Universidade de Campinas
IMECC
Geometria dos Números

Provas alternativas para os Teoremas de Pick e de Ehrhart e Semigrupos Numéricos

por

Matheus Bernardini de Souza
143790

Campinas
2014

1 Teorema de Pick

Nesta primeira seção, falaremos sobre um resultado de Pick que foi publicado em 1899. O Teorema de Pick relaciona a área de um polígono convexo com a quantidade de pontos inteiros dentro desse polígono. Primeiramente, vamos definir alguns números relacionados com um polígono e logo depois enunciar o teorema.

Definição 1. *Seja $\mathcal{P}$ um polígono. Definimos os números*

- $A_{\mathcal{P}}$:= *área de* $\mathcal{P}$;
- $I_{\mathcal{P}} := \#\{$*pontos inteiros no interior de* $\mathcal{P}\}$;
- $F_{\mathcal{P}} := \#\{$*pontos inteiros na fronteira de* $\mathcal{P}\}$.

Teorema de Pick. *Seja $\mathcal{P}$ um polígono convexo de vértices inteiros. Então*

$$A_{\mathcal{P}} = I_{\mathcal{P}} + \frac{F_{\mathcal{P}}}{2} - 1.$$

Nessas notas, vamos usar as ideias usadas em [3] para demonstrar esse Teorema. Murty e Thain usaram o Teorema de Minkowski para provar o Teorema de Pick e essa não é a demonstração original.

Demonstração: Faremos a prova deste teorema em 4 passos.

Passo 1. Se $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$, $\mathcal{P}_1$ e $\mathcal{P}_2$ são polígonos convexos que satisfazem o teorema e $\mathcal{P}_1 \cap \mathcal{P}_2$ é um segmento de reta, então $\mathcal{P}$ satisfaz o teorema.

Prova: Suponha que $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$, $\mathcal{P}_1$ e $\mathcal{P}_2$ são polígonos que satisfazem o teorema, isto é,

$$A_{\mathcal{P}_1} = I_{\mathcal{P}_1} + \frac{F_{\mathcal{P}_1}}{2} - 1$$

$$A_{\mathcal{P}_2} = I_{\mathcal{P}_2} + \frac{F_{\mathcal{P}_2}}{2} - 1$$

e $\mathcal{P}_1 \cap \mathcal{P}_2$ é uma aresta. Geometricamente,

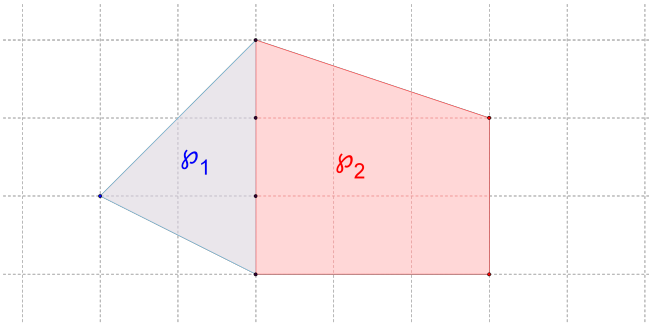

Figura 1: $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$

Seja $D = \#(\mathcal{P}_1 \cap \mathcal{P}_2)$. Note que

$$A_{\mathcal{P}} = A_{\mathcal{P}_1} + A_{\mathcal{P}_2} \Rightarrow A_{\mathcal{P}} = (I_{\mathcal{P}_1} + I_{\mathcal{P}_2}) + \frac{(F_{\mathcal{P}_1} + F_{\mathcal{P}_2})}{2} - 2,$$
$$I_{\mathcal{P}} = I_{\mathcal{P}_1} + I_{\mathcal{P}_2} + D - 2,$$
$$F_{\mathcal{P}} = (F_{\mathcal{P}_1} - D + 2) + (F_{\mathcal{P}_2} - D) = F_{\mathcal{P}_1} + F_{\mathcal{P}_2} - 2D + 2.$$

Assim,

$$\begin{aligned} I_{\mathcal{P}} + \frac{F_{\mathcal{P}}}{2} - 1 &= (I_{\mathcal{P}_1} + I_{\mathcal{P}_2} + D - 2) + \frac{(F_{\mathcal{P}_1} + F_{\mathcal{P}_2} - 2D + 2)}{2} - 1 \\ &= I_{\mathcal{P}_1} + I_{\mathcal{P}_2} + \frac{F_{\mathcal{P}_1} + F_{\mathcal{P}_2}}{2} + D - 2 - D + 1 - 1 \\ &= I_{\mathcal{P}_1} + I_{\mathcal{P}_2} + \frac{F_{\mathcal{P}_1} + F_{\mathcal{P}_2}}{2} - 2 = A_{\mathcal{P}}, \end{aligned}$$

donde concluímos que $\mathcal{P}$ satisfaz o teorema. Observe que podemos generalizar esse resultado se $\mathcal{P}$ puder ser escrito como uma união de um quantidade finita de polígonos (via indução).

Passo 2. Todo polígono convexo $\mathcal{P}$ pode ser escrito como $\mathcal{P} = \Delta_1 \cup \cdots \cup \Delta_n$, em que cada Δ_i é um triângulo e existe um vértice V de $\mathcal{P}$ que pertencem a todos os Δ_i's.

Prova: Seja V um dos vértices de $\mathcal{P}$. Ligando V a todos os demais vértices de $\mathcal{P}$, conseguimos decompor o polígono em triângulos. Observe que a quantidade de triângulos é igual à quantidade de lados do polígono menos 2.

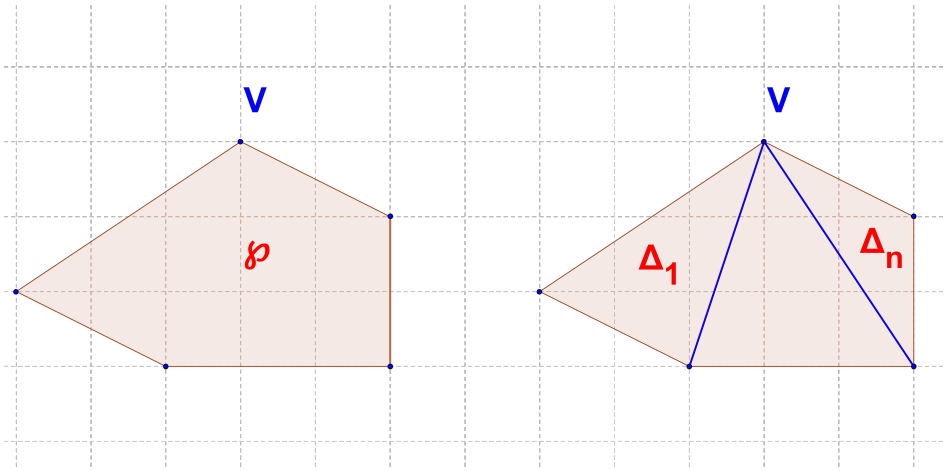

Figura 2: $\mathcal{P} = \Delta_1 \cup \cdots \cup \Delta_n$, com Δ_i triângulo

Passo 3. Cada Δ_i pode ser escrito como $\Delta_i = \Delta_{i1} \cup \cdots \cup \Delta_{ik}$, em que Δ_{in} é um triângulo elementar (triângulo cujos pontos inteiros são apenas os vértices).

Prova: Dado um ponto inteiro no interior de algum Δ_i, é possível ligá-lo por segmentos de reta aos 3 vértices de Δ_i. Fazendo esse procedimento indutivamente (o processo

para, pois existe uma quantidade finita de pontos inteiros dentro de um triângulo), conseguimos decompor cada triângulo em triângulos elementares.

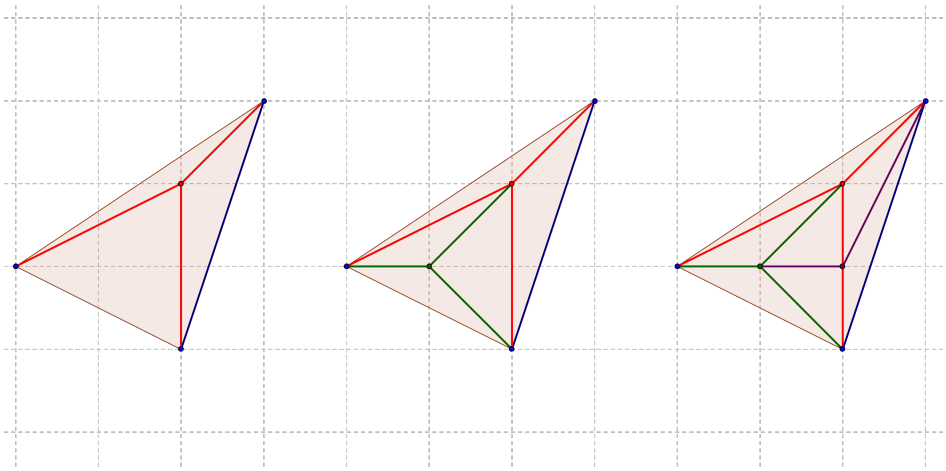

Figura 3: $\Delta_1 = \Delta_{11} \cup \cdots \cup \Delta_{1k}$, com Δ_{1i} triângulo elementar

Passo 4. A área de cada triângulo elementar é $\frac{1}{2}$.

Para demonstrar esse fato, vamos usar o seguinte resultado:

Lema (Teorema de Minkowski). *Seja C uma região convexa, simétrica e limitada em $\mathbb{R}^n$ com volume maior que 2^n. Então C contém pelo menos um ponto inteiro não nulo.*

Prova: (do Passo 4.) Vamos usar a Figura 4 para nos auxiliar. Seja ΔABC um triângulo elementar. Primeiramente, rotacione o triângulo ΔABC por cada um de seus vértices, obtendo os triângulos azul, verde e vermelho. Depois translade cada um desses triângulos para obter metade de um paralelepípedo e complete o paralelepípedo. Observe que existe um único ponto inteiro no interior do paralelepípedo. Tranlsadando a figura de tal forma que esse ponto coincida com a origem, obtemos uma região convexa, limitada e simétrica. Como não existem inteiros não nulos no interior do paralelepípedo, segue do Teorema de Minkowski que a área desse paralelepípedo é menor que ou igual a 4. Como a área é invariante por rotações e translações, temos que a área do paralelepípedo é igual a 8 vezes a área do ΔABC. Daí, $A_{\Delta ABC} \leq \frac{1}{2}$. Por outro lado, é possível calcular a área do ΔABC da seguinte forma: $A_{\Delta ABC} = \frac{1}{2}|\det M|$, em que

$$M = \begin{pmatrix} x_A & y_A & 1 \\ x_B & y_B & 1 \\ x_C & y_C & 1 \end{pmatrix},$$

$A = (x_A, y_A), B = (x_B, y_B)$ e $C = (x_C, y_C)$. Como as coordenadas de A, B e C são

inteiras e o triângulo é não degenerado, segue que $|\det(M)| \in \mathbb{N}$, isto é, $A_{\Delta ABC} \geq \frac{1}{2}$. Portanto, $A_{\Delta ABC} = \frac{1}{2}$.

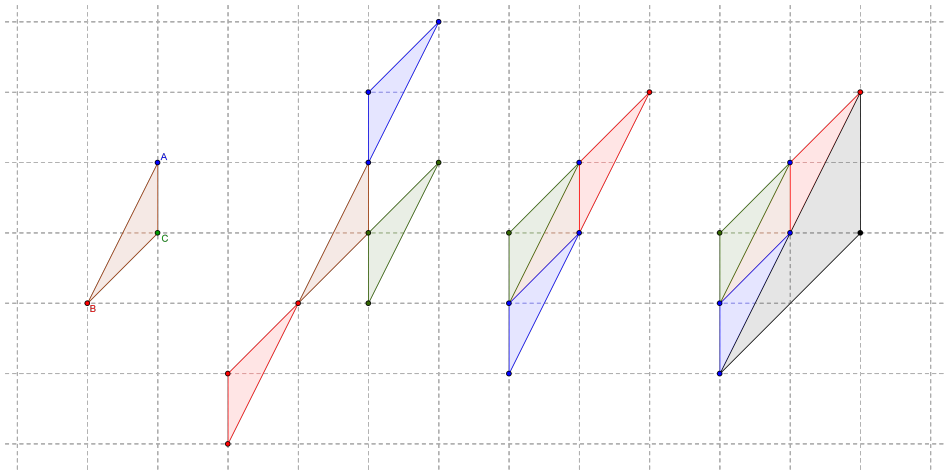

Figura 4: Ilustração da prova do **Passo 4**

Para concluir a demosntração, basta verificar que cada triângulo elementar Δ satisfaz o teorema. De fato,

$$A_\Delta = \frac{1}{2} = 0 + \frac{3}{2} - 1 = I_\Delta + \frac{F_\Delta}{2} - 1.$$

■

2 Teorema de Ehrhart

Antes de ir para o teorema desta seção, vamos dar algumas definições. Um politopo $\mathcal{P}$ em $\mathbb{R}^n$ é o fecho convexo de uma quantidade finita de pontos, isto é, dados $v_0, \ldots, v_k \in \mathbb{R}^n$, definimos o fecho convexo desses pontos por

$$\text{ConvHull}(v_0, \ldots, v_k) = \left\{ \sum_{i=0}^{k} a_i v_i : a_i \geq 0 \text{ e } \sum_{i=0}^{d} a_i = 1 \right\}.$$

Em alguns casos, um politopo pode ser definido como sendo $\{x \in \mathbb{R}^n : Ax \leq b\}$, em que $A \in \mathcal{M}_{m\times n}$ e $b \in \mathcal{M}_{m\times 1}$. A dimensão de um politopo é definida como a dimensão do espaço afim gerados pelas combinações convexas de elementos de $\mathcal{P}$, isto é, a dimensão de

$$\{x + ty : x, y \in \mathcal{P} \text{ e } t \in \mathbb{R}\}.$$

Denotamos a dimensão de $\mathcal{P}$ por $\dim \mathcal{P}$. Se um politopo $\mathcal{P}$ tiver dimensão $d \in \mathbb{N}$, diremos que $\mathcal{P}$ é um $d-$politopo. Temos que um $d-$politopo convexo tem pelo menos $d+1$ vértices. No caso em que a quantidade de vértices for precisamente $d+1$, diremos que o politopo é um $d-$simplexo. Por exemplo, todo triângulo é um 2-simplexo.

Para finalizar as definições, chamamos um politopo de inteiro (racional) quando os vértices tem coordenadas inteiras (racionais).

[1] é uma boa referência para essas definições e alguns resultados sobre esse tema. Estamos prontos para ir para a teoria.

Teorema de Ehrhart. *Se $\mathcal{P} \subset \mathbb{R}^n$ é um $d-$politopo inteiro convexo, então a função $\ell_{\mathcal{P}}(t) := \#(t\mathcal{P} \cap \mathbb{Z}^n)$ coincide com um polinômio de grau $d, \forall t \in \mathbb{N}_0$. Esse polinômio é denotado por $L_{\mathcal{P}}(t)$ e é chamado de polinômio de Ehrhart.*

Esse teorema foi demonstrado em 1962 por Ehrhart. Na demonstração original, ele usou a equivalência (i)-(iii) da seguinte Proposição.

Proposição 1. *Sejam $f : \mathbb{N}_0 \to \mathbb{C}$ uma função e $d \in \mathbb{N}_0$. São equivalentes:*

(i) *Existe $P(z) \in \mathbb{C}[z]$ com $\partial P \leq d$ tal que*

$$\sum_{t\geq 0} f(t) z^t = \frac{P(z)}{(1-z)^{d+1}}.$$

(ii) $\forall t \in \mathbb{N}_0$,

$$\sum_{k=0}^{d+1} (-1)^{d+1-k} \binom{d+1}{k} f(t+k) = 0.$$

(iii) *Existe um polinômio de grau $\leq d$ que coincide com $f(t), \forall t \in \mathbb{N}_0$.*

Em 2009, Sam [4] deu uma nova demonstração para o Teorema de Ehrhart em que ele usou a equivalência (ii)-(iii). Neste trabalho, vamos refazer as ideias usadas por ele, então vamos demonstrar apenas a equivalência (ii)-(iii) da Proposição 1.

Demonstração: (ii) $\Leftrightarrow$ (iii)

Suponha f não identicamente nula. Vamos por indução em d.

Caso base ($d = 0$):

(ii) $0 = \sum_{k=0}^{1}(-1)^{1-k}\binom{1}{k}f(t+k) = f(t+1) - f(t), \forall t \in \mathbb{N}_0$

(iii) $f(t)$ coincide com um polinômio de grau $\leq 0, \forall t \in \mathbb{N}_0$.

Note que (iii) $\Leftrightarrow f(t) =$ constante, $\forall t \in \mathbb{N}_0 \Leftrightarrow f(t+1) = f(t), \forall t \in \mathbb{N}_0 \Leftrightarrow$ (ii).

Suponha que (ii) $\Leftrightarrow$ (iii) para algum $d-1 \in \mathbb{N}$. Vamos mostrar a equivalência para d.

(iii) $\Rightarrow$ (ii): Por hipótese de indução, se $p(t)$ coincide com um polinômio de grau $\leq d-1, \forall t \in \mathbb{N}_0$, então $\sum_{k=0}^{d}(-1)^{d-k}\binom{d}{k}p(t+k) = 0$. Seja $\tilde{f}(t)$ um polinômio de grau $\leq d$. Então $g(t) := \tilde{f}(t+1) - \tilde{f}(t)$ é um polinômio de grau $\leq d-1$. Dado $t \in \mathbb{N}_0$, temos que $\tilde{f}(t) = f(t)$, daí:

$$
\begin{aligned}
0 &= \sum_{k=0}^{d}(-1)^{d-k}\binom{d}{k}\overbrace{[f(\underbrace{t+1+k}_{\in\mathbb{N}_0}) - f(\underbrace{t+k}_{\in\mathbb{N}_0})]}^{g(t+k)} \\
&= \sum_{k=0}^{d}(-1)^{d-k}\binom{d}{k}f(t+1+k) - \sum_{k=0}^{d}(-1)^{d-k}\binom{d}{k}f(t+k) \\
&= \sum_{k=1}^{d+1}(-1)^{d+1-k}\binom{d}{k-1}f(t+k) - \sum_{k=0}^{d}(-1)^{d-k}\binom{d}{k}f(t+k) \\
&= f(t+d+1) + (-1)^{d+1}f(t) + \sum_{k=1}^{d}(-1)^{d-k+1}\left[\binom{d}{k-1} + \binom{d}{k}\right]f(t+k) \\
&= \sum_{k=0}^{d+1}(-1)^{d-k+1}\binom{d+1}{k}f(t+k),
\end{aligned}
$$

em que usamos a relação de Stifel na última passagem.

(ii) $\Rightarrow$ (iii) Seja f tal que $\sum_{k=0}^{d+1}(-1)^{d-k+1}\binom{d+1}{k}f(t+k) = 0$. Pela construção anterior, temos que $g(t) := f(t+1) - f(t)$ satisfaz $\sum_{k=0}^{d}(-1)^{d-k}\binom{d}{k}g(t+k) = 0$. Por hipótese de indução, $g(t)$ coincide com um polinômio de grau $\leq d-1, \forall t \in \mathbb{N}_0$. Note que

$$f(t+1) = g(t) + f(t) = g(t) + g(t-1) + f(t-1) = \cdots = \sum_{k=0}^{t} g(k) + f(0) := S + f(0).$$

Suponha que $g(t) = g_0 + \cdots + g_{d-1}t^{d-1}, \forall t \in \mathbb{N}_0$. Daí,

$$S = \sum_{k=0}^{t}(g_0 + \cdots + g_{d-1}k^{d-1}) = g_0\sum_{k=0}^{t}1 + g_1\sum_{k=0}^{t}k + \cdots + \sum_{k=0}^{t}k^{d-1}.$$

Como para cada $r \in \{0, \ldots, d-1\}$, $\sum_{k=0}^{t} k^r$ é um polinômio em t de grau $r+1$, segue que S coincide com um polinômio em t de grau $\leq (d-1)+1 = d, \forall t \in \mathbb{N}_0$ ($\leq$, pois pode ocorrer $g_{d-1} = 0$). Como $f(0)$ é uma constante, segue que f coincide com um polinômio em t de grau $\leq d, \forall t \in \mathbb{N}_0$.

■

Definição 2. *Uma triangulação de um $d-$politopo convexo é uma coleção finita de $d-$simplexos $\mathcal{T} = \{\Delta_i\}$ tal que*

1. $\bigcup \Delta_i = \mathcal{P}$;
2. *Se Δ_i e $\Delta_j \in \mathcal{T}$, então $\Delta_i \cap \Delta_j$ é uma face comum de Δ_i e Δ_j.*

Lema 1. *Para todo politopo convexo $\mathcal{P}$, existe uma triangulação em simplexos $\{\Delta_i\}$ tal que o conjunto de vértice dos Δ_i's coincide com o conjunto de vértices de $\mathcal{P}$.*

Agora estamos prontos para demonstrar o Teorema de Ehrhart.
Demonstração: Pela Proposição 1, é suficiente mostrar que

$$\sum_{k=0}^{d+1} (-1)^{d+1-k} \binom{d+1}{k} \ell_{\mathcal{P}}(t+k) = 0, \forall t \in \mathbb{N}_0,$$

isto é,

$$\ell_{\mathcal{P}}(t+d+1) = \sum_{k=0}^{d} (-1)^{d-k} \binom{d+1}{k} \ell_{\mathcal{P}}(t+k), \forall t \in \mathbb{N}_0.$$

Pelo Lema 1, basta mostrar essa propriedade para $\mathcal{P}$ simplexo. Antes de formalizar, vamos verificar um exemplo geometricamente. Considere $\mathcal{P}$ o triângulo com vértices em $(0,0), (4,0)$ e $(4,4)$ ($d = 2$ e $t = 0$). Geometricamente, temos

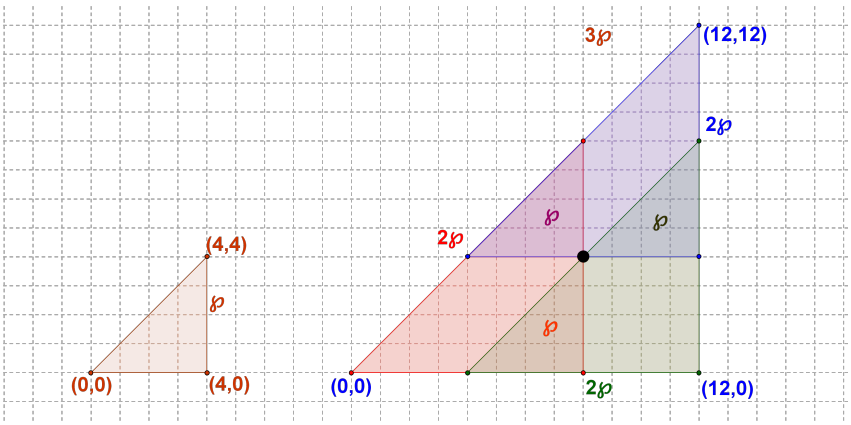

Figura 5: $\ell_{\mathcal{P}}(3) = 3\ell_{\mathcal{P}}(2) - 3\ell_{\mathcal{P}}(1) + 1$

É usado o princípio da inclusão-exclusão para contar a quantidade de pontos inteiros em $3\mathcal{P}$ nesse exemplo e essa é a ideia para o caso geral.

Considere o simplexo $\mathcal{P}$ de vértices $\{v_0, \ldots, v_d\}$ e $t \in \mathbb{N}_0$. Para cada $i \in \{0, \ldots, d\}$, considere $Q_i := (t+d)\mathcal{P} + v_i$ e defina $Q = \bigcup Q_i$. Intuitivamente, cada Q_i é uma cópia de um múltiplo de $\mathcal{P}$ tranladado pelo vértice v_i e $Q = (t+d+1)\mathcal{P}$.

Vamos usar o princípio da inclusão-exclusão para determinar $\#(Q \cap \mathbb{Z}^n)$:

$$\begin{aligned}\#(Q \cap \mathbb{Z}^n) &= \#\left(\bigcup_{i=0}^{d} Q_i \cap \mathbb{Z}^n\right) = \#\left(\bigcup_{i=0}^{d} (\underbrace{Q_i \cap \mathbb{Z}^n}_{R_i})\right) \\ &= \sum_{i=0}^{d} \#R_i - \sum_{0 \le i \le j \le d} \#R_i \cap R_j + \cdots + (-1)^d \#\left(\bigcap_{i=0}^{d} R_i\right)\end{aligned}$$

Para isso, precisaremos calcular a cardinalidade de todas as possíveis interseções dos Q_i's (pois $\bigcap R_i = \bigcap Q_i \cap \mathbb{Z}^n$).

Observe que, dado $j \in \{0, \ldots, d\}$, temos

$$\begin{aligned}Q_j &= \{v_j + (t+d)p : p \in \mathcal{P}\} \\ &= \left\{v_j + (t+d)\sum_{i=0}^{d} c_i v_i : c_i \ge 0 \text{ e } \sum_{i=0}^{d} c_i = 1\right\} \\ &= \left\{\sum_{i \ne j} \underbrace{(t+d)c_i}_{a_i} v_i + [\underbrace{(t+d)c_j + 1}_{a_j}]v_j : c_i \ge 0 \text{ e } \sum_{i=0}^{d} c_i = 1\right\} \\ &= \left\{\sum_{i=0}^{d} a_i v_i : a_i \ge 0, i \ne j, a_j \ge 1 \text{ e } \sum_{i=0}^{d} a_i = t+d+1\right\}.\end{aligned}$$

Para cada $I \subseteq \{0, \ldots, d\}$, temos:

$$\bigcap_{i \in I} Q_i = \left\{\sum_{i=0}^{d} a_i v_i : a_i \ge 0, \forall i \notin I, a_j \ge 1, \forall j \in I \text{ e } \sum_{i=0}^{d} a_i = t+d+1\right\};$$

Seja $R_I = (t+d+1-\#I)\mathcal{P} + \sum_{i \in I} v_i$. Então

$$\begin{aligned}R_I &= \left\{\sum_{i=0}^{d} (t+d+1-\#I)c_i v_i + \sum_{i \in I} v_i : c_i \ge 0, \sum_{i=0}^{d} c_i = 1\right\} \\ &= \left\{\sum_{i \notin I} \underbrace{(t+d+1-\#I)c_i}_{a_i, i \notin I} v_i + \sum_{i \in I} [\underbrace{(t+d+1-\#I)c_i + 1}_{a_i, i \in I}]v_i : c_i \ge 0, \sum_{i=0}^{d} c_i = 1\right\} \\ &= \left\{\sum_{i=0}^{d} a_i v_i : a_i \ge 0, i \notin I, a_i \ge 1, i \in I \text{ e } \sum_{i=0}^{d} a_i = t+d+1\right\}. \qquad (1)\end{aligned}$$

Vamos explicar um pouco melhor como chegamos à igualdade envolvendo o somatório em (1). Temos que

$$\#I \leq d+1 \Rightarrow t+d+1-\#I \geq t \geq 0 \text{ e } c_i \geq 0.$$

Daí, se $i \notin I$, então $a_i \geq 0$ e se $i \in I$, então $a_i \geq 1$. Também,

$$\begin{aligned}
\sum_{i=0}^{d} a_i &= \sum_{i\notin I}(t+d+1-\#I)c_i + \sum_{i\in I}[(t+d+1-\#I)c_i+1] \\
&= (t+d+1-\#I)\sum_{i\notin I} c_i + (t+d+1-\#I)\sum_{i\in I} c_i + \sum_{i\in I} 1 \\
&= (t+d+1-\#I)\underbrace{\sum_{i=0}^{d} c_i}_{1} + \#I \\
&= t+d+1
\end{aligned}$$

Portanto, concluímos que

$$\bigcap_{i\in I} Q_i = (t+d+1-\#I)\mathcal{P} + \sum_{i\in I} v_i.$$

Da igualdade anterior e usando o fato que cada v_i é inteiro, temos que, dado I tal que $\#I = k$ em que $k \in \{1,\ldots,d+1\}$,

$$\begin{aligned}
\#\left(\bigcap_{i\in I} Q_i \cap \mathbb{Z}^n\right) &= \#\left(\left((t+d+1-k)\mathcal{P} + \sum_{i\in I} v_i\right)\cap \mathbb{Z}^n\right) \\
&= \#((t+d+1-k)\mathcal{P}\cap\mathbb{Z}^n) = \ell_{\mathcal{P}}(t+d+1-k).
\end{aligned}$$

Pelo princípio da inclusão-exclusão (visto acima) e usando o fato que há $\binom{d+1}{k} = \binom{d+1}{d+1-k}$ subconjuntos de cardinalidade k, temos que

$$\begin{aligned}
\#(Q\cap\mathbb{Z}^n) &= \sum_{i=0}^{d}\#R_i - \sum_{0\leq i\leq j\leq d}\#R_i\cap R_j + \cdots + (-1)^d \#\left(\bigcap_{i=0}^{d} R_i\right) \\
&= \binom{d+1}{1}\ell_{\mathcal{P}}(t+d+1-1) - \binom{d+1}{2}\ell_{\mathcal{P}}(t+d+1-2) + \\
&+ \cdots + (-1)^d\binom{d+1}{d+1}\ell_{\mathcal{P}}(t+d+1-(d+1)) \\
&= \sum_{k=1}^{d+1}(-1)^{k-1}\binom{d+1}{k}\ell_{\mathcal{P}}(t+d+1-k) \\
&= \sum_{m=0}^{d}(-1)^{d-m}\binom{d+1}{m}\ell_{\mathcal{P}}(t+m),
\end{aligned}$$

em que $m = d+1-k$. Para finalizar essa parte, devemos verificar que $Q = (t+d+1)\mathcal{P}$ (daí, $\#(Q \cap \mathbb{Z}^n) = \ell_{\mathcal{P}}(t+d+1)$).
($\subseteq$) Seja $q \in Q$. Então $q \in Q_j$, para algum $j \in \{0, \ldots, d\}$. Daí $q = \sum_{i=0}^{d} a_i v_i$, com $a_i \geq 0$, para $i \neq j$, $a_j \geq 1$ e $\sum_{i=0}^{d} a_i = t+d+1$. Logo $\sum_{i=0}^{d} \frac{a_i}{t+d+1} = 1$ e $q = \sum_{i=0}^{d}(t+d+1)c_i v_i$, em que $c_i = \frac{a_i}{t+d+1} \geq 0, \forall i$. Portanto, $q \in (t+d+1)\mathcal{P}$.
($\supseteq$) Seja $q \in (t+d+1)\mathcal{P}$. Então $q = \sum_{i=0}^{d}(t+d+1)c_i v_i$, $c_i \geq 0$ e $\sum_{i=0}^{d} c_i = 1$. Logo $\sum_{i=0}^{d}(t+d+1)c_i = t+d+1$ e $a_i := (t+d+1)c_i \geq 0, \forall i$. Resta mostrar que existe $j \in \{0, \ldots, d\}$ tal que $a_j \geq 1$. Suponha que $0 \leq a_i < 1, \forall i$. Então $t+d+1 = \sum_{i=0}^{d} a_i < \sum_{i=0}^{d} 1 = d+1 \leq t+d+1$, o que é um absurdo. Portanto, $q \in Q_j$, para algum j, donde concluímos que $q \in Q$. Portanto, concluímos que

$$\ell_{\mathcal{P}}(t+d+1) = \sum_{k=0}^{d} (-1)^{d-k} \binom{d+1}{k} \ell_{\mathcal{P}}(t+k)$$

e pela Proposição 1, existe um polinômio $L_{\mathcal{P}}(t)$ de grau $\leq d$ tal que $\ell_{\mathcal{P}}(t) = L_{\mathcal{P}}(t), \forall t \in \mathbb{N}_0$. Para concluir a demonstração, devemos mostrar que o grau desse polinômio é exatamente d.

Transladado $\mathcal{P}$ de forma que v_0 coincida com a origem (se necessário), temos que $v_1, \ldots, v_d$ são vetores L.I., pois $\mathcal{P}$ é $d-$dimensional. Dados inteiros positivos $k_1, \ldots, k_d, \tilde{k}_1, \ldots, \tilde{k}_d \leq t$, temos que $k_1 v_1 + \cdots + k_d v_d = \tilde{k}_1 v_1 + \cdots + \tilde{k}_d v_d \Leftrightarrow k_i = \tilde{k}_i, \forall i$. Assim a quantidade de vetores distintos $v = k_1 v_1 + \cdots + k_d v_d$ é exatamente t^d. Note que todos os v escritos dessa maneira pertencem a $(dt\mathcal{P} \cap \mathbb{Z}^n)$, pois

- $v = \sum_{i=0}^{d} k_i v_i$, com $k_0 = 0$ e $\sum_{i=0}^{d} k_i \leq \sum_{i=1}^{d} t = td$.
- $v \in \mathbb{Z}^n$, pois $v_i \in \mathbb{Z}^n$ e $k_i \in \mathbb{Z}, \forall i$.

Assim, $\#(dt\mathcal{P} \cap \mathbb{Z}^n) = L_{\mathcal{P}}(dt) \geq t^d$. Isso implica que $\partial L_{\mathcal{P}} \geq d$, pois caso contrário, $t^d \leq L_{\mathcal{P}}(dt) = a_0 + \cdots + a_{d-1} d^{d-1} t^{d-1}, \forall t \in \mathbb{N}_0$, o que é um absurdo. Portanto, $\partial L_{\mathcal{P}} = d$.

■

Teorema de Ehrhart (Racional). *Se $\mathcal{P} \subset \mathbb{R}^n$ é um d-politopo racional convexo, então a função $\ell_{\mathcal{P}}(t) := \#(t\mathcal{P} \cap \mathbb{Z}^n)$ coincide com um quasi-polinômio de grau $d, \forall t \in \mathbb{N}_0$.*

Observação. *Um quasi-polinômio de grau d é uma função $f : \mathbb{N} \to \mathbb{C}$ da forma*

$$f(t) = c_d(t) t^d + \cdots c_0(t),$$

em que cada c_i é uma função periódica de período inteiro e $c_d \neq 0$.

Demonstração: A ideia é bem parecida com a demonstração do Teorema de Ehrhart. Vamos fazer uma pequena alteração ao tomarmos os conjuntos Q_i e R_I. Como o politopo é racional, existe $s \in \mathbb{N}$ tal que $s\mathcal{P}$ é um politopo inteiro. Dessa forma, dado $k \in \{0, \ldots, s-1\}$, considere $Q_i := (t+k+sd)\mathcal{P} + sv_i$, para cada $i \in \{0, \ldots, d\}$, e dado $I \subseteq \{0, \ldots, d\}$, considere $R_I := (t+k+s(d+1-\#I))\mathcal{P} + \sum_{i\in I} sv_i$. Verificamos que

$$\begin{aligned} Q_j &= \left\{ \sum_{i=0}^{d} a_i v_i : a_i \geq 0, i \neq j; a_j \geq s \text{ e } \sum_{i=0}^{d} a_i = t+k+s(d+1) \right\} \\ \bigcap_{i\in I} Q_i &= \left\{ \sum_{i=0}^{d} a_i v_i : a_i \geq 0, i \notin I; a_i \geq s, i \in I \text{ e } \sum_{i=0}^{d} a_i = t+k+s(d+1) \right\} \\ R_I &= \left\{ \sum_{i=0}^{d} a_i v_i : a_i \geq 0, i \notin I; a_i \geq s, i \in I \text{ e } \sum_{i=0}^{d} a_i = t+k+s(d+1) \right\}, \end{aligned}$$

donde concluímos que

$$\bigcap_{i\in I} Q_i = (t+k+s(d+1-\#I))\mathcal{P} + \sum_{i\in I} sv_i.$$

Verificamos também que

$$Q := \bigcup_{i=0}^{d} Q_i = (t+k+s(d+1))\mathcal{P}.$$

Usando o princípio da inclusão-exclusão, temos que

$$\begin{aligned} \#(Q \cap \mathbb{Z}^n) &= \# \left(\bigcup_{i=0}^{d} (Q_i \cap \mathbb{Z}^n) \right) \\ \ell_{\mathcal{P}}(t+k+s(d+1)) &= \sum_{m=0}^{d} (-1)^{d-m} \binom{d+1}{m} \ell_{\mathcal{P}}(t+k+sm) \end{aligned}$$

Suponha que $t+k \equiv 0 \pmod{s}$. Daí, para cada $m \in \{0, \ldots, d+1\}$, $\ell_{\mathcal{P}}(t+k+sm) = \ell_{\mathcal{P}}(s\frac{t+k}{s} + m) = \ell_{s\mathcal{P}}(\frac{t+k}{s} + m)$, pois $\ell_{\mathcal{P}}(st) = \#(st\mathcal{P} \cap \mathbb{Z}^n) = \#(t(s\mathcal{P}) \cap \mathbb{Z}^n) = \ell_{s\mathcal{P}}(t)$. Portanto,

$$\ell_{s\mathcal{P}} \left(\frac{t+k}{s} + d + 1 \right) = \sum_{m=0}^{d} (-1)^{d-m} \binom{d+1}{m} \ell_{s\mathcal{P}} \left(\frac{t+k}{s} + m \right)$$

e pela Proposição 1, existe um polinômio $L^k_{s\mathcal{P}}(t)$ de grau $\leq d$ tal que $\ell_{\mathcal{P}}(t) = L^k_{s\mathcal{P}}(t), \forall t \in \mathbb{N}_0$, com $t \equiv -k \pmod{s}$. A passagem para mostrar que o grau é exatamente d é análoga à do caso anterior.

Fazendo esse procedimento para cada $k \in \{0, \ldots, s-1\}$, obtemos s polinômios $L^k_{s\mathcal{P}}(t)$(a princípio distintos) de tal forma que $\ell_{\mathcal{P}}(t)$ coincide com algum $L^k_{s\mathcal{P}}(t)$, dependendo da classe de congruência de t módulo s.

■

3 Semigrupos Numéricos

Definição 3. *Dizemos que $H \subseteq \mathbb{N}_0 = \{0, 1, 2, \ldots\}$ é um semigrupo numérico se:*

- $0 \in H$;
- $a, b \in H \Rightarrow a + b \in H$;
- $\mathbb{N}_0 \setminus H$ *é um conjunto finito.*

Denotamos o conjunto das lacunas do semigrupo numérico H por $G(H) := \mathbb{N}_0 \setminus H$, o qual é um conjunto finito. Para não ficar artificial, vamos exemplificar essa definição.

Exemplo 1. *Considere o conjunto $H = \{0, 2, 4, 6, 8, \rightarrow\}$, em que $\rightarrow$ significa que todo inteiro positivo após o último número escrito (no exemplo o número é 8) aparece em H. Como $0 \in H$ e $G(H) = \mathbb{N}_0 \setminus H = \{1, 3, 5, 7\}$, basta verificar a propriedade do fechamento. Se a e $b \in H$, com $a, b \leq 8$, então a e b são pares. Logo $a + b$ também é par, donde concluímos que $a + b \in H$. Se $a, b \in H$, com $a, b > 8$, então $a + b$ é um inteiro maior que 8. Como todo inteiro maior que 8 pertence a H, temos que $a+b \in H$. Portanto, H é um semigrupo numérico.*

Considere $H_{p,q} := \langle p, q \rangle = \{ap + bq : a, b \in \mathbb{N}_0\}$, em que $1 < p < q$ e $\text{mdc}(p, q) = 1$. É possível mostrar que, sob essas condições, $H_{p,q}$ é um semigrupo numérico. Seja $G_{p,q} := G(H_{p,q})$ o conjunto das lacunas de $H_{p,q}$.

Problema. *Dados p e $q \in \mathbb{N}$ com $1 < p < q$ e $\text{mdc}(p, q) = 1$, defina*

$$\mathcal{H}_{p,q} := \{H \text{ semigrupo numérico} : H \supseteq H_{p,q}\} \text{ e}$$

$$n(p, q) = \#\mathcal{H}_{p,q}.$$

Existe uma fórmula explícita para o número $n(p, q)$? Essa fórmula depende apenas de p e q?

Observe que para resolver esse problema, devemos estudar o conjunto $G_{p,q}$ e determinar quais dos subconjuntos S de $G_{p,q}$ fazem com que $H_{p,q} \cup S$ seja ainda um semigrupo numérico.

Exemplo 2. *Considere o semigrupo numérico $H_{2,5}$. Temos que $G_{2,5} = \{1, 3\}$. Os subconjuntos S de $G_{2,5}$ que fazem com que $H_{2,5} \cup S$ seja ainda um semigrupo numérico são $S_0 = \emptyset, S_1 = \{3\}$ e $S_2 = \{1, 3\}$. Assim, $n(2, 5) = 3$.*

Existe uma forma de enxergar o conjunto $G_{p,q}$ que torna o problema mais "tratável".

Proposição 2. *Seja $k \in G_{p,q}$. Então existe um único $(a, b) \in \mathbb{N}_0^2$ tal que*

$$k = c - 1 - (ap + bq) = pq - (a + 1)p - (b + 1)q.$$

Dado $k \in G_{p,q}$, temos que $k > 0$. Da Proposição anterior, (a, b) satisfaz $(a+1)p + (b+1)q < pq$. Definindo $\Delta_0 := \{(a, b) \in \mathbb{N}_0^2 : (a+1)p + (b+1)q < pq\}$, conseguimos a bijeção

$$\begin{array}{rccc} \gamma & : & \Delta_0 & \longrightarrow & G_{p,q} \\ & & (a,b) & \longmapsto & c - 1 - (ap + bq) \end{array}$$

Observe que o conjunto Δ_0 corresponde aos pontos de $\mathbb{N}_0^2$ abaixo da reta

$$r : p(X+1) + q(Y+1) = pq.$$

Exemplo 3. *Considere o semigrupo numérico $H_{5,13}$. As lacunas são representadas por*

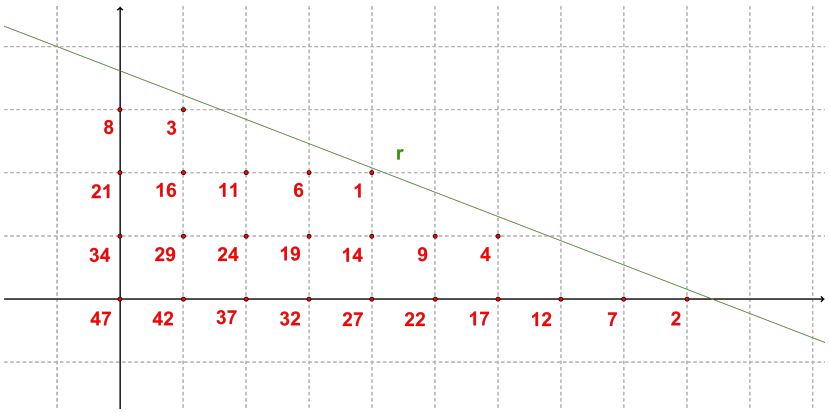

Figura 6: $G_{5,13}$ através da bijeção γ

Através dessa forma de enxergar o conjunto das lacunas e usando um pouco da teoria de caminhos reticulados, Hellus e Waldi [2] conseguiram encontrar uma bijeção entre $\mathcal{H}_{p,q}$ e $(\mathcal{A}_p \cap \{x_p = q\}) \cap \mathbb{N}_0^p$, em que $\mathcal{A}_p := \{x = (x_1, \ldots, x_p) \in \mathbb{R}_+^p : x \text{ satisfaz } (2)\}$ e

$$x_i + x_j \leq \begin{cases} x_{i+j}, \text{ se } i + j \leq p \\ x_p + x_{i+j-p}, \text{ se } i + j > p \end{cases} \tag{2}$$

Observe que $\mathcal{P} = \mathcal{A}_p \cap \{x_p = 1\}$ é um $(p-1)-$polítopo racional. De fato,

- o sistema de inequações que define $\mathcal{A}_p$ tem coeficientes inteiros (logo racionais), logo $\mathcal{A}_p$ é um politopo racional;
- $\mathcal{A}_p$ tem dimensão p e quando intersectado com o hiperplano $x_p = 1$, a dimensão cai em uma unidade, logo $\dim \mathcal{A}_p = p - 1$.

Pelo Teorema de Ehrhart (Racional), temos que $\#(q\mathcal{P} \cap \mathbb{Z}^n)$ é um quasi-polinômio em q de grau $p - 1$. Usando outros métodos, é possível demonstrar que esse quasi-polinômio tem coeficiente líder constante. Assim, temos o seguinte resultado:

Teorema 1. *O número $n(p,q)$ coincide com um quasi-polinômio em q de grau $p-1$ e coeficiente líder constante.*

Exemplo 4.

$$n(2,q) = \frac{1}{2}q + \frac{1}{2}.$$

Exemplo 5.

$$n(3,q) = \left\lfloor \frac{q^2}{12} + \frac{q}{2} \right\rfloor + 1 = \begin{cases} \frac{1}{12}q^2 + \frac{1}{2}q + \frac{2}{3}, \ \textit{se } q \equiv 0 \pmod 2 \\ \\ \frac{1}{12}q^2 + \frac{1}{2}q + \frac{5}{12}, \ \textit{se } q \equiv 1 \pmod 2 \end{cases}$$

Exemplo 6.

$$n(4,q) = \begin{cases} \frac{1}{72}q^3 + \frac{1}{6}q^2 + \frac{13}{24}q + \frac{5}{8}, \ \textit{se } q \equiv 1 \pmod 6 \\ \\ \frac{1}{72}q^3 + \frac{1}{6}q^2 + \frac{13}{24}q + \frac{1}{2}, \ \textit{se } q \equiv 3 \pmod 6 \\ \\ \frac{1}{72}q^3 + \frac{1}{6}q^2 + \frac{13}{24}q + \frac{7}{18}, \ \textit{se } q \equiv 5 \pmod 6 \end{cases}$$

Referências

[1] Beck, M. and Robins, S., *Computing the Continuous Discretely*, Undergraduate Texts in Mathematics, Springer, 2007.

[2] Hellus, M. and Waldi, R., *On the number of numerical semigroups containing two coprime integers p and q* (preprint).

[3] Murty, M.R. and Thain, N., *Pick's Theorem via Minkowski's Theorem*. Amer. Math. Monthly **114** (2007) no. 8, 732-736.

[4] Sam, S., *A bijective proof for a theorem of Ehrhart*. Amer. Math. Monthly **116** (2009) no. 8, 688-701.