q$ contém uma aresta $\alpha^{'}$paralela a $r$, ou seja, existe $\alpha \in Edge\,(f)$ tal que $\alpha$ é paralela a $r$, então $\Gamma$ não domina $Newt\,(f)$ na direção $r$. Contradição, logo $\Gamma^{'}$ domina $Q$ na direção $r$.

Vamos mostrar que $\Gamma^{'}$ é irredundante, para isto vamos supor que $\Gamma^{'}$ é redundante e chegaremos a uma contradição. Como $\Gamma^{'}$ é redundante, então podemos retirar um certo $\delta_j^{'}$ tal que $\delta_j^{'} \subset \delta_i^{'}+r\mathbb{R}_{\geq 0}$, porém $\delta_j = \delta_j^{'}+\delta_j^{''}$, logo $\delta_j \subset \delta_i^{'}+\delta_j^{''}+r\mathbb{R}_{\geq 0}$, então $\Gamma$ é redundante. Contradição, então $\Gamma^{'}$ é irredundante. □

Agora temos as ferramentas necessárias para provarmos o lema a seguir.

**Lema 5.5.1.** *Sejam* $f$*,*$Q$*,*$R$ *e* $\Gamma$ *como no enunciado do teorema 5.5.1. Suponha que seja dada uma* $K$*-fatoração de* $f$*, onde* $K = (k_\delta)_{\delta\in\Gamma}$*(mais especificamente, uma* $(\Gamma, K; Q, R)$*-fatoração). Para cada* $\delta \in \Gamma$*, denote por* $\delta^{'}$ *a face de* $Q$ *suportada por* $\ell_\delta - (h_{\delta'} - h_\delta)$*. Então existe* $\delta \in \Gamma$ *com as seguintes propriedades*

- *A face* $\delta^{'}$ *é uma aresta ( não apenas um vértice).*
- *O número de coeficientes não determinados de* $g^{\delta}_{k_\delta}$ *é não nulo mas estritamente menor que o número de pontos integrais sobre* $\delta^{'}$*.*
- *Todos os termos não determinados têm expoentes que são pontos integrais adjacentes sobre a linha suportada por* $\ell_\delta - (h_{\delta'} - h_\delta) + k_\delta$*.*

A figura 5.12 ilustra o lema 5.5.1.

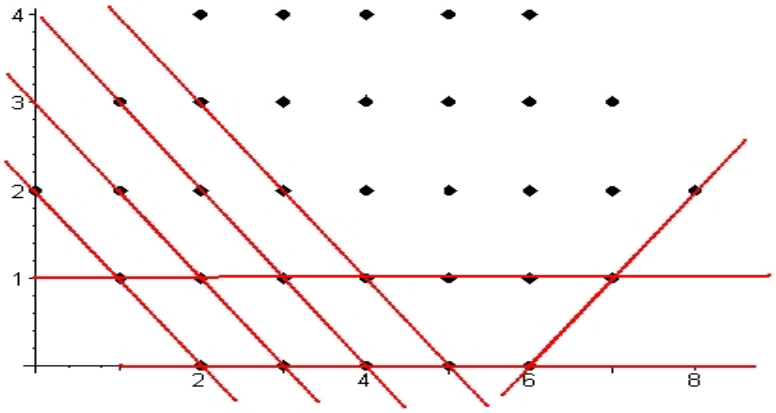


Figura 5.12: Coeficientes indeterminados do polinômio genérico

**Dem.:** Começamos definindo o polígono $\bar{Q}$ como:

$$\bar{Q} := \{r \in Q : \ell_\delta(r) \geq (h_{\delta'} - h_\delta) + k_\delta \forall \delta \in \Gamma\}$$

Note que os pontos inteiros em $\bar{Q}$ correspondem a coeficientes não determinados em $g$. Como já mostramos $\Lambda \neq \emptyset$, assim, seja $\bar{\delta}$ a face de $\bar{Q}$ suportada por $\ell_\delta - ((h_{\delta'} - h_\delta) - k_\delta)$ que, claramente, é paralela a $\delta'$. Note que cada $\bar{\delta}$ contém pelo menos um ponto inteiro. Como $\bar{\delta}$ é paralelo a $\delta'$ para todo $\delta \in \Lambda$, então a sequência de arestas $\left\{\bar{\delta}\right\}_{\delta\in\Lambda}$ forma uma sequência poligonal em $Q$. Assim, $\left\{\delta'\right\}_{\delta\in\Lambda}$ e $\left\{\bar{\delta}\right\}_{\delta\in\Lambda}$ satisfazem as hipóteses do lema 5.4.1. Portanto, existe no mínimo uma aresta $\delta \in \Lambda$ tal que $\delta'$ tem estritamente mais pontos inteiros que $\bar{\delta}$. Esta aresta $\delta$ tem as propriedades requeridas. Isto completa a prova. □

Antes de apresentarmos o próximo lema iremos definir o grau de um polinômio de Laurent.

**Definição 5.5.2.** *Seja o polinômio de Laurent* $f = \sum a_i z^i \in \mathbb{F}[z]$ *com* $i \in \mathbb{Z}$. *Onde o grau do polinômio de Laurent é a diferença entre o maior e o menor expoente, se o polinômio é não-nulo, e* $-\infty$ *caso contrário.*

**Exemplo 5.5.1.** *Seja o polinômio de Laurent* $f = 2z^{-2}+1+3z+5z^7 \in \mathbb{Z}[z]$. *Então* $grau(f) = 7-(-2) = 9$.

**Lema 5.5.2.** *Sejam* $f$,$Q$,$R$ *e* $\Gamma$ *como no enunciado do teorema 5.5.1. suponha que tenhamos uma* $K$*-fatoração de* $f$*, onde* $K = (k_\delta)_{\delta\in\Gamma}$. *Além disso, assuma que esta fatoração estende uma fatoração de arestas dominante coprima, isto é, os polinômios* $g_0^\delta$ *e* $h_0^\delta$ *são coprimos sob fatores monomiais para todo* $\delta \in \Gamma$. *Então existe* $\delta \in \Gamma$ *tal que os coeficientes de* $g_{k_\delta}^\delta$ *não estão todos determinados, mas eles podem ser determinados em no máximo um caminho consistente com as equações 5.3. Esta determinação pode ser computada em tempo polinomial em* $\neq Newt(f)$

**Dem.:** Selecione $\delta \in \Gamma$ tal que as propriedades do lema 5.5.1 sejam satisfeitas. Sejam $n_\delta$ e $m_\delta$ os números de pontos integrais sobre $\delta'$ e $\bar{\delta}$ respectivamente, onde $\delta'$ e $\bar{\delta}$ estão definidas como na prova do lema 5.5.1. Então temos que $n_\delta > m_\delta$ e $m_\delta \geq 1$. Com a aresta $\delta$ podemos definir a função primitiva afim associada a $\delta$ como $\ell_\delta = \gamma_1 e_1 + \gamma_2 e_2 - h_\delta$, onde $\gamma_1$ e $\gamma_2$ são coprimos. Sejam $z$ e $w$ as novas variáveis. Usando as transformadas

$$i_1 = e_1\zeta_2 - e_2\zeta_1, \text{ e } i_2 = e_1\gamma_1 - e_2\gamma_2 = \ell_\delta(e_1, e_2) + h_\delta,$$

qualquer monômio da forma $x^{e_1}y^{e_2}$ pode ser escrito como

$$x^{e_1}y^{e_2} = z^{i_1}w^{i_2} \tag{5.6}$$

Todo monômio em $g_i^\delta$ é da forma $x^{e_1}y^{e_2}$ onde $\ell_\delta(e_1, e_2) = h_{\delta'} - h_\delta + i$. Sejam os monômios $s$ e $t$ os termos de $g$ e $h$ respectivamente cujos expoentes vetoriais são os vértices começo das faces de $Q$ e $R$ definidas por $\ell_\delta - (h_{\delta'} - h_\delta)$ e $\ell_\delta + (h_{\delta'} - h_\delta) + h_\delta$, respectivamente (ou seja, os vértices começo de $\delta'$ e $\delta''$, respectivamente). Então após termos feito as mudanças de variáveis chegamos a:

$$g_i^\delta(z,w) = sw^iG_i(z),\ h_i^\delta(z,w) = tw^iH_i(z) \text{ e } f_i^\delta(z,w) = stw^iF_i(z),$$

onde $G_i(z)$, $H_i(z)$ e $F_i(z)$ são polinômios de Laurent univariados. Com esta construção $G_0(z)$, $H_0(z)$ e $F_0(z)$ são polinômios ordinários, ou seja, que contém apenas expoentes não negativos de $z$. Para $i < k_\delta$ todos os coeficientes nos polinômios

$G_i(z)$ e $H_i(z)$ foram determinados. Além disso $G_0(z)$ é de grau $n_\delta$, e também com excessão de $m_\delta$ coeficientes de $G_{k_\delta}(z)$ todos os outros foram deteminados(lema 5.5.1). Com esta mudança de variável as equações 5.3 podem ser escritas como $F_0(z) = G_0(z) F_0(z)$, e para $k \geq 1$ temos

$$G_k(z) H_0(z) + G_0(z) H_k(z) = F_k(z) - \sum_{j=1}^{k-1} G_j(z) H_{k-j}(z)$$

Sabemos que todos os coeficientes de $G_i(z)$ e $H_i(z)$ foram determinados para $0 \leq i < k_\delta$ em um caminho que começamos resolvendo $F_0 = G_0 H_0$ e as primeiras $k_\delta - 1$ equações acima. Então precisamos resolver a equação

$$G_{k_\delta} H_0 + G_0 H_{k_\delta} = F_{k_\delta} - \sum_{j=1}^{k_\delta - 1} G_j H_{k_\delta - j}. \tag{5.7}$$

para os coeficientes indeterminados de $G_{k_\delta}$ e $H_{k_\delta}$.

Primeiro calculamos, usando o algoritmo de Euclides estendido, polinômios ordinários únicos $U(z)$ e $V(z)$ tais que

$$V(z) H_0(z) + U(z) G_0(z) = 1$$

com $deg_z(U(z)) < deg_z(H_0(z))$ e $deg_z(V(z)) < deg_z(G_0(z))$. Note que $G_0(z)$ e $H_0(z)$ são coprimos já que temos uma fatoração coprima. Qualquer solução $G_{k_\delta}(z)$ da equação 5.7 deve ser da forma

$$G_{k_\delta} = \left\{ V \left( F_{k_\delta} - \sum_{j=1}^{k_\delta - 1} G_j H_{k_\delta - j} \right) \bmod G_0 \right\} + \epsilon G_0 \tag{5.8}$$

para algum polinômio de Laurent $\epsilon(z)$ com coeficientes indeterminados. Reescrevendo 5.8 temos

$$G_{k_\delta} - \left\{ V \left( F_{k_\delta} - \sum_{j=1}^{k_\delta - 1} G_j H_{k_\delta - j} \right) \bmod G_0 \right\} = \epsilon G_0 \tag{5.9}$$

Seja $d$ o grau do polinômio de Laurent do lado esquerdo de 5.9. Sabemos que $G_0$ e é um polinômio ordinário, ou seja, com termos cujos expoentes são não negativos, de grau $n_\delta - 1$ e com termo constante não nulo pois corresponde a aresta $\delta'$. Como $grau(G_o) = n_\delta - 1$ e $G_0$ não possui termos cujos expoentes são negativos então

$grau(\epsilon)G_0 \geq n_\delta - 1$. Se $d < n_\delta - 1$ então $\epsilon = 0$. Se $d \geq n_\delta - 1$ então $grau(\epsilon(z)) = d - (n_\delta - 1)$, logo $\epsilon(z)$ possui $d - (n_\delta - 1) + 1$ coeficientes indeterminados. Sabemos que $G_{k_\delta}$ possui $m_\delta$ coeficientes indeterminados e $\epsilon$ tem $d - n_\delta + 2$ coeficientes todos indeterminados. No lado esquerdo de 5.9 temos $d + 1$ termos, então para $G_{k_\delta}$ ser possível de ser determinado é necessário que $d + 1 \geq m_\delta + d - n_\delta + 2$. Por hipótese $m_\delta < n_\delta$ e assim $d + 1 - m_\delta \geq d - n_\delta + 2$.

**Como descobrir $\epsilon(z)$:**

Como $\epsilon(z)$ tem grau $d - (n_\delta + 1)$ então ele tem a seguinte forma:

$$\epsilon(z) = \underbrace{a_0 z^a + a_1 z^{a+1} + \cdots + a_{d-(n_\delta-1)} z^{a+d-(n_\delta-1)}}_{d-n_\delta+2 \text{ coeficientes indeterminados}}.$$

**Como descobrir $a$?**

Note que $G_0$ possui termo constante não nulo, pois este corresponde a um vértice de $Q$, fator do $Newt(f)$. E do mesmo modo como foi feito para $\epsilon$, $G_0$ tem a seguinte forma:

$$G_0(z) = \underbrace{c_0 + c_1 z^1 + \cdots + c_{n_\delta - 1} z^{n_{\delta-1}}}_{n_\delta \text{termos}}.$$

Então $\epsilon G_0 = c_0 a_0 z^a + \cdots$ e assim podemos encontrar $a$ igualando este termo ao termo de mais baixo grau no lado esquerdo de 5.9.

**Calculando os coeficientes indeterminados**

Seja $q = grau(G_{k_\delta})$.Sabemos que os $m_\delta$ coeficientes indeterminados de $G_{k_\delta}$ correspondem a termos adjacentes. Vamos supor que os $r$ termos mais baixos de $G_{k_\delta}$ tiveram seus coeficientes determinados e assim os $(q + 1) - (m_\delta + r)$ mais altos termos também. Então $G_{k_\delta}$ tem a seguinte forma:

$$G_{K_\delta} = \underbrace{b_0 z^b + b_1 z^{b+1} + \cdots + b_{r-1} z^{b+r-1}}_{r \text{ termos determinados}} + \underbrace{b_r z^{b+r} + \cdots + b_{r+m_\delta-1} z^{b+r+m_\delta-1}}_{m_\delta \text{ termos indeterminados}}$$
$$+ \quad \underbrace{b_{r+m_\delta} z^{b+r+m_\delta} + \cdots + b_q z^{b+q}}_{(q+1)-(r+m_\delta) \text{ termos determinados}}.$$

a qual nos leva a um sistema triangular. Podemos resolver para os $r$ mais baixos termos de $\epsilon$ igualando ambos os termos em 5.8. O mesmo pode ser feito para os coeficientes dos $(q+1)-(m_\delta+r)$ termos mais altos.

**Quando o sistema pode não ter solução ?**

No caso em que $d+1-m_\delta > d-n_\delta+2$, isto é, quando $n_\delta > m_\delta+1$ os sistemas podem não ter solução em comum. Neste caso pode não haver solução para a equação 5.8 e então, como será explicado posteriormente, iremos para outra aresta coprima do conjunto dominante irreduntante e faremos o mesmo sistema.

Se existir um $\epsilon(z)$ que satisfaça 5.9 então os coeficientes indeterminados de $G_{k_\delta}$ podem ser determinados. Tendo computado a solução de 5.9 para $G_{k_\delta}$ podemos substituir em 5.7 e descobrir $H_{k_\delta}$. Ou seja, computar

$$\frac{(F_{k_\delta} - \sum_{j=1}^{k_\delta-1} G_j H_{k_\delta-j}) - G_{k_\delta}H_0}{G_0}.$$

Isto completa a prova. □

Para provarmos o teorema 5.5.1 precisamos mostrar se à decomposição dada, $Newt(f) = Q+R$, corresponde ou não a uma fatoração $f = gh$ do polinômio. De acordo com o lema 5.5.1 sempre existe uma aresta do conjunto dominante irredundante $\Gamma$ que pode ser levantada, ou seja, que os coeficientes dos termos cujos expoentes vetoriais estão sobre ela podem ser determinados. No lema 5.5.2 observamos como esse levantamento é feito.

Quando escolhemos uma aresta de $\Gamma$ que satisfaça as condições do lema 5.5.1 para fazermos o levantamento, este nos leva a um sistema nas indeterminadas $g_q$ que pode ou não ter solução. Se o sistema tem solução continuamos o levantamento. Porém, se o sistema não tem solução vamos para outra aresta de $\Gamma$ que satisfaça o lema 5.5.1 e tentamos fazer o levantamento. Se todas as aresta de $\Gamma$ levam a sistemas que não possuem solução então o levantamento não pode continuar e podemos dizer que a decomposição do $Newt(f)$ dada não corresponde a uma fatoração $f = gh$ do polinômio.

Se conseguirmos fazer o levantamento até o final então teremos determinado todas as indeterminadas $g_q$ e $h_r$, ou seja, teremos dois polinômios $g$ e $h$ que correspondem à decomposição do $Newt(f)$ dada e que são candidatos a uma fatoração $f = gh$ . Um teste de divisão simples pode verificar se, de fato, $g$ e $h$ são fatores de $f$.

Para um maior esclarecimento do que foi discutido recomendamos uma leitura do apêndice B e do exemplo 5.5.2 que consta no final do presente capítulo.

**O algoritmo**

**Algoritmo 5.5.1.**

***Entrada***: *Um polinômio* $f \in \mathbb{F}[x, y]$.

***Saída***: *Uma fatoração de* $f$ *ou falhou.*

1. ***Passo***: *Calcular um conjunto dominante irredundante* $\Gamma$ *do* $Newt(f)$. *Para esta escolha de* $\Gamma$, *calcular todas* $(\Gamma; Q, R)-$*fatorações parciais coprimas de* $f$, *isto é, calcular todas as fatorações parciais coprimas relativas aos fatores* $Q$ *e* $R$ *e o conjunto dominante* $\Gamma$. *Note que,* $Q$ *e* $R$ *variam sobre todos os pares de fatores tais que* $Newt(f) = Q + R$.
2. ***Passo***: *Aplicando repetidamente o método usado na prova do lema 5.5.2, levante cada fatoração de arestas dominante coprima tanto quanto possível. Se qualquer um destes levantamentos levar a uma fatoração completa então retorne esta fatoração e pare o algoritmo. Se nenhum deles levar a uma fatoração completa então retorne falhou.*

O algoritmo sempre funcionará quando começar com um conjunto dominante irredundante $\Gamma$ do $Newt(f)$ tal que todos os polinômios $f_0^\delta$, para todo $\delta \in \Gamma$, são livres de quadrado sob fatores monomiais.

Podemos dizer que quando o algoritmo retornar falhou então o polinômio $f$ é irredutível, pois ele testa todos os pares de fatores do $Newt(f)$ para ver se algum deles leva a uma fatoração de $f$. Ou seja, se o algoritmo retornar falhou e

$f = gh$ então teríamos uma decomposição $P_f = P_g + P_h$. Como o algoritmo faz o levantamento para todos pares de fatores do $Newt(f)$ este deveria ter obtido sucesso.

Caso contrário o algoritmo retornará um candidato a fator do polinômio $f$.

**Exemplo 5.5.2.** *Neste exemplo vamos fatorar o polinômio* $f = x^2 + y^2 + x^3 + x^3y^2$ *via politopos nos números inteiros. Observe que, como visto no exemplo 5.4.1, o conjunto* $\Gamma = \{\delta_1, \delta_2\}$, *onde* $\delta_1$ *vai do vértice* $(0, 2)$ *ao* $(2, 0)$ *e* $\delta_2$ *vai do vértice* $(2, 0)$ *ao* $(3, 0)$, *é um conjunto dominante irredundante do* $Newt(f)$ *na direção* $r = (1, 1)$. *Note que* $f_0^{\delta_1} = x^2 + y^2$, $f_1^{\delta_1} = x^3$, $f_2^{\delta_1} = 0$, $f_3^{\delta_1} = x^3y^2$, $g_0^{\delta_1} = g_{02}y^2 + g_{11}xy + g_{20}x^2$, $g_1^{\delta_1} = g_{21}x^2y + g_{12}xy^2$, $g_2^{\delta_1} = g_{22}x^2y^2$, $h_0^{\delta_1} = h_{00}$, $h_1^{\delta_1} = h_{10}x$. *Fazendo a mudança de variável temos:* $F_0^{\delta_1} = z^2 + 1$, $F_1^{\delta_1} = z^2$, $F_2^{\delta_1} = 0$, $F_3^{\delta_1} = 1$, $G_0^{\delta_1} = g_{02} + g_{11}z + g_{20}z^2$, $G_1^{\delta_1} = g_{21}z + g_{12}$, $G_2^{\delta_1} = g_{22}$, $H_0^{\delta_1} = h_{00}$, $H_1^{\delta_1} = h_{10}$.

*De acordo com o lema 5.5.2 temos que*

$$F_0^{\delta_1} = G_0^{\delta_1} H_0^{\delta_1},$$

*ou seja,*

$$z^2 + 1 = (g_{02} + g_{11}z + g_{20}z^2)(h_{00}).$$

*Resolvendo o sistema encontramos* $g_{11} = 0$, $g_{02} = 1$, $g_{20} = 1$ *e* $h_{00} = 1$. *Que leva a* $G_0^{\delta_1} = z^2 + 1$ *e* $H_0^{\delta_1} = 1$. *Observe, que neste momento, determinamos os coeficientes sobre a reta* $\ell_{\delta_1} = 0$.

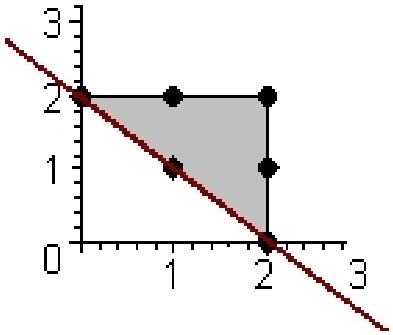


*Figura 5.13: coeficientes determinados sobre a reta* $\ell_{\delta_1} = 0$

*Note que a aresta* $\delta_1$ *tem as propriedades necessárias de acordo com o lema 5.5.1, logo, esta pode ser levantada. Ou seja,* $n_{\delta_1} = 3$ *e* $m_{\delta_1} = 2$ *conforme pode ser observado na figura 5.13. Calculamos* $V = 1$ *e* $U = 0$*. Precisamos resolver*

$$G_1^{\delta_1} - \{V(F_1^{\delta_1}) \bmod G_0^{\delta_1}\} = \epsilon G_0^{\delta_1},$$

*ou seja,*

$$(g_{21}z + g_{12}) - (-1) = \epsilon G_0^{\delta_1}.$$

*Note que* $d = 1$ *e* $n_{\delta_1} - 1 = 2$*, então* $\epsilon = 0$*. E assim, resolvendo o sistema, chegamos a* $g_{21} = 0$ *e* $g_{12} = -1$*. Logo,* $G_1^{\delta_1} = -1$*. Agora, calculamos* $H_1^{\delta_1}$*. Chegamos a* $h_{10} = 1$ *e assim* $H_1^{\delta_1} = 1$*. Observe, que neste momento, determinamos os coeficientes sobre a reta* $\ell_{\delta_1} = 1$*.*

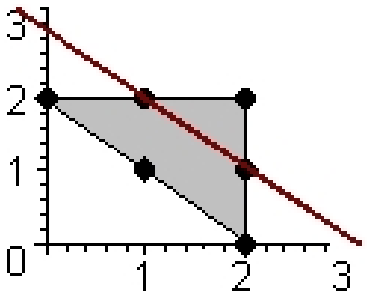


*Figura 5.14: coeficientes determinados sobre a reta* $\ell_{\delta_1} = 1$

*Note que a aresta* $\delta_1$ *tem as propriedades necessárias de acordo com o lema 5.5.1, logo, esta pode ser levantada. Ou seja,* $n_{\delta_1} = 3$ *e* $m_{\delta_1} = 1$ *conforme pode ser observado na figura 5.14. Agora, vamos calcular* $G_2^{\delta_1}$*. Precisamos resolver o seguinte sistema*

$$G_2^{\delta_1} - \{V(F_2^{\delta_1} - G_1^{\delta_1} H_1^{\delta_1}) \bmod G_0^{\delta_1}\} = \epsilon G_0^{\delta_1},$$

*ou seja,*

$$g_{22} - 1 = \epsilon(z^2 + 1).$$

*Note que* $d = 0$*. Então* $\epsilon = 0$*.Resolvendo o sistema, obtemos* $g_{22} = 1$*. Logo,* $G_2^{\delta_1} = 1$*. Observe, que neste momento, determinamos os coeficientes sobre a reta* $\ell_{\delta_1} = 2$*.*

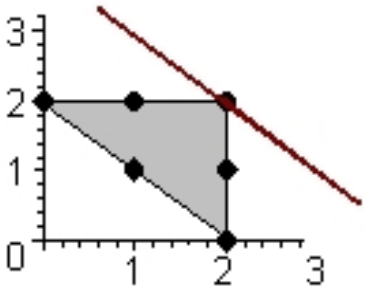


*Figura 5.15: coeficientes determinados sobre a reta* $\ell_{\delta_1} = 2$

*Fatorando via politopos encontramos*

$$x^2 + y^2 + x^3 + x^3y^2 = (x^2 + y^2 - xy^2 + x^2y^2)(1 + x).$$

# 6 CONCLUSÃO

Possivelmente nossa maior contribuicão presente nesta dissertação seja o seu texto, em português, sobre pesquisas recentes que ligam geometria à fatoração de polinômios, um tema inicialmente algébrico. Mais especificamente, estudamos decomposição de politopos e suas aplicações na fatoração de polinômios.

No capítulo 2 apresentamos um apanhado de resultados acerca de conjuntos convexos, especificamente politopos, que deram base para os capítulos posteriores. Estudamos as consequências que um politopo integralmente indecomponível tem sobre os polinômios. Ou seja, estudamos construções de politopos integralmente indecomponíveis que levam a critérios de irredutibilidade de polinômios.

Os algoritmos sobre decomponibilidade e indecomponibilidade de politopos, que nos trabalhos originais estavam obscuros, foram descritos detalhadamente no capítulo 4, sempre ilustrados com exemplos e comentários sobre suas possíveis aplicações.

Enquanto a dissertação estava sendo feita, uma pergunta continuava em aberto: Podemos fatorar o polinômio $f$ via a decomposição do seu politopo de Newton associado, ou seja, se $Newt(f) = Q + R$ existe um fator $g$ do polinômio $f$ cujo politopo de Newton associado é dado por $Q$.

Em 2004 a questão foi respondida. Fatima Abu Salem, Shuhong Gao e Alan G. B. Lauder desenvolveram um algoritmo derivado do método de Hensel para fatorar polinômios bivariados a partir da decomposição do seu politopo de Newton associado.

Depois de termos estudado todos estes problemas, podemos concluir que, em um certo sentido, todas as perguntas envolvendo o politopo de newton associado de um polinômio $f$ foram respondidas. Isto é, se o politopo de Newton associado ao polinômio $f$ for integralmente indecomponível então $f$ será absoluta-

mente irredutível. É bom relembrar, como pode ser visto no exemplo 4.4.5, que mesmo o politopo de Newton associado a $f$ sendo integralmente decomponível $f$ pode ou não ser redutível. No entanto, podemos procurar um fator do polinômio via politopos, graças ao algoritmo apresentado aqui. Naturalmente que ainda há problemas a serem resolvidos nesse ciclo, em particular, na busca de melhorias que tornem os algoritmos mais eficientes

Como trabalho a ser feito a partir desta dissertação, acreditamos que possamos contribuir efetivamente para uma melhor compreensão da área. Especificamente, queremos construir famílias de polinômios esparsos em $\mathbb{F}[x_1, \ldots, x_n]$ que quando reduzidos para $\mathbb{F}[x, y]$ continuem esparsos e, assim, usarmos o levantamento via politopos para sua fatoração.

# BIBLIOGRAFIA


[1] Aho, A. V., Hopcroft, J. E., and Ullman, J. D. *The Design and Analysis of Computer Algorithms*. Addison Wesley, 1974.

[2] Baase, S. *Computer Algorithms: Introduction to Design and Analysis*. Addison-Wesley, 1988.

[3] Ewald, G. *Combinatorial Convexity and Algebraic Geometry, GTM 168.* Springer, 1996.

[4] Gao, S. Absolute irreducibility of polynomials via newton polytopes. *J. of Algebra 237* (2001), 501–520.

[5] Gao, S. Factoring mutivariate polynomials via partial differential equations. *Mathematics of Computation 72* (2003), 801–822.

[6] Gao, S., and Lauder, A. Decomposition of polytopes and polynomials. *Discrete and Computational Geometry 26* (2001), 89–104.

[7] Gao, S., and Lauder, A. G. Hensel lifting and bivariate polynomial factorisation over finite fields. *Mathematics of Computation 71* (2002), 1663–1676.

[8] Gao, S., and Lauder, A. G. Fast absolute irreducibility testing via newton polytopes. *Pre print* (2004), 1–13.

[9] Gathen, J. V. Z., and Gerhard, J. *Modern Computer Algebra*. Cambridge University Press, 1999.

[10] Grahan, R. L. An efficient algorithm for determining the convex hull of a finite planar set. *Information Processing Letters 1* (1972), 132–133.

[11] Grünbaum, B. *Convex Polytopes*. Graduate Texts in Mathematics,Springer, 2003.

[12] Hilbert, D. Über die irreducibilität rationaler functionen mit ganzzahligen coefficientes. *Journal für die Reine und Angewandte Mathematik 110* (1892), 104–129.

[13] Hoppen, C. *Uma Generalização do Algoritmo de Gao para Fatoração de Polinômios*. Dissertação de Mestrado - PPG Matemática Aplicada - UFRGS, 2004.

[14] Kalai, G., and Ziegler, G. M. *Polytopes-Combinatorics and Computation*. Birkhäuser, 2000.

[15] Kaltofen, E. Effective noether irreducibility forms and aplications. *Journal of Computer and System Sciences 50* (1995), 274–295.

[16] Ostrowski, A. M. Über die bedeutung der theorie der konvexen polyeder für die formale algebra. *Jahresberichte Deutsche Math. 30* (1921), 98–99.

[17] Rourke, J. O. *Computational Geometry in C*. Cambridge University Press, 1998.

[18] Salem, F. A., Gao, S., and Lauder, A. G. Factoring polynomials via polytopes. *Proceeding of ISSAC 2004* (2004), 4–11.

[19] Salem, F. A., Gao, S., and Lauder, A. G. Factoring polynomials via polytopes: Extended version. *Report PRD-RR-04-07 Oxford University Computing Laboratory* (2004).

[20] Schneider, R. *Convex bodies: the Brunn-Minkowski theory - Encycopledia of Mathematics and its Applications*. Cambridge, 1993.

[21] Smilansky, Z. An indecomposable polytope all of whose facets are decomposable. *Mathematika 33*, 2 (1986), 192–196.

[22] Trevisan, V. Polynomial factorization ii. *Mathematica Contemporânea 7* (1994), 185–198.

[23] Zassenhauss, H. On hensel factorization, i. *Journal of Numberr Theory 1* (1969), 291–311.

[24] Ziegler, G. M. *Lectures on Polytopes*. Graduate Texts in Mathematics, Springer, 1995.

# APÊNDICE A LEVANTAMENTO DE HENSEL

Neste apêndice estudaremos as idéias básicas do levantamento de Hensel que podem ser encontradas na literatura em [9, 7, 22], pois precisaremos delas quando estivermos estudando o algoritmo de fatoração de polinômios via politopos.

Denote $T(n,q)$ o conjunto de todos os polinômios em $\mathbb{F}_q[x,y]$ de grau total $n$ que são mônicos em $x$ e tem grau $n$ em $x$. Seja $f \in T(n,q)$ com $f = gh$ onde $g$, $h \in \mathbb{F}_q[x][[y]]$ são séries de potência não constante. Diremos que $f = gh$ é uma fatoração analítica de $f$ no ideal primo gerado por $y$. Se ambos $g$ e $h$ estão no subanel $\mathbb{F}_q[x,y]$ então nos referimos a $f = gh$ como uma fatoração polinomial de $f$. Toda fatoração analítica de $f$ pode, em princípio, ser encontrada usando polígonos de Newton e uma forma de levantamento Hensel com respeito ao ideal primo $(y)$. Suponha que $f = gh$ para certas séries de potência $g$, $h \in \mathbb{F}_q[x][[y]]$. Primeiro de tudo devemos examinar como os coeficientes de $f$,$g$ e $h$ são descritos como expansões em $y$. Seja $f = \sum_{k=0}^{n} f_k y^k$, $g = \sum_{k\geq 0} g_k y^k$ e $h = \sum_{k\geq 0} h_k y^k$. Aqui $f_k$,$g_k$,$h_k \in \mathbb{F}_q[x]$. Já que $f \bmod y = gh \bmod y$ então temos que $f_0 = g_0 h_0$. Igualando os coeficientes de $y^k$ para $k \geq 1$ em ambos os lados de $f = gh$ vemos que

$$\begin{aligned} f_1 &= g_0 h_1 + g_1 h_0 \\ f_2 &= g_0 h_2 + g_1 h_1 + g_2 h_0 \\ &\vdots \quad \vdots \quad \vdots \\ f_k &= \sum_{i=0}^{k} g_i h_{k-i} \\ &\vdots \quad \vdots \quad \vdots \end{aligned}$$

Então para $k \geq 1$ temos que

$$g_0 h_k + g_k h_0 = f_k - \sum_{i=1}^{k-1} g_i h_{k-i}. \tag{A.1}$$

Agora, seja $d = mdc(g_0, h_0)$ com $u$ e $v$ escolhidos de tal forma que $ug_0 + vh_0 = d$ e $grau(u) < grau(h_0)$, $grau(v) < grau(g_0)$. Então $d$ divide o lado direito da equação e vemos que $g_k$ e $h_k$ devem ser da forma

$$g_k = v\frac{f_k - \sum_{i=1}^{k-1} g_i h_{k-i}}{d} + \omega_k \frac{g_0}{d} \tag{A.2}$$

$$h_k = u\frac{f_k - \sum_{i=1}^{k-1} g_i h_{k-i}}{d} - \omega_k \frac{h_0}{d} \tag{A.3}$$

para algum polinômio $\omega_k \in \mathbb{F}_q[x]$. Então obtemos equações que descrevem os coeficientes $f_k$, $g_k$ e $h_k$ das expansões de $f$,$g$ e $h$ respectivamente. Considere agora a situação na qual temos um polinômio $f = \sum_{k=0}^{n} f_k y^k$ e uma fatoração $f_0 = g_0 h_0 \in \mathbb{F}[x]$. É possível usar as equações A.2 e A.3 para definir uma sequência de polinômios $\{g_k\}_{k\geq 0}$ e $\{h_k\}_{k\geq 0}$ tal que $g = \sum_{k\geq 0} g_k y^k$ e $h = \sum_{k\geq 0} h_k y^k$ satisfaçam $f = gh \bmod y^{n+1}$? A resposta é sim, desde que a cada estágio $\omega_k$ é escolhido tal que $d$, o máximo divisor comum de $g_0$ e $h_0$ , divide o polinômio $f_k - \sum_{i=1}^{k-1} g_i h_{k-i}$. Se $d = mdc(g_0, h_0) \neq 1$ então a escolha de $\omega_k$ pode não ser única, logo resultando em muitas escolhas para $g_k$'s e $h_k$'s. Se $d = mdc(g_0, h_0) = 1$, a equação A determina unicamente $g_k$ e $h_k$ quando $grau(g_k) < grau(h_0)$ e $grau(h_k) < grau(g_0)$. Isto significa que o levantamento pode ser feito de maneira única.

Estamos interessados em fatoração polinomial mais que em fatoração analítica arbitrária e assim mais algumas observações podem ser feitas. Suponha que tenhamos uma fatoração $f = gh$. Além disso, assumimos que $f$,$g$ e $h$ estão em $\mathbb{F}_q[x, y]$ e $n = grau(f)$, $r = grau(g)$ e $s = grau(h)$. Então $r + s = n$. Por isso para $0 \leq k \leq n$ temos $grau(g_k) \leq r - k$ e $grau(h_k) \leq s - k$. Isto significa que $g_k$ e $h_k$ deveriam ser zero nos casos em que $r - k$ e $s - k$ são menores do que zero, respectivamente.

Suponha agora que tenhamos um polinômio $f \in \mathbb{F}_q[x, y]$ e uma fatoração $f_0 = g_0 h_0$ onde $f = \sum_{k=0}^{n} f_k y^k$ e $g_0$ e $h_0$ são polinômios em $\mathbb{F}_q[x]$ com $grau(g_0) = r$, $grau(h_0) = s$. Desejamos levantar esta fatoração para $\mathbb{F}_q[x, y]$. Quando usarmos as equações A.2 e A.3 para definirmos os polinômios $g_k$ e $h_k$ devemos escolher $\omega_k$ com condições apropriadas sobre os graus. No caso que $grau(f_0) = n$

as restrições são $grau(g_k) < r - k$ e $grau(h_k) \leq s - k$. Quando $mdc(g_0, h_0) = 1$ existirá no máximo um modo disto ser feito. Defina $g_k$ e $h_k$ pelas equações

$$g_k = v(f_k - \sum_{i=1}^{k-1} g_i h_{k-i}) \bmod g_0 \tag{A.4}$$

$$h_k = u(f_k - \sum_{i=1}^{k-1} g_i h_{k-i}) \bmod h_0 \tag{A.5}$$

e então cheque que $grau(g_k) \leq r - k$ e $grau(h_k) \leq s - k$.

Para $n \geq 1$, seja $M(n, q) \subseteq T(n, q)$ o subconjunto de todos os polinômios cuja redução módulo $y$ é livre de quadrados.

**Algoritmo A.0.2 (Levantamento de Hensel).** *Entrada: Um polinômio* $f = \sum_{k=0}^{n} f_k y^k$ *em* $M(n, q)$*, onde* $f_k \in \mathbb{F}_q[x]$*. Saída: Todos os fatores mônicos de* $f$ *com grau total entre* $1$ *e* $\lfloor n/2 \rfloor$*.*

*Passo 1: Usar um algoritmo de fatoração polinomial univariada para fatorar* $f_0$*, um polinômio livre de quadrados. Se* $f_0$ *é irredutível então pare o algoritmo. Por isso, assuma que* $f_0$ *é redutível. Listar todos os pares* $(g_0, h_0)$ *de fatores mônicos com* $f_0 = g_0 h_0$ *e* $1 \leq grau(g_0) \leq grau(h_0)$*. Para cada par* $(g_0, h_0)$*, faça os passos* $2 - 4$ *onde* $r = grau(g_0)$ *logo* $1 \leq r \leq \lfloor n/2 \rfloor$*.*

*Passo 2: Computar polinômios* $u$ *e* $v$ *com* $ug_0 + vh_0 = 1$ *e* $grau(u) < grau(h_0)$*,* $grau(v) < grau(g_0)$*.*

*Passo 3: Para* $k$ *de* $1$ *até* $\lfloor n/2 \rfloor$*, computar*

$$g_k = v \left\{ f_k - \sum_{i=1}^{k-1} g_i h_{k-i} \right\} \bmod g_0 \tag{A.6}$$

*e*

$$h_k = u \left\{ f_k - \sum_{i=1}^{k-1} g_i h_{k-i} \right\} \bmod h_0 \tag{A.7}$$

*No caso que* $r \geq k$ *cheque que* $grau(g_k) \leq r - k$*, e no caso que* $k > r$ *cheque de qualquer forma* $g_k = 0$*. Se uma dessas duas condições não for satisfeita então pare a computação para este par.*

*Passo 4: cheque que* $g := \sum_{k=0}^{r} g_k y^k$ *divide* $f$*. Se sim então retorne* $g$*.*

Esta é a essência do levantamento de Hensel para fatorar polinômios, e uma prova de sua corretude segue facilmente do que já foi discutido.

# APÊNDICE B EXEMPLO DE FATORAÇÃO VIA POLITOPOS

**Exemplo B.0.3.** *Neste exemplo vamos fatorar o polinômio* $f = (x^8+x^4)y^6+(x^7+x^4+x^8)y^5+(x^8+2x^6+2x^4+2x^{10}+x^7+2x^2)y^4+(x^2+2x^7+x^4+x^{10}+x^5+x^9)y^3+(x^7+2x^8+x^{12}+x^{10}+1+3x^4+x^6+2x^2)y^2+(x^9+x^5+x^7+x^8+x^4)y+x^4+2x^6+x^{10}+x^2+x^8$, *cujo politopo de Newton associado é dado pela figura B.1, via politopos.*

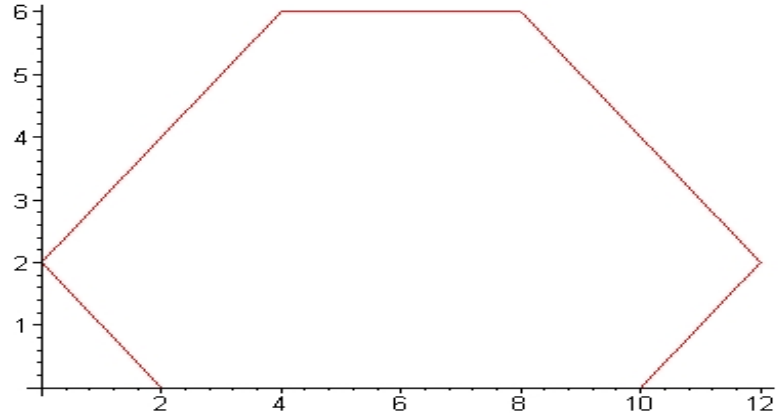


*Figura B.1: politopo de Newton associado a f*

*Usando o algoritmo 4.4.2 encontramos as decomposições integrais de* $P_f$ *tais que* $P_f = P_g + P_h$. *Escolhemos a decomposição dada pelas figuras B.2 para g e B.3 para h.*

*Então os polinômios genéricos associados a B.2 e B.3 são, respectivamente:* $g := g_{20}x^2 + g_{30}x^3 + g_{40}x^4 + g50x^5 + g_{60}x^6 + g_{11}x^1y^1 + g_{21}x^2y + g_{31}x^3y + g_{41}x^4y + g_{51}x^5y + g_{61}x^6y + g_{71}x^7y + g_{02}y^2 + g_{12}xy^2 + g_{22}x^2y^2 + g_{32}x^3y^2 + g_{42}x^4y^2 + g_{52}x^5y^2 + g_{62}x^6y^2 + g_{72}x^7y^2 + g_{82}x^8y^2 + g_{13}xy^3 + g_{23}x^2y^3 + g_{33}x^3y^3 + g_{43}x^4y^3 + g_{53}x^5y^3 + g_{63}x^6y^3 + g_{73}x^7y^3 + g_{24}x^2y^4 + g_{34}x^3y^4 + g_{44}x^4y^4 + g_{54}x^5y^4 + g_{64}x^6y^4$ *e* $h := h_{00} + h_{10}x + h_{20}x^2 + h_{30}x^3 + h_{40}x^4 + h_{11}xy + h_{21}x^2y + h_{31}x^3y + h_{22}x^2y^2$.

*Seja* $\delta_1$ *a aresta do* $newt(f)$ *que vai do vértice* $(0,2)$ *ao vértice* $(2,0)$, $\delta_2$ *a aresta do* $newt(f)$ *que vai do vértice* $(2,0)$ *ao vértice* $(10,0)$ *e* $\delta_3$ *a aresta do*

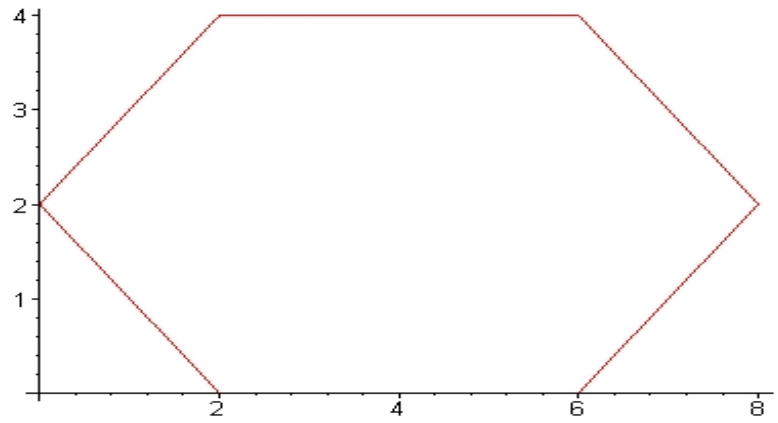


*Figura B.2: politopo de Newton $P_g$ associado ao polinômio genérico g*

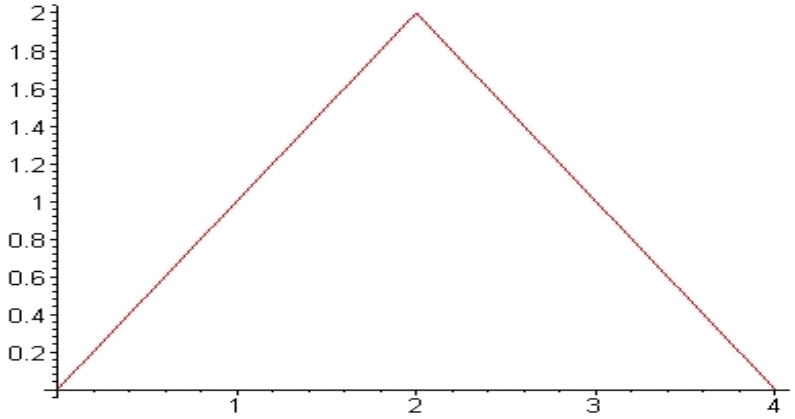


*Figura B.3: politopo de Newton $P_h$ associado ao polinômio genérico h*

*$newt(f)$ que vai do vértice $(10, 0)$ ao vértice $(12, 2)$. Note que $\Gamma = \{\delta_1, \delta_2, \delta_3\}$ é um conjunto dominante irredundante do $Newt(f)$ na direção $r = (0, 1)$, conforme pode ser observado na figura B.4.*

*Agora, para $\delta_1$, vamos calcular as $f_i^{\delta_1}(x, y)$ para $i \geq 0$. Note que, os termos de $f_i^{\delta_1}$ são os termos do polinômio $f$ cujos expoentes vetoriais estão sobre a reta $\ell_{\delta_1} = i$.*

$$f_0^{\delta_1}(x, y) = x^2 + y^2,$$

$$f_1^{\delta_1}(x, y) = 0,$$

$$f_2^{\delta_1}(x, y) = 2x^2y^2 + x^4,$$

$$f_3^{\delta_1}(x, y) = x^2y^3 + x^4y,$$

$$f_4^{\delta_1}(x, y) = 2x^6 + 2x^2y^4 + 3x^4y^2 + x^5y,$$

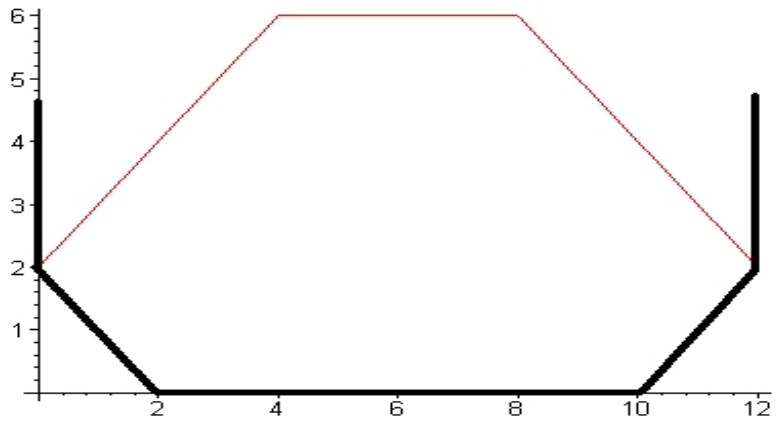


*Figura B.4: conjunto dominante irredundante do $Newt(f)$*

$$f_5^{\delta_1}(x,y) = x^4y^3,$$

$$f_6^{\delta_1}(x,y) = x^8 + x^6y^2 + x^7y + 2x^4y^4 + x^5y^3,$$

$$f_7^{\delta_1}(x,y) = x^8y + x^4y^5 + x^7y^2,$$

$$f_8^{\delta_1}(x,y) = x^{10} + x^4y^6 + x^9y + 2x^8y^2 + 2x^6y^4 + 2x^7y^3,$$

$$f_9^{\delta_1}(x,y) = x^7y^4,$$

$$f_{10}^{\delta_1}(x,y) = x^{10}y^2 + x^9y^3 + x^7y^5 + x^8y^4,$$

$$f_{11}^{\delta_1}(x,y) = x^{10}y^3 + x^8y^5 \ \ e$$

$$f_{12}^{\delta_1}(x,y) = x^{12}y^2 + x^8y^6 + 2x^{10}y^4.$$

*Observe que os $g_i^{\delta_1}$ e $h_i^{\delta_1}$ são obtidos do mesmo modo. Fazendo as mudanças de variável descritas no lema 5.5.2 para $\delta_1$, obtemos:*

$$F_0^{\delta_1} = 1 + z^2,$$

$$F_1^{\delta_1} = 0,$$

$$F_2^{\delta_1} = 2 + z^2,$$

$$F_3^{\delta_1} = z^{-1} + z,$$

$$F_4^{\delta_1} = 2z^2 + 2z^{-2} + 3 + z,$$

$$F_5^{\delta_1} = z^{-1},$$

$$F_6^{\delta_1} = z^2 + 1 + z + 2z^{-2} + z^{-1},$$

$$F_7^{\delta_1} = z + z^{-3} + 1,$$

$$F_8^{\delta_1} = z^2 + z^{-4} + z + 2 + 2z^{-2} + 2z^{-1},$$

$$F_9^{\delta_1} = z^{-2},$$

$$F_{10}^{\delta_1} = 1 + z^{-1} + z^{-3} + z^{-2},$$

$$F_{11}^{\delta_1} = z^{-1} + z^{-3} \ e$$

$$F_{12}^{\delta_1} = 1 + z^{-4} + 2z^{-2}.$$

*Note que esta mudança de variável funciona do mesmo jeito para os polinômiuos genéricos $g$ e $h$. Assim como, a mudança de variável das arestas $\delta_2$ e $\delta_3$ seguem de modo similar.*

*Agora estamos prontos para começar a fatoração do polinômio $f$ via politopos sobre os números inteiros.*

***Passo 1 do algoritmo 5.5.1***

*Começamos calculando $G_0^{\delta}$ e $H_0^{\delta}$ para as arestas do conjunto dominante irredundante.*

*Calculando para $\delta_1$:*

$$F_0^{\delta_1} = G_0^{\delta_1} H_0^{\delta_1}.$$

$$(1 + z^2) = (g_{20}z^2 + g_{11}z + g_{02})(h_{00}). \tag{B.1}$$

*Note que $g_{20} \neq 0$, $g_{02} \neq 0$ e $h_{00} \neq 0$, pois correspondem a vértices dos polígonos $P_g$ e $P_h$. Resolvendo o sistema que obtemos quando igualamos os coeficientes dos polinômios de $z$ em ambos os lados da equação B.1, obtemos: $g_{11} = 0$, $g_{20} = 1$, $h_{00} = 1$ e $g_{02} = 1$. Logo,*

$$G_0^{\delta_1} = z^2 + 1 \ e \ H_0^{\delta_1} = 1.$$

*Conforme pode ser observado na figura B.5, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico $g$ cujos expoentes vetoriais estão sobre a reta $\ell_{\delta_1} = 0$.*

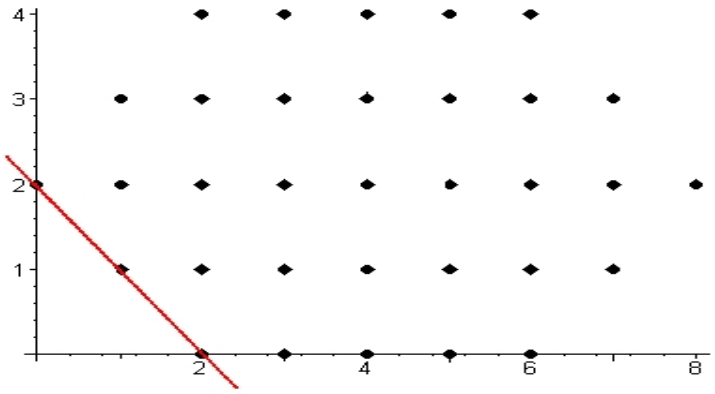


*Figura B.5:* $\ell_{\delta_1} = 0$

*Calculando para* $\delta_2$*:*

$$F_0^{\delta_2} = G_0^{\delta_2} H_0^{\delta_2}$$

$$(1+z^2+2z^4+z^6+z^8) = (1+g_{30}z+g_{40}z^2+g_{50}z^3+g_{60}z^4)(1+h_{10}z+h_{20}z^2+h_{30}z^3+h_{40}z^4) \tag{B.2}$$

*Note que* $g_{60} \neq 0$ *e* $H_{40} \neq 0$*. Resolvendo o sistema que obtemos quando igualamos os coeficientes dos polinômios de* $z$ *em ambos os lados da equação B.2, temos:* $g_{30} = 0$*,* $g_{40} = 0$*,* $g_{50} = 0$*,* $g_{60} = 1$*,* $h_{10} = 0$*,* $h_{20} = 1$*,* $h_{30} = 0$ *e* $h_{40} = 1$*. Logo:*

$$G_0^{\delta_2} = 1 + z^4 \text{ e } H_0^{\delta_2} = 1 + z^2 + z^4.$$

*Conforme pode ser observado na figura B.6, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico* $g$ *cujos expoentes vetoriais estão sobre a reta* $\ell_{\delta_2} = 0$*.*

*Calculando para* $\delta_3$*:*

$$F_0^{\delta_3} = G_0^{\delta_3} H_0^{\delta_3}$$

$$(1 + z^2) = (1 + g_{71}z + g_{82}z^2)(1) \tag{B.3}$$

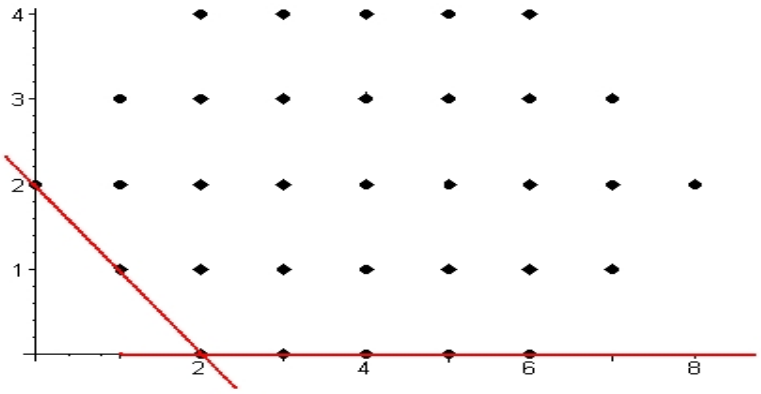


*Figura B.6:* $\ell_{\delta_2} = 0$

*Note que* $g_{82} \neq 0$. *Resolvendo o sistema que obtemos quando igualamos os coeficientes de* $z$ *em B.3, obtemos:* $g_{71} = 0$ *e* $g_{82} = 1$. *Logo,*

$$G_0^{\delta_3} = 1 + z^2 \text{ e } H_0^{\delta_3} = 1.$$

*Conforme pode ser observado na figura B.7, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico* $g$ *cujos expoentes vetoriais estão sobre a reta* $\ell_{\delta_3} = 0$.

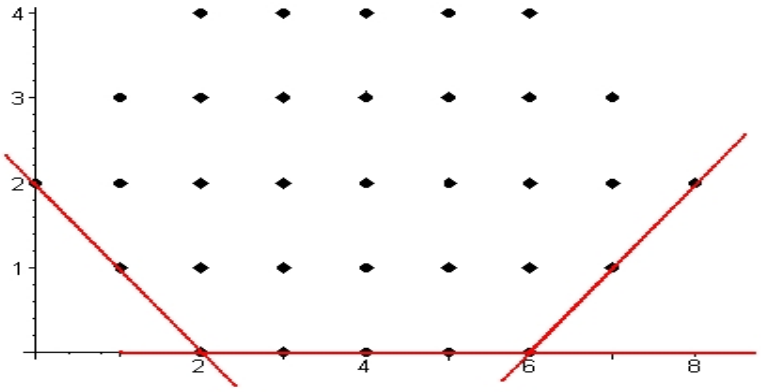


*Figura B.7:* $\ell_{\delta_3} = 0$

***Passo 2 do algoritmo 5.5.1***

*Neste momento observe que de acordo com a figura B.7 temos:*

$$n_{\delta_1} = 3 \quad n_{\delta_2} = 5 \quad n_{\delta_3} = 3$$
$$m_{\delta_1} = 2 \quad m_{\delta_2} = 5 \quad m_{\delta_3} = 2$$

*De acordo com o lema 5.5.1 as arestas* $\delta_1$ *e* $\delta_2$ *podem ser levantadas. Escolhemos* $\delta_1$ *para iniciar o levantamento. Vamos calcular* $V_{\delta_1}$ *e* $U_{\delta_1}$ *tais que*

$$V_{\delta_1} H_0^{\delta_1} + U_{\delta_1} G_0^{\delta_1}.$$

*Encontramos:*

$$V_{\delta_1} = 1 \text{ e } U_{\delta_1} = 0.$$

*Vamos calcular* $G_1^{\delta_1} = \underbrace{g_{21}z + g_{12}}_{m_{\delta_1}=2}$.

$$G_1^{\delta_1} - \{V^{\delta_1}(F_1^{\delta_1}) \bmod G_0^{\delta_1}\} = \epsilon G_0^{\delta_1}.$$

$$(\underbrace{g_{21}z + g_{12}}_{d=1}) = \epsilon(1 + z^2) \tag{B.4}$$

*Como* $d = 1 < n_{\delta_1} - 1 = 2$ *então* $\epsilon = 0$. *Igualando os polinômios em B.4 e resolvendo o sistema obtemos* $g_{21} = 0$ *e* $g_{12} = 0$. *Temos que:*

$$G_1^{\delta_1} = 0 \text{ e } H_1^{\delta_1} = 0.$$

*Conforme pode ser observado na figura B.8, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico g cujos expoentes vetoriais estão sobre a reta* $\ell_{\delta_1} = 1$.

*Neste momento observe que de acordo com a figura B.8 temos:*

$$n_{\delta_1} = 3 \quad n_{\delta_2} = 5 \quad n_{\delta_3} = 3$$
$$m_{\delta_1} = 3 \quad m_{\delta_2} = 4 \quad m_{\delta_3} = 2$$

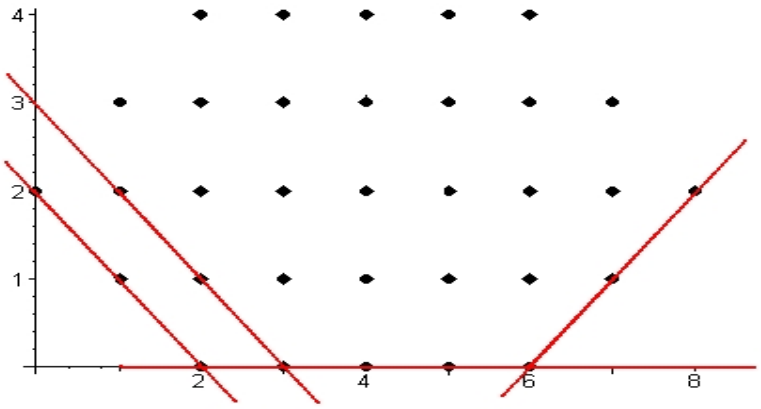


*Figura B.8:* $\ell_{\delta_1} = 1$

*Então, de acordo com o lema 5.5.1, as arestas* $\delta_2$ *e* $\delta_3$ *podem ser levantadas. Escolhemos a aresta* $\delta_2$*. Vamos calcular* $G_1^{\delta_2} = \underbrace{g_{31}z + g_{41}z^2 + g_{51}z^3 + g_{61}z^4}_{m_{\delta_2}=4}$*. Temos que:*

$$V_{\delta_2} = -z^2 \text{ e } U_{\delta_2} = 1 + z^2.$$

*Vamos resolver:*

$$G_1^{\delta_2} - \{V^{\delta_2}(F_1^{\delta_2}) \bmod G_0^{\delta_2}\} = \epsilon G_0^{\delta_2}.$$

$$\underbrace{g_{31}z + g_{41}z^2 + (g_{51} - 1)z^3 + g_{61}z^4}_{d=3} = \epsilon(1 + z^4) \tag{B.5}$$

*Como* $d = 3 < n_{\delta_2} - 1 = 4$ *então* $\epsilon = 0$*. Igualando os polinômios em B.5 e resolvendo o sistema obtemos* $g_{31} = 0$*,* $g_{41} = 0$*,* $g_{51} = 1$ *e* $g_{61} = 0$*. Logo* $G_1^{\delta_2} = z^3$*. Vamos calcular* $H_1^{\delta_2} = h_{11}z + h_{21}z^2 + h_{31}z^3$*.*

$$H_1^{\delta_2} = \frac{F_1^{\delta_2} - G_1^{\delta_2}H_0^{\delta_2}}{G_0^{\delta_2}} = z^2.$$

$$h_{11}z + h_{21}z^2 + h_{31}z^3 = z^2. \tag{B.6}$$

*Igualando os polinômios em B.6 obtemos:* $h_{11} = 0$*,* $h_{21} = 1$ *e* $h_{31} = 0$*. Temos que*

$$G_1^{\delta_2} = z^3 \text{ e } H_1^{\delta_2} = z^2.$$

*Conforme pode ser observado na figura B.9, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico g cujos expoentes vetoriais estão sobre a reta* $\ell_{\delta_2} = 1$*.*

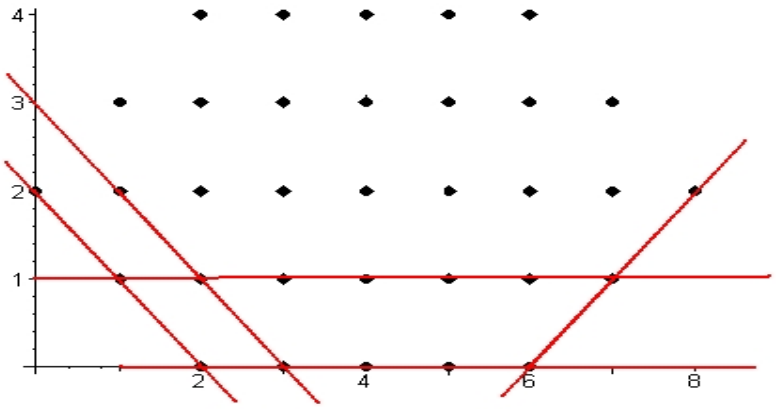


*Figura B.9:* $\ell_{\delta_2} = 1$

*Neste momento observe que de acordo com a figura B.9 temos:*

$$n_{\delta_1} = 3 \quad n_{\delta_2} = 5 \quad n_{\delta_3} = 3$$
$$m_{\delta_1} = 2 \quad m_{\delta_2} = 6 \quad m_{\delta_3} = 1$$

*Então, de acordo com o lema 5.5.1, as arestas* $\delta_1$ *e* $\delta_3$ *podem ser levantadas. Escolhemos a aresta* $\delta_1$*. Vamos calcular* $G_2^{\delta_1} = \underbrace{g_{22} + g_{13}z^{-1}}_{m_{\delta_1}=2}$*.*

$$G_2^{\delta_1} - \{V^{\delta_1}(F_2^{\delta_1} - G_1^{\delta_1}H_1^{\delta_1}) \bmod (G_0^{\delta_1})\} = \epsilon G_0^{\delta_1}.$$

$$\underbrace{(g_{22} - 1) + g_{13}z^{-1}}_{d=1} = \epsilon(z^2 + 1) \tag{B.7}$$

*Como* $d = 1 < n_{\delta_1} - 1 = 2$ *então* $\epsilon = 0$*. Igualando os polinômios em B.7 e resolvendo o sistema obtemos* $g_{22} = 1$ *e* $g_{13} = 0$*. Logo:*

$$G_2^{\delta_1} = 1 \text{ e } H_2^{\delta_1} = 1.$$

*Conforme pode ser observado na figura B.10, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico g cujos expoentes vetoriais estão sobre a reta* $\ell_{\delta_1} = 2$*.*

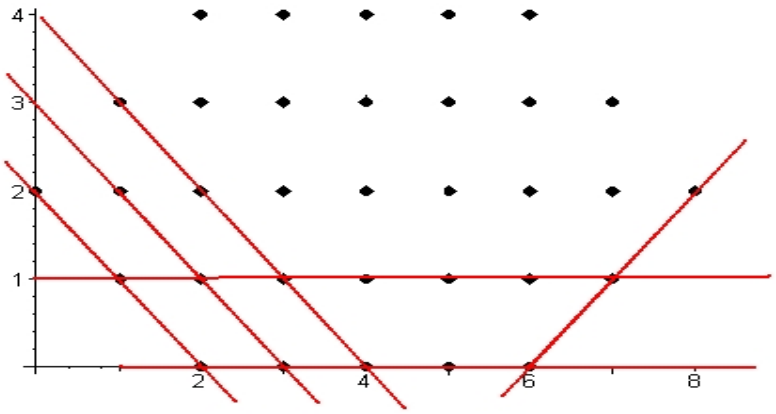


*Figura B.10:* $\ell_{\delta_1} = 2$

*Neste momento observe que de acordo com a figura B.10 temos:*

$$n_{\delta_1} = 3 \quad n_{\delta_2} = 5 \quad n_{\delta_3} = 3$$

$$m_{\delta_1} = 2 \quad m_{\delta_2} = 5 \quad m_{\delta_3} = 1$$

*Então, de acordo com o lema 5.5.1, as arestas* $\delta_1$ *e* $\delta_3$ *podem ser levantadas. Escolhemos a aresta* $\delta_1$*. Vamos calcular* $G_3^{\delta_1} = \underbrace{g_{32} + g_{23}z^{-1}}_{m_{\delta_1}=2}$.

$$G_3^{\delta_1} - \{V_{\delta_1}(F_3^{\delta_1} - \sum_{j=1}^{2} G_j^{\delta_1} H_{3-j}^{\delta_1}) \bmod G_0^{\delta_1}\} = \epsilon G_0^{\delta_1}.$$

$$\underbrace{(g_{23} - 1)z^{-1} + g_{32} - z}_{d=2} = \epsilon(1 + z^2) \tag{B.8}$$

*Como* $d = 2 = n_{\delta_1} - 1 = 2$ *então* $grau(\epsilon) = d - (n_{\delta_1} - 1) = 2 - 2 = 0$*. Logo,* $\epsilon = bz^a$*. Onde* $z^a$ *é igual ao termo de mais baixo grau no lado esquerdo de B.8. Então* $a = -1$ *e* $\epsilon = bz^{-1}$*. Resolvendo o sitema obtido quando igualamos os polinômios em B.*8 *obtemos:* $b = -1$*,* $g_{32} = 0$ *e* $g_{23} = 0$*. Logo:*

$$G_3^{\delta_1} = 0 \text{ e } H_3^{\delta_1} = z^{-1}.$$

*Conforme pode ser observado na figura B.11, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico g cujos expoentes vetoriais estão sobre a reta* $\ell_{\delta_1} = 3$.

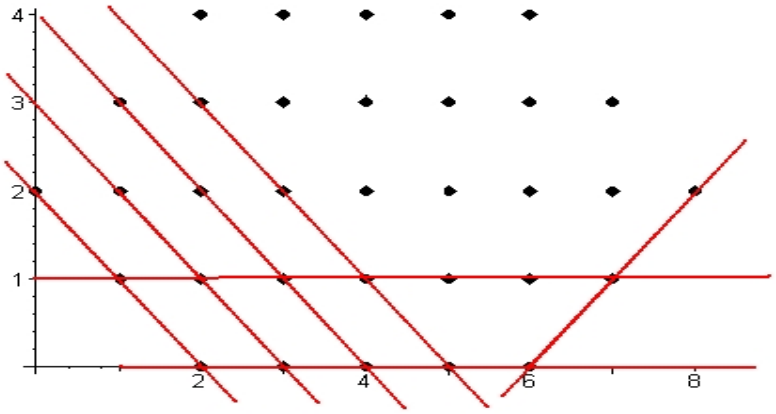


*Figura B.11:* $\ell_{\delta_1} = 3$

*Neste momento observe que de acordo com a figura B.11 temos:*

$$n_{\delta_1} = 3 \quad n_{\delta_2} = 5 \quad n_{\delta_3} = 3$$
$$m_{\delta_1} = 3 \quad m_{\delta_2} = 4 \quad m_{\delta_3} = 1$$

*Então, de acordo com o lema 5.5.1, as arestas* $\delta_2$ *e* $\delta_3$ *podem ser levantadas. Escolhemos a aresta* $\delta_2$*. Vamos calcular*

$$G_2^{\delta_2} = z^{-2} + 1 + \underbrace{g_{42}z^2 + g_{52}z^3 + g_{62}z^4 + g_{72}z^5}_{m_{\delta_2}=4} + z^6.$$

$$\underbrace{z^{-2} + (g_{42}+2)z^2 + g_{52}z^3 + g_{62}z^4 + g_{72}z^5 + z^6}_{d=8} = \epsilon(1+z^4). \tag{B.9}$$

*Como* $d = 8 > n_{\delta_2} - 1 = 4$ *então o* $grau(\epsilon) = 8 - 4 = 4$*. Logo,* $\epsilon$ *tem 5 termos.* $\epsilon = bz^a + cz^{a+1} + dz^{a+2} + ez^{a+3} + fz^{a+4}$*. Onde* $z^a$ *é igual ao termo de mais baixo grau no lado esquerdo de B.9. Logo* $z^a = z^{-2}$ *e assim,* $\epsilon = bz^{-2} + cz^{-1} + d + ez + fz^2$*. Igualando os polinômios em B.9 e resolvendo o sistema, obtemos:* $g_{42} = 0$*,* $g_{52} = 0$*,* $g_{62} = 0$ *e* $g_{72} = 0$*. Agora, vamos calcular* $H_2^{\delta_2} = h_{22}z^2$*.*

$$H_2^{\delta_2} = \frac{F_2^{\delta_2} - G_1^{\delta_2}H_1^{\delta_2} - G_2^{\delta_2}H_0^{\delta_2}}{G_0^{\delta_2}} = z^2.$$

$$h_{22}z^2 = z^2. \tag{B.10}$$

*Igualando os polinômios em B.10, obtemos:* $h_{22} = 1$*. Então:*

$$G_2^{\delta_2} = z^{-2} + 1 + z^6 \text{ e } H_2^{\delta_2} = z^2.$$

*Conforme pode ser observado na figura B.12, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico g cujos expoentes vetoriais estão sobre a reta* $\ell_{\delta_2} = 2$.

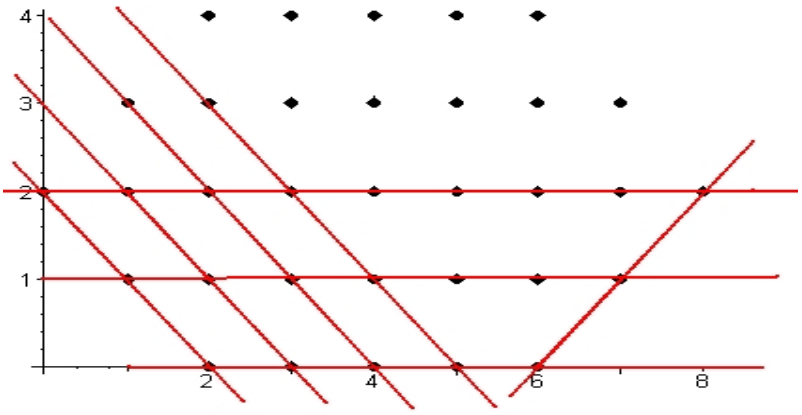


*Figura B.12:* $\ell_{\delta_2} = 2$

*Neste momento observe que de acordo com a figura B.12 temos:*

$$n_{\delta_1} = 3 \quad n_{\delta_2} = 5 \quad n_{\delta_3} = 3$$

$$m_{\delta_1} = 2 \quad m_{\delta_2} = 5 \quad m_{\delta_3} = 1$$

*Então, de acordo com o lema 5.5.1, as arestas* $\delta_1$ *e* $\delta_3$ *podem ser levantadas. Escolhemos a aresta* $\delta_1$. *Vamos calcular* $G_4^{\delta_1} = z^2 + z + \underbrace{g_{33}z^{-1} + g_{24}z^{-2}}_{m_{\delta_1}=2}$.

$$\underbrace{(g_{24} - 2)z^{-2} + g_{33}z^{-1} + z^2}_{d=4} = \epsilon(1 + z^2) \tag{B.11}$$

*Como* $d = 4 > n_{\delta_1} - 1 = 2$ *então* $grau(\epsilon) = 4 - 2 = 2$, *logo,* $\epsilon$ *possui 3 termos. Como feito anteriormente, temos que:* $\epsilon = az^{-2} + bz^{-1} + c$. *Igualando os polinômios em B.11 e resolvendo o sistema temos que :* $g_{33} = 0$ *e* $g_{24} = 1$. *Então:*

$$G_4^{\delta_1} = z^2 + z + z^{-2} \text{ e } H_4^{\delta_1} = 1 + z^{-2}.$$

*Conforme pode ser observado na figura B.13, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico g cujos expoentes vetoriais estão sobre a reta* $\ell_{\delta_1} = 4$.

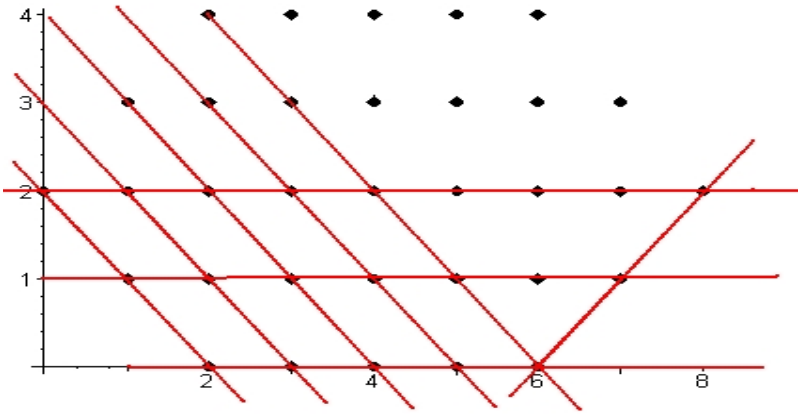


*Figura B.13:* $\ell_{\delta_1} = 4$

*Neste momento observe que de acordo com a figura B.13 temos:*

$$n_{\delta_1} = 3 \quad n_{\delta_2} = 5 \quad n_{\delta_3} = 3$$
$$m_{\delta_1} = 2 \quad m_{\delta_2} = 4 \quad m_{\delta_3} = 1$$

*Então, de acordo com o lema 5.5.1, todas as arestas podem ser levantadas. Escolhemos a aresta* $\delta_2$*. Vamos calcular*

$$G_3^{\delta_2} = \underbrace{g_{43}z^2 + g_{53}z^3 + g_{63}z^4 + g_{73}z^5}_{m_{\delta_2}=4}.$$

$$\underbrace{g_{43}z^2 + (g_{53} - 1)z^3 + g_{63}z^4 + g_{73}z^5}_{d=3} = \epsilon(1 + z^4). \tag{B.12}$$

*Como* $d = 3 < n_{\delta_2} - 1 = 4$ *então* $\epsilon = 0$*. Igualando os polinômios em B.12 e resolvendo o sistema, obtemos:* $g_{43} = 0$*,* $g_{53} = 1$*,* $g_{63} = 0$ *e* $g_{73} = 0$*. Então:*

$$G_3^{\delta_2} = z^3 \text{ e } H_3^{\delta_2} = z^{-1}.$$

*Conforme pode ser observado na figura B.14, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico g cujos expoentes vetoriais estão sobre a reta* $\ell_{\delta_2} = 3$*.*

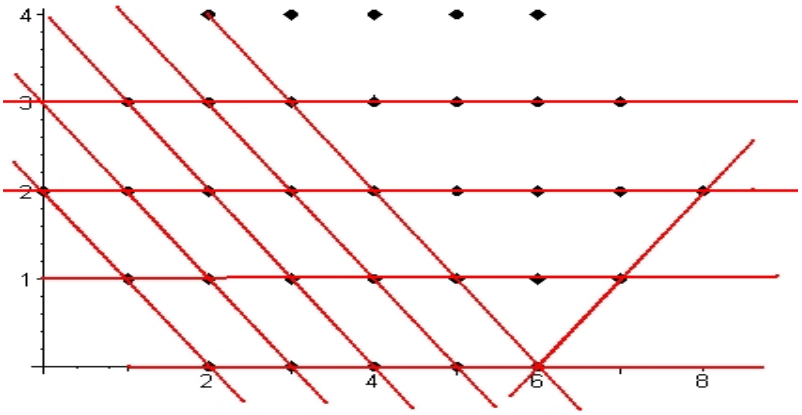


*Figura B.14:* $\ell_{\delta_2} = 3$

*Neste momento observe que de acordo com a figura B.14 temos:*

$$n_{\delta_1} = 3 \quad n_{\delta_2} = 5 \quad n_{\delta_3} = 3$$
$$m_{\delta_1} = 1 \quad m_{\delta_2} = 4 \quad m_{\delta_3} = 1$$

*Então, de acordo com o lema 5.5.1, todas as arestas podem ser levantadas. Escolhemos a aresta* $\delta_2$*. Vamos calcular*

$$G_4^{\delta_2} = 1 + \underbrace{g_{34}z + g_{44}z^2 + g_{54}z^3 + g_{64}z^4}_{m_{\delta_2}=4}.$$

$$\underbrace{1 + g_{34}z + g_{44}z^2 + g_{54}z^3 + g_{64}z^4}_{d=4} = \epsilon(1 + z^4). \tag{B.13}$$

*Como* $d = 4 = n_{\delta_2} - 1 = 4$ *então* $grau(\epsilon) = 0$*. Logo, como feito anteriormente* $\epsilon = a$*. Igualando os polinômios em B.13 e resolvendo o sistema obtemos:* $g_{34} = 0$*,* $g_{44} = 0$*,* $g_{54} = 0$ *e* $g_{64} = 1$*. Então:*

$$G_4^{\delta_2} = 1 + z^4.$$

*Conforme pode ser observado na figura B.15, neste momento acabamos de determinar os coeficientes dos termos do polinômio genérico g cujos expoentes vetoriais estão sobre a reta* $\ell_{\delta_2} = 4$*.*

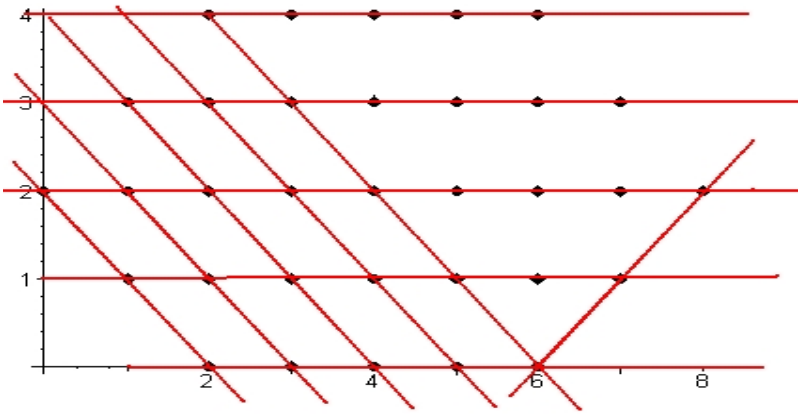


*Figura B.15:* $\ell_{\delta_2} = 4$

*Fazendo a fatoração via politopos obtemos:*

$$g = x^2 + x^6 + x^2y^2 + y^2 + x^8y^2 + x^5y^3 + x^2y^4 + x^6y^4 + x^5y$$

*e*

$$h = 1 + x^2 + x^4 + x^2y + x^2y^2.$$