Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Problemas Diretos em Teoria Aditiva via Método Polinomial: generalização do Teorema de Cauchy-Davenport e da Conjectura de Erdös-Heilbronn

por

Olimpio Ribeiro Gomes

Brasília
2008

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Problemas Diretos em Teoria Aditiva via Método Polinomial: generalização do Teorema de Cauchy-Davenport e da Conjectura de Erdös-Heilbronn

Olimpio Ribeiro Gomes

Tese apresentada ao Departamento de Matemática da Universidade de Brasília como parte dos requisitos para obtenção do grau de

DOUTOR EM MATEMÁTICA

Brasília
2008

Agradecimentos

Agradeço à minha esposa, Rhubia, ao meu pai, Abadio, à minha mãe, Aldenoura e às minhas irmãs, Rubia e Raquel, pelo suporte famliar, ao meu filho, Lucas, por encher minha vida de momentos de indescritível felicidade, a diversos amigos que contribuiram para a concretização deste trabalho entre os quais, Célius Magalhães e Alexandre Zaghetto e ao meu orientador Professor Hemar Godinho por sua paciente e atenciosa orientação.

Resumo

Sejam $A_0, A_1, \cdots, A_{h-1}$ subconjuntos finitos e não vazios de um corpo K e seja $s_k(x_0, x_1, \cdots, x_{h-1})$ o polinômio simétrico elementar de grau k em h variáveis. Apresentamos estimativas para o número de elementos dos conjuntos das imagens de todas as h-uplas de $A_0 \times A_1 \times \cdots \times A_{h-1}$ pelo polinômio s_k, com e sem a restrição de que os elementos em cada upla sejam dois a dois distintos. Em nosso desenvolvimento somos levados a estudar o conjunto das (0,1)-matrizes cuja soma dos vetores-linha é igual ao vetor $\mathbf{c} \in \mathbb{Z}^h$ e cuja soma dos vetores-coluna é igual ao vetor $\mathbf{r} \in \mathbb{Z}^t$. Uma fórmula para o cálculo do número de tais matrizes é apresentada no caso particular em que todas as coordenadas do vetor $\mathbf{r}$ são iguais.

PALAVRAS-CHAVE: Teoria Aditiva, Método Polinomial, $(0,1)$-Matrizes, Caminhos em $\mathbb{Z}^h$.

Abstract

Let $A_0, A_1, \cdots, A_{h-1}$ be finite non empty subsets of a field K and let $s_k(x_0, x_1, \cdots, x_{h-1})$ be the elementary symmetric polinomial of degree k in h indeterminates. Here we present some estimates for the cardinality of the sets of the images of all h-uplas of $A_0 \times A_1 \times \cdots \times A_{h-1}$ by the polinomial s_k, with and without the restriction that the elements of the h-uplas are pairwise distincts. For this purpose, a study of the set of (0,1)-matrices in which the addiction of row-vectors is the vector $\mathbf{c} \in \mathbb{Z}^h$ and in which addiction of the column-vectors is the vector $\mathbf{r} \in \mathbb{Z}^t$ is presented. A formula for the precise number of such matrices is shown in the particular case where all the coordinates of the vector $\mathbf{r}$ are equal.

KEYWORDS: Additive Theory, Polinomial Method, $(0,1)$-Matrices, Paths in $\mathbb{Z}^h$.

Sumário

Lista de Símbolos

Γ	Conjunto de vetores $\beta \in \mathbb{Z}^h$ com exatamente k coordenadas iguais a 1 e $h-k$ coordenadas nulas
$\Omega(\mathbf{c})$	Conjunto de matrizes de zeros e uns com soma dos vetores-linha igual ao vetor $\mathbf{c} \in \mathbb{Z}^h$ e com k uns em cada linha
$P_k(\mathbf{0}, \mathbf{c})$	Número de k-caminhos da origem até o vetor $\mathbf{c}$
Ω_{FG}	$= \{F(a_0, \cdots, a_{h-1}) / a_i \in A_i,\ i = 0, 1, \cdots h-1,\ \text{e}\ G(a_0, \cdots, a_{h-1}) \neq 0\}$
$\mathcal{C}(t)$	$= \{\mathbf{c} = (c_0, \cdots, c_{h-1}) \in \mathbb{Z}^h : 0 \leq c_j \leq t \text{ e } c_0 + \cdots + c_{h-1} = kt\}$
$\mathcal{T}(t)$	$= \left\{(s_0, \cdots, s_{h-1}) \in \mathbb{Z}^h : 0 \leq s_0 < \cdots < s_{h-1} \leq t+h-1 \text{ e } \sum_{i=0}^{h-1} s_i = kt + \binom{h}{2}\right\}$
$\mathbb{T}(t)$	$= \left\{(s_0, \cdots, s_{h-1}) \in \mathbb{Z}^h : 0 \leq s_0 \leq \cdots \leq s_{h-1} \leq t+h-1 \text{ e } \sum_{i=0}^{h-1} s_i = kt + \binom{h}{2}\right\}$
$\mathbf{x}^{\mathbf{v}}$	$= x_0^{v_0} x_1^{v_1} \cdots x_{h-1}^{v_{h-1}}$
$\sigma(\mathbf{x})$	$= (x_{\sigma(0)}, x_{\sigma(1)}, \cdots, x_{\sigma(h-1)})$
$\epsilon(a)$	$= \begin{cases} 0 & \text{se} \quad a = 0 \\ 1 & \text{se} \quad a \neq 0. \end{cases}$
$\Gamma_{t,n}$	Conjunto das funções $\alpha : \{1, 2, \cdots, t\} \to \mathbb{N}$ tais que $\alpha(i) \leq n$ para $i = 1, \cdots, t$

Introdução

Em 1813 Augustin Louis Cauchy publicou um artigo ([5]) onde apresentou uma demonstração para um resultado devido a Lagrange que afirma que a equação

$$ax^2 + by^2 + c \equiv 0(modp)$$

tem solução para todo primo p e para todos $a, b \not\equiv 0(modp)$. Para auxiliar em sua demonstração do resultado de Lagrange, Cauchy demonstrou o seguinte teorema:

Teorema. *Seja p um número primo, sejam $A, B \subset \mathbb{Z}_p$ e denote por $A + B$ o conjunto $\{a + b : a \in A, b \in B\}$. Então $|A + B| \geq min\{p, |A| + |B| - 1\}$.*

De fato, sabendo que existem $\frac{p-1}{2}$ resíduos quadráticos módulo p, Cauchy tomou $A = B = \{\text{resíduos quadráticos módulo } p\} \bigcup \{0\}$ e usou o teorema acima para concluir que $|A + B| \geq \frac{p-1}{2} + 1 + \frac{p-1}{2} + 1 - 1 = p$ que implica o resultado de Lagrange.

Mais de cem anos depois, Davenport ([6], 1935), sem conhecimento do trabalho de Cauchy, demonstrou o mesmo resultado, mas publicou uma nota histórica doze anos mais tarde ([7], 1947) onde dizia que o teorema já havia sido provado por Cauchy, razão pela qual o teorema se consagrou com o nome Teorema de Cauchy-Davenport.

Em Teoria Aditiva dos Números, resultados como o de Cauchy-Davenport, nos quais se começa com conjuntos A e B e se busca informações sobre o conjunto $A + B$, são conhecidos como *Problemas Diretos*. Em um *Problema Inverso*, começa-se com $A + B$ e tenta-se deduzir informações sobre os conjuntos A e B. O problema inverso de caracterizar os conjuntos A e B para os quais vale a igualdade no Teorema de Cauchy-Davenport (os chamados *conjuntos críticos*) foi resolvido em 1956 por Vosper ([23]):

Teorema. (Vosper) *Os conjuntos $A, B \subset \mathbb{Z}_p$ são críticos se uma das seguintes condições ocorre:*

1. $|A| + |B| > p$;
2. $min(|A|, |B|) = 1$;
3. *A e B podem ser representados como progressões aritméticas de mesma razão;*
4. $A = (\mathbb{Z}_p - (c - B))$, *para algum* $c \in \mathbb{Z}_p$.

O Teorema de Cauchy-Davenport tem sido generalizado em diversas direções. Por exemplo, através de um exercício fácil de indução (veja [19], pág 44) é possível mostrar que

$$|A_0 + A_1 + \cdots + A_{h-1}| \geq min\{p, |A_0| + |A_1| + \cdots + |A_{h-1}| - h + 1\}. \tag{1}$$

Uma generalização do Teorema de Cauchy-Davenport consiste no seguinte: para inteiros $1 \leq k \leq h$, seja

$$s_k(x_0, x_1, \cdots, x_{h-1}) = \sum_{0 \leq i_0 < i_1 < \cdots < i_{k-1} \leq h-1} x_{i_0} x_{i_1} \cdots x_{i_{k-1}}$$

o polinômio simétrico elementar de grau k em h variáveis. Denotando por $s_k(A_0, A_1, \cdots, A_{h-1})$ o conjunto

$$\{s_k(a_0, a_1, \cdots, a_{h-1}) : (a_0, a_1, \cdots, a_{h-1}) \in A_0 \times A_1 \times \cdots \times A_{h-1}\}$$

Dias da Silva e Godinho ([8], 2002. Veja também [13]) provaram que, para p suficientemente grande,

$$|s_k(A_0, A_1, \cdots, A_{h-1})| \geq \frac{|A_0| + |A_1| + \cdots + |A_{h-1}| - h}{k} + 1. \tag{2}$$

Um problema inspirado por, mas diverso daquele sobre o qual versa o Teorema de Cauchy-Davenport, foi considerado por Erdös e Heilbronn nos anos 60:

Conjectura. *Para p primo e $A \subset \mathbb{Z}_p$ seja $2^\wedge A = \{a + a' : a, a' \in A \text{ com } a \neq a'\}$. Então $|2^\wedge A| \geq min\{p, 2|A| - 3\}$.*

Em [11], 1980, os autores se admiram pelo fato de esta conjectura ainda não ter sido provada,

> ... It is surprising that this old question of Erdös and Heilbronn is still open.
> (pag 95, l 13-14)

mas só em 1994 Dias da Silva e Hamidoune ([9]), usando resultados de algebra multilinear, espaços de Grassmann e teoria de representações de um grupo simétrico, demonstraram que a conjectura era verdadeira. Na verdade, provaram um resultado bem mais geral:

Teorema. (Dias da Silva-Hamidoune) *Sejam A um subconjunto finito de um corpo K e p a característica de K se ela é finita e $p = \infty$ se ela é zero. Denotando por $h^\wedge A$ o conjunto $\{a_0 + a_1 + \cdots + a_{h-1} : a_0, a_1, \cdots, a_{h-1} \in A \text{ com } a_i \neq a_j \text{ se } i \neq j\}$, tem se $|h^\wedge A| \geq min\{p, h|A| - h^2 + 1\}$.*

Seja $\hat{s}_k(A) = \{s_k(a_0, a_1, \cdots, a_{h-1}) : a_0, a_1, \cdots, a_{h-1} \in A \text{ onde } a_i \neq a_j \text{ se } i \neq j\}$. Em 2005, generalizando as idéias de Dias da Silva e Hamidoune, Caldeira ([4]) demonstrou que, com as mesmas hipóteses do teorema acima e para $p > h$, se $k = 1$ ou $k = h - 1$, então

$$|\hat{s}_k(A)| \geq min\left\{p, \left[\frac{h(|A| - h)}{k}\right] + 1\right\}, \tag{3}$$

onde $[x]$ indica a parte inteira do número real x.

Voltando a 1994, em [18] Nathanson demonstrou o teorema de Dias da Silva-Hamidoune substituindo a teoria de representações por caminhos em $\mathbb{Z}^h$ (um caminho em $\mathbb{Z}^h$ é uma sequência finita de vetores em $\mathbb{Z}^h$ tais que dois vetores consecutivos diferem apenas por uma unidade em apenas uma coordenada), e em 1995, Alon, Nathanson e Ruzsa ([2], veja também [19], pág 106-107), usando apenas propriedades elementares de polinômios (abordagem denominada *Método Polinomial*), reobtiveram o teorema de Dias da Silva-Hamidoune como um caso particular de um resultado um pouco mais geral:

Teorema. (Alon-Nathanson-Ruzsa) *Sejam $A_0, A_1, \cdots, A_{h-1}, h \geq 2$, subconjuntos finitos não vazios de um corpo K e p a característica de K se ela é finita e $p = \infty$ se ela é zero. Considere $|A_i| = k_i$ para $i = 0, 1, \cdots, h-1$ e suponha que $k_i \neq k_j$ se $i \neq j$. Sendo*

$$A_0 \overset{\wedge}{+} A_1 \overset{\wedge}{+} \cdots \overset{\wedge}{+} A_{h-1} = \{a_0 + a_1 + \cdots + a_{h-1} : a_i \in A_i \text{ com } a_i \neq a_j \text{ se } i \neq j\},$$

tem se

$$|A_0 \overset{\wedge}{+} A_1 \overset{\wedge}{+} \cdots \overset{\wedge}{+} A_{h-1}| \geq min\left\{p, \sum_{i=0}^{h-1} k_i - \frac{h(h+1)}{2} + 1\right\}.$$

Se $A = \{b_1, b_2, \cdots, b_m\}$ com $m \geq h$, o teorema de Dias da Silva e Hamidoune pode então ser obtido do teorema de Alon, Nathanson & Ruzsa aplicando-se este com $A_0 = A,\ A_1 = A\backslash\{b_1\},\ A_2 = A\backslash\{b_1, b_2\}, \cdots,\ A_{h-1} = A\backslash\{b_1, b_2, \cdots, b_{h-1}\}$.

Seja $\overset{\wedge}{s_k}\ (A_0, A_1, \cdots, A_{h-1}) = \{s_k(a_0, a_1, \cdots, a_{h-1}) : a_i \in A_i \text{ onde } a_i \neq a_j \text{ se } i \neq j\}$ e $n = \frac{h!}{k!(h-k)!}$. Combinando o Método Polinomial com uma extensão da idéia de caminhos do Nathanson, o presente trabalho apresenta a demonstração do resultado a seguir que generaliza o teorema acima (que é o caso $k = 1$) e a estimativa (3) de Caldeira (para todo $k \in \{1, 2, \cdots, h-1\}$):

Teorema 1. *Seja $t = \left[\frac{\sum_{j=0}^{h-1} k_j - \frac{h(h+1)}{2}}{k}\right]$ e suponha que $p > \frac{(t+n-1)!}{\left(\left[\frac{t}{n}\right]!\right)^n (n-1)!}$ quando a característica de K for positiva. Se $k_i \neq k_j$ para $i \neq j$ e $k_i \leq t + h$ para todo $i = 0, 1, \cdots h-1$, então*

$$|\ \overset{\wedge}{s_k}\ (A_0, A_1, \cdots, A_{h-1})| \geq min\{p, t+1\}.$$

Esta abordagem polinomial também permite obter a estimativa (2) que Dias da Silva e Godinho ([8], [13]) obtiveram usando resultados de algebra multilinear, agora estimando quão grande a característica de K deve ser:

Teorema 2. *Seja* $t = \left[\frac{\left(\sum_{j=0}^{h-1} k_j\right)-h}{k}\right]$ *e suponha que* $p > \frac{(t+n-1)!}{\left(\left[\frac{t}{n}\right]!\right)^n (n-1)!}$ *quando a característica de* K *for positiva. Se* $k_i \leq t+1$ *para todo* $i = 0, 1, \cdots, h-1$*, então*

$$|s_k(A_0, A_1, \cdots, A_{h-1})| \geq min\{p, t+1\}.$$

Um comentário sobre a hipótese a que estão sujeitos os números $k_i = |A_i|$, $i = 0, 1, \cdots, h-1$: é fácil ver que se $A_{k-1} = A_k = \cdots = A_{h-1} = \{0\}$, então $s_k(A_0, A_1, \cdots, A_{h-1}) = \{0\}$ para quaisquer $A_0, A_1, \cdots, A_{k-2} \subset K$. Seria possível escolher os conjuntos $A_0, A_1, \cdots, A_{k-2}$ com elementos o suficiente para dar um contra-exemplo a este teorema? Por exemplo, se escolhermos os conjuntos $A_0, A_1, \cdots, A_{k-3}$ todos com k elementos e A_{k-2} com $k-1$ elementos, no Teorema 2 teremos $t = k-2$ de modo que a cota dada pelo teorema não é válida. No entanto, isto ocorre porque neste caso os números de elementos dos conjuntos $A_0, A_1, \cdots, A_{k-2}$ não cumprem a hipótese $|A_i| \leq t+1$. No Exemplo 4.7 mostramos que a única forma de os conjuntos $A_0, A_1, \cdots, A_{k-2}$ satisfazerem a hipótese do teorema é que cada um deles tenha apenas um elemento. Mas neste caso, a cota dada pelo teorema é válida e é atingida.

Sejam h e t inteiros positivos e sejam $\mathbf{r} = (r_1, r_2, \cdots, r_t)$ e $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1})$ vetores com coordenadas inteiras não negativas. No desenvolvimento da teoria que resultou nos Teoremas 1 e 2 fomos levados a estudar o conjunto $\Omega(\mathbf{r}, \mathbf{c})$ de todas as matrizes $t \times h$ cujos elementos são zeros ou uns e tais que a soma dos vetores-linha é igual a $\mathbf{c} \in \mathbb{Z}^h$ e a soma dos vetores-coluna é igual a $\mathbf{r} \in \mathbb{Z}^t$. O conjunto $\Omega(\mathbf{r}, \mathbf{c})$ foi objeto de intenso estudo no fim dos anos 50 e início dos anos 60 por H. J. Ryser, D. R. Fulkerson, R. M. Haber e D. Gale e muitos importantes teoremas foram provados (veja [3] para mais detalhes). Em [24] e [17] os autores obtiveram fórmulas para o número preciso de matrizes em $\Omega(\mathbf{r}, \mathbf{c})$, embora elas sejam ainda difíceis de serem usadas. Esta fórmula considera os números $p_i = |\{r_j : r_j = i\}|$ para $i = 1, 2, \cdots, t$ e $Q_j = c_j - \sum_{i=0}^{j-1} p_{t-i}$, para $j = 1, 2, \cdots, t-1$.

Teorema. (Perez Salvador, et al) *O número preciso de matrizes em* $\Omega(\mathbf{r}, \mathbf{c})$ *é*

$$|\Omega(\mathbf{r}, \mathbf{c})| = \sum_{T_{ij} \geq 0} \prod_{j=1}^{t-1} \prod_{i=1}^{t-j} \binom{N_{ij}}{M_{ij}},$$

onde N_{ij} *e* M_{ij} *são funções de* p_i, Q_j *e* T_{ij} *definidas pelas seguintes fórmulas de recorrência*

1. $M_{i,j} = T_{i,j}$ *para* $j = 1, 2, \cdots, t-2$ *e* $i = 2, 3, \cdots, t-j$,
2. $M_{1,1} = Q_1 - \sum_{k=2}^{t-1} M_{k,1}$,
3. $M_{1,j} = Q_j + \sum_{k=1}^{j-1} M_{t-j+1,k} - \sum_{k=2}^{t-j}$ *para* $j = 2, 3, \cdots, t-1$,
4. $N_{i,1} = p_i$ *para* $i = 1, 2, \cdots, t-1$,
5. $N_{i,j} = N_{i,j-1} - M_{i,j-1} + M_{i+1,j-1}$ *para* $j = 2, 3, \cdots, t-1$ *e* $i = 1, 2, \cdots, t-j$.

e onde a variação de $T_{i,j}$ *é dado pelas desigualdades de recorrência e* $0 \leq T_{i,j} \leq N_{i,j}$ *e* $Q_j + \sum_{k=1}^{j-1} T_{t-j+1,k} - N_{1,j} \leq \sum_{k=2}^{t-j} T_{k,j} \leq \sum_{k=1}^{j-1} T_{t-j+1,k}$

Fórmulas mais simples (que na verdade são ainda complexas!) são conhecidas apenas no caso particular em que todas as coordenadas do vetor $\mathbf{r}$ são iguais a um certo número k e todas as coordenadas de $\mathbf{c}$ são iguais a um número s e, mesmo assim, apenas para pequenos valores de k e s (veja, por exemplo, [20], [21] e [22]). No presente trabalho, no caso em que apenas o vetor $\mathbf{r}$ tem todas as coordenadas iguais ao número k, apresentamos uma fórmula mais simples que aquela apresentada por Perez Salvador, et al, mas sem a restrição de que k seja pequeno:

Teorema 3. *Seja* $n = \frac{h!}{k!(h-k)!}$, *sejam* $\beta_i, i = 1, 2, \cdots, n$, *todos os vetores com exatamente* k *coordenadas iguais a 1 e* $n-k$ *coordenadas iguais a 0 e seja* $\mathbf{c} \in \mathbb{Z}^h$. *Se* $\mathbf{r} = (k, k, \cdots, k) \in \mathbb{Z}^t$, *tem-se*

$$|\Omega(\mathbf{r}, \mathbf{c})| = \sum_{\substack{t_1 + \cdots + t_n = t \\ t_1\beta_1 + \cdots + t_n\beta_n = \mathbf{c}}} \frac{t!}{t_1! \cdots t_n!}.$$

O estudo das (0,1) matrizes é apresentado logo no Capítulo 1 onde é demonstrado o Teorema 3 acima. Também é aí que, generalizando a noção de caminho em $\mathbb{Z}^h$ definida por Nathanson, apresentamos o conceito de k-caminho em $\mathbb{Z}^h$, o que fornecerá a técnica necessária para o cálculo dos coeficientes de certos produtos polinomiais mais adiante, e então relacionamos os k-caminhos em $\mathbb{Z}^h$ com as $(0,1)$-matrizes.

No Capítulo 2 descrevemos o Método Polinomial sobre o qual estão fundamentados os principais resultados deste trabalho.

No Capítulo 3 estudamos os coeficientes do polinômio $(s_k)^t$ e do produto polinomial $(s_k)^t\Delta_h$, onde Δ_h é o polinômio de Vandermond em h variáveis e $t \geq 0$ é um inteiro, e fornecemos condições suficientes para garantir que certos coeficientes são não nulos, o que é um requisito para se aplicar o Método Polinomial.

No Capítulo 4 "juntamos as peças"para concluir a demonstração dos Teoremas 1 e 2 e mostramos como usar o Teorema 1 para obter a estimativa (3).

Finalmente no Capítulo 5 discutimos a aplicação dos métodos apresentados ao longo do trabalho a outros tipos de polinômios.

Capítulo 1

Miscelânea Combinatória

Este capítulo tem o objetivo de apresentar alguns resultados de combinatória que serão necessários no cálculo dos coeficientes de alguns produtos polinomiais. Começamos com um estudo sobre matrizes de zeros e uns com soma de linhas e soma de colunas prescritos. Em seguida, estudamos sequências em $\mathbb{Z}^h$ onde vetores consecutivos diferem em exatamente k coordenadas por apenas uma unidade.

1.1 $(0,1)$-Matrizes

A situação problema que nos preocupamos por hora é a de, dado um vetor $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$, estudar as matrizes com entradas zero ou um cujo número de uns em cada linha é k e cuja soma dos vetores-linha seja igual a $\mathbf{c} \in \mathbb{Z}^h$, ou seja, o número de uns na j-ésima coluna é igual a c_j. Iniciamos definindo exatamente quais são essas matrizes:

Definição 1.1. *Sejam h, k e t inteiros positivos com $k \leq h$ e seja $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1})$ um vetor com coordenadas inteiras não negativas. Uma $k\mathbf{c}$-matriz de ordem $t \times h$ é uma matriz $A = (a_{i,j})_{t\times h}$ satisfazendo (estamos indexando as colunas de A com os números de 0 a $h-1$):*

1. *$a_{i,j} \in \{0,1\}, \forall i \in \{1, 2, \cdots, t\}$ e $\forall j \in \{0, 1, \cdots, h-1\}$;*
2. *Para cada $1 \leq i \leq t$, $\sum_{j=0}^{h-1} a_{i,j} = k$;*

3. Para cada $0 \leq j \leq h-1$, $\sum_{i=1}^{t} a_{i,j} = c_j$.

Denotamos por $\Omega(\mathbf{c})$ *o conjunto de todas as* $k\mathbf{c}$*-matrizes.*

Assim, uma matriz de 0's e 1's está em $\Omega(\mathbf{c})$ desde que a soma de seus vetores-linha seja igual a $\mathbf{c}$ e o número de uns em cada linha seja k.

Exemplo 1.2. *Tomando* $h = 7$, $k = 4$, $t = 5$ *e* $\mathbf{c} = (2, 1, 3, 2, 3, 5, 4)$, *temos que*

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

é uma $4\mathbf{c}$*-matriz de ordem* 5×7.

A primeira questão que se põe é a da existência de uma $k\mathbf{c}$-matriz. A proposição a seguir fornece condições necessárias e suficientes.

Proposição 1.3. *Dados inteiros positivos* h, k *e* t *com* $k \leq h$ *e um vetor* $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1})$ *com coordenadas inteiras não negativas, existe uma* $k\mathbf{c}$*-matriz de ordem* $t \times h$ *se, e somente se, o vetor* $\mathbf{c}$ *cumpre as seguintes condições:*

$$\begin{array}{ll} (i) & \sum_{j=0}^{h-1} c_j = kt; \\ (ii) & 0 \leq c_j \leq t, \forall j \ \in \{0, 1, \cdots, h-1\}. \end{array} \tag{1.1}$$

Demonstração. Se existe uma $k\mathbf{c}$-matriz, fazendo uso dos axiomas 2 e 3 da Definição 1.1, a primeira condição segue da igualdade

$$\sum_{j=0}^{h-1} c_j = \sum_{j=0}^{h-1} \left[\sum_{i=1}^{t} a_{i,j} \right] = \sum_{i=1}^{t} \left[\sum_{j=0}^{h-1} a_{i,j} \right] = \sum_{i=1}^{t} k = kt$$

enquanto que a segunda segue diretamente do fato de que, pelo axioma 1, em cada coluna da matriz há no mínimo 0 e máximo t elementos iguais a 1 e a soma deles, pelo axioma 3, é igual ao c_j correspondente. Isto demonstra a necessidade.

A suficiência é demonstrada por indução sobre t. Quando $t = 1$, as condições (1.1) impõem que $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ tem exatamente k coordenadas iguais a um e

as demais são nulas. Assim, a $k\mathbf{c}$-matriz procurada é uma matriz linha que coincide com o vetor $\mathbf{c}$. Seja $t \geq 1$ e suponhamos que as condições (1.1) sejam suficientes para a existência de uma $k\mathbf{c}'$-matriz para todo vetor $\mathbf{c}' = (c'_0, c'_1, \cdots, c'_{h-1}) \in \mathbb{Z}^h$ que as satisfaça. Seja $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ um vetor satisfazendo às condições

$$\begin{array}{ll} (1) & \sum_{j=0}^{h-1} c_j = k(t+1); \\ (2) & 0 \leq c_j \leq (t+1), \forall j \in \{0, 1, \cdots, h-1\}. \end{array}$$

Note que o número de coordenadas não nulas no vetor $\mathbf{c}$ é maior do que ou igual a k. De fato, se fosse menor, a condição (2) faria com que a soma em (1) fosse $\sum_{j=0}^{h-1} c_j < k(t+1)$. Sejam $c_{j_1}, \cdots, c_{j_k}$ as k maiores coordenadas de $\mathbf{c}$ (usando qualquer critério de desempate em caso de igualdade) e defina o vetor $\mathbf{c}'$ por

$$c'_j = \begin{cases} c_j - 1 & \text{se } j \in \{j_1, \cdots, j_k\} \\ c_j & \text{caso contrário.} \end{cases}$$

Note que a condição (1) impõe que o número de coordenadas de $\mathbf{c}$ que são maiores do que t não excede a k, pois o contrário implicaria que $\sum_{j=0}^{h-1} c_j > k(t+1)$. Assim, é fácil ver que o vetor $\mathbf{c}'$ satisfaz às condições (1.1) e, por hipótese de indução, existe uma $k\mathbf{c}'$-matriz $A_{t\times h}$. Acrescentando a esta matriz um vetor-linha com 1's nas coordenadas de posições $j_1, \cdots, j_k$ e 0 nas demais coordenadas, temos uma $k\mathbf{c}$-matriz e a demonstração está completa[1].

□

A demonstração acima nos fornece um algoritmo para se construir uma $k\mathbf{c}$-matriz $A = (a_{i,j})_{t\times h}$ quando o vetor $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ satisfaz às condições (1.1):

Algoritmo 1.4. *Seja* $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ *um vetor satisfazendo às condições (1.1).*

Passo 1. *Faça* $\mathbf{v}_t = \mathbf{c}$*;*

Passo 2. *Para i variando de maneira decrescente de t até* 1 *faça*

[1] A demonstração da Proposição 1.3 também pode ser feita pelo uso direto das caracterizações de Ford-Fulkerson ou de Gale-Ryser das (0,1)-matrizes (veja [3]). Em verdade, somente tomamos conhecimento dessas caracterizações algumas semanas após concluirmos a demonstração aqui apresentada. Decidimos manter esta demonstração por seu aspecto construtivo, que deu origem ao Algoritmo 1.4.

- *Sendo $j_1, j_2, \cdots, j_k$ as posições das k maiores coordenadas de $\mathbf{v}_i$ (escolhendo-se aquelas coordenadas de menor índice em caso de igualdade) defina*

$$\beta_{i-1} = (\beta_{i-1,0}, \beta_{i-1,1}, \cdots, \beta_{i-1,h-1}) \in \mathbb{Z}^h$$

onde, para $j \in \{0, 1, \cdots, h-1\}$,

$$\beta_{i-1,j} = \begin{cases} 1 & se \quad j \in \{j_1, j_2, \cdots, j_k\} \\ 0 & se \quad j \notin \{j_1, j_2, \cdots, j_k\} \end{cases}$$

- $a_{t+1-i,j} = \beta_{i-1,j}$ (*definição do elemento da $t+1-i$-ésima linha e j-ésima coluna da matriz $A = (a_{i,j})_{t \times h}$*).

- $\mathbf{v}_{i-1} = \mathbf{v}_i - \beta_{i-1}$.

A despeito das dificuldades inerentes à notação matemática, o algoritmo é simples: escolhe-se as k maiores coordenadas do vetor $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ (usando como critério de desempate a escolha daquelas coordenadas mais à esquerda) e subtrai-se uma unidade de cada uma dessas coordenadas obtendo-se um novo vetor $\mathbf{c}' = (c'_0, c'_1, \cdots, c'_{h-1}) \in \mathbb{Z}^h$ (que ainda satisfaz às condições (1.1)) e constrói-se uma linha da matriz colocando-se k elementos iguais a 1 naquelas colunas cujo índice coincide com as posições dos k maiores elementos de $\mathbf{c}$ e zero nas demais posições. Observe que o critério de desempate foi escolhido de tal maneira que cada vetor $\mathbf{v} = (v_0, v_1, \cdots, v_{h-1})$ produzido pelo Algoritmo 1.4 satisfaz à propriedade $v_0 \leq v_1 \leq \cdots \leq v_{h-1}$. Isto será útil mais adiante. Não fosse por essa razão, qualquer critério de desempate poderia ser escolhido, desde que fosse usado em todas as iterações do algoritmo. O exemplo a seguir ilustra o uso do algoritmo.

Exemplo 1.5. *Sejam $k = 5,\ h = 10,\ t = 12$ e $\mathbf{c} = (2, 4, 4, 4, 5, 6, 6, 9, 10, 10) \in \mathbb{Z}^{10}$. Note que $\sum_{j=0}^{h-1} c_j = 60$ e que as condições (1.1) são satisfeitas. Cada vetor da sequência a seguir representa uma iteração do algoritmo. A matriz que segue é tal que a i-ésima linha*

corresponde à i-ésima iteração.

$$
\begin{aligned}
\mathbf{v}_{12} &= (2,4,4,4,5,6,6,9,10,10)\\
\mathbf{v}_{11} &= (2,4,4,4,5,5,5,8,9,9)\\
\mathbf{v}_{10} &= (2,4,4,4,4,4,5,7,8,8)\\
\mathbf{v}_{9} &= (2,3,4,4,4,4,4,6,7,7)\\
\mathbf{v}_{8} &= (2,3,3,3,4,4,4,5,6,6)\\
\mathbf{v}_{7} &= (2,3,3,3,3,3,4,4,5,5)\\
\mathbf{v}_{6} &= (2,2,3,3,3,3,3,3,4,4)\\
\mathbf{v}_{5} &= (2,2,2,2,2,3,3,3,3,3)\\
\mathbf{v}_{4} &= (2,2,2,2,2,2,2,2,2,2)\\
\mathbf{v}_{3} &= (1,1,1,1,1,2,2,2,2,2)\\
\mathbf{v}_{2} &= (1,1,1,1,1,1,1,1,1,1)\\
\mathbf{v}_{1} &= (0,0,0,0,0,1,1,1,1,1)
\end{aligned}
$$

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

No exemplo acima, escolhemos um vetor cujas coordenadas estão postas em ordem crescente. Mas isso não é uma exigência do algoritmo, ele funciona sem esta restrição.

De agora em diante nesta seção, a menos que se diga explicitamente o contrário, estaremos supondo que o vetor $\mathbf{c}$ satisfaz às condições (1.1). Entendidas as condições a que o vetor $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ deve se submeter para garantir a existência

de uma $k\mathbf{c}$-matriz, a próxima questão que se põe é a de determinar o número de $k\mathbf{c}$-matrizes. Uma primeira observação neste sentido é notar que se a matriz $A_{t\times h}$ é uma $k\mathbf{c}$-matriz, então a matriz $B_{t\times h}$ obtida por uma permutação das linhas de $A_{t\times h}$ também é uma $k\mathbf{c}$-matriz (naturalmente, para o mesmo vetor $\mathbf{c}$), pois cada linha continuará tendo exatamente k elementos iguais a 1 e a soma dos elementos em cada coluna não se altera ao mudarmos a ordem dos elementos na adição. Esta simples observação permite definir sobre o conjunto $\Omega(\mathbf{c})$ de todas as $k\mathbf{c}$-matrizes uma relação de equivalência. Primeiramente, fixemos alguma notação. Seja S_t o grupo das permutações dos inteiros $1, 2, \cdots, t$ e defina uma ação do grupo S_t sobre $\Omega(\mathbf{c})$ como segue: para $\sigma \in S_t$ e $A = (a_{i,j})_{t\times h} \in \Omega(\mathbf{c})$ colocamos $\sigma A = (a_{\sigma(i),j})$, que é a matriz obtida de A permutando suas linhas segundo a permutação σ. É claro que $\sigma A \in \Omega(\mathbf{c})$ para todos $\sigma \in S_t$ e para toda matriz $A \in \Omega(\mathbf{c})$.

Definição 1.6. *Sejam $A, B \in \Omega(\mathbf{c})$. Dizemos que A é congruente a B módulo S_t (notação: $A \equiv B(mod S_t)$) se existe $\sigma \in S_t$ tal que $B = \sigma A$.*

É fácil perceber que isto define uma relação de equivalência sobre o conjunto $\Omega(\mathbf{c})$. Elegeremos como representante canônico de uma dada classe de equivalência da relação acima aquela matriz cujos vetores-linha estão organizados de cima para baixo em ordem crescente segundo a ordem lexicográfica.

Exemplo 1.7. *O representante canônico da classe de equivalência da matriz A dada no Exemplo 1.5 é a matriz B da direita a seguir. A matriz da esquerda é a mesma matriz daquele exemplo.*

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

A matriz abaixo é a representante de outra classe. Comparando B com C encontramos diferenças já na segunda linha.

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

Seja $\Gamma \subset \mathbb{Z}^h$ o conjunto de todos os vetores com exatamente k coordenadas iguais a um e as demais coordenadas nulas, isto é, o vetor $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{h-1})$ está em Γ se, e somente se, $\alpha_i \in \{0,1\}, \forall i \in \{0,1,\cdots,h-1\}$ e $\sum_{i=0}^{h-1} \alpha_i = k$. O número de elementos do conjunto Γ coincide com o número de maneiras de se escolher k coordenadas entre as h possíveis para preenchermos com o número 1, que é igual ao número $n = \frac{h!}{k!(h-k)!}$. Sejam $\beta_1, \beta_2, \cdots, \beta_n$ todos os elementos de Γ, organizados em ordem crescente segundo a ordem lexicográfica, ou seja,

$$\begin{aligned} \beta_1 &= (\underbrace{0,0,\cdots,0}_{h-k},\underbrace{1,1,\cdots,1}_{k}) \\ \beta_2 &= (\underbrace{0,\cdots,0}_{h-k-1},1,0,\underbrace{1,\cdots,1}_{k-1}) \\ &\vdots \\ \beta_n &= (\underbrace{1,1,\cdots,1}_{k},\underbrace{0,0,\cdots,0}_{h-k}) \end{aligned}$$

Seja $X \subset \Omega(\mathbf{c})$ uma classe de equivalência na relação definida acima cujo representante canônico é a matriz $A \in \Omega(\mathbf{c})$. Os vetores-linha de A são elementos de Γ. Como ilustram as matrizes do Exemplo 1.7, bem pode acontecer que a matriz A possua algumas linhas iguais entre si. Seja t_i, com $i = 1, 2, \cdots, n$, o número de linhas de A iguais ao vetor β_i

(Naturalmente, pode acontecer que $t_i = 0$ para alguns índices i). Assim,

$$\sum_{i=1}^{n} t_i \beta_i = \mathbf{c},$$

e como A tem t linhas, temos

$$t_1 + t_2 + \cdots + t_n = t.$$

Agora note que se $B \in \Omega(\mathbf{c})$ é o representante de outra classe, denotando por t'_i, com $i = 1, 2, \cdots, n$, o número de linhas de B iguais ao vetor β_i, então $t_j \neq t'_j$ para pelo menos dois índices j. Isto mostra que cada classe de equivalência dá origem a uma única solução não negativa da equação linear com coeficientes unitários

$$x_1 + x_2 + \cdots + x_n = t \tag{1.2}$$

e que classes diferentes dão origem a soluções diferentes desta equação (pode ocorrer que algumas soluções desta equação não sejam provenientes de nenhuma classe de equivalência) e assim o número ω de classes de equivalência não excede ao número de soluções de (1.2), ou seja (veja [15], pág 74),

$$\omega \leq \frac{(t+n-1)!}{t!(n-1)!}. \tag{1.3}$$

Além disso, o número de elementos na classe X é igual ao número de permutações com repetição de t vetores-linha, ou seja,

$$|X| = \frac{t!}{t_1! \cdots t_n!}. \tag{1.4}$$

Usando o fato de que a relação de equivalência da Definição 1.6 particiona o conjunto $\Omega(\mathbf{c})$ em uma união disjunta de classes de equivalência, temos uma fórmula para o cálculo do número preciso de $k\mathbf{c}$-matrizes:

Teorema 1.8. $|\Omega(\mathbf{c})| = \displaystyle\sum_{\substack{t_1+\cdots+t_n=t \\ t_1\beta_1+\cdots+t_n\beta_n=\mathbf{c}}} \frac{t!}{t_1! \cdots t_n!}.$

Neste teorema, a soma se dá sobre todas as soluções $(t_1, \cdots, t_n)$ de (1.2) que se originam em alguma classe de equivalência, o que ocorrerá quando $t_1\beta_1 + \cdots + t_n\beta_n = \mathbf{c}$.

É interessante notar que quando $k = 1$, temos $n = h$ e os vetores $\beta_1, \cdots, \beta_h$ formam a base canônica do $\mathbb{R}^h$, de modo que a igualdade $t_1\beta_1 + \cdots + t_h\beta_h = \mathbf{c}$ só é possível para uma única h-upla $(t_1, \cdots, t_h)$, a saber, $t_1 = c_0, t_2 = c_1, \cdots, t_h = c_{h-1}$. Assim, neste caso o somatório do teorema acima tem apenas uma parcela.

Podemos também obter uma estimativa para o número de elementos do conjunto $\Omega(\mathbf{c})$ mais fácil de calcular do que o número preciso dado pelo teorema acima. Iniciamos com o seguinte lema:

Lema 1.9. *Sejam $t \geq 0$, $n \geq 1$ e $t_1, \cdots, t_n$ inteiros não negativos tais que $t_1 + \cdots + t_n = t$. Sejam q e r o quociente e o resto da divisão euclidiana de t por n. Então*

$$q!^{n-r} \cdot (q+1)!^r \leq t_1! \cdot t_2! \cdots t_n!. \tag{1.5}$$

Demonstração. A demonstração é feita por indução sobre t. Se $t = 0$, então $t_1 = \cdots = t_n = 0$ e $q = r = 0$ de modo que (1.5) é óbvia neste caso. Seja $t \geq 0$ e suponha que (1.5) valha para toda n-upla de inteiros não negativos $(t_1, \cdots, t_n)$ tal que $t_1 + \cdots + t_n = t$. Seja $(t_1^{'}, \cdots, t_n^{'})$ uma n-upla de inteiros não negativos tal que $t_1^{'} + \cdots + t_n^{'} = t + 1$ e suponha, sem perda de generalidade, que $t_1^{'} \leq t_2^{'} \leq \cdots \leq t_n^{'}$. Note que $q + 1 \leq t_n^{'}$, pois o contrário implicaria que $t_1^{'} + \cdots + t_n^{'} \leq q \cdot n \leq t < t + 1$. Sejam q' e r' o quociente e o resto da divisão euclidiana de $t + 1$ por n. Há dois casos a considerar:
Caso 1. Se $q' = q$, então $r' = r + 1$. Como a n-upla $(t_1^{'}, \cdots, t_{n-1}^{'}, t_n^{'} - 1)$ é tal que $t_1^{'} + \cdots + t_{n-1}^{'} + (t_n^{'} - 1) = t$, a hipótese de indução implica que

$$q!^{n-r} \cdot (q+1)!^r \leq t_1^{'}! \cdots t_{n-1}^{'}! \cdot (t_n^{'} - 1)!,$$

e como $q + 1 \leq t_n^{'}$, temos

$$q!^{n-r} \cdot (q+1)!^r \cdot (q+1) \leq t_1^{'}! \cdots t_{n-1}^{'}! \cdot (t_n^{'} - 1)! \cdot t_n^{'}$$

o que nos dá

$$q!^{n-r-1} \cdot (q+1)!^{r+1} \leq t_1^{'}! \cdots t_{n-1}^{'}! \cdot t_n^{'}!,$$

ou seja,

$$q'!^{n-r'} \cdot (q'+1)!^{r'} \leq t_1^{'}! \cdots t_{n-1}^{'}! \cdot t_n^{'}!$$

o que conclui a demonstração neste caso.

Caso 2. Se $q' = q + 1$, então $r' = 0$, o que implica que $r = n - 1$. Aplicando novamente a hipótese de indução à n-upla $(t_1^{'}, \cdots, t_{n-1}^{'}, t_n^{'} - 1)$ temos

$$q!^{n-(n-1)} \cdot (q+1)!^{n-1} \leq t_1^{'}! \cdots t_{n-1}^{'}! \cdot (t_n^{'} - 1)!,$$

e como $q + 1 \leq t_n^{'}$, temos

$$(q+1) \cdot q! \cdot (q+1)!^{n-1} \leq t_1^{'}! \cdots t_{n-1}^{'}! \cdot (t_n^{'} - 1)! \cdot t_n^{'}$$

o que nos dá

$$(q+1)!^n \leq t_1^{'}! \cdots t_{n-1}^{'}! \cdot t_n^{'}!,$$

ou seja,

$$q'!^{n-r'} \cdot (q'+1)!^{r'} \leq t_1^{'}! \cdots t_{n-1}^{'}! \cdot t_n^{'}!$$

o que conclui a demonstração do lema.

□

Representando por $[x]$ a parte inteira do número real x, com a notação do lema acima, temos $\left[\frac{t}{n}\right] = q$. Isto nos dá o

Corolário 1.10. *Sejam $t \geq 0$, $n \geq 1$ e $t_1, \cdots, t_n$ inteiros não negativos tais que $t_1 + \cdots + t_n = t$. Então*

$$\left(\left[\frac{t}{n}\right]!\right)^n \leq t_1! \cdot t_2! \cdots t_n!. \tag{1.6}$$

São curiosas as semelhanças e diferenças entre a fórmula do corolário acima e a relação entre as médias aritmética e geométrica dos números $t_1, \cdots, t_n$:

$$\frac{t_1 + \cdots + t_n}{n} \geq \sqrt[n]{t_1 \cdot t_2 \cdots t_n}. \tag{1.7}$$

Pelo corolário e por (1.4) temos também que

$$|X| = \frac{t!}{t_1! \cdots t_n!} \leq \frac{t!}{\left(\left[\frac{t}{n}\right]!\right)^n}. \tag{1.8}$$

As estimativas (1.3) e (1.8) nos fornecem a seguinte estimativa para o número de elementos de $\Omega(\mathbf{c})$:

Proposição 1.11. *Sejam $k, h, t \in \mathbb{Z}$ com $1 \leq k \leq h$ e $t \geq 1$, seja $n = \frac{h!}{k!(h-k)!}$ e seja $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$. Então*

$$|\Omega(\mathbf{c})| \leq \frac{(t+n-1)!}{\left(\left[\frac{t}{n}\right]!\right)^n (n-1)!}. \tag{1.9}$$

1.2 k-Caminhos em $\mathbb{Z}^h$

Relembremos que $\Gamma \subset \mathbb{Z}^h$ é o conjunto de todos os vetores com exatamente k coordenadas iguais a um e as demais coordenadas nulas. Um k-caminho em $\mathbb{Z}^h$ é uma sequência finita de vetores em $\mathbb{Z}^h$ tais que dois vetores consecutivos diferem apenas por uma unidade em exatamente k coordenadas. Mais precisamente,

Definição 1.12. *Sejam $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^h$. Um k-caminho de $\mathbf{a}$ a $\mathbf{b}$ é uma sequência finita de pontos $\mathbf{a} = \mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_t = \mathbf{b}$ em $\mathbb{Z}^h$ tal que $\mathbf{v}_j - \mathbf{v}_{j-1} \in \Gamma$ para todo $j = 1, 2, \cdots, t$. Dizemos que dois pontos consecutivos $\mathbf{v}_{j-1}, \mathbf{v}_j$ sobre um k-caminho formam um k-passo na direção β_i se $\mathbf{v}_j - \mathbf{v}_{j-1} = \beta_i$.*

Se $\mathbf{a} = \mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_t = \mathbf{b}$ é um k-caminho de $\mathbf{a}$ até $\mathbf{b}$ e $\mathbf{d} \in \mathbb{Z}^h$, então $\mathbf{a} + \mathbf{d} = \mathbf{v}_0 + \mathbf{d}, \mathbf{v}_1 + \mathbf{d}, \cdots, \mathbf{v}_t + \mathbf{d} = \mathbf{b} + \mathbf{d}$ é um k-caminho de $\mathbf{a} + \mathbf{d}$ a $\mathbf{b} + \mathbf{d}$. Assim, denotando por $P_k(\mathbf{a}, \mathbf{b})$ o número de k-caminhos de $\mathbf{a}$ até $\mathbf{b}$, temos que a função $P_k(\mathbf{a}, \mathbf{b})$ é invariante por translações no sentido em que $P_k(\mathbf{a}, \mathbf{b}) = P_k(\mathbf{a} + \mathbf{d}, \mathbf{b} + \mathbf{d})$. Em particular,

$$P_k(\mathbf{a}, \mathbf{b}) = P_k(\mathbf{0}, \mathbf{b} - \mathbf{a}), \tag{1.10}$$

razão pela qual podemos considerar apenas k-caminhos que começam na origem. Definamos $P_k(\mathbf{a}, \mathbf{a}) = 1$, ou seja, há apenas uma sequência que começa e termina em $\mathbf{a}$. Como os k-passos são vetores com coordenadas iguais a zero ou um, vemos que uma condição necessária para a existência de um k-caminho da origem até o vetor $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ é que este último tenha todas as suas coordenadas não negativas.

Definição 1.13. *Dizemos que o vetor $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ é não negativo se $c_i \geq 0$, para todo $i = 0, 1, \cdots, h-1$ e escreveremos $\mathbf{a} \leq \mathbf{b}$ se o vetor $\mathbf{b} - \mathbf{a}$ é não negativo.*

Seja $\mathbf{c} \in \mathbb{Z}^h$ um vetor não negativo e seja $\mathbf{v}_0, \mathbf{v}_0 + \beta_{i_1} = \mathbf{v}_1, \cdots, \mathbf{v}_{t-1} + \beta_{i_t} = \mathbf{v}_t$ um k-caminho da origem até $\mathbf{c}$. Então a matriz $A_{t\times h}$ cujos vetores-linha são os vetores $\beta_{i_1}, \beta_{i_2}, \cdots, \beta_{i_t}$ é uma $k\mathbf{c}$-matriz. Reciprocamente, dada qualquer $k\mathbf{c}$-matriz $A_{t\times h}$, fazendo $\beta_{i_m} = m$-ésima linha da matriz A, temos que a sequência $\mathbf{0} = \mathbf{v}_0, \mathbf{v}_0 + \beta_{i_1} = \mathbf{v}_1, \cdots, \mathbf{v}_{t-1} + \beta_{i_t} = \mathbf{v}_t = \mathbf{c}$ é um k-caminho da origem até $\mathbf{c}$. Isto fornece uma correspondência biunívoca e mostra que o número de k-caminhos da origem até $\mathbf{c}$ coincide com o número de $k\mathbf{c}$-matrizes, ou seja,

$$P_k(\mathbf{0}, \mathbf{c}) = |\Omega(\mathbf{c})|. \tag{1.11}$$

Além da equação acima, os comentários do parágrafo anterior, juntamente com a Proposição 1.3, fornecem condições necessárias e suficientes para a existência de um k-caminho da origem até o vetor $\mathbf{c}$:

Proposição 1.14. *Dados $k, h \in \mathbb{Z}$ com $1 \leq k \leq h$ e $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ existe um k-caminho da origem até $\mathbf{c}$ se, e somente se, existe $t \in \mathbb{N}$ tal que $\sum_{j=0}^{h-1} c_j = kt$ e $0 \leq c_j \leq t$ para todo $j = 0, 1, \cdots h-1$.*

Em verdade, a aplicação do Algoritmo 1.4 com $t = \frac{1}{k}\sum_{j=0}^{h-1} c_j$ constrói um k-caminho (veja o Exemplo 1.5).

Se $\mathbf{0} = \mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_t = \mathbf{c}$ é um k-caminho da origem até $\mathbf{c}$, com $t \geq 1$, então

$$\mathbf{v}_{t-1} = \mathbf{c} - \beta_i$$

para algum $i \in \{1, 2, \cdots, n\}$ e existe um único k-caminho de $\mathbf{c} - \beta_i$ até $\mathbf{c}$. Disto segue que a função $P_k(\mathbf{0}, \mathbf{c})$ satisfaz a seguinte equação de diferenças

$$P_k(\mathbf{0}, \mathbf{c}) = \sum_{i=1}^{n} P_k(\mathbf{0}, \mathbf{c} - \beta_i). \tag{1.12}$$

Esta fórmula desempenhará um importante papel no cálculo dos coeficientes de potências do k-ésimo polinômio simétrico elementar.

1.3 Caminhos Crescentes e Estritamente Crescentes

Outro conceito importante para o nosso desenvolvimento é o de *caminho estritamente crescente* que passamos a descrever.

Definição 1.15. *Dizemos que o vetor* $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ *é crescente se* $c_0 \leq c_1 \leq \cdots \leq c_{h-1}$*, e estritamente crescente se* $c_0 < c_1 < \cdots < c_{h-1}$*. E dizemos que o* k*-caminho* $\mathbf{0} = \mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_t = \mathbf{c}$ *da origem até* $\mathbf{c}$ *é crescente se o* j*-ésimo vetor é não negativo e crescente, para todo* $j \in \{0, 1, \cdots, t\}$

Denotaremos por $B_k(\mathbf{c}) = B_k(c_0, c_1, \cdots, c_{h-1})$ o número de k-caminhos crescentes da origem até $\mathbf{c}$. Observe que $B_k(0, 0, \cdots, 0) = 1$ e que:

Proposição 1.16. *Dados* $k, h \in \mathbb{Z}$ *com* $1 \leq k \leq h$ *e* $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ *existe um* k*-caminho crescente da origem até* $\mathbf{c}$ *se, e somente se, o vetor* $\mathbf{c}$ *é crescente e existe* $t \in \mathbb{N}$ *tal que* $\sum_{j=0}^{h-1} c_j = kt$ *e* $0 \leq c_j \leq t$ *para todo* $j = 0, 1, \cdots, h-1$*.*

Demonstração. A Proposição 1.14 nos dá condições necessárias e suficientes para a existência de um k-caminho da origem até o vetor $\mathbf{c}$. Assim, precisamos somente verificar que o fato do vetor $\mathbf{c}$ ser crescente é condição necessária e suficiente para que um k-caminho da origem até $\mathbf{c}$ seja crescente. Se $B_k(\mathbf{c}) > 0$, então o vetor $\mathbf{c}$ é crescente porque todos os vetores do k-caminho crescente são crescentes. Reciprocamente, dado um vetor crescente $\mathbf{c}$ para o qual existe um tal número $t \in \mathbb{N}$, o Algoritmo 1.4 fornece um k-caminho da origem até $\mathbf{c}$. Ocorre que, sendo $\mathbf{c}$ um vetor crescente, a escolha do critério de desempate do algoritmo já fornecerá um k-caminho crescente.

□

Note que, dado um vetor crescente $\mathbf{c} \in \mathbb{Z}^h$, para cada $\beta_i \in \Gamma$, existe, no máximo, um k-caminho crescente de $\mathbf{c} - \beta_i$ até $\mathbf{c}$, e quando tal k-caminho não existe, tem-se que $\mathbf{c} - \beta_i$ não é um vetor crescente, de modo que, pela Proposição 1.16, $B_k(\mathbf{c} - \beta_i) = 0$. Assim, vemos que a função $B_k(c_0, c_1, \cdots, c_{h-1})$ satisfaz a equação de diferenças

$$B_k(\mathbf{c}) = \sum_{i=1}^{n} B_k(\mathbf{c} - \beta_i), \tag{1.13}$$

que, juntamente com a condição inicial $B_k(0, 0, \cdots, 0) = 1$, determina completamente a função $B_k(c_0, c_1, \cdots, c_{h-1})$.

Há um problema combinatório equivalente: suponha que o vetor inicial seja $\mathbf{a}^* = (0, 1, 2, \cdots, h-1)$ e que o vetor final é $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1})$.

Definição 1.17. *Dizemos que o k-caminho $\mathbf{a}^* = \mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_t = \mathbf{c}$ de $\mathbf{a}^*$ até $\mathbf{c}$ é estritamente crescente se o j-ésimo vetor é não negativo e estritamente crescente, para todo $j \in \{0, 1, \cdots, t\}$.*

Note que não existe um k-caminho estritamente crescente iniciando na origem, pois o vetor $\mathbf{0}$ não é estritamente crescente. Essa é a razão da escolha do vetor $\mathbf{a}^*$. Seja $\hat{B}_k\ (\mathbf{c}) = \hat{B}_k\ (c_0, c_1, \cdots, c_{h-1})$ o número de k-caminhos estritamente crescentes de $\mathbf{a}^*$ até $\mathbf{c}$. Note que $\hat{B}_k\ (0, 1, \cdots, h-1) = 1$. Há uma relação simples entre os números $B_k(\mathbf{c})$ e $\hat{B}_k\ (\mathbf{c})$. O vetor $\mathbf{v} = (v_0, v_1, \cdots, v_{h-1})$ é não negativo e estritamente crescente se, e somente se, o vetor $\mathbf{v}' = \mathbf{v} - \mathbf{a}^*$ é não negativo e crescente. Segue que $\mathbf{a}^* = \mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_t = \mathbf{c}$ é um k-caminho estritamente crescente de $\mathbf{a}^*$ até $\mathbf{c}$ se, e somente se, $\mathbf{0} = \mathbf{v}_0 - \mathbf{a}^*, \mathbf{v}_1 - \mathbf{a}^*, \cdots, \mathbf{v}_t - \mathbf{a}^* = \mathbf{c} - \mathbf{a}^*$ é um k-caminho crescente da origem até $\mathbf{c} - \mathbf{a}^*$. Assim

$$\hat{B}_k\ (c_0, c_1, \cdots, c_{h-1}) = B_k(c_0, c_1 - 1, \cdots, c_{h-1} - (h-1)). \tag{1.14}$$

Já que $0 + 1 + 2 + \cdots + (h-1) = \binom{h}{2}$, como consequência da equação (1.14) e da Proposição 1.16 temos

Proposição 1.18. *Dados $k, h \in \mathbb{Z}$ com $1 \leq k \leq h$ e $\mathbf{c} = (c_0, c_1, \cdots, c_{h-1}) \in \mathbb{Z}^h$ existe um k-caminho estritamente crescente da origem até $\mathbf{c}$ se, e somente se, $\mathbf{c}$ é um vetor estritamente crescente e existe $t \in \mathbb{N}$ tal que $\sum_{j=0}^{h-1} c_j = kt + \binom{h}{2}$ e $j \leq c_j \leq t + j$, para todo $j = 0, 1, \cdots, h-1$.*

A função $\hat{B}_k\ (\mathbf{c})$ também satisfaz a uma equação de diferenças:

Proposição 1.19.

$$\hat{B}_k\ (\mathbf{c}) = \sum_{i=1}^{n} \hat{B}_k\ (\mathbf{c} - \beta_i). \tag{1.15}$$

Demonstração. De fato, indicando as coordenadas de um vetor $\beta_i \in \Gamma$ por $\beta_{i,0}, \beta_{i,1}, \cdots, \beta_{i,h-1}$, onde o primeiro índice identifica o vetor $\beta_i \in \Gamma$ e o segundo índice

indica a posição da coordenada, e usando as equações (1.13) e (1.14), temos

$$\begin{aligned}
\hat{B}_k(\mathbf{c}) &= \hat{B}_k(c_0, c_1, \cdots, c_{h-1}) \\
&= B_k(c_0, c_1 - 1, \cdots, c_{h-1} - (h-1)) \\
&= \sum_{i=1}^{n} B_k(c_0 - \beta_{i,0}, c_1 - 1 - \beta_{i,1}, \cdots, c_{h-1} - (h-1) - \beta_{i,h-1}) \\
&= \sum_{i=1}^{n} B_k(c_0 - \beta_{i,0}, (c_1 - \beta_{i,1}) - 1, \cdots, (c_{h-1} - \beta_{i,h-1}) - (h-1)) \\
&= \sum_{i=1}^{n} \hat{B}_k(c_0 - \beta_{i,0}, c_1 - \beta_{i,1}, \cdots, c_{h-1} - \beta_{i,h-1}) \\
&= \sum_{i=1}^{n} \hat{B}_k(\mathbf{c} - \beta_i).
\end{aligned}$$

□

Tal como a fórmula (1.12), a fórmula dada na proposição acima desempenhará um importante papel mais adiante, esta no cálculo dos coeficientes de potências do k-ésimo polinômio simétrico elementar multiplicado pelo polinômio de Vandermond, aquela no cálculo dos coeficientes de potências do k-ésimo polinômio simétrico elementar.

Capítulo 2

O Método Polinomial

Neste capítulo sistematizamos uma técnica usada para resolver certos problemas em Teoria Aditiva dos Números que denominamos de Método Polinomial. O método se baseia em um teorema conhecido como alq 'Combinatorial Nullstellensatz". Nosso acesso a este teorema se deu por meio de [1] e nossa demonstração é uma adaptação das idéias de [19].

2.1 Combinatorial Nullstellensatz

Iniciamos com dois lemas auxiliares.

Lema 2.1 (Nathanson [19], pág 81)**.** *Seja A um subconjunto finito e não vazio de um corpo K com $|A| = k$. Para cada $m \geq 0$ existe um polinômio $g_m(x) \in K[x]$ de grau no máximo $k-1$ tal que $g_m(a) = a^m$, para todo $a \in A$.*

Demonstração. Seja $A = \{a_0, a_1, \cdots, a_{k-1}\}$. Nós devemos mostrar que existe um polinômio $u(x) = u_0 + u_1 x + \cdots + u_{k-1}x^{k-1} \in K[x]$ tal que

$$u(a_i) = u_0 + u_0 a_i + \cdots + u_{k-1}a_i^{k-1} = a_i^m, \ \forall \ i = 0, 1, \cdots, k-1.$$

Mas estas igualdades dão origem a um sistema linear de k equações em k incógnitas $u_0, u_1, \cdots, u_{k-1}$ que, como sabemos, tem solução única se, e somente se, a matriz dos coeficiente tem determinante não nulo. Mas tal determinante é exatamente o determinante

de Vandermond:

$$\begin{vmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{k-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{k-1} & a_{k-1}^2 & \cdots & a_{k-1}^{k-1} \end{vmatrix} = \prod_{0 \leq i < j \leq k-1} (a_j - a_i) \neq 0$$

□

Lema 2.2 (N. Alon [1])**.** *Seja $h \geq 1$ e sejam $A_0, A_1, \cdots, A_{h-1}$ subconjuntos finitos e não vazios de um corpo K com $|A_i| = k_i$, $i = 0, 1, \cdots, h-1$. Seja $f(x_0, x_1, \cdots, x_{h-1}) \in K[x_0, x_1, \cdots, x_{h-1}]$ um polinômio de grau no máximo $k_i - 1$ em x_i para $i = 0, 1, \cdots, h-1$. Se $f(a_0, a_1, \cdots, a_{h-1}) = 0$ para todos $(a_0, a_1, \cdots, a_{h-1}) \in A_0 \times A_1 \times \cdots \times A_{h-1}$, então $f(x_0, x_1, \cdots, x_{h-1})$ é o polinômio nulo.*

Demonstração. A demonstração será feita por indução sobre o número de variáveis. Para $h = 1$, o lema é simplesmente a conhecida afirmação de que um polinômio não nulo de grau $k_0 - 1$ em $K[x_0]$ não pode ter k_0 raízes em K ou em qualquer extensão de K (veja [14], pág 217).

Seja agora $h \geq 2$ e suponhamos que o lema seja válido para polinômios em até $h-1$ variáveis. Nós podemos escrever

$$f(x_0, x_1, \cdots, x_{h-1}) = \sum_{j=0}^{k_0-1} f_j(x_1, \cdots, x_{h-1}) x_0^j,$$

onde $f_j(x_1, \cdots, x_{h-1})$ é um polinômio nas $h-1$ variáveis $x_1, \cdots, x_{h-1}$ cujo grau em x_i é, no máximo, $k_i - 1$, para $i = 1, \cdots, h-1$. Fixando uma $(h-1)$-upla

$$(a_1, \cdots, a_{h-1}) \in A_1 \times \cdots \times A_{h-1},$$

temos que

$$g(x_0) = f(x_0, a_1, \cdots, a_{h-1}) = \sum_{j=0}^{k_0-1} f_j(a_1, \cdots, a_{h-1}) x_0^j$$

é um polinômio de grau no máximo $k_0 - 1$ em x_0 e tal que $g(a_0) = 0$, para todo $a_0 \in A_0$. Como $|A_0| = k_0 > k_0 - 1 = deg(g(x_0))$, temos que $g(x_0)$ é identicamente nulo. Mas isto só é possível se $f_j(a_1, \cdots, a_{h-1}) = 0$ para todo $j = 1, \cdots, h-1$ e para todos $(a_1, \cdots, a_{h-1}) \in$

$A_1 \times \cdots \times A_{h-1}$. Segue da hipótese de indução que $f_j \equiv 0$ para todo $j = 1, \cdots, h-1$ e então f é o polinômio nulo.

□

O termo "Nullstellensatz"é usualmente associado a um teorema fundamental devido a Hilbert que afirma que se K é um corpo algebricamente fechado e $f, g_1, \cdots, g_m$ são polinômios no anel de polinômios $K[x_0, \cdots, x_{n-1}]$, onde f se anula em todos os zeros comuns de $g_1, \cdots, g_m$, então existem polinômios $h_1, \cdots, h_m$ em $K[x_0, \cdots, x_{n-1}]$ e um inteiro s tais que

$$f^s = \sum_{i=1}^{m} h_i g_i.$$

Inspirado no resultado de Hilbert, Noga Alon ([1], 1999) demonstrou o teorema a seguir que ele mesmo chamou de Combinatorial Nullstellensatz por força de suas numerosas aplicações em matemática combinatória. A demonstração que apresentamos não é a original de Noga Alon, mas uma adaptação das idéias de [19].

Teorema 2.3 (Combinatorial Nullstellensatz [1])**.** *Seja K um corpo e considere que $f(x_0, x_1, \cdots, x_{h-1}) \in K[x_0, x_1, \cdots, x_{h-1}]$ é um polinômio de grau $\sum_{i=0}^{h-1}(k_i - 1)$. Suponha que o coeficiente de $x_0^{k_0-1}x_1^{k_1-1}\cdots x_{h-1}^{k_{h-1}-1}$ em f seja não nulo. Se $A_0, A_1, \cdots, A_{h-1}$ são subconjuntos de K com $|A_i| \geq k_i, i = 0, 1, \cdots, h-1$, então existe $(a_0, a_1, \cdots, a_{h-1}) \in A_0 \times A_1 \times \cdots \times A_{h-1}$ tal que $f(a_0, a_1, \cdots, a_{h-1}) \neq 0$.*

Demonstração. Claramente, se o teorema vale com $|A_i| = k_i$, então também valerá quando $|A_i| \geq k_i$. Assim, podemos supor que $|A_i| = k_i$, para todo $i = 0, 1, \cdots, h-1$. Pelo Lema 2.1, para $i = 0, 1, \cdots, h-1$ e para cada $m \geq k_i$, existe um polinômio $g_{i,m}(x_i) \in K[x_i]$ de grau no máximo $k_i - 1$ e tal que $g_{i,m}(a) = a^m$ para todo $a \in A_i$. Nós usamos $g_{i,m}(x_i)$ para construir um polinômio $f^*(x_0, x_1, \cdots, x_{h-1}) \in K[x_0, x_1, \cdots, x_{h-1}]$ a partir de $f(x_0, x_1, \cdots, x_{h-1})$ como segue: se $x_0^{b_0}x_1^{b_1}\cdots x_{h-1}^{b_{h-1}}$ é um monômio de $f(x_0, x_1, \cdots, x_{h-1})$, então nós substituimos $x_i^{b_i}$ por $g_{i,b_i}(x_i)$, para todo i tal que $b_i \geq k_i$. Como $deg(f) = \sum_{i=0}^{h-1}(k_i - 1)$, segue que se $b_i \geq k_i$ para algum i em um dado monômio, então $b_j < k_j - 1$ para algum $j \neq i$ no mesmo monômio. Disto segue que o coeficiente do monômio $x_0^{k_0-1}x_1^{k_1-1}\cdots x_{h-1}^{k_{h-1}-1}$ em f^* é exatamente o mesmo coeficiente deste monômio em f e este coeficiente é, por hipótese, não nulo. Além disso, pela própria construção de f^*, temos

que o grau de f^* em x_i é exatamente $k_i - 1$ e

$$f^*(a_0, a_1, \cdots, a_{h-1}) = f(a_0, a_1, \cdots, a_{h-1})$$

para todos $(a_0, a_1, \cdots, a_{h-1}) \in A_0 \times A_1 \times \cdots \times A_{h-1}$. Agora, pelo Lema 2.2, f^* não pode se anular em todas as h-uplas de $A_0 \times A_1 \times \cdots \times A_{h-1}$, pois do contrário, seria o polinômio nulo, o que contradiria o fato de que o coeficiente de $x_0^{k_0-1}x_1^{k_1-1}\cdots x_{h-1}^{k_{h-1}-1}$ em f^* é não nulo.

□

2.2 O Método Polinomial

Agora passamos a descrever o Método Polinomial. Seja K um corpo e seja p a característica de K se a característica é um número primo e seja $p = \infty$ se a característica é zero. Sejam $h \geq 2$,

$$F(x_0, x_1, \cdots, x_{h-1}), G(x_0, x_1, \cdots, x_{h-1}) \in K[x_0, x_1, \cdots, x_{h-1}]$$

e $A_0, A_1, \cdots, A_{h-1}$ subconjuntos finitos e não vazios de K com $|A_i| = k_i$ para $i = 0, 1, \cdots, h-1$, tais que o número

$$t = \left[\frac{1}{deg(F)}\left(\sum_{i=0}^{h-1} k_i - h - deg(G)\right)\right] \tag{2.1}$$

seja não negativo. Seja ainda

$$\Omega_{FG} = \{F(a_0, a_1, \cdots, a_{h-1}) : a_i \in A_i,\ i = 0, 1, \cdots h-1,\ \text{e}\ G(a_0, a_1, \cdots, a_{h-1}) \neq 0\}.$$

Teorema 2.4 (Método Polinomial)**.** *Se o coeficiente de* $x_0^{k_0-1}x_1^{k_1-1}\cdots x_{h-1}^{k_{h-1}-1}$ *na expansão do produto* $[F(x_0, x_1, \cdots, x_{h-1})]^t G(x_0, x_1, \cdots, x_{h-1})$ *é diferente de zero, então* $|\Omega_{FG}| \geq min\{p, t+1\}$.

Demonstração. Mostraremos inicialmente que, se o teorema vale com a hipótese adicional de que $t \leq p-1$, então ele também vale para $t \geq p$. Se $t \geq p$, escolhamos inteiros positivos $k_i' \leq k_i$, $i = 0, 1, \cdots, h-1$, tais que

$$\left[\frac{1}{deg(F)}\left(\sum_{i=0}^{h-1} k_i' - h - deg(G)\right)\right] = p - 1,$$

e em seguida escolhamos $A_i^{'} \subset A_i$ tal que $|A_i^{'}| = k_i^{'}, i = 0, 1, \cdots, h-1$. Agora, $\Omega_{FG}(A_0, A_1, \cdots, A_{h-1}) \supseteq \Omega_{FG}(A_0^{'}, A_1^{'}, \cdots, A_{h-1}^{'})$, de modo que

$$\begin{aligned} |\Omega_{FG}(A_0, A_1, \cdots, A_{h-1})| &\geq |\Omega_{FG}(A_0^{'}, A_1^{'}, \cdots, A_{h-1}^{'})| \\ &\geq min\left\{p, \left[\frac{1}{deg(F)}\left(\sum_{i=0}^{h-1} k_i^{'} - h - deg(G)\right)\right] + 1\right\} \\ &= p = min\{p, t+1\}. \end{aligned}$$

Assim, podemos supor agora que $t < p$, de modo que $min\{p, t+1\} = t+1$. Portanto, devemos mostrar que $|\Omega_{FG}(A_0, A_1, \cdots, A_{h-1})| \geq t+1$. Sem perda de generalidade, passando a subconjuntos de $A_0, \cdots, A_{h-1}$ se necessário, podemos supor que

$$t = \frac{1}{deg(F)}\left(\sum_{i=0}^{h-1} k_i - h - deg(G)\right).$$

Suponhamos por contradição que $|\Omega_{FG}(A_0, A_1, \cdots, A_{h-1})| \leq t$ e escolhamos um subconjunto finito $E \subset K$ tal que $\Omega_{FG} \subset E$ e $|E| = t$. Agora definamos o polinômio

$$H(x_0, x_1, \cdots, x_{h-1}) = G(x_0, x_1, \cdots, x_{h-1}) \prod_{e \in E} (F(x_0, x_1, \cdots, x_{h-1}) - e)$$

(convencionamos que $H(x_0, x_1, \cdots, x_{h-1}) = G(x_0, x_1, \cdots, x_{h-1})$ se $E = \emptyset$). Como $|E| = t$, temos que $deg(H) = deg(G) + tdeg(F) = \sum_{i=0}^{h-1} k_i - h$. Além disso, se $(a_0, a_1, \cdots, a_{h-1}) \in A_0 \times A_1 \times \cdots \times A_{h-1}$, então ou $G(a_0, a_1, \cdots, a_{h-1}) = 0$ ou $F(a_0, a_1, \cdots, a_{h-1}) \in \Omega_{FG} \subset E$. Em todo caso, $H(a_0, a_1, \cdots, a_{h-1}) = 0$, para todos $(a_0, a_1, \cdots, a_{h-1}) \in A_0 \times A_1 \times \cdots \times A_{h-1}$. Mas

$$H(x_0, x_1, \cdots, x_{h-1}) = G(x_0, x_1, \cdots, x_{h-1}) F(x_0, x_1, \cdots, x_{h-1})^t + \text{“termos de menor grau”}$$

e, por hipótese, o coeficiente de $x_0^{k_0-1} x_1^{k_1-1} \cdots x_{h-1}^{k_{h-1}-1}$ em $H(x_0, x_1, \cdots, x_{h-1})$ é diferente de zero, o que contradiz o Teorema 2.3.

□

No caso em que

$$F = s_k(x_0, x_1, \cdots, x_{h-1}) = \sum_{0 \leq i_0 < i_1 < \cdots < i_{k-1} \leq h-1} x_{i_0} x_{i_1} \cdots x_{i_{k-1}}$$

é o polinômio simétrico elementar de grau k em h variáveis e

$$G = \Delta_h(x_0, x_1, \cdots, x_{h-1}) = \prod_{0 \leq i < j \leq h-1} (x_j - x_i),$$

é o polinômio de Vandermond em h variáveis, temos que o conjunto Ω_{FG} definido acima coincide com

$$\{s_k(a_0, a_1, \cdots, a_{h-1}) : a_i \in A_i,\ i = 0, 1, \cdots h-1,\ \text{com } a_i \neq a_j \text{ se } i \neq j\},$$

ou seja $\Omega_{s_k\Delta_h} = \hat{s_k}\ (A_0, A_1, \cdots, A_{h-1})$. Como $deg(s_k) = k$ e $deg(\Delta_h) = \frac{h(h-1)}{2}$ a equação (2.1) se torna

$$t = \left[\frac{1}{k}\left(\sum_{i=1}^{h-1} k_i - h - \frac{h(h-1)}{2}\right)\right] = \left[\frac{1}{k}\left(\sum_{i=1}^{h-1} k_i - \frac{h(h+1)}{2}\right)\right]. \tag{2.2}$$

Assim, o Teorema 2.4 nos dá a estimativa

$$|\ \hat{s_k}\ (A_0, A_1, \cdots, A_{h-1})| \geq min\left\{p, \left[\frac{1}{k}\left(\sum_{i=0}^{h-1} k_i - \frac{h(h+1)}{2}\right)\right] + 1\right\}, \tag{2.3}$$

desde que o coeficiente de $x_0^{k_0-1}x_1^{k_1-1}\cdots x_{h-1}^{k_{h-1}-1}$ na expansão do produto $[s_k]^t\Delta_h$ seja não nulo.

De modo semelhante, quando

$$F = s_k(x_0, x_1, \cdots, x_{h-1}) = \sum_{0 \leq i_0 < i_1 < \cdots < i_{k-1} \leq h-1} x_{i_0}x_{i_1}\cdots x_{i_{k-1}}$$

é o polinômio simétrico elementar de grau k em h variáveis e G é um polinômio constante não nulo, temos que o conjunto Ω_{FG} definido acima coincide com

$$\{s_k(a_0, a_1, \cdots, a_{h-1}) : a_i \in A_i,\ i = 0, 1, \cdots h-1\},$$

Como $deg(s_k) = k$ e $deg(G) = 0$ a equação (2.1) se torna

$$t = \left[\frac{1}{k}\sum_{i=1}^{h-1}(k_i - 1)\right]. \tag{2.4}$$

Assim, o Teorema 2.4 nos dá a estimativa

$$|s_k(A_0, A_1, \cdots, A_{h-1})| \geq min\left\{p, \left[\frac{1}{k}\sum_{i=0}^{h-1}(k_i - 1)\right] + 1\right\}, \tag{2.5}$$

desde que o coeficiente de $x_0^{k_0-1}x_1^{k_1-1}\cdots x_{h-1}^{k_{h-1}-1}$ na expansão de $[s_k]^t$ seja não nulo.

Nos próximos capítulos, determinamos condições sobre os números $k_0, k_1, \cdots, k_{h-1}$ suficientes para garantir que os coeficientes sejam não nulos nos respectivos polinômios.

Capítulo 3

Os Coeficientes de $(s_k)^t$ e de $(s_k)^t \cdot \Delta$

Para a comodidade do leitor, iniciamos este capítulo relembrando algumas notações. Sejam $k, h, t \in \mathbb{Z}$ com $1 \leq k \leq h$ e $t \geq 0$. Relembremos que

$$s_k(x_0, x_1, \cdots, x_{h-1}) = \sum_{0 \leq i_0 < i_1 < \cdots < i_{k-1} \leq h-1} x_{i_0} x_{i_1} \cdots x_{i_{k-1}} \tag{3.1}$$

é o polinômio simétrico elementar de grau k em h variáveis e

$$\Delta(x_0, x_1, \cdots, x_{h-1}) = \prod_{0 \leq i < j \leq h-1} (x_j - x_i), \tag{3.2}$$

é o polinômio de Vandermond em h variáveis.

Seja $\Gamma \subset \mathbb{Z}^h$ o conjunto de todos os vetores com extamente k coordenadas iguais a um e as demais coordenadas nulas. Já vimos que o número de elementos do conjunto Γ é igual a $n = \frac{h!}{k!(h-k)!}$. Sejam $\beta_1, \beta_2, \cdots, \beta_n$ todos os elementos de Γ, organizados em ordem crescente segundo a ordem lexicográfica, ou seja,

$$\begin{aligned}
\beta_1 &= (\underbrace{0, 0, \cdots, 0}_{h-k}, \underbrace{1, 1, \cdots, 1}_{k}) \\
\beta_2 &= (\underbrace{0, \cdots, 0}_{h-k-1}, 1, 0, \underbrace{1, \cdots, 1}_{k-1}) \\
&\vdots \\
\beta_n &= (\underbrace{1, 1, \cdots, 1}_{k}, \underbrace{0, 0, \cdots, 0}_{h-k})
\end{aligned}$$

Escreveremos um vetor $\beta_i \in \Gamma$ como $\beta_i = (\beta_{i,0}, \beta_{i,1}, \cdots, \beta_{i,h-1})$.

Como o polinômio s_k consiste na soma de todos os produtos de exatamente k dentre as h variáveis $x_0, x_1, \cdots, x_{h-1}$, a notação acima permite reescrevê-lo de forma mais conveniente:

$$s_k(x_0, x_1, \cdots, x_{h-1}) = \sum_{j=1}^{n} x_0^{\beta_{j,0}} x_1^{\beta_{j,1}} \cdots x_{h-1}^{\beta_{j,h-1}}. \tag{3.3}$$

Também será conveniente escrever o polinômio de Vandermond de outra maneira. Como

$$\prod_{0 \le i < j \le h-1} (x_j - x_i) = \begin{vmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{h-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{h-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{h-1} & x_{h-1}^2 & \cdots & x_{h-1}^{h-1} \end{vmatrix}$$

temos, pela definição de determinante de uma matriz,

$$\Delta(x_0, x_1, \cdots, x_{h-1}) = \sum_{\sigma \in S_h} sign(\sigma) x_0^{\sigma(0)} x_1^{\sigma(1)} \cdots x_{h-1}^{\sigma(h-1)}, \tag{3.4}$$

onde S_h é o grupo das permutações dos inteiros $\{0, 1, \cdots, h-1\}$.

3.1 Cálculo dos Coeficientes de $(s_k(\mathbf{x}))^t$

Passamos agora a calcular os coeficientes de $(s_k)^t$. Em verdade, esses coeficientes já foram calculados por Dias da Silva & Godinho em [8]. Aqui, apresentamos um cálculo alternativo usando a linguagem dos k-caminhos. Iniciamos observando que tal polinômio é homogêneo, pois é produto de polinômios homogêneos, e que $deg((s_k)^t) = kt$.

Na demonstração do teorema a seguir, faremos uso do conjunto $\mathcal{C}(t) = \{\mathbf{c} = (c_0, \cdots, c_{h-1}) \in \mathbb{Z}^h : 0 \le c_j \le t \text{ e } c_0 + \cdots + c_{h-1} = kt\}$.

Teorema 3.1. *Para todo $t \ge 0$,*

$$(s_k(x_0, \cdots, x_{h-1}))^t = \sum_{\mathbf{c} \in \mathcal{C}(t)} P_k(\mathbf{0}, \mathbf{c}) x_0^{c_0} x_1^{c_1} \cdots x_{h-1}^{c_{h-1}},$$

onde $P_k(\mathbf{0}, \mathbf{c})$ é o número de k-caminhos da origem até $\mathbf{c}$ (veja a Seção 1.2, pág 22 e 23).

Demonstração. A demonstração é feita por indução sobre t. Para $t = 0$, temos $\mathcal{C}(0) = \{\mathbf{0}\}$. Assim, os dois membros na igualdade do teorema são iguais a 1. Admita que

o teorema vale para algum $t \geq 0$. Então, notando que cada elemento em $\mathcal{C}(t+1)$ pode ser escrito como a soma de um elemento de $\mathcal{C}(t)$ com um elemento de Γ, fazendo uso da Proposição 1.14 e da equação (1.12), temos

$$\begin{aligned}
(s_k(\mathbf{x}))^{t+1} &= s_k(\mathbf{x}) \cdot (s_k(\mathbf{x}))^t \\
&= \left(\sum_{j=1}^{n} x_0^{\beta_{j,0}} \cdots x_{h-1}^{\beta_{j,h-1}} \right) \left(\sum_{\mathbf{c} \in \mathcal{C}(t)} P_k(\mathbf{0}, \mathbf{c}) x_0^{c_0} x_1^{c_1} \cdots x_{h-1}^{c_{h-1}} \right) \\
&= \sum_{\mathbf{c} \in \mathcal{C}(t)} \sum_{j=1}^{n} P_k(\mathbf{0}, \mathbf{c}) x_0^{c_0+\beta_{j,0}} x_1^{c_1+\beta_{j,1}} \cdots x_{h-1}^{c_{h-1}+\beta_{j,h-1}} \\
&= \sum_{\mathbf{b} \in \mathcal{C}(t+1)} \sum_{j=1}^{n} P_k(\mathbf{0}, \mathbf{b} - \beta_j) x_0^{b_0} x_1^{b_1} \cdots x_{h-1}^{b_{h-1}} \\
&= \sum_{\mathbf{b} \in \mathcal{C}(t+1)} P_k(\mathbf{0}, \mathbf{b}) x_0^{b_0} x_1^{b_1} \cdots x_{h-1}^{b_{h-1}},
\end{aligned}$$

o que finaliza a demonstração do teorema.

□

Vale lembrar que o número $P_k(\mathbf{0}, \mathbf{c})$ coincide com o número de $k\mathbf{c}$-matrizes, de modo que o teorema acima fornece uma maneira indireta de se calcular o número de tais matrizes.

3.2 Cálculo dos Coeficientes de $(s_k(\mathbf{x}))^t \cdot \Delta(\mathbf{x})$

O cálculo dos coeficientes de $(s_k(\mathbf{x}))^t \cdot \Delta(\mathbf{x})$ exigirá um pouco mais de trabalho. Iniciamos observando que tal polinômio é homogêneo, pois é produto de polinômios homogêneos. Além disso,

$$deg((s_k)^t \Delta) = t \cdot deg(s_k) + deg(\Delta) = kt + \binom{h}{2}. \tag{3.5}$$

Mais ainda, como o grau de cada variável em s_k não excede a uma unidade e em Δ não excede a $h-1$, vemos que o grau de cada variável em $(s_k)^t \Delta$ é menor do que ou igual a $t+h-1$. Estes comentários motivam o estudo do seguinte conjunto:

$$\mathcal{T}(t) = \left\{ (s_0, \cdots, s_{h-1}) \in \mathbb{Z}^h : 0 \leq s_0 < \cdots < s_{h-1} \leq t+h-1 \text{ e } s_0 + \cdots + s_{h-1} = kt + \binom{h}{2} \right\}.$$

Convém observar que se $(s_0, \cdots, s_{h-1}) \in \mathcal{T}(t)$, então

$$j \leq s_j \leq t + j, \forall j \in \{0, 1, \cdots, h-1\}. \tag{3.6}$$

No que segue, usaremos também o conjunto

$$\mathbb{T}(t) = \left\{ (s_0, \cdots, s_{h-1}) \in \mathbb{Z}^h : 0 \leq s_0 \leq \cdots \leq s_{h-1} \leq t+h-1 \text{ e } s_0+\cdots+s_{h-1} = kt+\binom{h}{2} \right\}.$$

A diferença entre os conjuntos $\mathcal{T}(t)$ e $\mathbb{T}(t)$ é que, no primeiro, as coordenadas de cada vetor são dispostas em ordem estritamente crescente, equanto que no segundo, a ordem não é estrita.

Proposição 3.2. *Para cada* $(s_0, \cdots, s_{h-1}) \in \mathcal{T}(t+1)$, *existem* $(t_0, \cdots, t_{h-1}) \in \mathcal{T}(t)$ *e* $\beta = (\beta_0, \beta_1, \cdots, \beta_{h-1}) \in \Gamma$ *tais que* $(s_0, \cdots, s_{h-1}) = (t_0 + \beta_0, \cdots, t_{h-1} + \beta_{h-1})$.

Demonstração. A demonstração é apenas um estudo de caso:

Caso 1. Se $s_0 > 0$ e $s_{h-1} < t + h$, basta tomar $t_0 = s_0 - 1, \cdots, t_{k-1} = s_{k-1} - 1$, $t_k = s_k, \cdots, t_{h-1} = s_{h-1}$ e $\beta = (\underbrace{1, 1, \cdots, 1}_{k}, \underbrace{0, 0, \cdots, 0}_{h-k})$.

Caso 2. Se $s_0 = 0$ e $s_{h-1} < t + h$, seja i_0 a posição da primeira coordenada tal que $s_{i_0} + 1 < s_{i_0+1}$ (tal número existe, pois se $s_j + 1 = s_{j+1}, \forall j \in \{0, 1, \cdots, h-1\}$, como $s_0 = 0$, teríamos $s_j = j, \forall j \in \{0, 1, \cdots, h-1\}$ e então $\sum_{j=0}^{h-1} s_j = \binom{h}{2} < k(t+1) + \binom{h}{2}$). Pela minimalidade de i_0 é fácil perceber que $s_j = j, \forall j \in \{0, 1, \cdots, i_0\}$. Agora note que $i_0 < (h-1) - k$. De fato, se $i_0 \geq (h-1) - k$, então, usando a desigualdade (3.6), teríamos

$$\begin{aligned}
k(t+1) + \binom{h}{2} &= s_0 + \cdots + s_{i_0} + s_{i_0+1} + \cdots + s_{h-1} \\
&= 0 + 1 + \cdots + i_0 + s_{i_0+1} + \cdots + s_{h-1} \\
&\leq 0 + 1 + \cdots + i_0 + \underbrace{((t+1)+i_0) + \cdots + ((t+1)+(h-1))}_{(h-1)-i_0} \\
&= 0 + 1 + \cdots + i_0 + (i_0+1) + \cdots + (h-1) + \underbrace{t + \cdots + t}_{(h-1)-i_0} \\
&= \frac{(h-1)h}{2} + ((h-1) - i_0)t \\
&= \binom{h}{2} + ((h-1) - i_0)t \\
&\leq kt + \binom{h}{2}, \text{ uma contradição.}
\end{aligned}$$

Assim, tomamos $t_0 = s_0, \cdots,\ t_{i_0} = s_{i_0},\ t_{i_0+1} = s_{i_0+1} - 1,\ t_{i_0+k} = s_{i_0+k} - 1, \cdots,\ t_{i_0+k+1} = s_{i_0+k+1}, \cdots,\ t_{h-1} = s_{h-1}$ e $\beta = (\underbrace{0, \cdots, 0}_{i_0}, \underbrace{1, \cdots, 1}_{k}, \underbrace{0, \cdots, 0}_{h-i_0-k})$.

Caso 3. Se $s_0 > 0$ e $s_{h-1} = t + h$, caso $k = h$, tudo estará resolvido com $t_j = s_j - 1, \forall j \in \{0, 1, \cdots, h-1\}$ e $\beta = (1, \cdots, 1)$. Assim podemos supor $k < h$. Neste caso, seja i_1 a posição da última coordenada tal que $s_{i_1} + 1 < s_{i_1+1}$ (tal número existe, pois se $s_j + 1 = s_{j+1}, \forall j \in \{0, 1, \cdots, h-1\}$, como $s_{h-1} = t + h$, teríamos $s_j = (t+1) + j, \forall j \in \{0, 1, \cdots, h-1\}$ e então $\sum_{j=0}^{h-1} s_j = h(t+1) + \binom{h}{2} > k(t+1) + \binom{h}{2}$). Pela maximilidade de i_1, temos que $s_j = (t+1) + j$ para todo $j \in \{i_1 + 1, \cdots, h-1\}$ e $s_{i_1} < (t+1) + i_1$. Além disso, $s_0 > 0$, juntamente com a desigualdade inferior em (3.6), implica que $s_j \geq j + 1, \forall j \in \{0, 1, \cdots, h-1\}$. Agora note que $i_1 > (h-1) - k$. De fato, se $i_1 \leq (h-1) - k$, então

$$\begin{aligned}
k(t+1) + \binom{h}{2} &= s_0 + \cdots + s_{i_1} + s_{i_1+1} + \cdots + s_{h-1} \\
&\geq 1 + 2 + \cdots + (i_1 + 1) + s_{i_1+1} + \cdots + s_{h-1} \\
&= 1 + 2 + \cdots + (i_1 + 1) + \\
&\quad \underbrace{((t+1) + (i_1 + 1)) + \cdots + ((t+1) + (h-1))}_{(h-1)-i_1} \\
&= (i_1 + 1) + 0 + 1 + \cdots + i_1 + \\
&\quad ((i_1 + 1) + (i_1 + 2) \cdots + (h-1)) + (h - 1 - i_1)(t+1) \\
&= (i_1 + 1) + \binom{h}{2} + (h - 1 - i_1)(t+1) \\
&\geq (i_1 + 1) + \binom{h}{2} + k(t+1) \\
&> k(t+1) + \binom{h}{2}, \text{ uma contradição.}
\end{aligned}$$

Assim, tomamos $t_0 = s_0 - 1, \cdots,\ t_{k+i_1+1-h} = s_{k+i_1+1-h} - 1,\ t_{k+i_1+2-h} = s_{k+i_1+2-h}, \cdots,\ t_{h-1-i_1-1} = s_{h-1-i_1-1},\ t_{h-1-i_1} = s_{h-1-i_1} - 1 \cdots,\ t_{h-1} = s_{h-1} - 1$ e $\beta = (\underbrace{1, \cdots, 1}_{k+i_1+1-h}, \underbrace{0, \cdots, 0}_{h-k}, \underbrace{1, \cdots, 1}_{h-1-i_1})$.

Caso 4. Se $s_0 = 0$ e $s_{h-1} = t + h$, sejam i_0 e i_1 como acima. Iniciamos observando

que $i_1 \geq (h-1)-k$. De fato, se $i_1 < (h-1)-k$, então

$$\begin{aligned} k(t+1)+\binom{h}{2} &= s_0+\cdots+s_{i_1}+s_{i_1+1}+\cdots+s_{h-1} \\ &\geq 0+1+\cdots+i_1+s_{i_1+1}+\cdots+s_{h-1} \\ &= 0+1+\cdots+i_1+\underbrace{((t+1)+(i_1+1))+\cdots+((t+1)+(h-1))}_{(h-1)-i_1} \\ &= \binom{h}{2}+((h-1)-i_1)(t+1) \\ &> k(t+1)+\binom{h}{2}, \text{ uma contradição.} \end{aligned}$$

Quando $i_1 = (h-1)-k$, tudo estará resolvido com $t_0 = s_0, \cdots,\ t_{i_1} = s_{i_1}$, $t_{i_1+1} = s_{i_1+1}-1, \cdots,\ t_{h-1} = s_{h-1}-1$ e $\beta = (\underbrace{0,\cdots,0}_{i_1+1},\underbrace{1,\cdots,1}_{k})$. Assim, podemos supor $i_1 > (h-1)-k$. É claro das definições que $i_0 \leq i_1$. Como antes, temos $i_0 \leq (h-1)-k$. Assim, tomamos $t_0 = s_0, \cdots,\ t_{i_0} = s_{i_0},\ t_{i_0+1} = s_{i_0+1}-1, \cdots,\ t_{i_0+k-h+i_1+1} = s_{i_0+k-h+i_1+1}-1$, $t_{i_0+k-h+i_1+2} = s_{i_0+k-h+i_1+2}, \cdots,\ t_{i_1} = s_{i_1}, t_{i_1+1} = s_{i_1+1}-1, \cdots,\ t_{h-1} = s_{h-1}-1$ e $\beta = (\underbrace{0,\cdots,0}_{i_0+1},\underbrace{1,\cdots,1}_{k-h+i_1+1},\underbrace{0,\cdots,0}_{h-k-1-i_0},\underbrace{1,\cdots,1}_{h-1-i_1})$.

□

Na Proposição 3.2 mostramos que todo elemento de $\mathcal{T}(t+1)$ pode ser escrito como uma soma de um elemento de $\mathcal{T}(t)$ com um elemento de Γ, ou seja, quando as uplas $(t_0,\cdots,t_{h-1})$ percorrem o conjunto $\mathcal{T}(t)$ e os vetores $\beta = (\beta_0,\beta_1,\cdots,\beta_{h-1})$ percorrem o conjunto Γ, as somas $(t_0+\beta_0,\cdots,t_{h-1}+\beta_{h-1})$ atingem todos os elementos do conjunto $\mathcal{T}(t+1)$. Mas também, pode ocorrer que, dados $(t_0,t_1,\cdots,t_{h-1}) \in \mathcal{T}(t)$ e $\beta = (\beta_0,\beta_1,\cdots,\beta_{h-1}) \in \Gamma$, o vetor $(t_0+\beta_0, t_1+\beta_1,\cdots,t_{h-1}+\beta_{h-1})$, embora ainda seja um vetor crescente, não esteja em $\mathcal{T}(t+1)$, e isso ocorrerá quando ele possuir duas ou mais coordenadas iguais. Como as coordenadas de β são apenas zeros ou uns e como o vetor $(t_0,\cdots,t_{h-1})$ é estritamente crescente, vemos que quando o vetor $(t_0+\beta_0,\cdots,t_{h-1}+\beta_{h-1})$ não está em $\mathcal{T}(t+1)$, suas coordenadas serão iguais aos pares, ou seja, não é possível que hajam três ou mais coordenadas iguais entre si.

Definição 3.3. *Dizemos que o vetor $(x_0,\cdots,x_{h-1}) \in \mathbb{Z}^h$ possui coordenadas iguais aos pares se existem inteiros distintos $i_1,j_1,i_2,j_2,\cdots,i_m,j_m \in \{0,1,\cdots,h-1\}$ tais que*

$x_{i_1} = x_{j_1}, x_{i_2} = x_{j_2}, \cdots, x_{i_m} = x_{j_m}$ *e* $x_i \neq x_j$ *se* $(i,j) \notin \{(i_1,j_1),(i_2,j_2),\cdots,(i_m,j_m)\}$.

Relembramos que o grupo simétrico S_h age sobre $\mathbb{Z}^h$ como segue: para $\sigma \in S_h$ e $\mathbf{x} = (x_0, x_1, \cdots, x_{h-1}) \in \mathbb{Z}^h$, defina $\sigma(\mathbf{x}) = (x_{\sigma(0)}, x_{\sigma(1)}, \cdots, x_{\sigma(h-1)})$. Note que $\sigma(\mathbf{x}+\mathbf{y}) = \sigma(\mathbf{x}) + \sigma(\mathbf{y})$ e que $\sigma(\tau(\mathbf{x})) = (\sigma \circ \tau)(\mathbf{x})$, para todos $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^h$, e todos $\sigma, \tau \in S_h$. Note também que, dado $\mathbf{x} \in \mathbb{Z}^h$, o conjunto $H_{\mathbf{x}} = \{\sigma \in S_h : \sigma(\mathbf{x}) = \mathbf{x}\}$ é um subgrupo de S_h, que é o *subgrupo estabilizador de* $\mathbf{x}$ *em* S_h.

No caso em que $\mathbf{x} \in \mathbb{Z}^h$ possui coordenadas iguais aos pares, com a notação da definição acima, denotemos por $\tau_q = (i_q, j_q) \in S_h$, $1 \leq q \leq m$, à transposição que permuta os inteiros i_q e j_q e fixa os demais. Assim, $\tau_q(\mathbf{x}) = \mathbf{x}$ para todo $1 \leq q \leq m$ e também, como os inteiros $i_1, j_1, i_2, j_2, \cdots, i_m$ e j_m são distintos, temos $\tau_q \circ \tau_r = \tau_r \circ \tau_q$, para todos $1 \leq q, r \leq m$.

Proposição 3.4. *Seja* $\mathbf{x} \in \mathbb{Z}^h$ *com coordenadas iguais aos pares (com a notação da definição acima). Se* $\sigma \in S_h$ *é tal que* $\sigma(\mathbf{x}) = \mathbf{x}$*, então existem únicos* $\epsilon_1, \cdots, \epsilon_m \in \{0,1\}$ *tais que* $\sigma = \tau_1^{\epsilon_1} \circ \cdots \circ \tau_m^{\epsilon_m}$.

Demonstração. Como o vetor $\mathbf{x}$ possui as coordenadas x_{i_q} e x_{j_q}, $q \in \{1, 2, \cdots, m\}$, iguais e todas as demais coordenadas diferentes destas duas, qualquer permutação $\sigma \in S_h$ que fixe $\mathbf{x}$, ou permutará estas duas coordenadas, ou as manterá em suas respectivas posições. Assim, σ é a composição de algumas dentre as transposições $\tau_1, \cdots, \tau_m$. A unicidade segue diretamente do fato de estas transposições serem duas a duas disjuntas. □

Conforme mostra a proposição acima, se $\mathbf{x} \in \mathbb{Z}^h$ possui coordenadas iguais ao pares, então o subgrupo estabilizador de $\mathbf{x}$ em S_h, $H_{\mathbf{x}} \subset S_h$, é gerado pelas transposições $\tau_q = (i_q, j_q) \in S_h$, $1 \leq q \leq m$. Pelos comentários que precedem a proposição, este subgrupo é abeliano. Assim, como um corolário, vemos que a ordem do subgrupo $H_{\mathbf{x}}$ é 2^m. Mas podemos concluir mais:

Corolário 3.5. *Se* $\mathbf{x} \in \mathbb{Z}^h$ *possui coordenadas iguais aos pares, então o número de permutações pares em* $H_{\mathbf{x}}$ *é igual ao número de permutações ímpares.*

Demonstração. Pela Proposição 3.4, para cada inteiro $0 \leq i \leq m$, existem $\binom{m}{i}$ permutações formadas como produto de exatamente i transposições dentre aquelas que

fixam $\mathbf{x}$, e cada uma dessas permutações é par se, e somente se, i é um número par. Agora, cada permutação ímpar contribui com um sinal negativo e cada permutação par com um sinal positivo na soma

$$\sum_{i=0}^{m}(-1)^i\binom{m}{i}.$$

Pelo binômio de Newton, esta soma é igual a $(1-1)^m = 0$, de modo que os números de permutações pares e ímpares são iguais.

□

Finalmente, podemos calcular os coeficientes de $(s_k(\mathbf{x}))^t \cdot \Delta(\mathbf{x})$. Por simplicidade de notação, se $\mathbf{v} = (v_0, v_1, \cdots, v_{h-1})$ tem coordenadas inteiras não negativas, indicaremos o monômio $x_0^{v_0}x_1^{v_1}\cdots x_{h-1}^{v_{h-1}}$ por $\mathbf{x}^{\mathbf{v}}$. Com esta notação, as igualdades (3.3) e (3.4) se escrevem, respectivamente, como

$$s_k(\mathbf{x}) = \sum_{j=1}^{n}\mathbf{x}^{\beta_j} \tag{3.7}$$

e, com $\mathbf{a}^* = (0, 1, 2, \cdots, h-1)$,

$$\Delta(\mathbf{x}) = \sum_{\sigma\in S_h} sign(\sigma)\mathbf{x}^{\sigma(\mathbf{a}^*)} \tag{3.8}$$

onde S_h é o grupo das permutações dos inteiros $\{0, 1, \cdots, h-1\}$.

Teorema 3.6. *Para todo $t \geq 0$,*

$$\begin{aligned}(s_k(\mathbf{x}))^t \cdot \Delta(\mathbf{x}) &= \sum_{\sigma\in S_h}\sum_{\mathbf{c}\in\mathcal{T}(t)} sign(\sigma)\ \hat{B}_k(\mathbf{c})\mathbf{x}^{\sigma(\mathbf{c})} \\ &= \sum_{\sigma\in S_h}\sum_{(c_0,c_1,\cdots,c_{h-1})\in\mathcal{T}(t)} sign(\sigma)\ \hat{B}_k(c_0, c_1, \cdots, c_{h-1})x_0^{c_{\sigma(0)}}x_1^{c_{\sigma(1)}}\cdots x_{h-1}^{c_{\sigma(h-1)}},\end{aligned}$$

onde $\hat{B}_k(\mathbf{c}) = B_k(c_0, c_1, \cdots, c_{h-1})$ é o número de k-caminhos estritamente crescentes que chegam a $\mathbf{c}$ (veja a Seção 1.2, pág 24).

Demonstração. A demonstração é feita por indução sobre t. Para $t = 0$ as condições sobre $c_0, c_1, \cdots, c_{h-1}$ são $0 \leq c_0 < c_1 < \cdots < c_{h-1} \leq h-1$ e $c_0 + c_1 + \cdots + c_{h-1} = \binom{h}{2}$, de modo que $c_j = j,\ \forall j \in \{0, 1, \cdots, h-1\}$. Assim, apenas a upla $(0, 1, \cdots, h-1)$ satisfaz

estas condições e, como sabemos, $\hat{B}_k\,(0,1,\cdots,h-1)=1$. Portanto, o somatório no membro direito se torna $\sum_{\sigma\in S_h} sign(\sigma)x_0^{\sigma(0)}x_1^{\sigma(1)}\cdots x_{h-1}^{\sigma(h-1)}$, enquanto que o primeiro membro, para $t=0$, é $\Delta(x_0,x_1,\cdots,x_{h-1})$. Assim, a igualdade segue por (3.4). Suponhamos agora que o teorema valha para algum $t\geq 0$. Então

$$\begin{aligned}
(s_k(\mathbf{x}))^{t+1}\cdot\Delta(\mathbf{x}) &= s_k(\mathbf{x})\cdot(s_k(\mathbf{x}))^t\cdot\Delta(\mathbf{x})\\
&= \left(\sum_{j=1}^{n}\mathbf{x}^{\beta_j}\right)\left(\sum_{\sigma\in S_h}\sum_{\mathbf{c}\in\mathcal{T}(t)} sign(\sigma)\ \hat{B}_k\,(\mathbf{c})\mathbf{x}^{\sigma(\mathbf{c})}\right)\\
&= \sum_{\sigma\in S_h} sign(\sigma)\left(\sum_{j=1}^{n}\mathbf{x}^{\beta_j}\right)\left(\sum_{\mathbf{c}\in\mathcal{T}(t)}\hat{B}_k\,(\mathbf{c})\mathbf{x}^{\sigma(\mathbf{c})}\right)\\
&= \sum_{\sigma\in S_h} sign(\sigma)\sum_{\mathbf{c}\in\mathcal{T}(t)}\left\{\left(\sum_{j=1}^{n}\mathbf{x}^{\beta_j}\right)\hat{B}_k\,(\mathbf{c})\mathbf{x}^{\sigma(\mathbf{c})}\right\}\\
&= \sum_{\sigma\in S_h} sign(\sigma)\sum_{\mathbf{c}\in\mathcal{T}(t)}\sum_{j=1}^{n}\hat{B}_k\,(\mathbf{c})\mathbf{x}^{\sigma(\mathbf{c})+\beta_j}. \qquad (3.9)
\end{aligned}$$

É fácil ver que todo vetor $\mathbf{c}=(c_0,\cdots,c_{h-1})\in\mathcal{T}(t)$ pode ser escrito na forma $\mathbf{c}=(b_0-\beta_{i,0},\cdots,b_{h-1}-\beta_{i,h-1})$ para algum $\mathbf{b}=(b_0,\cdots,b_{h-1})\in\mathbb{T}(t+1)$ e algum $\beta_i\in\Gamma$. Como todo vetor em $\mathcal{T}(t+1)$ pode ser escrito como soma de um vetor de $\mathcal{T}(t)$ com um vetor de Γ (veja a Proposição 3.2), (3.9) se torna

$$s_k(\mathbf{x}))^{t+1}\cdot\Delta(\mathbf{x}) = \sum_{\sigma\in S_h} sign(\sigma)\sum_{\mathbf{b}\in\mathbb{T}(t+1)}\sum_{j=1}^{n}\hat{B}_k\,(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}. \qquad (3.10)$$

Em (3.10), quando $\mathbf{b}\in\mathbb{T}(t+1)$, a diferença $\mathbf{b}-\beta_j$ pode não estar em $\mathcal{T}(t)$. Mas neste caso, pela Proposição 1.18, $\hat{B}_k\,(\mathbf{b}-\beta_j)=0$, de modo que apenas acrescentamos algumas parcelas nulas à soma na passagem de (3.9) para (3.10). Reorganizando os somatórios em (3.10) temos

$$=\sum_{\sigma\in S_h} sign(\sigma)\left\{\sum_{\mathbf{b}\in\mathcal{T}(t+1)}\sum_{j=1}^{n}\hat{B}_k\,(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}+\sum_{\mathbf{b}\in\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)}\sum_{j=1}^{n}\hat{B}_k\,(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}\right\}$$

$$= \sum_{\sigma\in S_h} sign(\sigma) \sum_{\mathbf{b}\in\mathcal{T}(t+1)} \sum_{j=1}^{n} \hat{B}_k\,(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})} + \sum_{\sigma\in S_h} sign(\sigma) \sum_{\mathbf{b}\in\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)} \sum_{j=1}^{n} \hat{B}_k\,(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}$$

$$= \sum_{\sigma\in S_h} sign(\sigma) \sum_{\mathbf{b}\in\mathcal{T}(t+1)} \sum_{j=1}^{n} \hat{B}_k\,(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})} + \sum_{\mathbf{b}\in\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)} \sum_{j=1}^{n} \sum_{\sigma\in S_h} sign(\sigma)\ \hat{B}_k\,(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}. \tag{3.11}$$

Agora, pela equação (1.15) temos que (3.11) se torna

$$\sum_{\sigma\in S_h} sign(\sigma) \sum_{\mathbf{b}\in\mathcal{T}(t+1)} \hat{B}_k\,(\mathbf{b})\mathbf{x}^{\sigma(\mathbf{b})} + \sum_{\mathbf{b}\in\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)} \sum_{j=1}^{n} \sum_{\sigma\in S_h} sign(\sigma)\ \hat{B}_k\,(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})}$$

de modo que, para finalizar a demonstração, é suficiente mostrar que

$$\sum_{\mathbf{b}\in\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)} \sum_{j=1}^{n} \sum_{\sigma\in S_h} sign(\sigma)\ \hat{B}_k\,(\mathbf{b}-\beta_j)\mathbf{x}^{\sigma(\mathbf{b})} = 0. \tag{3.12}$$

Em (3.12), se uma upla $\mathbf{b} = (b_0, \cdots, b_{h-1})$ em $\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)$ possui três ou mais coordenadas iguais, $b_i = b_{i+1} = b_{i+2} = \cdots$, então, para cada $j = 1, 2, \cdots, n$, o vetor $(b_0 - \beta_{j,0}, \cdots, b_{h-1} - \beta_{j,h-1})$ não possui todas as suas coordenadas distintas, pois isso exigiria que as coordenadas $b_i - \beta_{j,i}$ e $b_{i+2} - \beta_{j,i+2}$ diferissem por pelo menos duas unidades, o que é impossível pois $b_i = b_{i+2}$ e $\beta_{j,i}, \beta_{j,i+2} \in \{0, 1\}$. Assim, para as uplas $\mathbf{b} = (b_0, \cdots, b_{h-1}) \in \mathbb{T}(t+1)\setminus\mathcal{T}(t+1)$ que possuem três ou mais coordenadas iguais, pela Proposição 1.18, temos $\hat{B}_k\,(\mathbf{b}-\beta_j) = 0$, para todo $j = 1, 2, \cdots, n$, de modo que estas uplas não contribuem para a soma em (3.12). Podemos, portanto, considerar apenas as uplas em $\mathbb{T}(t+1)\setminus\mathcal{T}(t+1)$ que possuem as coordenadas iguais aos pares.

Fixemos $\mathbf{b} \in \mathbb{T}(t+1)\setminus\mathcal{T}(t+1)$ com coordenadas iguais aos pares e $\beta_j \in \Gamma$. Sejam $\sigma_1, \cdots, \sigma_r \in S_h$, $r \geq 1$, todas as permutações de S_h tais que $\sigma_i(\mathbf{b}) \neq \sigma_j(\mathbf{b})$ se $i \neq j$.

Para cada $l = 1, 2, \cdots, r$, seja $H_l = \{\delta \in S_h : \delta(\mathbf{b}) = \sigma_l(\mathbf{b})\}$. Note que, se $\delta \in H_l$, a permutação $\gamma = \delta \circ \sigma_l^{-1}$ pertence ao subgrupo $H_{\sigma_l(\mathbf{b})}$ estabilizador de $\sigma_l(\mathbf{b})$ em S_h, pois $\gamma(\sigma_l(\mathbf{b})) = \delta \circ \sigma_l^{-1}(\sigma_l(\mathbf{b})) = \delta(\mathbf{b}) = \sigma_l(\mathbf{b})$. Em verdade, a função $\phi_l : H_l \to H_{\sigma_l(\mathbf{b})}$ dada por $\phi_l(\delta) = \delta \circ \sigma_l^{-1}$ é bijetora. Assim, como $S_h = \bigcup_{l=1}^{r} H_l$, temos

$$\begin{aligned}
\sum_{\sigma \in S_h} sign(\sigma)\ \hat{B}_k\ (\mathbf{b} - \beta_j)\mathbf{x}^{\sigma(\mathbf{b})} &= \sum_{l=1}^{r} \sum_{\delta \in H_l} sign(\delta)\ \hat{B}_k\ (\mathbf{b} - \beta_j)\mathbf{x}^{\delta(\mathbf{b})} \\
&= \sum_{l=1}^{r} \sum_{\delta\sigma_l^{-1} \in H_{\sigma_l(\mathbf{b})}} sign(\delta)\ \hat{B}_k\ (\mathbf{b} - \beta_j)\mathbf{x}^{\delta(\mathbf{b})} \\
&= \sum_{l=1}^{r} \sum_{\gamma \in H_{\sigma_l(\mathbf{b})}} sign(\gamma\sigma_l)\ \hat{B}_k\ (\mathbf{b} - \beta_j)\mathbf{x}^{\gamma\sigma_l(\mathbf{b})} \\
&= \sum_{l=1}^{r} sign(\sigma_l) \sum_{\gamma \in H_{\sigma_l(\mathbf{b})}} sign(\gamma)\ \hat{B}_k\ (\mathbf{b} - \beta_j)\mathbf{x}^{\gamma(\sigma_l(\mathbf{b}))}
\end{aligned}$$

Pelo Corolário 3.5, o número de permutações pares $\gamma_1 \in H_{\sigma_l(\mathbf{b})}$ e de permutações ímpares $\gamma_2 \in H_{\sigma_l(\mathbf{b})}$ tais que $\mathbf{x}^{\gamma_1(\sigma_l(\mathbf{b}))} = \mathbf{x}^{\gamma_2(\sigma_l(\mathbf{b}))}$ é o mesmo, e assim

$$\sum_{\gamma \in H_{\sigma_l(\mathbf{b})}} sign(\gamma)\ \hat{B}_k\ (\mathbf{b} - \beta_j)\mathbf{x}^{\gamma(\sigma_l(\mathbf{b}))} = 0,$$

e então

$$\sum_{\sigma \in S_h} sign(\sigma)\ \hat{B}_k\ (\mathbf{b} - \beta_j)\mathbf{x}^{\sigma(\mathbf{b})} = 0,$$

o que é suficiente para anular o somatório em (3.12) e finalizar a demonstração do teorema.

□

Capítulo 4

Generalização do Teorema de Cauchy-Davenport e da Conjectura de Erdös-Heilbronn

É chegado o momento de juntar as informações apresentadas nos capítulos anteriores para demonstrar os Teoremas 1 e 2 cujos enunciados reapresentamos abaixo. Iniciamos relembrando algumas notações. Considere $k, h \in \mathbb{N}$ com $h \geq 2$ e $k \leq h$ e seja $n = \frac{h!}{k!(h-k)!}$. Sejam $A_0, A_1, \cdots, A_{h-1}$ subconjuntos finitos não vazios de um corpo K de característica p se ela é positiva e $p = \infty$ se ela é zero e sejam $|A_i| = k_i$ para $i = 0, 1, \cdots, h-1$. Considere ainda os conjuntos

$$s_k(A_0, A_1, \cdots, A_{h-1}) = \{s_k(a_0, a_1, \cdots, a_{h-1}) : a_i \in A_i\}$$

e

$$\overset{\wedge}{s_k}(A_0, A_1, \cdots, A_{h-1}) = \{s_k(a_0, a_1, \cdots, a_{h-1}) : a_i \in A_i \text{ com } a_i \neq a_j \text{ se } i \neq j\}$$

e os números $l = \left[\frac{\sum_{j=0}^{h-1} k_j - h}{k}\right]$ e $t = \left[\frac{\sum_{j=0}^{h-1} k_j - \frac{h(h+1)}{2}}{k}\right] = \left[\frac{\sum_{j=0}^{h-1}(k_j - (j+1))}{k}\right]$, onde $[x]$ indica a parte inteira de x.

Teorema 4.1. *Suponha que* $p > \frac{(t+n-1)!}{\left(\left[\frac{t}{n}\right]!\right)^n (n-1)!}$ *quando a característica de* K *for positiva. Se* $k_i \neq k_j$ *para* $i \neq j$ *e* $k_i \leq t + h$ *para todo* $i = 0, 1, \cdots h-1$, *então*

$$|\overset{\wedge}{s_k}(A_0, A_1, \cdots, A_{h-1})| \geq min\{p, t+1\}.$$

Teorema 4.2. *Suponha que* $p > \frac{(l+n-1)!}{\left(\left[\frac{l}{n}\right]!\right)^n (n-1)!}$ *quando a característica de* K *for positiva. Se* $k_j \leq l+1, j = 0, 1, \cdots, h-1$, *então*

$$|s_k(A_0, A_1, \cdots, A_{h-1})| \geq min\{p, l+1\}.$$

Como um corolário do Teorema 4.1, podemos obter a estimativa (3) obtida por Caldeira em [4] usando técnicas de álgebra multilinear. Em verdade, o resultado de Caldeira é o caso particular $k = 1$ ou $k = h-1$ do corolário.

Corolário 4.3. *Seja* $\overset{\wedge}{s_k}(A) = \{s_k(a_0, a_1, \cdots, a_{h-1}) : a_i \in A \text{ onde } a_i \neq a_j \text{ se } i \neq j\}$. *Se* $p > \frac{(t+n-1)!}{\left(\left[\frac{t}{n}\right]!\right)^n (n-1)!}$ *quando a característica de* K *for positiva, então para todo* $k \in \{1, 2, \cdots, h\}$ *tem-se*

$$|\overset{\wedge}{s_k}(A)| \geq min\left\{p, \left[\frac{h(|A|-h)}{k}\right] + 1\right\}. \tag{4.1}$$

Demonstração. Sejam $A_0, \cdots, A_{h-1}$ subconjuntos de A tais que $|A_i| = k_i = |A| - i$, para $i \in \{0, 1, \cdots, h-1\}$. Então

$$\begin{aligned} t &= \left[\frac{\sum_{i=0}^{h-1} k_i - \frac{h(h+1)}{2}}{k}\right] \\ &= \left[\frac{\sum_{i=0}^{h-1}(|A|-i) - \frac{h(h+1)}{2}}{k}\right] \\ &= \left[\frac{h|A| - \frac{h(h-1)}{2} - \frac{h(h+1)}{2}}{k}\right] \\ &= \left[\frac{h(|A|-h)}{k}\right]. \end{aligned}$$

Agora, é fácil ver que $\overset{\wedge}{s_k}(A) \supseteq \overset{\wedge}{s_k}(A_0, A_1, \cdots, A_{h-1})$, o que dá, pelo Teorema 4.1,

$$|\overset{\wedge}{s_k}(A)| \geq min\left\{p, \left[\frac{h(|A|-h)}{k}\right] + 1\right\}. \tag{4.2}$$

□

A última "peça"que falta para podermos iniciar a demonstração do Teorema 4.1 é dada no lema abaixo.

Lema 4.4. *Sejam $1 \leq k_0 < k_1 < \cdots < k_{h-1}$ inteiros. Então existem inteiros positivos $k_0', k_1', \cdots, k_{h-1}'$ tais que $k_i' < k_j'$ para $i < j$, $k_i' \leq k_i$ para todo $i = 0, 1, \cdots, h-1$, e $\frac{\sum_{j=0}^{h-1}(k_j'-(j+1))}{k} = \left[\frac{\sum_{j=0}^{h-1}(k_j-(j+1))}{k}\right]$.*

Demonstração. Faremos a demonstração por indução sobre h. Para $h = 1$, como k é um número natural que não excede a h, temos que $k = 1$ e a afirmação do lema será válida com $k_0' = k_0$. Suponhamos então que a afirmação do lema seja válida para toda $(h-1)$-upla $(l_0, l_1, \cdots, l_{h-2})$ satisfazendo as hipóteses. Seja $(k_0, k_1, \cdots, k_{h-1})$ uma h-upla que satisfaz às hipóteses do lema e seja r o resto da divisão euclidiana de $\sum_{j=0}^{h-1}(k_j-(j+1))$ por k. Note que $0 \leq r \leq k-1 < h$. Se $r = 0$, podemos tomar $k_j' = k_j$ e a afirmação do lema é válida neste caso. Assim, podemos supor que $r > 0$. Se $k_0 \geq 2$, podemos tomar $k_j' = k_j - 1$ para $j = 0, 1, \cdots, r-1$ e $k_j' = k_j$ para $j = r, r+1, \cdots, h-1$, e também neste caso temos a validade da afirmação do lema. Vamos supor então que $k_0 = 1$. Aplicando a hipótese de indução à $(h-1)$-upla definida por $l_{j-1} = k_j - 1$, $j = 1, 2, \cdots, h-1$ (note que $l_0 \geq 1$, pois $k_1 \geq 2$), existem inteiros positivos $l_0', l_1', \cdots, l_{h-2}'$ tais que $l_i' < l_j'$ para $i < j$, $l_i' \leq l_i$ para todo $i = 0, 1, \cdots, h-2$, e $\frac{\sum_{j=0}^{h-2}(l_j'-(j+1))}{k} = \left[\frac{\sum_{j=0}^{h-2}(l_j-(j+1))}{k}\right]$. Fazendo $k_0' = k_0 = 1$ e $k_j' = l_{j-1}' + 1$ para $j = 1, \cdots, h-1$ temos

$$\begin{aligned}
\left[\frac{\sum_{j=0}^{h-1}(k_j-(j+1))}{k}\right] &= \left[\frac{\sum_{j=1}^{h-1}(k_j-(j+1))}{k}\right] = \left[\frac{\sum_{j=1}^{h-1}((k_j-1)-j)}{k}\right] \\
&= \left[\frac{\sum_{j=1}^{h-1}((l_{j-1})-j)}{k}\right] = \left[\frac{\sum_{j=0}^{h-2}(l_j-(j+1))}{k}\right] \\
&= \frac{\sum_{j=0}^{h-2}(l_j'-(j+1))}{k} = \frac{\sum_{j=1}^{h-1}(l_{j-1}'-j)}{k} \\
&= \frac{\sum_{j=1}^{h-1}((k_j'-1)-j)}{k} = \frac{\sum_{j=1}^{h-1}(k_j'-(j+1))}{k} \\
&= \frac{\sum_{j=0}^{h-1}(k_j'-(j+1))}{k},
\end{aligned}$$

o que finaliza a demonstração.

□

4.1 Demonstração do Teorema 4.1

Sem perda de generalidade, podemos supor que $k_0 < k_1 < \cdots < k_{h-1}$. Pelo Lema 4.4, existem inteiros positivos $k_0^{'}, k_1^{'}, \cdots, k_{h-1}^{'}$ que ainda satisfazem as hipóteses do teorema e tais que $t = \frac{\sum_{j=0}^{h-1} k_j^{'} - \frac{h(h+1)}{2}}{k}$. Tomemos subconjuntos $A_i^{'} \subset A_i$, com $|A_i| = k_i^{'}$, $i = 0, 1, \cdots, h-1$. Aplicando o Teorema 2.4 com

$$F = s_k(x_0, x_1, \cdots, x_{h-1}) = \sum_{0 \leq i_0 < i_1 < \cdots < i_{k-1} \leq h-1} x_{i_0} x_{i_1} \cdots x_{i_{k-1}},$$

o polinômio simétrico elementar de grau k em h variáveis e

$$G = \Delta_h(x_0, x_1, \cdots, x_{h-1}) = \prod_{0 \leq i < j \leq h-1} (x_j - x_i),$$

temos que o conjunto Ω_{FG} coincide com

$$\{s_k(a_0, a_1, \cdots, a_{h-1}) : a_i \in A_i^{'},\ i = 0, 1, \cdots h-1, \text{ com } a_i \neq a_j \text{ se } i \neq j\},$$

ou seja $\Omega_{s_k \Delta_h} = \hat{s_k}\ (A_0^{'}, A_1^{'}, \cdots, A_{h-1}^{'})$. Como $deg(s_k) = k$ e $deg(\Delta_h) = \frac{h(h-1)}{2}$ a equação (2.1) se torna

$$t = \left[\frac{\sum_{i=0}^{h-1} k_i^{'} - h - \frac{h(h-1)}{2}}{k} \right] = \frac{\sum_{i=0}^{h-1} k_i^{'} - \frac{h(h+1)}{2}}{k}. \tag{4.3}$$

Assim, o Teorema 2.4 nos dá a estimativa

$$|\ \hat{s_k}\ (A_0^{'}, A_1^{'}, \cdots, A_{h-1}^{'})| \geq min\{p, t+1\}, \tag{4.4}$$

desde que o coeficiente de $x_0^{k_0^{'}-1} x_1^{k_1^{'}-1} \cdots x_{h-1}^{k_{h-1}^{'}-1}$ na expansão do produto $(s_k)^t \Delta_h$ seja não nulo. Como $k_0^{'} < k_1^{'} < \cdots < k_{h-1}^{'}$, pelo Teorema 3.6 o coeficiente de $x_0^{k_0^{'}-1} x_1^{k_1^{'}-1} \cdots x_{h-1}^{k_{h-1}^{'}-1}$ é, a menos de um sinal, o número $\hat{B}_k\ (k_0^{'} - 1, k_1^{'} - 1, \cdots, k_{h-1}^{'} - 1)$ que, quando K tem característica zero e pela Proposição 1.18, é não nulo pois $\mathbf{c} = (k_0^{'} - 1, k_1^{'} - 1, \cdots, k_{h-1}^{'} - 1)$ é um vetor estritamente crescente e o número $t \in \mathbb{N}$ é tal que $\sum_{j=0}^{h-1}(k_j^{'} - 1) = kt + \binom{h}{2}$ e $j \leq k_j^{'} - 1 \leq t + j$, para todo $j = 0, 1, \cdots, h-1$.

Quando a característica de K é um número primo, o fato de que o número de k-caminhos estritamente crescentes é menor do que o número total de k-caminhos de

$\mathbf{a}^* = (0, 1, \cdots, h-1)$ até $\mathbf{b} = (k_0' - 1, k_1' - 1, \cdots, k_{h-1}' - 1)$, combinado com as equações (1.10) e (1.11), com $\mathbf{c} = (k_0' - 1, \cdots, (k_j' - 1) - j, \cdots, (k_{h-1}' - 1) - (h-1))$, e com a desigualdade (1.9) nos dá

$$\begin{aligned} 0 < \hat{B}_k\,(k_0 - 1, k_1 - 1, \cdots, k_{h-1} - 1) &\leq P_k(\mathbf{a}^*, \mathbf{b}) \\ &= P_k(\mathbf{0}, \mathbf{b} - \mathbf{a}^*) \\ &= |\Omega(\mathbf{b} - \mathbf{a}^*)| \\ &= |\Omega(\mathbf{c})| \\ &\leq \frac{(t+n-1)!}{\left(\left[\frac{t}{n}\right]!\right)^n (n-1)!} \\ &< p, \end{aligned}$$

e portanto, também neste caso o coeficiente é não nulo. Isto finaliza a demonstração.

□

4.2 Demonstração do Teorema 4.2

Tomemos subconjuntos $A_i' \subset A_i$, com $|A_i| = k_i', i = 0, 1, \cdots, h-1$, de modo que as hipóteses do teorema ainda sejam satisfeitas e que se tenha $l = \frac{\sum_{j=0}^{h-1} k_j' - h}{k}$. Aplicando o Teorema 2.4 com $F = s_k(x_0, x_1, \cdots, x_{h-1})$ e G um polinômio constante não nulo, temos que o conjunto Ω_{FG} coincide com $\{s_k(a_0, a_1, \cdots, a_{h-1}) : a_i \in A_i, i = 0, 1, \cdots h-1\}$. Como $deg(s_k) = k$ e $deg(G) = 0$ a equação (2.1) se torna

$$\frac{1}{k}\left(\sum_{i=0}^{h-1} k_i' - h\right) = l. \tag{4.5}$$

Assim, o Teorema 2.4 nos dá a estimativa

$$|s_k(A_0, A_1, \cdots, A_{h-1})| \geq min\{p, l+1\}, \tag{4.6}$$

desde que o coeficiente de $x_0^{k_0'-1} x_1^{k_1'-1} \cdots x_{h-1}^{k_{h-1}'-1}$ na expansão do produto $(s_k)^l$ seja não nulo. Pelo Teorema 3.1 tal coeficiente é o número $P_k(\mathbf{0}, \mathbf{c})$, onde

$\mathbf{c} = (k_0' - 1, k_1' - 1, \cdots, k_{h-1}' - 1)$, que, quando K tem característica zero e pela Proposição 1.14, é não nulo pois o número l é tal que $\sum_{j=0}^{h-1}(k_j' - 1) = kl$ e $0 \leq k_j' - 1 \leq l$ para todo $j = 0, 1, \cdots h-1$.

Quando a característica de K é um número primo a equação (1.11), com $\mathbf{c} = (k_0' - 1, k_1' - 1, \cdots, k_{h-1}' - 1)$, e a desigualdade (1.9) nos dá $0 < P_k(\mathbf{0}, \mathbf{c}) < p$ e portanto, também neste caso o coeficiente é não nulo.

□

4.3 Alguns Exemplos

Apresentamos agora alguns exemplos para ilustrar os teoremas acima. É interessante notar que as cotas dadas nos teoremas são atingidas em alguns casos.

Exemplo 4.5. *Se* $A_0 = \{a_0\}$, $A_1 = \{a_0, a_1\}$, $A_2 = \{a_0, a_1, a_2\}$, $A_2 = \{a_0, a_1, a_2\} \cdots$, $A_{h-1} = \{a_0, a_1, a_2, \cdots, a_{h-1}\}$, *então o limite inferior no Teorema 4.1 é atingido:*

$$|\overset{\wedge}{s_k}(A_0, A_1, \cdots, A_{h-1})| = 1 = \left[\frac{\sum_{i=0}^{h-1}(i+1) - \frac{h(h+1)}{2}}{k}\right] + 1.$$

Exemplo 4.6. *Suponha que* $h = 3$, $k = 2$, $A_0 = \{0, a_0, a_1\}$, $A_1 = \{0, a_0, a_1, a_2\}$ *e* $A_2 = \{0, a_0, a_1, a_2, a_3\}$, *onde* $a_1 = -a_0$, $a_3 = -a_2$. *Então*

$$s_2(x_0, x_1, x_2) = x_0x_1 + x_0x_2 + x_1x_2$$

e os elementos de $\overset{\wedge}{s_2}(A_0, A_1, A_2)$ *são*

$$s_2(0, a_0, a_1) = -a_0^2,$$

$$s_2(0, a_0, a_2) = -a_1a_2,$$

$$s_2(0, a_0, a_3) = a_1a_2,$$

$$s_2(0, a_1, a_2) = a_1a_2,$$

$$s_2(0, a_1, a_3) = -a_1a_2,$$

$$s_2(0, a_2, a_3) = -a_2^2,$$

$$s_2(a_0, a_1, a_2) = -a_0^2,$$
$$s_2(a_0, a_1, a_3) = -a_0^2,$$
$$s_2(a_0, a_2, a_3) = -a_2^2,$$

e

$$s_2(a_1, a_2, a_3) = -a_2^2.$$

Assim, $|\overset{\wedge}{s_2}(A_0, A_1, A_2)| = 4 = \left[\frac{1}{2}\left(3 + 4 + 5 - \frac{3\times 4}{2}\right)\right] + 1$ *e novamente o limite inferior no Teorema 4.1 é atingido.*

Exemplo 4.7. *Sejam* $A_0, A_1, \cdots, A_{h-1}, h \geq 2$, *subconjuntos finitos não vazios de* K *com* $A_{k-1} = A_k = \cdots = A_{h-1} = \{0\}$. *Neste caso,* $s_k(A_0, A_1, \cdots, A_{h-1}) = \{0\}$ *de modo que* $|s_k(A_0, A_1, \cdots, A_{h-1})| = 1$. *Vamos estudar que restrições as hipóteses do Teorema 4.2 impõem sobre os números de elementos dos outros conjuntos. Como* $|A_{k-1}| = |A_k| = \cdots = |A_{h-1}| = 1$, *uma das condições sobre os números* $k_j = |A_j|, j = 0, 1, \cdots, h-1$ *dá, para todo* $j_0 = 0, 1, \cdots, k-2$,

$$\begin{aligned} k_{j_0} &\leq 1 + \frac{1}{k}\left(\sum_{j=0}^{h-1} k_j - h\right) \\ &\leq \frac{1}{k}\left(k + \sum_{j=0}^{k-2} k_j + ((h-1) - (k-2)) - h\right) \\ &\leq \frac{1}{k}\left(\sum_{j=0}^{k-2} k_j + 1\right). \end{aligned} \tag{4.7}$$

Por outro lado, como cada um dos conjuntos $A_j, j = 0, 1, \cdots, k-2$, *é não vazio, temos* $k - 1 \leq \sum_{j=0}^{k-2} k_j$, *com igualdade se, e somente se,* $k_0 = k_1 = \cdots = k_{k-2} = 1$. *Se esta igualdade não ocorresse, teríamos* $k - 1 < \sum_{j=0}^{k-2} k_j$ *que é, como mostram alguns cálculos simples, equivalente a*

$$\frac{1}{k}\left(\sum_{j=0}^{k-2} k_i + 1\right) < \frac{1}{k-1}\sum_{j=0}^{k-2} k_i$$

e então a condição (4.7) nos dá, para todo $j_0 = 0, 1, \cdots, k-2$,

$$k_{j_0} < \frac{1}{k-1}\sum_{j=0}^{k-2} k_i,$$

o que é impossível, pois teríamos que todos os $k-1$ *números* $k_0, k_1, \cdots, k_{k-2}$ *seriam menores que sua média aritmética. Assim,* $k_0 = k_1 = \cdots = k_{h-2} = 1$ *e a estimativa dada pelo Teorema 4.2 é*

$$|s_k(A_0, A_1, \cdots, A_{h-1})| \geq \frac{\sum_{i=0}^{h-1} k_i - h}{k} + 1 = 1.$$

Mas também há situações em que a cota inferior dada pelo Teorema 4.1 não é atingida:

Exemplo 4.8. *Suponha que* $h = 3$, $k = 2$, $A_0 = \{a_0, a_1\}$, $A_1 = \{a_0, a_1, a_2\}$ *e* $A_2 = \{0, a_0, a_1, a_2, a_3\}$, *onde* $a_1 = -a_0$, $a_3 = -a_2$. *Então*

$$s_2(x_0, x_1, x_2) = x_0x_1 + x_0x_2 + x_1x_2$$

e os elementos de $\overset{\wedge}{s_2}(A_0, A_1, A_2)$ *são*

$$s_2(a_0, a_1, 0) = a_0a_1 + a_00 + a_10 = -a_0^2,$$
$$s_2(a_0, a_1, a_2) = a_0a_1 + a_0a_2 + a_1a_2 = -a_0^2,$$
$$s_2(a_0, a_1, a_3) = a_0a_1 + a_0a_3 + a_1a_3 = -a_0^2,$$
$$s_2(a_0, a_2, 0) = a_0a_2 + a_00 + a_20 = -a_1a_2$$
$$s_2(a_0, a_2, a_3) = a_0a_2 + a_0a_3 + a_2a_3 = -a_2^2,$$
$$s_2(a_1, a_2, 0) = a_1a_2 + a_10 + a_20 = a_1a_2$$

e

$$s_2(a_1, a_2, a_3) = a_1a_2 + a_1a_3 + a_2a_3 = -a_2^2.$$

Assim, $|\overset{\wedge}{s_2}(A_0, A_1, A_2)| = 4 > 3 = \left[\frac{1}{2}\left(2 + 3 + 5 - \frac{3\times 4}{2}\right)\right] + 1$ *e o limite inferior no Teorema 4.1 não é atingido.*

Exemplo 4.9. *Quando os conjuntos* $A_0, A_1, \cdots, A_{h-1}, h \geq 2$, *são disjuntos dois a dois, temos* $\overset{\wedge}{s_k}(A_0, A_1, \cdots, A_{h-1}) = s_k(A_0, A_1, \cdots, A_{h-1})$ *e então, para* p *suficientemente grande,*

$$\begin{aligned} |\overset{\wedge}{s_k}(A_0, \cdots, A_{h-1})| &= |s_k(A_0, \cdots, A_{h-1})| \\ &\geq \left[\frac{\sum_{j=0}^{h-1} k_j - h}{k}\right] + 1 \\ &> \left[\frac{\sum_{j=0}^{h-1} k_j - \frac{h(h+1)}{2}}{k}\right] + 1. \end{aligned}$$

Assim, a cota do Teorema 4.1 não é atingida neste caso.

O limite inferior dado pelo corolário do Teorema 4.1 é atingido, pelo menos, nos casos especiais dos próximos três exemplos:

Exemplo 4.10. *Se $|A| = h$, então, para todo $k \in \{1, 2, \cdots, h\}$,*

$$|\overset{\wedge}{s_k}(A)| = 1 = \frac{h(|A| - h)}{k} + 1.$$

Exemplo 4.11. *Suponha que $h = 3$, $k = 2$ e $A = \{a_0, a_1, a_2, a_3\}$, onde $a_1 = -a_0$, $a_3 = -a_2$ e $|A| = 4$. Então $s_2(x_0, x_1, x_2) = x_0x_1 + x_0x_2 + x_1x_2$ e os elementos de $\overset{\wedge}{s_2}(A)$ são*

$$s_2(a_0, a_1, a_2) = a_0a_1 + a_0a_2 + a_1a_2 = -a_0^2,$$

$$s_2(a_0, a_1, a_3) = a_0a_1 + a_0a_3 + a_1a_3 = -a_0^2,$$

$$s_2(a_0, a_2, a_3) = a_0a_2 + a_0a_3 + a_2a_3 = -a_2^2$$

e

$$s_2(a_1, a_2, a_3) = a_1a_2 + a_1a_3 + a_2a_3 = -a_2^2.$$

Assim, $|\overset{\wedge}{s_2}(A)| = 2 = \left[\frac{3(4-3)}{2}\right] + 1$.

Exemplo 4.12. *Se $k = h$, $|A| = h + 1$ e $0 \in A$, então o limite inferior é atingido.*

Mas há também situações simples onde o limite inferior não é atingido:

Exemplo 4.13. *Se $h = k = 2$, $|A| = 4$ e p é suficientemente grande, então*

$$|\overset{\wedge}{s_2}(A)| > 3 = \frac{2(4-2)}{2} + 1.$$

Capítulo 5

Outros Polinômios

Neste capítulo discutimos a aplicação do Método Polinomial a outros tipos de polinômios. O caso mais simples é, certamente, aquele em que se estudam combinações lineares de $s_k(\mathbf{x})$ para diferentes valores de k. Combinações lineares de outro tipo de polinômio também são consideradas.

5.1 Combinações Lineares de $s_k(\mathbf{x})$

Como antes, sejam $1 \leq k \leq h$ inteiros, $n = \frac{h!}{k!(h-k)!}$ e $s_k(x_0, \cdots, x_{h-1})$ o polinômio simétrico elementar de grau k em h variáveis. Seja $\mathbf{w}_k = (w_{k,0}, \cdots, w_{k,h-1}) \in \mathbb{Z}^h$ um vetor com $w_{k,0} \geq w_{k,1} \geq \cdots \geq w_{k,h-1} \geq 1$ e considere o polinômio

$$g_{\mathbf{w}_k}(x_0, x_1, \cdots, x_{h-1}) = s_k(x_0^{w_{k,0}}, x_1^{w_{k,1}}, \cdots, x_{h-1}^{w_{k,h-1}}).$$

Note que $deg(g_{\mathbf{w}_k}) = w_{k,0} + w_{k,1} + \cdots + w_{k,k-1} = \sum_{i=0}^{k-1} w_{k,i}$.

Proposição 5.1. *Se $t \geq 0$, o coeficiente de $x_0^{b_0}, x_1^{b_1}, \cdots, x_{h-1}^{b_{h-1}}$ em $(g_{\mathbf{w}_k}(\mathbf{x}))^t$ é diferente de zero se, e somente se, $w_{k,i}$ divide b_i e $0 \leq b_i \leq w_{k,i} \cdot t$, para todo $i = 0, 1, \cdots, h-1$, e $\sum_{i=0}^{h-1} \frac{b_i}{w_{k,i}} = k \cdot t$; nesse caso, tal coeficiente é igual a $P_k(\mathbf{0}, \mathbf{c})$ onde $\mathbf{c} = \left(\frac{b_0}{w_{k,0}}, \cdots, \frac{b_{h-1}}{w_{k,h-1}}\right)$*

Demonstração. Aplicando o Teorema 3.1, temos

$$g_{\mathbf{w}_k}(x_0, \cdots, x_{h-1})^t = (s_k(x_0^{w_{k,0}}, \cdots, x_{h-1}^{w_{k,h-1}}))^t = \sum_{\mathbf{c} \in \mathcal{C}(t)} P_k(\mathbf{0}, \mathbf{c}) x_0^{w_{k,0}c_0} x_1^{w_{k,1}c_1} \cdots x_{h-1}^{w_{k,h-1}c_{h-1}},$$

onde $\mathcal{C}(t) = \{\mathbf{c} = (c_0, \cdots, c_{h-1}) \in \mathbb{Z}^h : 0 \leq c_j \leq t \text{ e } c_0 + \cdots + c_{h-1} = kt\}$. Fazendo $b_0 = w_{k,0}c_0, \cdots, b_{h-1} = w_{k,h-1}c_{h-1}$ e aplicando a equação (1.11) e a Proposição 1.3, o resultado segue.

□

Sejam $A_0, A_1, \cdots, A_{h-1}$ subconjuntos finitos não vazios de um corpo K de característica p se ela é positiva e $p = \infty$ se ela é zero. Considere ainda o conjunto

$$g_{\mathbf{w}_k}(A_0, A_1, \cdots, A_{h-1}) = \{g_{\mathbf{w}_k}(a_0, a_1, \cdots, a_{h-1}) : a_i \in A_i\}$$

e o número

$$t_k = \left[\frac{1}{\sum_{i=0}^{k-1} w_{k,i}}\left(\sum_{j=0}^{h-1}(|A_j| - h)\right)\right].$$

Proposição 5.2. *Suponha que* $p > \frac{(t_k+n-1)!}{\left(\left[\frac{t_k}{n}\right]!\right)^n (n-1)!}$ *quando a característica de* K *for positiva. Se* $w_{k,i}$ *divide* $|A_i|-1$, $|A_i|-1 \leq w_{k,i} \cdot t_k$ *para todo* $i = 0, 1, \cdots, h-1$ *e* $\sum_{i=0}^{h-1} \frac{|A_i|-1}{w_{k,i}} = k \cdot t_k$ *então*

$$|g_{\mathbf{w}_k}(A_0, A_1, \cdots, A_{h-1})| \geq min\{p, t_k + 1\}.$$

Demonstração. Pelas hipóteses, podemos aplicar a Proposição 5.1 para concluir que o coeficiente de $x_0^{|A_0|-1} \cdots x_0^{|A_0|-1}$ em $(g_{\mathbf{w}_k}(\mathbf{x}))^{t_k}$ é diferente de zero. Aplicando o Método Polinomial (Teorema 2.4) com $F = g_{\mathbf{w}_k}(\mathbf{x})$ e $G(\mathbf{x})$ um polinômio constante não nulo, temos o resultado desejado.

□

Para $a \in K$, definamos

$$\epsilon(a) = \begin{cases} 0 & \text{se} \quad a = 0 \\ 1 & \text{se} \quad a \neq 0. \end{cases}$$

Sejam $a_0, a_1, \cdots, a_h \in K$ e definamos o polinômio

$$f(x_0, x_1, \cdots, x_{h-1}) = \sum_{k=0}^{h} a_k g_{\mathbf{w}_k}(x_0, x_1, \cdots, x_{h-1}).$$

Teorema 5.3. *Com as mesmas hipóteses da Proposição 5.2, temos*

$$|f(A_0, A_1, \cdots, A_{h-1})| \geq min\left\{p, \sum_{k=1}^{h}(t_k + 1)^{\epsilon(a_k)} - h\right\}.$$

Demonstração. Como, para todos $a \in K$ e $A \subset K$ vale $|a + A| = |A|$, temos

$$\begin{aligned} |f(A_0, A_1, \cdots, A_{h-1})| &= |\sum_{k=0}^{h} a_k g_{\mathbf{w}_k}(A_0, A_1, \cdots, A_{h-1})| \\ &= |\sum_{k=1}^{h} a_k g_{\mathbf{w}_k}(A_0, A_1, \cdots, A_{h-1})|. \end{aligned}$$

Pelo Teorema de Cauchy-Davenport (estimativa (1)), temos

$$|f(A_0, A_1, \cdots, A_{h-1})| \geq min\left\{p, \sum_{k=1}^{h} |a_k g_{\mathbf{w}_k}(A_0, A_1, \cdots, A_{h-1})| - h\right\}.$$

Usando o fato de que $|a \cdot A| = |A|^{\epsilon(a)}$, fica

$$|f(A_0, A_1, \cdots, A_{h-1})| \geq min\left\{p, \sum_{k=1}^{h} |g_{\mathbf{w}_k}(A_0, A_1, \cdots, A_{h-1})|^{\epsilon(a_k)} - h\right\},$$

e, finalmente, usando a Proposição 5.2 chegamos ao resultado desejado.

□

Vale observar que, quando $a_k \neq 0$ e $a_0 = \cdots = a_{k-1} = a_{k+1} = \cdots = a_{h-1} = 0$, reobtemos a Proposição 5.2. Se, além disso, $w_{k,0} = \cdots = w_{k,h-1} = 1$, então temos o Teorema 4.2.

5.2 Um Polinômio Semelhante a $s_k(\mathbf{x})$

Por simplicidade de notação, se $\mathbf{v} = (v_0, v_1, \cdots, v_{h-1})$ tem coordenadas inteiras não negativas, continuamos indicando o monômio $x_0^{v_0} x_1^{v_1} \cdots x_{h-1}^{v_{h-1}}$ por $\mathbf{x}^{\mathbf{v}}$. Lembremos que $\Gamma = \{\beta_1, \cdots, \beta_n\}$ é o conjunto de todos os vetores $\beta_j = (\beta_{j,0}, \beta_{j,1}, \cdots, \beta_{j,h-1})$ com exatamente k coordenadas iguais a 1 e $h - k$ coordenadas nulas. Dados $a_1, \cdots, a_n \in K$, seja

$$r_k(\mathbf{x}) = \sum_{j=1}^{n} a_j \mathbf{x}^{\beta_j}. \tag{5.1}$$

A diferença entre este polinômio e s_k é apenas a presença dos coeficientes $a_1, \cdots, a_n$. Nosso interesse é estudar o coeficiente de $x_0^{c_0} x_1^{c_1} \cdots x_{h-1}^{c_{h-1}}$ em $r_k(\mathbf{x})^t$, onde $t \geq 1$.

Seja $\Gamma_{t,n}$ o conjunto de todas as funções $\alpha : \{1, 2, \cdots, t\} \to \mathbb{N}$ tais que $\alpha(i) \leq n$ para todo $i = 1, 2, \cdots, t$.

Proposição 5.4. *Se $x_0^{c_0}x_1^{c_1}\cdots x_{h-1}^{c_{h-1}}$ aparece na expansão de $r_k(\mathbf{x})^t$ com coeficiente não nulo, então $\sum_{j=0}^{h-1} c_j = kt$ e $0 \leq c_j \leq t$ para todo $j \in \{0,1,\cdots,h-1\}$.*

Demonstração. É fácil ver que

$$r_k(\mathbf{x})^t = \sum_{\alpha\in\Gamma_{t,n}} a_{\alpha(1)}\mathbf{x}^{\beta_{\alpha(1)}}\cdots a_{\alpha(t)}\mathbf{x}^{\beta_{\alpha(t)}}. \tag{5.2}$$

Em virtude de (5.2), os monômios que aparecem em $r_k(\mathbf{x})^t$ provém de um produto de exatamente t monômios cujos expoentes são vetores com exatamente k coordenadas iguais a um e exatamente $h-k$ coordenadas nulas. Assim, se $x_0^{c_0}x_1^{c_1}\cdots x_{h-1}^{c_{h-1}}$ aparece na expansão de $r_k(\mathbf{x})^t$, então, para algum $\alpha \in \Gamma_{t,n}$, tem-se $c_j = \sum_{i=1}^{t}\beta_{\alpha(i),j}$ de onde a condição $0 \leq c_j \leq t, \forall j \in \{0,1,\cdots,h-1\}$ é facilmente percebida. Além disso,

$$\sum_{j=0}^{h-1} c_j = \sum_{j=0}^{h-1}\sum_{i=1}^{t}\beta_{\alpha(i),j} = \sum_{i=1}^{t}\sum_{j=0}^{h-1}\beta_{\alpha(i),j} = \sum_{i=1}^{t} k = kt.$$

□

Dado um vetor $\mathbf{c} = (c_0,\cdots,c_{h-1}) \in \mathbb{Z}^h$ satisfazendo as condições da Proposição 5.4, não podemos garantir necessariamente que o monômio $\mathbf{x}^{\mathbf{c}}$ apareça com coeficiente não nulo na expansão de $r_k(\mathbf{x})^t$ porque, não conhecendo os "números" $a_1,\cdots,a_n \in K$, não podemos assegurar que não hajam cancelamentos para diferentes funções $\alpha \in \Gamma_{t,n}$ (veja (5.2)). Mas podemos estar certos de que, antes de proceder tais possíveis cancelamentos, o monômio $\mathbf{x}^{\mathbf{c}}$ estará presente na expansão de $r_k(\mathbf{x})^t$. De fato, pela Proposição 1.14, existe um k-caminho $\mathbf{v}_0, \mathbf{v}_0+\beta_{i_1} = \mathbf{v}_1, \cdots, \mathbf{v}_{t-1}+\beta_{i_t} = \mathbf{v}_t$ da origem até $\mathbf{c}$. De posse deste caminho, é fácil escolher uma função $\alpha \in \Gamma_{t,n}$ que forneça $\mathbf{x}^{\mathbf{c}}$ em (5.2).

Sejam $\alpha \in \Gamma_{t,n}$ e $\mathbf{c} = (c_0,\cdots,c_{h-1}) \in \mathbb{Z}^h$. Definamos os conjuntos

$$\Delta_{\alpha,i} = \{j \in \{1,2,\cdots,t\} : \beta_{\alpha(j),i} = 1\},\ i = 0,1,\cdots,h-1,$$

e

$$\mathcal{G}(\mathbf{c}) = \{\alpha \in \Gamma_{t,n} : c_i = |\Delta_{\alpha,i}|, i = 0,1,\cdots,h-1\}.$$

Como $\mathbf{x}^{\beta_{\alpha(1)}}\cdot\mathbf{x}^{\beta_{\alpha(2)}}\cdots\mathbf{x}^{\beta_{\alpha(t)}} = x_0^{|\Delta_{\alpha,0}|}\cdot x_1^{|\Delta_{\alpha,1}|}\cdots x_{h-1}^{|\Delta_{\alpha,h-1}|}$, por (5.2), o coeficiente de $x_0^{c_0}\cdots x_{h-1}^{c_{h-1}}$ na expansão de $r_k(\mathbf{x})^t$ é igual a

$$\sum_{\alpha\in\mathcal{G}(\mathbf{c})} a_{\alpha(1)}\cdot a_{\alpha(2)}\cdots a_{\alpha(t)}. \tag{5.3}$$

Em função da Proposição 5.4 e dos comentários que a seguem, temos que $\mathcal{G}(\mathbf{c}) \neq \emptyset$ se, e somente se, o vetor $\mathbf{c}$ satisfaz $\sum_{j=0}^{h-1} c_j = kt$ e $0 \leq c_j \leq t$ para todo $j \in \{0, 1, \cdots, h-1\}$. Mas podemos concluir mais:

Proposição 5.5. *Seja $\mathbf{c} = (c_0, \cdots, c_{h-1}) \in \mathbb{Z}^h$ satisfazendo as condições da Proposição 5.4. Então existe uma correspondência biunívoca entre o conjunto $\mathcal{G}(\mathbf{c})$ definido acima e o conjunto $\Omega(\mathbf{c})$ das $k\mathbf{c}$-matrizes.*

Demonstração. Seja $\lambda : \mathcal{G}(\mathbf{c}) \to \Omega(\mathbf{c})$ dada por

$$\lambda(\alpha) = \begin{bmatrix} \beta_{\alpha(1)} \\ \beta_{\alpha(2)} \\ \vdots \\ \beta_{\alpha(t)} \end{bmatrix}.$$

Esta aplicação está bem definida, pois $\alpha \in \Gamma_{t,n}$ implica que $\sum_{j=1}^{t} \beta_{\alpha(i),j} = |\Delta_{\alpha,i}| = c_i$. Para ver que λ é injetora, se $\alpha, \gamma \in \mathcal{G}(\mathbf{c})$ e, para algum $j \in \{1, 2, \cdots, t\}$, $\alpha(j) \neq \gamma(j)$, então $\beta_{\alpha(j)} \neq \beta_{\gamma(j)}$. Para ver que é sobrejetora, dado $A = \begin{bmatrix} \beta_{i_1} \\ \vdots \\ \beta_{i_t} \end{bmatrix} \in \Omega(\mathbf{c})$, basta definir $\alpha \in \Gamma_{t,n}$ por $\alpha(1) = i_1, \cdots, \alpha(t) = i_t$ e teremos $\lambda(\alpha) = A$.

□

Por causa da bijeção acima, quando $a_1 = \cdots = a_n = 1$, (5.3) se torna

$$\sum_{\alpha \in \mathcal{G}(\mathbf{c})} 1 = |\mathcal{G}(\mathbf{c})| = |\Omega(\mathbf{c})| = P_k(\mathbf{0}, \mathbf{c}). \tag{5.4}$$

Assim, o Teorema 3.1 pode ser obtido como uma espécie de corolário da argumentação desta seção. Na verdade, foi seguindo estas idéias que Dias da Silva & Godinho provaram este teorema em [8].

Como na seção anterior, seja $\mathbf{w}_k = (w_{k,0}, \cdots, w_{k,h-1}) \in \mathbb{Z}^h$ com $w_{k,0} \geq w_{k,1} \geq \cdots \geq w_{k,h-1} \geq 1$ e considere o polinômio

$$h_{\mathbf{w}_k}(x_0, x_1, \cdots, x_{h-1}) = r_k(x_0^{w_{k,0}}, x_1^{w_{k,1}}, \cdots, x_{h-1}^{w_{k,h-1}}).$$

Note que $deg(h_{\mathbf{w}_k}) = w_{k,0} + w_{k,1} + \cdots + w_{k,k-1} = \sum_{i=0}^{k-1} w_{k,i}$.

Proposição 5.6. *Se $t \geq 0$ e o coeficiente de $x_0^{b_0}, x_1^{b_1}, \cdots, x_{h-1}^{b_{h-1}}$ em $(h_{\mathbf{w}_k}(\mathbf{x}))^t$ é diferente de zero, então $w_{k,i}$ divide b_i e $0 \leq b_i \leq w_{k,i} \cdot t$, para todo $i = 0, 1, \cdots, h-1$, e $\sum_{i=0}^{h-1} \frac{b_i}{w_{k,i}} = k \cdot t$.*

Demonstração. A exemplo da demonstração da Proposição 5.1, basta aplicar a Proposição 5.4 fazendo a mudança de variáveis $\mathbf{x} \to \mathbf{x}^{\mathbf{w}_k}$ e o resultado segue.

□

O principal interesse em estudar os polinômios $h_{\mathbf{w}_k}(\mathbf{x})$ se dá porque um número considerável de polinômios $F(x_0, \cdots, x_{h-1}) \in K[x_0, \cdots, x_{h-1}]$ pode ser escrito como uma soma

$$F(\mathbf{x}) = \sum_{k=0}^{h} h_{\mathbf{w}_k}(\mathbf{x}).$$

Apesar disto, ainda não nos foi possível obter um teorema geral para todos esses polinômios, pois ainda não fomos capazes de aplicar nossos métodos para encontrar condições suficientes para garantir que os coeficientes em $h_{\mathbf{w}_k}(\mathbf{x})^t$ são não nulos, o que é um requisito para se aplicar o Método Polinomial. Entretanto, em alguns casos particulares isso já é possível. Por exemplo, se K é um subcorpo dos números reais e os números $a_1, \cdots, a_n \in K$ (coeficientes de $r_k(\mathbf{x})$) são todos positivos, então, pelos comentários que seguem a Proposição 5.4, o coeficiente de $x_0^{b_0}, x_1^{b_1}, \cdots, x_{h-1}^{b_{h-1}}$ em $(h_{\mathbf{w}_k}(\mathbf{x}))^t$ é diferente de zero se, e somente se, $w_{k,i}$ divide b_i e $0 \leq b_i \leq w_{k,i} \cdot t$, para todo $i = 0, 1, \cdots, h-1$, e $\sum_{i=0}^{h-1} \frac{b_i}{w_{k,i}} = k \cdot t$. Neste caso, denotando como antes

$$t_k = \left\lfloor \frac{1}{\sum_{i=0}^{k-1} w_{k,i}} \left(\sum_{j=0}^{h-1} (|A_j| - h) \right) \right\rfloor.$$

temos:

Proposição 5.7. *Se $w_{k,i}$ divide $|A_i| - 1$ e $|A_i| - 1 \leq w_{k,i} \cdot t_k$ para todo $i = 0, 1, \cdots, h-1$ e $\sum_{i=0}^{h-1} \frac{|A_i|-1}{w_{k,i}} = k \cdot t_k$ então*

$$|h_{\mathbf{w}_k}(A_0, A_1, \cdots, A_{h-1})| \geq t_k + 1.$$

Demonstração. Como o coeficiente de $x_0^{|A_0|-1} \cdots x_0^{|A_0|-1}$ em $(h_{\mathbf{w}_k}(\mathbf{x}))^{t_k}$ é diferente de zero podemos aplicar o Método Polinomial (Teorema 2.4) com $F = h_{\mathbf{w}_k}(\mathbf{x})$ e $G(\mathbf{x})$ um polinômio constante não nulo, para obter o resultado desejado.

□

Como conseqüência da proposição acima temos uma estimativa semelhante àquela dada pelo Teorema 5.3:

Teorema 5.8.

$$|F(A_0, A_1, \cdots, A_{h-1})| \geq \sum_{k=1}^{h} t_k + 1.$$

Demonstração. Como, para todos $a \in K$ e $A \subset K$ vale $|a + A| = |A|$, temos

$$\begin{aligned} |F(A_0, A_1, \cdots, A_{h-1})| &= |\sum_{k=0}^{h} h_{\mathbf{w}_k}(A_0, A_1, \cdots, A_{h-1})| \\ &= |\sum_{k=1}^{h} h_{\mathbf{w}_k}(A_0, A_1, \cdots, A_{h-1})|. \end{aligned}$$

Pelo Teorema de Cauchy-Davenport (estimativa (1)), temos

$$|F(A_0, A_1, \cdots, A_{h-1})| \geq \sum_{k=1}^{h} |h_{\mathbf{w}_k}(A_0, A_1, \cdots, A_{h-1})| - h + 1.$$

Finalmente, usando a Proposição 5.7 chegamos ao resultado desejado.

□

Considerações Finais

Nesta tese estudamos os problemas diretos em Teoria Aditiva dos Números de determinar cotas inferiores para o número de elementos de certos tipos de conjuntos. Apresentamos uma demonstração polinomial para um teorema devido a Dias da Silva e Godinho ([8]) que generaliza o famoso Teorema de Cauchy-Davenport e uma generalização para a conhecida Conjectura de Erdös-Heilbronn (Teoremas 4.2 e 4.1).

Na demonstração dos Teoremas 4.1 e 4.2 usamos o fato de que todos os números inteiros positivos menores do que um dado número primo p podem ser vistos como elementos não nulos no corpo finito dos inteiros módulo p. Isso foi importante para garantir que certos coeficientes em $(s_k)^t$ e $(s_k)^t \cdot \Delta$ fossem não nulos, o que é um requisito essencial para se aplicar o Método Polinomial (Teorema 2.4). A estratégia, então, foi tomar o número p, característica do corpo K no qual se tomam os coeficientes polinomiais, "suficientemente grande"a fim de que os coeficientes fossem elementos não nulos neste corpo. Para dar uma idéia de quão grande esse número p deveria ser, e sabendo que os referidos coeficientes não excedem ao número de (0,1)-matrizes com soma de linhas e colunas prescritas, usamos a Proposição 1.11. Entretanto, a estimativa dada por esta proposição nos parece demasiado grande e afirmamos que certamente há espaço para melhora neste resultado. Só para citar um exemplo, quando $h = 8$, $k = 2$ e $\mathbf{c} = (1, 1, 1, 1, 1, 2, 2, 3)$ o número de $k\mathbf{c}$-matrizes, dado pelo Teorema 1.8, é 190 800 enquanto que a estimativa da Proposição 1.11 é 797 448 960. Em diversos outros casos particulares que fizemos os cálculos, também a diferença entre o número exato de $k\mathbf{c}$-matrizes e a estimativa da Proposição 1.11 é considerável.

Outra direção de pesquisa nesta área é a de estudar o problema inverso relacionado com os Teoremas 4.1 e 4.2 de caracterizar os conjuntos críticos para os quais as cotas

inferiores dadas por esses teoremas são atingidas. Naturalmente, tal estudo deve levar em consideração o Teorema de Vosper que caracteriza os conjuntos críticos para a estimativa dada pelo Teorema de Cauchy-Davenport.

Referências Bibliográficas

[1] Alon, N. (1999) **Combinatorial Nullstellensatz**. *Combinatorics, Probability and Computing*. **8** 7-29.

[2] Alon, N., Nathanson, M. B. & Ruzsa, I. Z. (1995) **Adding distinct congruence classes modulo a prime**. *Am. Math. Monthly*. **102** 250-255.

[3] Brualdi, R.A.(1980) **Matrices of Zeros and Ones with Fixed Row and Column Sum Vectors**. *Linear Algebra and its Aplications*. **33** 159-231.

[4] Caldeira, C. (2005) **Generalized derivations restricted to Grassmann spaces and additive theory**. *Linear Algebra and its Aplications*. **401** 11-27.

[5] Cauchy, A. (1813) **Recherches sur les Nombres**. *J. École Politech*. **9** 99-116.

[6] Davenport, H. (1935) **On the addition residue classes**. *J. London Math. Soc.* **10** 30-32.

[7] Davenport, H. (1947) **A historical note**. *J. London Math. Soc.* **22** 100-101.

[8] Dias da Silva, J. A. & Godinho, H. (2002) **Generalized derivations and theory additive**. *J. London Math. Soc.* **342** 1-15.

[9] Dias da Silva, J. A. & Hamidoune, Y.O. (1994) **Cyclic Spaces for Grassmann Derivatives and Additive Theory**. *Bull. London Math. Soc.* **26** 140-146.

[10] Erdös, P. (1963) **On the addition of residue classes** (*modp*). *In Proceedings of the 1963 Number Theory Conference at the University of Colorado*. Pages 16-17, Boulder. University of Colorado.

[11] Erdös, P. & Graham, R. (1980) **Old and new problems and results in combinatorial number theory**. *Enseign. Math.* **25** 1-128.

[12] Erdös, P. & Heilbronn, H. (1964) **On the addition of residue classes** (*modp*). *Acta Arith*. **9** 149-159.

[13] Godinho, H. (2002) **Linear algebraic techniques in theory additive and a generalization of the Caucht-Davenport theorem**. *Mat. Contemporânea* **21** 105-115.

[14] Herstein, I. (1970) *Tópicos de Álgebra*, Editora da Univ. e Polígono, São Paulo.

[15] Mello, M. P., Murari, I. T. C. & Santos, J. P. O. (1998) *Introdução à Análise Combinatória*, Editora da Unicamp, Campinas.

[16] Pinto, Aline G. S. (2002) **Um Problema de Teoria Aditiva dos Números via Álgebra Multilinear e Representações do Grupo Simétrico**. *Dissertação de Mestrado*. **UnB**.

[17] Perez Salvador, Blanca Rosa, et al. (2002) **A reduced formula for the precise number of (0,1) matrices in** $\Omega(R, C)$. *Discrete Mathematics* **256** 361-372.

[18] Nathanson, M. B. (1994) **An inverse theorem for sums of sets of lattice points**. *J. Number Theory* **46** 29-59.

[19] Nathanson, M. B. (1996) *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, New York.

[20] Shanzhen, G. & Zhonghua, T. (2005) **(0,1) matrices with constant row and column sums**. *Congressus Numerantium* **177** 3-13.

[21] Shanzhen, G., Zhonghua, T. & Niederhausen, H. (2006) **Enumeration of the (0,1) matrices with constant row and column sums**. *Appl. Math. J. Chinese Univ. Ser B* **21(4)** 479-486.

[22] Shanzhen, G. & Zhonghua, T. (2006) **Some Formulas Of (0,1) Matrices**. *Congressus Numerantium* **182** 53-63.

[23] Vosper, A. G. (1956) **Critical pairs of sumsets of a group of prime order**. *J. London Math. Soc.* **31** 200-205.

[24] Wang, B. (1988) **Precise Number of (0,1) matrices in** $\Omega(R, C)$. *Sci Sinica Ser A* **31** 1-6.

Índice Remissivo