PICME/IME/USP COMBINATÓRIA

NOTAS - 2010 (SEMESTRE 2)

YOSHIHARU KOHAYAKAWA E GUILHERME MOTA (IME/USP)

1. Conjuntos de Sidon

11/08/2010

Seja $A \subset \mathbb{N} = \{0, 1, 2, \ldots\}$. Definimos a *densidade de Shnirelman* como $\sigma(A) = \inf_{n\geq 1} A(n)/n$, onde $A(n) = |A \cap [n]|$. Shnirelman provou que se $0 \in A$ e $\sigma(A) > 0$, então A é uma *base de ordem finita*, isto é, existe um h tal que todo número natural pode ser escrito como soma de no máximo h elementos de A.

Fixado $A \subset \mathbb{N}$, definimos $r_n(A)$ como a quantidade de pares (a, a') com $a < a'$, onde $a, a' \in A$ e $a + a' = n$. Ademais, definimos $r'_n(A)$ como a quantidade de pares (a, a') com $a \leq a'$, onde $a, a' \in A$ e $a + a' = n$, isto é, permitimos pares (a, a') tais que $a = a'$. Podemos observar que $r'_n(A) = r_n(A) + 1$ se temos n par com $n/2 \in A$, e $r'_n(A) = r_n(A)$ caso contrário.

Definição 1. *Dizemos que um conjunto $S \subset \mathbb{N}$ é* Sidon *se $r'_n(S) \leq 1$ para todo $n \in \mathbb{N}$.*

Sidon propôs o seguinte problema, que encontra-se em aberto até os dias de hoje.

Problema 2. *Existe $A \subset \mathbb{N}$ tal que $r'_n(A) > 0$ e $r'_n(A)$ é "pequeno" (por exemplo, no máximo $10^{10^{10}}$) para todo n suficientemente grande?*

Paul Erdős obteve o seguinte resultado utilizando o método probabilístico.

Teorema 3. *Existe $A \subset \mathbb{N}$ tal que $r'_n(A) = \Theta(\log n)$ para todo n suficientemente grande.*

Estamos interessados em estudar o "tamanho" de conjuntos de Sidon. Podemos analisar conjuntos de Sidon em dois contextos, finito e infinito. Por enquanto, sobre o caso infinito, citaremos dois resultados de Erdős.

1) Todo $S \subset \mathbb{N}$ Sidon é tal que
$$\liminf_{n\to\infty} \frac{S(n)}{\sqrt{n}} = 0.$$

Notas por Guilherme Mota

2) Existe $S \subset \mathbb{N}$ Sidon tal que
$$\limsup_{n\to\infty} \frac{S(n)}{\sqrt{n}} \geq \frac{1}{2}.$$

Por enquanto, nos concentraremos no caso finito. Seja $F_2(n) = \max\{|S|\colon S \subset [n] \text{ é Sidon}\}$. O seguinte fato é simples de ser verificado.

Fato 4. $F_2(n) \leq 2\sqrt{n}$.

Demonstração. Suponha que $S \subset [n]$ seja um conjunto de Sidon. Temos que as $\binom{|S|}{2} + |S|$ somas da forma $s + s'$ com $s, s' \in S$ e $s \leq s'$ devem ser distintas. Mas observe que todas estas somas pertencem ao conjunto $\{2, 3, \ldots, 2n\}$. Desta forma,
$$\binom{|S|+1}{2} = \binom{|S|}{2} + |S| \leq 2n - 1.$$
Assim,
$$\frac{|S|^2}{2} \leq 2n - 1 \leq 2n,$$
de onde concluímos que $|S| \leq 2\sqrt{n}$. $\square$

Sidon observou que $F_2(n) \geq cn^{1/4}$ para algum $c > 0$ e todo $n \geq n_0$, onde $n_0 \in \mathbb{N}$. Podemos provar uma cota inferior do tipo $cn^{1/3}$ utilizando um método guloso, isto é, adicionando elementos a um conjunto S, inicialmente vazio, sempre que a adição de tal elemento não faça com que S deixe de ser Sidon (veja o exercício 1.1.1).

Veremos que $F_2(n) = (1 + o(1))\sqrt{n}$, isto é, $\lim_{n\to\infty}(F_2(n)/\sqrt{n}) = 1$. Erdős e Turán, em 1941, provaram que $\limsup_{n\to\infty}(F_2(n)/\sqrt{n}) \leq 1$, como veremos mais adiante no Teorema 5. Ademais, conjecturaram que $\lim_{n\to\infty}(F_2(n)/\sqrt{n}) = 1$. Três anos mais tarde, Chowla [3] mostrou que, de fato, $\liminf_{n\to\infty}(F_2(n)/\sqrt{n}) \geq 1$, onde a demonstração é feita utilizando resultados de Singer envolvendo corpos finitos [7].

Teorema 5 (Erdős–Turán [4])**.** $F_2(n) \leq \sqrt{n} + O(n^{1/4})$.

Demonstração. Seja $r = F_2(n)$ e $a_1 < \ldots < a_r$ um conjunto de Sidon S, de tamanho máximo, contido em $[n]$. Fixe um inteiro u, onde $1 \leq u < n$. Provaremos a cota $r < (n+u+n^2/u^2)^{1/2} + n/u$. Não é difícil ver que, tomando $u = \lfloor n^{3/4} \rfloor$, o resultado segue.

Considere os $n + u$ intervalos $I_m = [-u + m, -1 + m]$, onde $m = 1, 2, \ldots, n + u$. Note que $|I_m \cap \mathbb{Z}| = u$. Definindo $A_m = |S \cap I_m|$ como os elementos de S que estão em I_m, obtemos

$$\sum_{m=1}^{n+u} A_m = ru. \tag{1}$$

Considere agora um grafo bipartido G onde, em uma parte, estão todos os $\binom{r}{2}$ pares (a_i, a_j) de elementos de S, onde $i < j$ e, na outra parte, estão os $n + u$ intervalos I_m. Estimaremos a quantidade de arestas deste grafo através de dupla contagem.

Seja N a quantidade de arestas de G. Analisando os vizinhos dos intervalos I_m, obtemos que $N = \sum_{m=1}^{n+u} \binom{A_m}{2}$. Como $\binom{x}{2}$ é uma função convexa, temos, pela desigualdade de Jensen, que

$$
\begin{aligned}
N &\geq (n+u)\binom{\left(\sum_{m=1}^{n+u} A_m\right)/(n+u)}{2} \\
&= (n+u)\binom{ru/(n+u)}{2} \\
&= \frac{ru}{2}\left(\frac{ru}{n+u} - 1\right),
\end{aligned} \tag{2}
$$

onde a igualdade do meio segue de (1).

Fixe (a_i, a_j) com $i < j$. Suponha $a_j - a_i = d$. Então, há $u - d$ arestas incidentes ao vértice (a_i, a_j) em G. Entretanto, para um dado d, existe no máximo um par (a_i, a_j) com diferença d. Assim, temos que

$$
\begin{aligned}
N &\leq \sum_{d=1}^{u-1} (u - d) \\
&= \frac{u(u-1)}{2} \\
&= \binom{u}{2}.
\end{aligned} \tag{3}
$$

Portanto, de (2) e (3), obtemos $r((ru)/(n+u) - 1) \leq \binom{u}{2}$. Multiplicando por $(n + u)$ dos dois lados e lembrando que $u < n$, temos que $r(ru - 2n) < u(n + u)$, de onde concluímos que $ur^2 - 2nr - un - u^2 < 0$. Resolvendo esta inequação, o resultado segue.

□

1.1. **Problemas e exercícios.** Todos estão convidados a trabalhar no seguinte exercício.

1. Mostre que $F_2(n) \geq cn^{1/3}$ para todo n suficientemente grande e algum $c > 0$ (Dica: utilize o método guloso).

2. Conjuntos de Sidon - continuação

31/08/2010

Mostraremos que $F_2(n) \geq (1+o(1))\sqrt{n}$. Tal resultado, que segue de um caso particular do seguinte teorema, foi obtido, independentemente, por Erdős e Chowla.

Teorema 6 (Bose–Chowla [2])**.** *Se m é uma potência de primo e $h \geq 2$ é um inteiro, então existem inteiros $a_1, \ldots, a_m$ (considere $1 \leq a_1 \leq \ldots \leq a_m \leq m^h - 1$) tais que todas as somas*

$$a_{j_1} + \ldots + a_{j_h} \pmod{m^h - 1}$$

são diferentes para $1 \leq j_1 \leq \ldots \leq j_h \leq m$.

O seguinte corolário segue do teorema acima, fazendo $h = 2$.

Corolário 7. *Se m é uma potência de primo, então $F_2(m^2 - 1) \geq m$.*

Notando que a razão entre o n-ésimo e o $(n+1)$-ésimo primo tende a 1 quando n tende a infinito, temos, para n arbitrário, que $F_2(n) \geq (1+o(1))\sqrt{n}$. Sendo assim, para obter tal cota inferior, nos concentraremos em provar o Teorema 6. Para tal, precisamos comentar alguns resultados sobre corpos finitos.

Um corpo é uma tripla $(K, +, .)$ composta de um conjunto K e duas operações binárias sobre os elementos de K, onde $(K, +)$ e $(K^* = K \setminus \{0\}, .)$ são grupos abelianos e vale a distributividade, i.e., $a(b + c) = ab + ac$ para todos $a, b, c \in K$.

Exemplos importantes de corpos são o conjunto dos números racionais com as operações usuais de soma e multiplicação $(\mathbb{Q}, +, .)$ e a classe residual módulo p munida das operações de soma e multiplicação módulo p, para p primo, $(\mathbb{Z}/p\mathbb{Z}, +, .)$, que é um corpo finito (possui p elementos).

Os seguintes fatos sobre corpos finitos serão úteis. Em todos os fatos enunciados abaixo, p representa um número primo.

Fato 8. *Se $r \in \mathbb{N}$, com $r \geq 1$, então existe um corpo (único, a menos de isomorfismos) com p^r elementos. Denotamos tal corpo por $GF(p^r) = \mathbb{F}_{p^r}$.*

Fato 9. *Se $d|r$, então $GF(p^d)$ é um subcorpo de $GF(p^r)$.*

Fato 10. *$GF^*(p^r) = (GF(p^r))^*$ é um grupo cíclico, isto é, existe um elemento θ, chamado de* gerador *de $GF^*(p^r)$, tal que*

$$GF^*(p^r) = \langle\theta\rangle = \{\theta, \theta^2, \ldots, \theta^{p^r-1} = 1\}.$$

Fato 11. *Seja* $G = \langle \theta \rangle$ *finito com* $|G| > 1$ *e* H *um subgrupo de* G*. Então, temos que* $H = \langle \theta^h \rangle$*, onde* $h = \min\{q \colon \theta^q \in H,\ q > 0\}$*.*

Para entender o Fato 9, observe que se $d|r$, então $p^d - 1 | p^r - 1 = p^{dl} - 1$, para $r = dl$. Pondo

$$q = \frac{p^{dl} - 1}{p^d - 1} = 1 + p^d + \ldots + p^d(l-1),$$

temos que $GF^*(p^d) = \langle \theta^q \rangle = \{\theta^q, \theta^{2q}, \ldots, (\theta^q)^{p^d-1}\}$. Podemos ver $GF(p^r)$ como um espaço vetorial sobre o corpo $GF(p^d)$.

Dizemos que θ é *algébrico* sobre $GF(p^d)$ se existe um polinômio $p(x) \in GF(p^d)[x]$, isto é, $p(x)$ possui coeficientes em $GF(p^d)$, tal que $p(\theta) = 0$. Se θ é gerador, então temos que θ é algébrico, pois o polinômio $p(x) = x^{p^r-1} - 1$ é nulo quando $x = \theta$.

Seja θ algébrico. Dizemos que θ possui grau h sobre $GF(p^d)$ se h é o menor grau de um polinômio que é nulo em θ, isto é, $h = \min\{\text{grau de } p \colon 0 \not\equiv p \in GF(p^d)[x] \text{ com } p(\theta) = 0\}$. Se θ possui grau h em $GF(p^d)$ e $d|r$, então $\sum_{j=0}^{h-1} c_j \theta^j$ é uma enumeração (sem repetição) dos elementos de $GF(p^r)$, onde $c_j \in GF(p^d)$ para todo $0 \leq j \leq h-1$. Assim, temos que $(p^d)^h = p^r$, de onde concluímos que $hd = r$. O seguinte fato é fundamental para a prova do Teorema 6.

Fato 12. *Se* $d|r$ *e* $GF(p^d)$ *é subcorpo de* $GF(p^r)$ *com* $GF^*(p^r) = \langle \theta \rangle$*, então* θ *é algébrico sobre* $GF(p^d)$ *e possui grau* $h = r/d$*.*

Demonstração do Teorema 6. Seja m uma potência de primo e $h \geq 2$. Seja $m = p^u$, com p primo e $GF(p^u)$ subcorpo de $GF(p^{hu})$, com $GF^*(p^{hu}) = \langle \theta \rangle$. Considere a seguinte coleção de m elementos não nulos de $GF(p^{hu})$.

$$\{\theta + c \colon c \in GF(p^u)\} = \{\theta^{a_1}, \theta^{a_2}, \ldots, \theta^{a_m}\},$$

onde $1 \leq a_1 \leq \ldots \leq a_m \leq m^h - 1$.

Precisamos mostrar que os elementos $a_1, \ldots, a_m$ possuem a propriedade que queremos. Suponha que $1 \leq j_1 \leq \ldots \leq j_h \leq m$ e $1 \leq j'_1 \leq \ldots \leq j'_h \leq m$ são duas sequências distintas de índices. Queremos provar que $a_{j_1} + \ldots + a_{j_h} \neq a_{j'_1} + \ldots + a_{j'_h}$ módulo $m^h - 1$. Considere os polinômios lineares $L_a(x) = x + c$, onde $\theta + c = \theta^a$ e $c \in GF(p^u)$. Assim, temos que $L_a(x) \in GF(p^u)[x]$. Considere agora o seguinte polinômio em $GF(p^u)[x]$.

$$\begin{aligned} F(x) &= \prod_{\nu=1}^{h} L_{a_{j_\nu}}(x) - \prod_{\nu=1}^{h} L_{a_{j'_\nu}}(x) \\ &= (x + c_{j_1}) \ldots (x + c_{j_h}) - (x + c_{j'_1}) \ldots (x + c_{j'_h}), \end{aligned}$$

onde $\theta + c_{j_i} = \theta^{a_{j_i}}$ e $\theta + c_{j'_i} = \theta^{a_{j'_i}}$ para $1 \leq i \leq h$. Observe que $F(x)$ tem grau menor que h e $F(x) \not\equiv 0$. Assim, $F(\theta) \neq 0$, pois θ tem grau h e, portanto, o menor grau de um polinômio em $GF(p^u)[x]$ que é nulo em θ é h (veja Fato 12). Com isso, temos

$$\begin{aligned} 0 \neq F(\theta) &= (\theta + c_{j_1}) \ldots (\theta + c_{j_h}) - (\theta + c_{j'_1}) \ldots (\theta + c_{j'_h}) \\ &= \theta^{a_{j_1}} \theta^{a_{j_2}} \ldots \theta^{a_{j_h}} - \theta^{a_{j'_1}} \theta^{a_{j'_2}} \ldots \theta^{a_{j'_h}} \\ &= \theta^{a_{j_1} + \ldots + a_{j_h}} - \theta^{a_{j'_1} + \ldots + a_{j'_h}}. \end{aligned}$$

O resultado segue.

$\square$

3. Densidade da soma de conjuntos de inteiros positivos

14/09/2010 e 21/09/2010

Dado $A \subset \mathbb{N} = \{0, 1, 2, \ldots\}$, denotamos a densidade de Shnirelman por $\sigma(A) = \inf_{n \geq 1} A(n)/n$, onde $A(n) = |A \cap [n]|$. Definimos $A + B = \{a + b \colon a \in A,\ b \in B\}$. Em 1942, Mann provou o seguinte teorema sobre a densidade da soma de conjuntos de inteiros positivos, que é mais forte que o Teorema de Shnirelman.

Teorema 13 (Mann [6]). *Sejam $A, B \subset \mathbb{N}$ tais que $0 \in A \cap B$. Se $\sigma(A) + \sigma(B) \leq 1$, então*

$$\sigma(A + B) \geq \sigma(A) + \sigma(B).$$

A seguir, enunciamos alguns resultados importantes sobre a densidade de Shnirelman (para saber mais sobre o Teorema de Shnirelman e para ver provas dos Lemas 14, 15 e 16, veja seção 13 das notas de aula do primeiro semestre de 2010). Deste ponto em diante, vamos considerar $\sigma(A) = \alpha$ e $\sigma(B) = \beta$. Ademais, faremos $\sigma(C) = \gamma$, onde $C = A + B$.

Lema 14. *$\sigma(A) + \sigma(B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B)$.*

Lema 15. *Se $A(n) + B(n) < n - 1$, então $n \in A + B$.*

Lema 16. *Se $\sigma(A) > 0$, então existe $k \in \mathbb{N}$ tal que $\sum_{i=1}^{k} A = \mathbb{N}$.*

O seguinte lema é a parte principal da prova do Teorema 13.

Lema 17 (Lema Fundamental). *Se $n \in \mathbb{N}^*$, então existe $1 \leq m \leq n$ tal que*

$$C(n) - C(n - m) > (\alpha + \beta)m.$$

Demonstração. Dizemos que um conjunto N é *normal* em um segmento $[0, n]$ se, dados $f, f' \notin N$, então $f + f' - n \notin N$. Vamos considerar alguns casos.

- Caso 1: $n \in C$.

$$C(n) - C(n - 1) = 1 \geq (\alpha + \beta).$$

- Caso 2: $n \notin C$ e C é normal.

  Seja m o menor inteiro positivo tal que $m \notin C$ e considere s tal que $n - m < s < n$. Assim, $s \in C$ (caso contrário, $0 < s - n + m < m$, contrariando a normalidade de C). Com

[1]Os resultados desta seção foram apresentados pelo aluno Tássio Naia dos Santos

isso, $C(n) - C(n-m) = m-1$. Como $m \notin C$, temos, pelo Lema 15, que $A(m)+B(m) \leq m-1$, de onde concluímos que

$$C(n) - C(n-m) \geq A(m) + B(m) \geq (\alpha + \beta)m. \tag{4}$$

- Caso 3: $n \notin C$ e C não é normal.

  Como C não é normal, existem c, c' no segmento $[0, n]$ com $c, c' \notin C$ tal que $c + c' - n \in C$. Assim, existem $a \in A$ e $b \in B$ tais que

$$c + c' - n = a + b. \tag{5}$$

  Dizemos que o menor b satisfazendo a igualdade (5), para todos os valores possíveis de c, c' e a, é uma *base da extensão canônica*, denotada por β_0.

  Seja $C^* = \{c\colon c+c'-n = a+\beta_0,\ \text{com } c, c' \notin C \text{ e } a \in A\}$. Definimos a extensão canônica C_1 de C como $C_1 = C \cup C^*$. Ademais, definimos $B^* = \{\beta_0 + n - c\colon c \in C^*\}$. Pela definição de C^*, temos que $B^* = \{c' - a\colon c' \in C^*, \text{ para algum } a \in A\}$. Portanto, podemos concluir que $B^* \cap B = \varnothing$, pois, se existisse $b \in B^* \cap B$, então $b = c' - a$, para algum $a \in A$ e $c' \in C^*$, implicando que $c' \in C$, uma contradição.

  Seja $B_1 = B \cup B^*$ a extensão canônica de B, vamos provar que $A + B_1 = C_1$.

  - ($A + B_1 \subset C_1$): Sejam $a \in A$ e $b_1 \in B_1$. Vamos considerar dois casos.
    - $b_1 \in B$.

      Temos que $a + b_1 \in (A + B) = C \subset C_1$.
    - $b_1 \in B^*$.

      Temos que $c = a + b_1 = a + \beta_0 + n - c'$, com $c' \in C^*$. Portanto, $c + c' - n = a + \beta_0$, de onde concluímos que $c \in C^* \subset C_1$.
  - ($C_1 \subset A + B_1$): Seja $c_1 \in C_1$. Vamos considerar dois casos.
    - $c_1 \in C$.

      Existem $a \in A$ e $b \in B$ tais que $c_1 = a + b \in A + B \subset A + B_1$.
    - $c_1 \in C^*$.

      Existe $a \in A$ tal que $b^* = c_1 - a \in B^*$. Assim, $a + b^* = c_1 \in A + B^* \subset A + B_1$.

  Observe agora que $n \notin C_1$, pois, caso contrário, teríamos que $n + c' - n = a + \beta_0$, de onde concluímos que $c' \in C$, uma contradição.

Se C_1 não é normal, então A, B_1 e C_1 satisfazem as condições para uma nova extensão. Assim, conseguimos obter extensões $B = B_0 \subset B_1 \subset \ldots \subset B_h$ e $C = C_0 \subset C_1 \subset \ldots \subset C_h$, com $A + B_h = C_h$, onde C_h é normal e temos $B_{\mu+1} = B_\mu \cup B_\mu^*$ e $C_{\mu+1} = C_\mu \cup C_\mu^*$, para $0 \leq \mu \leq h-1$.

Para continuar a prova do Lema Fundamental, precisamos provar três lemas auxiliares, relacionados com as propriedades das extensões canônicas.

Lema 18. *$\beta_\mu > \beta_{\mu-1}$, para $1 \leq \mu \leq h-1$.*

Demonstração. Sabemos que $\beta_\mu \in B_\mu = B_{\mu-1} \cup B_{\mu-1}^*$. Se $\beta_\mu \in B_{\mu-1}^*$, então $\beta_\mu = \beta_{\mu-1} + n - c$, com $c \in C_{\mu-1}^*$, portanto, $c < n$. Assim, $\beta_\mu > \beta_{\mu-1}$. Por outro lado, se $\beta_\mu \in B_{\mu-1}$, então existem $c, c' \notin C_\mu$, com $a \in A$ tal que $c + c' - n = a + \beta_\mu \in C_\mu$. Mas observe que, como $\beta_\mu \in B_{\mu-1}$, também é verdade que $c + c' - n = a + \beta_\mu \in C_{\mu-1}$. Por causa da minimalidade de $\beta_{\mu-1}$, temos que $\beta_\mu \geq \beta_{\mu-1}$. Se $\beta_\mu = \beta_{\mu-1}$, pela definição de $C_{\mu-1}^*$, teríamos que $c \in C_{\mu-1}^*$ e $c' \in C_{\mu-1}^*$, mas isto é falso, pois $c, c' \notin C_\mu \supset C_{\mu-1}^*$. Portanto, $\beta_\mu > \beta_{\mu-1}$. $\square$

Lema 19. *Seja m o menor inteiro positivo tal que $m \notin C_h$. Se $c \in C_\mu^*$ $(0 \leq \mu \leq h-1)$ e $n - m < c < n$, então $c > n - m + \beta_\mu$.*

Demonstração. Como $n - m < c < n$, temos que $0 < c - n + m < m$. Portanto, pela definição de m, segue que $c - n + m \in C_h$. Mas lembre que $C_h = C_\mu \cup C_\mu^* \cup C_{\mu+1}^* \cup \ldots \cup C_{h-1}^*$. Dividiremos a prova em casos.

- Caso 1: $c - n + m \in C_\mu$.
  Existem $a \in A$ e $b \in B_\mu$ tais que $c - n + m = a + b > a + \beta_\mu$, pois se $c - n + m = a + \beta_\mu$, teríamos $m \in C_\mu^*$ (que é falso), uma vez que $m \notin C_h \supset C_\mu$ e $c \notin C_\mu$. Portanto, temos que $c - n + m > a + \beta_\mu \geq \beta_\mu$.
- Caso 2: $c - n + m \in C_\nu^*$ $(\mu \leq \nu \leq h-1)$.
  Existem $a \in A$ e $c'' \in C_\nu^*$ tais que $c - n + m \geq c - n + m - a = \beta_\nu + n - c'' > \beta_\nu$. Portanto, pelo Lema 18, temos que $c - n + m > \beta_\mu$.

$\square$

Lema 20. *Se m é o menor inteiro positivo tal que $m \notin C_h$, então, para $1 \leq \mu \leq h-1$,*

$$C_\mu^*(n) - C_\mu^*(n-m) = B_\mu^*(m-1).$$

Demonstração. Vamos analisar a expressão $b = \beta_\mu + n - c$. Temos que $b \in B_\mu^*$ se e somente se $c \in C_\mu^*$. Se também é verdade que $n - m + \beta_\mu < c < n$, então $\beta_\mu < b < m$ e vice-versa.

Portanto,

$$C_\mu^*(n) - C_\mu^*(n - m + \beta_\mu) = B_\mu^*(m) - B_\mu^*(\beta_\mu).$$

Mas, como $b = \beta_\mu + n - c$ e $0 \leq c < n$, temos $b > \beta_\mu$. Assim, $B_\mu^*(\beta_\mu) = 0$. Pelo Lema 19, temos $C_\mu^*(n - m + \beta_\mu) = C_\mu^*(n - m)$. Portanto,

$$\begin{aligned} C_\mu^*(n) - C_\mu^*(n - m) &= B_\mu^*(m) - B_\mu^*(\beta_\mu) \\ &= B_\mu^*(m - 1), \end{aligned}$$

onde a última desigualdade segue do fato de $m \notin B_\mu^*$. □

De posse do Lema 20, podemos completar a prova do Lema Fundamental. Como C_h é normal, sabemos que $C_h(n) - C_h(n-m) \geq A(m) + B_h(m)$, onde m é o menor inteiro positivo tal que $m \notin C_h$. Mas C_h e B_h são uniões de subconjuntos disjuntos. Assim,

$$C_h(n) - C_h(n - m) = C(n) - C(n - m) + \sum_{\mu=0}^{h-1} \left(C_\mu^*(n) - C_\mu^*(n - m)\right);$$

$$B_h(m) = B(m) + \sum_{\mu=0}^{h-1} B_\mu^*(m).$$

Portanto,

$$C_h(n) - C_h(n - m) + \sum_{\mu=0}^{h-1} \left(C_\mu^*(n) - C_\mu^*(n - m)\right) \geq A(m) + B(m) + \sum_{\mu=0}^{h-1} B_\mu^*(m).$$

Pelo Lema 20,

$$C_h(n) - C_h(n - m) \geq A(m) + B(m).$$

Assim, o Lema Fundamental está provado.

□

Daremos agora uma prova do Teorema 13 dada por Artin e Scherk em 1943 [1].

Demonstração do Teorema 13. Pelo Lema 17 (Lema Fundamental), temos, para $n \in \mathbb{N}^*$, que

$$\begin{aligned} C(n) - C(n - m_1) &\geq (\alpha + \beta)m_1 \\ C(n - m_1) - C(n - m_1 - m_2) &\geq (\alpha + \beta)m_2 \\ &\vdots \\ C(n - m_1 - \ldots - m_{k-1}) - C(0) &\geq (\alpha + \beta)m_k. \end{aligned}$$

Somando as desigualdades acima, obtemos $C(n) - C(0) \geq (\alpha + \beta)(m_1 + \ldots + m_k)$, de onde concluímos que $C(n)/n \geq (\alpha + \beta)$. Assim, o resultado segue. $\square$

4. Jogo de Penney

28/09/2010 – 30/11/2010

Considere o seguinte jogo para dois jogadores, A e B, conhecido como "Penney's game": temos uma moeda honesta que, ao ser lançada, nos dá o resultado "sucesso" (S) ou "fracasso" (F), cada um com probabilidade 1/2. Cada jogador escolhe uma sequência de tamanho $n \geq 3$ dentro do espaço de sequências $\{S, F\}^n$. A moeda é jogada repetidamente até que apareça a sequência de um dos jogadores. O jogador cuja sequência aparecer primeiro vence o jogo.

A primeira observação é que, para toda sequência escolhida por A, existe uma sequência que, se escolhida por B, o deixa com uma chance maior de vencer. Vamos analisar o caso em que as sequências possuem tamanho $n = 3$. Deste ponto em diante, sejam X e Y, respectivamente, os instantes em que temos a primeira ocorrência das sequências escolhidas por A e B (Vamos considerar que, mesmo que um jogador vença, o jogo continua até a ocorrência da sequência escolhida pelo outro jogador). Se SSS é a sequência escolhida por A, ao escolher a sequência FSS, o jogador B possui 7 vezes mais chances de vencer do que o jogador A, ou seja, $\Pr(A \text{ vencer}) = \Pr(X < Y) = 1/8$ e $\Pr(B \text{ vencer}) = \Pr(Y < X) = 7/8$. De fato, ao aparecer um F, o jogador A fica impossibilitado de vencer. Com isso, sua única chance de vitória é que sua sequência (SSS) apareça inicialmente. Portanto, realmente temos $\Pr(X < Y) = 1/8$.

Considerando uma moeda qualquer, com probabilidade de sucesso $0 < q < 1$ e probabilidade de fracasso $p = 1 - q$, podemos calcular qual o menor valor de q para que o jogador A, que escolheu a sequência SSS, tenha chance maior de vitória do que o jogador B, que escolheu a sequência FSS. Pela mesma análise feita no parágrafo anterior, conseguimos ver que $\Pr(X < Y) = q^3$. Assim, para que $\Pr(X < Y) > \Pr(Y < X)$, é necessário que $q > 1/2^{1/3}$.

Temos, neste ponto, um fenômeno curioso. Pois, fazendo $1/2 < q < 1/2^{1/3}$, podemos observar que ao lançar 3 vezes a moeda, a chance de aparecer a sequência SSS é maior que a de aparecer a sequência FSS, porém, vimos que é mais provável que, ao lançar repetidamente a moeda, vejamos a sequência FSS antes da sequência SSS. Assim, temos respostas diferentes para as seguintes perguntas.

- Qual sequência é mais provável no lançamento de 3 moedas?
- Qual sequência aparece primeiro se a moeda é lançada repetidas vezes?

Considere agora, invés de sequências de tamanho 3, sequências de tamanho n. Seja $SSS \ldots S$ a sequência escolhida por A e $FSS \ldots S$ a sequêcia escolhida por B. Pelo que já foi discutido, é fácil

[1] Os resultados desta seção foram apresentados pelo professor Miguel Abadi.

ver que $\Pr(X < Y) = q^n$. Portanto, para que A tenha uma chance de vencer que seja maior que a chance de B, é necessário que $q > 1/2^{1/n}$. Desta forma, podemos concluir que, ao aumentar o valor de n, só pioramos a situação para o jogador B, pois $q \to 1$ quando n tende a infinito. A ocorrência deste fenômeno está relacionada ao "encaixe" das sequências, que definiremos mais à frente.

Uma outra pergunta a ser feita diz respeito ao valor esperado do tempo de aparição das sequências. Seja $\{A_1, \ldots, A_{2^n}\}$ o conjunto das sequências possíveis de tamanho n. Denotamos por t_i o tempo até a aparição da sequência A_i. Qual sequência A_i é tal que, em média, t_i é mínimo? Formalmente, queremos saber qual sequência A_i possui menor valor de $\mathbb{E}(t_i) = \sum_{k=0}^{\infty} k \Pr(t_i = k)$, dentre todas as sequências. Se $m = \min_{i=0}^{2^n} \mathbb{E}(t_i)$, queremos saber que sequências A_i são tais que $\mathbb{E}(t_i) = m$.

Sejam $\mathcal{A} = \{S, F\}$ e $n \in \mathbb{N}$. Denotamos por $\mathcal{A}^n$ o espaço de sequências de tamanho n formadas por elementos de $\mathcal{A}$.

Definição 21. *Dada uma sequência $x = (a_1, \ldots, a_n) \in \mathcal{A}^n$, dizemos que x possui um inteiro positivo d como* período *se x se repete após a posição d, isto é, $(a_{d+1}, \ldots, a_n) = (a_1, \ldots, a_{n-d})$. Ademais, denotamos por $P_n(k)$ o conjunto das sequências com n elementos que possuem k como período.*

Definição 22. *definimos o tempo de encaixe $T_n(x)$ da sequência x como sendo o menor período de x, isto é, $T_n(x) = \min\{d \colon (a_{d+1}, \ldots, a_n) = (a_1, \ldots, a_{n-d})\}$.*

Claramente, $1 \leq T_n(x) \leq n$. Desejamos estudar o comportamento de $T_n \colon \mathcal{A}^n \to \{1, \ldots, n\}$. Veja que, se $m \neq n$, então T_n e T_m estão definidas em espaços diferentes. Podemos uniformizar os espaços considerando o domínio $\{0,1\}^{\mathbb{N}}$, onde $\mathbb{T}_n \colon \{0,1\}^{\mathbb{N}} \to \{0,1\}^n$ é a projeção das primeiras n coordenadas de uma sequência. Assim, fazemos $\tilde{T}_n(x) = T_n(\mathbb{T}_n(x))$. Pensaremos em T_n, algumas vezes como definido em $\{0,1\}^n$, algumas vezes em $\{0,1\}^{\mathbb{N}}$.

Observe que, se $(b_1, b_2, \ldots, b_n)$ é uma sequência fixa em $\{0,1\}^n$ e tomamos o conjunto de sequências $A_n = \{(a_1, a_2, \ldots) \colon (a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)\}$, então T_n é constante sobre A_n. Veja também que se $x = (1, 1, \ldots)$, então $T_n(x) = 1$. Porém, intuitivamente, a idéia é que o valor de T_n seja pequeno somente para poucas sequências. Isto é, T_n deve ter valor assintoticamente igual a n para a grande maioria das sequências. De fato, isto é o que acontece e pode ser visto no seguinte teorema, onde definimos os seguintes conjuntos: $\{T_n = k\} = \{x \in \{0,1\}^n \colon T_n(x) = k\}$ e $\{T_n < k\} = \{x \in \{0,1\}^n \colon T_n(x) < k\}$.

Teorema 23. *Para todo $0 < \varepsilon < 1$,*

$$\lim_{n \to \infty} \frac{\left|\left\{\frac{T_n}{n} < 1 - \varepsilon\right\}\right|}{2^n} = 0.$$

Antes de provar o teorema acima, vamos estudar os conjuntos $\{T_n = k\}$ com $1 \leq k \leq n$. O seguinte teorema é um resultado clássico, conhecido como Teorema de Fine e Wilf, lembrando que dados inteiros positivos p e q, denotamos o máximo divisor comum de p e q por (p, q).

Teorema 24 (Fine–Wilf [5])**.** *Se p e q são inteiros positivos, então toda sequência com tamanho pelo menos $p + q - (p, q)$ que possui períodos p e q, possui também o período (p, q). Ademais, existe uma sequência de tamanho $p + q - (p, q) - 1$ com períodos p e q que não possui período (p, q).*

Para a prova do teorema acima, veja o exercício 4.1.1.

Definição 25. *Seja $1 \leq k \leq n-1$. Definimos $B(k) = \{x \in \{0, 1\}^{\mathbb{N}} \colon x = (x_1, \ldots, x_k, x_1, \ldots, x_k, \ldots)\}$. Ademais, definimos $B_n(k) = \mathbb{T}_n(B(k))$.*

Deste ponto em diante, denotaremos $(x_1, \ldots, x_n)$ por x_1^n. Não é difícil ver que $\{T_n = k\} \subset B_n(k)$. Porém, a sequência $x = (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$ pertence a $B_{12}(4)$ mas $T_{12}(x) = 2 \neq 4$, logo, $\{T_n = k\} \neq B_n(k)$. Isto acontece por causa da repetição de padrões que ocorre dentro da sequência. Claramente, se $x \in B_n(k)$, então $T_n(x) \leq k$. Ademais, se supormos $k \leq \lfloor n/2 \rfloor$, então temos o seguinte resultado.

Lema 26. *Se $k \leq \lfloor n/2 \rfloor$, então $B_n(k) = \{x \in \{0, 1\}^n \colon T_n(x) = d,\ d | k\}$.*

Demonstração. Se x é uma sequência de tamanho n com $T_n(x) = d$, onde d divide k, então temos que $x \in B_n(k)$. Suponha agora que $x \in B_n(k)$. Desta forma, $x = (y^r, \bar{y})$, onde y^r denota uma sequência formada pela concatenação de r sequências $y = (y_1, \ldots, y_k)$, e $\bar{y} = (y_1, \ldots, y_l)$, com $0 \leq l < k$. Considere $y = z^q$ de forma que q seja o maior possível (z seja o menor possível). Por exemplo, fazendo $k = 6$, se $x = (1, 2, 3, 4, 5, 6, 1, 2, 3, 4, 5, 6)$, temos $y = (1, 2, 3, 4, 5, 6)$ e $z = (1, 2, 3, 4, 5, 6)$ com $q = 1$, e se $x = (1, 2, 3, 1, 2, 3, 1, 2, 3, 1, 2, 3)$, temos $y = (1, 2, 3, 1, 2, 3)$ e $z = (1, 2, 3)$ com $q = 2$. Assim, seja $d = |z|$. Claramente, $d | k$ e x possui período d. Queremos mostrar que d é o menor período de x, isto é, que $T_n(x) = d$. É óbvio que $T_n(x) \leq d$, uma vez que d é período de x. Suponha, por contradição, que $T_n(x) < d$, isto é, existe $d' < d$ que é período de x. Desta forma, como $k \leq \lfloor n/2 \rfloor$, temos que $n \geq d + d' - (d, d')$ e, pelo Teorema 24, concluímos que x possui período (d, d'), uma contradição com a escolha de z e q, pois z seria da forma u^s, com $s \geq 2$, para alguma sequência u. □

Se $k > n/2$, não é possível obter a igualdade do Lema 26. Por exemplo, observe que a sequência $x = (0, 0, a_3, \ldots, a_{n-2}, 0, 0)$ com $a_i \neq 0$ para $3 \leq i \leq n-2$, está em $B_n(n-1)$ mas $T_n(x) = n-2$, que não divide $n - 1$.

Demonstração do Teorema 23. Fixe $0 < \varepsilon < 1$. Temos

$$\{T_n < (1-\varepsilon)n\} \subset \bigcup_{j=1}^{(1-\varepsilon)n} B_n(j).$$

Portanto, observando que $|B_n(j)| = 2^j$,

$$\begin{aligned}
\frac{|\{T_n < (1-\varepsilon)n\}|}{2^n} &\leq \frac{1}{2^n} \sum_{j=1}^{(1-\varepsilon)n} 2^j \\
&\leq \frac{2^{(1-\varepsilon)n+1}}{2^n} \\
&\to 0.
\end{aligned}$$

□

Estudaremos agora alguns conjuntos de sequências intimamente relacionados com os conjuntos $B_n(k)$.

Definição 27. *Seja $1 \leq k \leq n-1$. Definimos $R_n(k) = \{x \in \{0,1\}^n \colon x_1^k = x_{n-k+1}^n\}$, isto é, $R_n(k)$ é o conjunto das sequências com n elementos onde seus primeiros k elementos são iguais aos seus últimos k elementos.*

Os próximos dois lemas mostram que $P_n(k) = B_n(k) = R_n(n-k)$, para $1 \leq k \leq n-1$.

Lema 28. *$B_n(k) = P_n(k)$, para $1 \leq k \leq n-1$.*

Demonstração. Se $x \in B_n(k)$, então é claro que k é período de x. Se $x = (x_1, \ldots, x_n) \in P_n(k)$, então $(x_{k+1}, \ldots, x_n) = (x_1, \ldots, x_{n-k})$. Assim, temos que $(x_{2k+1}, \ldots, x_n) = (x_1, \ldots, x_{n-2k})$, uma vez que $(x_{2k+1}, \ldots, x_n) = (x_{k+1}, \ldots, x_{n-k}) = (x_1, \ldots, x_{n-2k})$, e assim por diante. Portanto, é verdade que $x \in B_n(k)$. □

Lema 29. *$R_n(n-k) = P_n(k)$ para $1 \leq k \leq n-1$.*

Demonstração. A prova segue diretamente das definições de $P_n(k)$ e $R_n(n-k)$. □

Sabendo que $|B_n(k)| = 2^k$, temos, pelos Lemas 28 e 29, que $|R_n(k)| = 2^{n-k}$. Assim, o seguinte resultado é imediato, onde $\Pr(R_n(k)) = |R_n(k)|/2^n$.

Lema 30. *A seguinte igualdade é verdadeira para todo inteiro positivo $k \leq n/2 - 1$.*

$$\Pr\left(R_n(k)\right) = \Pr\left(R_{2(\lfloor \frac{n}{2} \rfloor - 1)}(k)\right).$$

Lema 31. *A seguinte igualdade é verdadeira para todo inteiro positivo $k \leq n/2 - 1$.*

$$\Pr\left(\bigcup_{k \leq j \leq \frac{n}{2}-1} R_n(j)\right) = \Pr\left(\bigcup_{k \leq j \leq \frac{n}{2}-1} R_{2(\lfloor \frac{n}{2} \rfloor -1)}(j)\right)$$

Demonstração. Se $x_1^n \in R_n(j)$, então $x_1^n = x_1^j w_1 w w_2 x_1^j$, onde $w_1, w_2 \in \{0,1\}^{\lfloor n/2 \rfloor -1-j}$ e $w \in \{0,1\}^l$, com $l = n - 2(\lfloor n/2 \rfloor - 1)$. Desta forma, dada a sequência x_1^n, existem 2^l sequências tais que, removendo w, obtemos a subsequência $x_1^j w_1 w_2 x_1^j$ de x_1^n. Portanto,

$$\Pr\left(\bigcup_{k \leq j \leq \frac{n}{2}-1} R_n(j)\right) = \frac{\left|\bigcup_{k \leq j \leq \frac{n}{2}-1} R_n(j)\right|}{2^n}.$$

$$\Pr\left(\bigcup_{k \leq j \leq \frac{n}{2}-1} R_{2(\lfloor \frac{n}{2} \rfloor -1)}(j)\right) = \frac{\left|\bigcup_{k \leq j \leq \frac{n}{2}-1} R_{2(\lfloor \frac{n}{2} \rfloor -1)}(j)\right|}{2^{n-l}} = \frac{\left|\bigcup_{k \leq j \leq \frac{n}{2}-1} R_n(j)\right|}{2^n}.$$

□

Observe que a probabilidade de uma sequência $w \in \{0,1\}^k$ ser obtida através de k lançamentos sucessivos de uma moeda que dá cara com probabilidade p e coroa com probabilidade $1-p$, onde cara representa 1 e coroa representa 0, é $p^{i_w}(1-p)^{k-i_w}$, com i_w sendo a quantidade de posições que possuem valor 1 em w. Assim,

$$\begin{aligned}
\sum_{w_k \in \{0,1\}^k} \Pr(w_k)^m &= \sum_{w_k \in \{0,1\}^k} (p^m)^{i_w}((1-p)^m)^{k-i_w} \\
&= \sum_{i=0}^{k} \binom{k}{i} (p^m)^i((1-p)^m)^{k-i} \\
&= (p^m + (1-p)^m)^k.
\end{aligned}$$

Fazendo $p = 1/2$, temos $\sum_{w_k \in \{0,1\}^k} \Pr(w_k)^m = 1/2^{(m-1)k}$. Desta forma, se $k|n$, então

$$\begin{aligned}
\Pr(B_n(k)) &= \sum_{x_1^k \in \{0,1\}^k} \Pr(x_1^k)^{n/k} \\
&= \left(\frac{1}{2}\right)^{n-k}.
\end{aligned}$$

Definição 32. *Dada uma sequência $x \in \{0,1\}^n$, definimos $S_n(x) = n - T_n(x)$, isto é, $S_n(x)$ é o tamanho máximo das sobreposições de x.*

Como usual, $\{S_n = k\} = \{x \in \{0,1\}^n \colon S_n(x) = k\}$ e $\{S_n \geq k\} = \{x \in \{0,1\}^n \colon S_n(x) \geq k\}$.

Teorema 33. *Para $k \geq 1$, as seguintes asserções são verdadeiras, com $a_{n,k}$, a_k, $b_{n,k}$, $b_k \in [0,1]$.*

a) $\Pr(S_n \geq k) = (1/2)^k + a_{n,k}$;
b) $\Pr(S_n = k) = (1/2)^k - b_{n,k}$;
c) $\lim_{n\to\infty} \Pr(S_n \geq k) = (1/2)^k + a_k$;
d) $\lim_{n\to\infty} \Pr(S_n = k) = (1/2)^k - b_k$.

Demonstração. Observe que $|\{S_n = k\}| = |\{S_n \geq k\}| - |\{S_n \geq k+1\}|$. Vamos assumir $n \geq 4k$ e, por clareza na exposição dos resultados, vamos considerar n par.

Demonstração de a).

Uma vez que $\{S_n \geq k\} = \bigcup_{j=k}^{n-1} R_n(j)$, temos o seguinte, onde $G_n(k) = \Pr(S_n \geq k)$.

$$\begin{aligned}
G_n(k) &= \Pr\left(\bigcup_{j=k}^{n-1} R_n(j)\right) \\
&= \Pr\left(\bigcup_{j=k}^{n/2-1} R_n(j)\right) + \Pr\left(\bigcup_{j=n/2}^{n-1} R_n(j) \Bigg\backslash \bigcup_{j=k}^{n/2-1} R_n(j)\right) \\
&= \Pr\left(\bigcup_{j=k}^{n/2-1} R_{n-2}(j)\right) + \Pr\left(\bigcup_{j=n/2}^{n-1} R_n(j) \Bigg\backslash \bigcup_{j=k}^{n/2-1} R_n(j)\right) \\
&= \Pr\left(\bigcup_{j=k}^{n-3} R_{n-2}(j)\right) + \Pr\left(\bigcup_{j=n/2}^{n-1} R_n(j) \Bigg\backslash \bigcup_{j=k}^{n/2-1} R_n(j)\right) \\
&\qquad - \Pr\left(\bigcup_{j=n/2}^{n-3} R_{n-2}(j) \Bigg\backslash \bigcup_{j=k}^{n/2-1} R_{n-2}(j)\right) \\
&= G_{n-2}(k) + \Pr\left(\bigcup_{j=n/2}^{n-1} R_n(j) \Bigg\backslash \bigcup_{j=k}^{n/2-1} R_n(j)\right) \\
&\qquad - \Pr\left(\bigcup_{j=n/2}^{n-3} R_{n-2}(j) \Bigg\backslash \bigcup_{j=k}^{n/2-1} R_{n-2}(j)\right).
\end{aligned}$$

Similarmente, temos

$$G_{n-2}(k) = G_{n-4}(k) + \Pr\left(\bigcup_{j=n/2-1}^{n-3} R_{n-2}(j) \Bigg\backslash \bigcup_{j=k}^{n/2-2} R_{n-2}(j)\right) - \Pr\left(\bigcup_{j=n/2-1}^{n-5} R_{n-4}(j) \Bigg\backslash \bigcup_{j=k}^{n/2-2} R_{n-4}(j)\right).$$

Portanto, iterando esta fórmula, obtemos

$$\begin{aligned} G_n(k) &= G_{2k}(k) + \Pr\left(\bigcup_{j=n/2}^{n-1} R_n(j) \Bigg\backslash \bigcup_{j=k}^{n/2-1} R_n(j)\right) \\ &\quad + \sum_{i=k+1}^{n/2} \Pr\left(R_{2i}(i) \Bigg\backslash \bigcup_{j=k}^{i-1} R_{2i}(j)\right) \\ &\quad - \Pr\left(\bigcup_{j=k+1}^{2k-1} R_{2k}(j) \Bigg\backslash \bigcup_{j=k}^{k} R_{2k}(j)\right) \\ &= \Pr(R_{2k}(k)) + a_{n,k} \\ &= \Pr(B_{2k}(k)) + a_{n,k} \\ &= \left(\frac{1}{2}\right)^k + a_{n,k}, \end{aligned}$$

onde fizemos

$$a_{n,k} = \Pr\left(\bigcup_{j=n/2}^{n-1} R_n(j) \Bigg\backslash \bigcup_{j=k}^{n/2-1} R_n(j)\right) + \sum_{i=k+1}^{n/2} \Pr\left(R_{2i}(i) \Bigg\backslash \bigcup_{j=k}^{i-1} R_{2i}(j)\right).$$

Demonstração de b).

Observe que $\Pr(S_n = k) = G_n(k) - G_n(k+1)$. Desta forma, temos

$$\begin{aligned}
\Pr(S_n = k) = \Pr(R_{2k}(k)) - \Pr(R_{2(k+1)}(k+1) \\
- \Pr\left(\bigcup_{j=n/2}^{n-1} (R_n(j) \cap R_n(k)) \Big\backslash \bigcup_{j=k+1}^{n/2-1} R_n(j)\right) \\
- \sum_{i=k+2}^{n/2} \Pr\left(R_{2i}(i) \cap R_{2i}(k) \Big\backslash \bigcup_{j=k+1}^{i-1} R_{2i}(j)\right) \\
+ \Pr\left(R_{2(k+1)}(k+1) \Big\backslash \bigcup_{j=k}^{k} R_{2(k+1)}(j)\right).
\end{aligned}$$

Desta forma, obtemos

$$\begin{aligned}
\Pr(S_n = k) &= \Pr(R_{2k}(k)) - \Pr\left(\bigcup_{j=n/2}^{n-1} R_n(j) \cap R_n(k) \Big\backslash \bigcup_{j=k+1}^{n/2-1} R_n(j)\right) \\
&\quad - \sum_{i=k+1}^{n/2} \Pr\left(R_{2i}(i) \cap R_{2i}(k) \Big\backslash \bigcup_{j=k+1}^{i-1} R_{2i}(j)\right) \\
&= \left(\frac{1}{2}\right)^k - b_{n,k}.
\end{aligned}$$

onde fizemos

$$b_{n,k} = \Pr\left(\bigcup_{j=n/2}^{n-1} R_n(j) \cap R_n(k) \Big\backslash \bigcup_{j=k+1}^{n/2-1} R_n(j)\right) + \sum_{i=k+1}^{n/2} \Pr\left(R_{2i}(i) \cap R_{2i}(k) \Big\backslash \bigcup_{j=k+1}^{i-1} R_{2i}(j)\right)$$

Demonstração de c) e d).

Para provar c), fazemos $a_k = \sum_{k+1}^{\infty} \Pr(R_{2i}(i) \backslash \bigcup_{j=k}^{i-1} R_{2i}(j))$ e vamos mostrar que $\lim_{n\to\infty} a_{n,k} = a_k$. Para isto, basta observar que $\Pr(\cup_{j=n/2}^{n-1} R_n(j) \setminus \cup_{j=k}^{n/2-1} R_n(j)) \leq \sum_{j=n/2}^{n-1} \Pr(R_n(j)) = \sum_{j=1}^{n/2}(B_n(j))$, mas $\sum_{j=1}^{n/2}(B_n(j))$ tende a zero quando $n \to \infty$. Analogamente, d) segue. $\square$

O seguinte lema limita superiormente $\Pr(\bigcup_{j=1}^{l} B_n(j))$ quando $l < n/2$.

Lema 34. *Para todo $l < n/2$, existe $C > 0$ tal que*

$$\Pr\left(\bigcup_{j=1}^{l} B_n(j)\right) = \Pr\left(\bigcup_{j=n-l}^{n-1} R_n(j)\right) \leq C\left(\frac{1}{\sqrt{2}}\right)^{n-l}.$$

Demonstração. Considere r tal que $n = j\lfloor n/j \rfloor + r$, com $0 \le r < j$. Se $w = w_j \dots w_j w_r \in B_n(j)$, onde $w_j = w_r w_{j-r}$. Lembrando que $\sum_{w_m \in \{0,1\}^m} \Pr(w_m)^k = (p^k + (1-p)^k)^m$ e denotando $p^k + (1-p)^k$ por m_k, temos

$$\begin{aligned}
\Pr(B_n(j)) &\le \sum_{w_j \in \{0,1\}} \Pr(w_j)^{\lfloor n/j \rfloor} \\
&= \left(p^{\lfloor n/j \rfloor} + (1-p)^{\lfloor n/j \rfloor}\right)^j \\
&= \left[\left(m_{\lfloor n/j \rfloor}\right)^{\frac{1}{\lfloor n/j \rfloor}}\right]^{j\lfloor n/j \rfloor} \\
&\le \left[\left(m_{\lfloor n/j \rfloor}\right)^{\frac{1}{\lfloor n/j \rfloor}}\right]^{n-j} \\
&\le (m_2)^{\frac{n-j}{2}},
\end{aligned}$$

onde a última desigualdade segue do fato de $(m_\alpha)^{1/\alpha} \le (m_2)^{1/2}$ para todo $\alpha \ge 2$. Com isso, temos, para algum $C > 0$,

$$\begin{aligned}
\sum_{j=1}^{l} \Pr(B_n(j)) &\le \sum_{j=1}^{l} (m_2)^{(n-j)/2} \\
&= \frac{(m_2)^{(n-l)/2} - (m_2)^{n/2}}{1 - (m_2)^{1/2}} \\
&\le C(m_2)^{(n-l)/2} \\
&= C\left(\sqrt{p^2 + (1-p)^2}\right)^{n-l} \\
&= C\left(\frac{1}{\sqrt{2}}\right)^{n-l},
\end{aligned}$$

onde fizemos $p = 1/2$ na última igualdade. □

Seria interessante obter, por exemplo, limites superiores para os seguintes valores.

$$|\Pr(S_n \ge k) - \lim \Pr(S_n \ge k)| = |a_{n,k} - a_k|;$$

$$|\Pr(S_n = k) - \lim \Pr(S_n = k)| = |b_{n,k} - b_k|.$$

A seguinte proposição nos dá uma idéia de que tipo de limite é possível conseguir.

Proposição 35. *Dado $k \ge 1$, para todo $n \ge 4k$, existe $C > 1$ tal que*

a)
$$\sum_{i=n/2+1}^{\infty} \Pr(R_{2i}(i) \cap R_{2i}(k)) = \left(\frac{m_4}{m_2^2}\right)^k \frac{m_2^{n/2+1}}{1 - m_2};$$

b)
$$m_2^{n/2}\left(\frac{m_3}{m_2^{3/2}}\right)^k \leq \Pr\left(\bigcup_{j=n/2}^{n-1} R_n(j)\cap R_n(k)\Bigg\backslash\bigcup_{j=k+1}^{n/2-1} R_n(j)\right) \leq C m_2^{n/2}\left(\frac{m_3}{m_2^{3/2}}\right)^k.$$

Demonstração. Por simplicidade, assumimos n par. Seja $w \in (R_{2i}(i) \cap R_{2i}(k))$. Assim, temos que $w = w_1w_1$ e $w = w_2zw_2$, com $|w_1| = i$ e $|w_2| = k$, de onde concluímos que $w = w_2yw_2w_2yw_2$, para algum y tal que $|y| = i - 2k$. Portanto, $\Pr(w) = \Pr(w_2)^4 \Pr(y)^2$. Desta forma, temos

$$\begin{aligned}\Pr(R_{2i}(i)\cap R_{2i}(k)) &= \sum_{w_2\in\{0,1\}^k}\Pr(w_2)^4\sum_{y\in\{0,1\}^{i-2k}}\Pr(y)^2\\ &= m_4^k m_2^{i-2k}.\end{aligned}$$

Somando os termos a partir de $n/2+1$, temos

$$\begin{aligned}\sum_{i=n/2+1}^{\infty}\Pr(R_{2i}(i)\cap R_{2i}(k)) &= \sum_{i=n/2+1}^{\infty} m_4^k m_2^{i-2k}\\ &= \left(\frac{m_4}{m_2^2}\right)^k\frac{m_2^{n/2+1}}{1-m_2}.\end{aligned}$$

Isto é, provamos o ítem a).

Observe que $B_n(k) \subset B_n(2k) \subset \ldots \subset B_n(\ell)$, para todo ℓ múltiplo de k. Usando a relação $R_n(k) = B_n(n-k)$, obtemos

$$\begin{aligned}\bigcup_{j=k+1}^{n/2-1} R_n(j) &= \bigcup_{j=n/2+1}^{n-(k+1)} B_n(j)\\ &= \bigcup_{j=1}^{n/2-k} B_n(j)\cup\bigcup_{j=n/2+1}^{n-(k+1)} B_n(j).\end{aligned}$$

Assim,

$$\begin{aligned}\bigcup_{j=n/2}^{n-1} R_n(j)\Bigg\backslash\bigcup_{j=k+1}^{n/2-1} R_n(j) &= \bigcup_{j=1}^{n/2} B_n(j)\Bigg\backslash\bigcup_{j=n/2+1}^{n-(k+1)} B_n(j)\\ &= \bigcup_{j=1}^{n/2} B_n(j)\Bigg\backslash\bigcup_{j=1}^{n/2-k} B_n(j)\cup\bigcup_{j=n/2+1}^{n-(k+1)} B_n(j)\\ &= \bigcup_{j=n/2-k+1}^{n/2} B_n(j)\Bigg\backslash\bigcup_{j=1}^{n/2-k} B_n(j)\cup\bigcup_{j=n/2+1}^{n-(k+1)} B_n(j)\,.\end{aligned}$$

De onde concluímos que

$$\bigcup_{j=n/2}^{n-1} R_n(j) \cap R_n(k) \Big\backslash \bigcup_{j=k+1}^{n/2-1} R_n(j) = \bigcup_{j=n/2-k+1}^{n/2} B_n(j) \cap R_n(k) \Big\backslash \bigcup_{j=n/2+1}^{n-k-1} B_n(j)\ .$$

Dividindo em dois casos, precisamos encontrar limites superiores para

$$\bigcup_{j=n/2-k+1}^{n/2-k/2} B_n(j) \cap R_n(k);$$
$$\bigcup_{j=n/2-k/2+1}^{n/2} B_n(j) \cap R_n(k).$$

Considerando a primeira das duas fórmulas acima, observamos que $n/2 - k + 1 \leq j \leq n/2 - k/2$ se e somente se $n - 2k + 2 \leq 2j \leq n - k$. Seja $w \in (B_n(j) \cap R_n(k))$. Assim, temos que $w = w_b w_b w_r$ e $w = w_h w_m w_h$, de onde concluímos que $w = w_1 w_2 w_1 w_2 w_3 w_1$, com $|w_1| = k$ e $|w_2| = j - k$. Portanto, $\Pr(w) = \Pr(w_1)^3 \Pr(w_2)^2 \Pr(w_3)$. Desta forma, para algum ρ positivo,

$$\begin{aligned}\sum_{w \in B_n(j) \cap R_n(k)} \Pr(w) &\leq \sum_{w_1 \in \{0,1\}^k} \Pr(w_1)^3 \sum_{w_2 \in \{0,1\}^{j-k}} \Pr(w_2)^2 \rho^{n-2j-k} \\ &= m_3^k m_2^{j-k} \rho^{n-2j-k}.\end{aligned}$$

Para o restante da prova, veja o exercício 4.1.2. □

4.1. **Problemas e exercícios.** Todos estão convidados a trabalhar no seguinte exercício.

1. Prove o Teorema 24.
2. Complete a prova da Proposição 35.

5. Árvore de sufixos

23/11/2010

Seja Σ um alfabeto finito e Σ^* o conjunto das palavras (sequências finitas) não vazias sobre Σ. Por exemplo, se $\Sigma = \{a, b, x\}$, então $s = xabxac \in \Sigma^*$ e $|s| = 6$, onde $|s|$ denota a quantidade de elementos de s. Observe que os *fatores* xa, a e x ocorrem duas vezes em s, com xa sendo o fator mais longo que ocorre mais de uma vez.

Desejamos obter um algoritmo eficiente para, dados um alfabeto Σ e uma palavra $s \in \Sigma^*$, encontrar um fator que:

i) ocorre mais de uma vez em s;
ii) é o mais longo possível.

Uma maneira de conseguir um bom algoritmo é fazendo uso do que chamamos de *vetor de sufixos*. O vetor de sufixos para uma palavra s de tamanho $|s|$ é um vetor v com $|s|+1$ posições, de modo que $v[i]$ contém a palavra s sem os i primeiros elementos. Assim, $v[0]$ contém exatamente a palavra s e $v[|s|]$ é a palavra vazia λ. Uma vez que temos o vetor de sufixos, para obter o algoritmo que queremos, basta ordenar lexicograficamente o vetor e comparar cada elemento do vetor com o próximo elemento na ordenação. Tal procedimento pode ser realizado em tempo $O(k|s|)$, onde k é o tamanho do maior fator que ocorre mais de uma vez em s (isto é possível se realizarmos um procedimento eficiente de ordenação, que leva tempo $O(|s|)$).

Existe uma maneira mais eficiente de representar os sufixos de uma dada palavra s, através de uma *árvore de sufixos*. Tal árvore permite, assim como no vetor de sufixos, a representação de todos os sufixos de uma palavra $|s|$. Uma árvore de sufixos para s é uma árvore enraizada onde cada aresta contém uma substring de s e todas as arestas que saem de um mesmo vértice são rotuladas de modo que tenham prefixos diferentes. A Figura 1 mostra a árvore de sufixos para a palavra $s = xabxac$. É possível construir tal árvore em tempo $O(|s|)$.

Tais estruturas são muito úteis em algoritmos de compressão de dados. Vamos apresentar o algoritmo de compressão de Ziv–Lempel. No que segue, vamos considerar a palavra $s = abacabaxabz$ para facilitar o entendimento. Seja $\text{prior}_i(s)$ o maior prefixo de $s[i \dots n]$ que ocorre em $s[1 \dots i-1]$ como fator, para $i \in [n]$, onde n é o tamanho de s. Ademais, denotamos $|\text{prior}_i(s)|$ por $l_i(s)$. Desta forma, temos que $\text{prior}_6(s) = ba$ e $l_6(s) = 2$. Se $\text{prior}_i(s) = \lambda$, então dizemos que $l_i(s) = 0$. Por fim, denotamos por $s_i(s)$ a posição do primeiro caractere do primeiro fator de $s[1 \dots i-1]$ que é igual a $\text{prior}_i(s)$. Podemos agora apresentar o algoritmo de Ziv–Lempel.

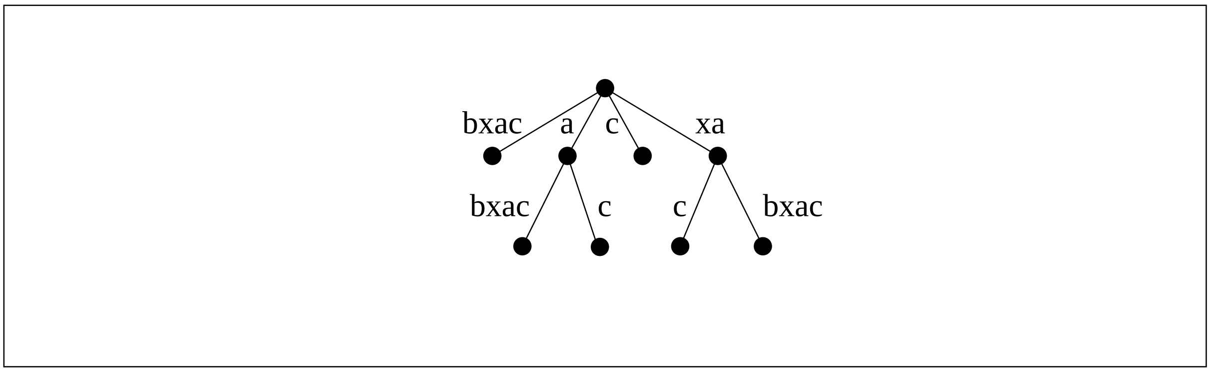

FIGURA 1. Árvore de sufixos para a palavra $s = xabxac$.

Entrada: Palavra s de tamanho n.
Saída: Codificação de s.

$i = 1$.
enquanto $i \leq n$ **faça**
  compute $(s_i(s), l_i(s))$.
  se $l_i(s) > 0$ **então**
    imprima $(s_i(s), l_i(s))$.
    $i = i + l_i(s)$.
  fim
  senão
    imprima $s[i]$.
    $i = i + 1$.
  fim
fim

Algorithm 1: Algoritmo de Ziv–Lempel

É possível implementar tal algoritmo em tempo $O(n)$, utilizando árvore de sufixos e, claramente, o processo de descompressão da saída do algoritmo é óbvio. Se aplicarmos o algoritmo de Ziv–Lempel à palavra $s = (ab)^{2^k}$, para $k > 1$, obtemos a saída $ab(1,2)(1,4)(1,8)\ldots(1,2^k)$, que é muito menor que a palavra original s. Este exemplo mostra bem a capacidade de compressão do algoritmo.

Referências

[1] E. Artin and P. Scherk, *On the sum of two sets of integers*, Ann. of Math. (2) **44** (1943), 138–142.

[2] R. C. Bose and S. Chowla, *Theorems in the additive theory of numbers*, Comment. Math. Helv. **37** (1962/1963), 141–147.

[3] S. Chowla, *Solution of a problem of Erdős and Turán in additive-number-theory*, Proc. Lahore Philos. Soc. **6** (1944), 13–14.

[4] P. Erdős and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212–215.

[5] N. J. Fine and H. S. Wilf, *Uniqueness theorems for periodic functions*, Proc. Amer. Math. Soc. **16** (1965), 109–114.

[6] H. B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers*, Ann. of Math. (2) **43** (1942), 523–527.

[7] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), no. 3, 377–385.