Pseudoaleatoriedade em Combinatória e Teoria da Computação

Domingos Dellamonica Junior e Yoshiharu Kohayakawa

20 de junho de 2005

Resumo

Nesta monografia, pretendemos apresentar alguns tópicos estudados durante o primeiro semestre do Mestrado de Domingos Dellamonica Junior, sob orientação de Yoshiharu Kohayakawa.

1 Introdução

Abordaremos os principais tópicos descritos no Projeto de Estudo de Mestrado de uma maneira expositiva, isto é, daremos uma idéia inicial sobre o que consiste cada tópico e depois apresentaremos algum resultado relacionado para exemplificar e solidificar os conceitos envolvidos.

2 Pseudoaleatoriedade

Definição 2.1. *Um* extractor *é uma função computável em tempo polinomial, que leva palavras de m bits em palavras de n bits. Queremos que tais extractors possuam a seguinte propriedade: "sempre que a distribuição da entrada é 'boa', a saída do extractor é estatisticamente próxima da distribuiçqão uniforme U_n".*

Definição 2.2. (Min-entropia) *Para uma variável aleatória $\mathcal{X}$, definimos*

$$H^\infty(\mathcal{X}) = \min_{x \in \mathrm{supp}(\mathcal{X})} -\log \mathbf{P}[\mathcal{X} = x].$$

Observe que se uma variável tem um valor grande para sua min-entropia então sua distribuição é 'boa' — isso porque nenhum valor x pode ocorrer com uma probabilidade muito maior que os demais valores.

Definição 2.3. *Por* distância estatística *entre duas distribuições $\mathcal{X}$, $\mathcal{X}'$ queremos dizer*

$$\mathrm{dist}(\mathcal{X}, \mathcal{X}') = \frac{1}{2} \sum_{i \in \mathrm{supp}(\mathcal{X}) \cup \mathrm{supp}(\mathcal{X}')} \big|\mathbf{P}[\mathcal{X} = i] - \mathbf{P}[\mathcal{X}' = i]\big|.$$

Seeded Extractors – Além da entrada usual, requisitamos uma pequena quantidade de bits uniformemente distribuídos. Essa entrada adicional é chamada de semente do extractor. Estado da arte: é possível obter extractors que usam sementes de tamanho $O(\log n)$. Pode-se enumerar todas as sementes e assim simular qualquer algoritmo probabilístico com um overhead polinomial. Vamos tentar entender isso melhor.

Seja $\mathcal{A}$ um algoritmo probabilístico[1] que depende de n bits aleatórios. Usando nosso seeded extractor de última geração, que denotaremos por $\mathrm{Ext} : \{0,1\}^m \times \{0,1\}^{O(\log n)} \to \{0,1\}^n$ obtemos uma saída que é próxima a U_n. Então, se $\mathcal{X} \in \{0,1\}^m$ é o valor observado na fonte de alta min-entropia, podemos obter todos os possíveis valores de $\mathrm{Ext}(\mathcal{X}, \{0,1\}^{O(\log n)})$ em tempo polinomial e rodar o algoritmo $\mathcal{A}$ com cada possível valor.

Seedless Extractors – O overhead polinomial dos seeded extractors, ou a falta de segurança destes para aplicações em criptografia são motivações para a definição de extractors sem semente. O artigo trata desse tipo de extractor.

Dispersers – Uma construção mais fraca do que os extractors. Em vez de exigirmos uma saída que seja estatisticamente próxima a uniforme, passamos a exigir apenas que o suporte contenha todas as palavras binárias de tamanho n (ou uma fração considerável delas).

Para a consturção de extractors e dispersers são usados resultados recentes de teoria aditiva dos números. Em particular, são usados resultados similares aos de Erdős-Szemeredi, como o

Teorema 2.1. *Existe uma constante ε_0 tal que para todo corpo finito $\mathbb{F}$ cuja ordem é um primo, e todo $A \subseteq \mathbb{F}$ com $|A| < |\mathbb{F}|^{0,99}$ temos*

$$\max\{|A + A|, |A \cdot A|\} > |A|^{1+\varepsilon_0}.$$

Como corolário, qualquer A nas condições do teorema satisfaz $|A \cdot A + A| > |A|^{1+\varepsilon_0}$. Isso sugere a idéia de que a funçaõ $f(a,b,c) = a \cdot b + c$, se iterada diversas vezes (dando origem a uma função cujo domínio é $\mathbb{F}^{3^k}$) possa ser empregada como um disperser. O artigo nos diz ainda que é possível provar um análogo estatístico de tal corolário e isso implica na construção de extractors usando f. A definição é como segue.

Definimos $\mathrm{Ext}^0 : \mathbb{F}^{3^0} = \mathbb{F} \to \mathbb{F}$ como a função identidade e, indutivamente, $\mathrm{Ext}^{i+1} : \mathbb{F}^{3^{i+1}} \to \mathbb{F}$ como

$$\mathrm{Ext}^{i+1}(x_1, x_2, x_3) = \mathrm{Ext}^i(x_1) \cdot \mathrm{Ext}^i(x_2) + \mathrm{Ext}^i(x_3),$$

onde $x_1, x_2, x_3 \in \mathbb{F}^{3^i}$.

[1] Um algoritmo da classe **BPP**, ie, um algoritmo polinomial e probabilístico que erra com uma probabilidade limitada por uma constante menor que $1/2$.

3 Discrepância

Seja $(V, \mathcal{S})$ um hipergrafo, ou seja, V é um conjunto base e $\mathcal{S}$ é uma coleção de subconjuntos de V. Queremos colorir os elementos de V em duas cores de forma que cada $S_i \in \mathcal{S}$ tenha um número balanceado de elementos de cada cor. Definimos $\chi : V \to \{-1, 1\}$ como uma "coloração" dos elementos de V. A discrepância de um conjunto S_i com relação a χ é definida por

$$\chi(S_i) = \sum_{s \in S_i} \chi(s).$$

O maior valor de $|\chi(S_i)|$ sobre todo $S_i \in \mathcal{S}$ é a discrepância do sistema de conjuntos dada a coloração χ. Quando nenhuma coloração em particular é fixada, a *discrepância* do sistema de conjuntos, denotada por $D_\infty(\mathcal{S})$, refere-se a menor discrepância dentre todas as possíveis colorações.

3.1 O Método das Funções Ortogonais

Seja $\mathbf{q} = (q_1, \ldots, q_d)$ um ponto do cubo unitário $[0, 1]^d$. Denotamos por $B_\mathbf{q}$ a caixa $[0, q_1) \times \cdots \times [0, q_d)$. Dado um conjunto P de n pontos no cubo unitário, a discrepância volume $D(\mathbf{q})$ é a diferença entre o número esperado de pontos contidos na caixa $B_\mathbf{q}$ (se os pontos de P fossem escolhidos de maneira uniforme) e o número de pontos que de fato estão na caixa, ou seja

$$D(\mathbf{q}) = n \cdot \mathrm{vol}(B_\mathbf{q}) - |P \cap B_\mathbf{q}| = nq_1 \ldots q_d - |P \cap B_\mathbf{q}|.$$

Teorema 3.1. *[1, teo. 3.1, p. 135] Dados n pontos em $[0, 1]^d$, a média quadrática da discrepância para caixas paralelas aos eixos satisfaz*

$$\int_{[0,1]^d} D(\mathbf{q})^2 d\mathbf{q} > c(\log n)^{d-1},$$

para alguma constante $c = c(d) > 0$.

Mostaremos o caso $d = 2$ que pode ser generalizado para dimensões maiores. Considere o espaço de funções $\mathcal{L}^2(X)$, ie, o espaço das funções $f : X \to \mathbb{C}$ com $\|f\| < \infty$, onde a norma é definida em termos do produto interno

$$\langle f, g \rangle = \int_X f g \, d\mathbf{q}.$$

Para este teorema, tomaremos $X = [0, 1]^2$. O método desta prova é escolher uma função $F : [0, 1]^2 \to \mathbb{R}$ com $\int F^2$ limitada superiormente por um valor conhecido e cujo produto $\langle F, D \rangle$ possa ser facilmente estimado por baixo. Utilizando a desigualdade de Cauchy-Schwarz ($\langle a, b \rangle^2 \leq \|a\|^2 \|b\|^2$), temos a seguinte cota inferior

$$\int D^2 \geq \Big(\int FD \Big)^2 \Big/ \int F^2. \tag{1}$$

Vamos supor que $n = 2^m$. (Isso não acarreta em perda de generalidade. Podemos encolher o quadrado unitário para um quadrado $[0, u]^2$ contendo o número de pontos adequados; se isso não for possível, tome uma ε-perturbação de P, já que $\|D\|$ não é sensível a pequenas mudanças em P.) Definimos

$$F = f_0 + \cdots + f_{m+1},$$

onde cada f_i é definida da forma a seguir. Para todo $i = 0, \ldots, m+1$, seja G_i o grid obtido dividindo $[0, 1]^2$ em $2n = 2^{m+1}$ retângulos de área $2^{-i} \times 2^{i-m-1}$.

As funções f_i são definidas de acordo com a "interação" de P e cada célula R de G_i.

- Se $P \cap R \neq \emptyset$ defina $f_i = 0$ em toda a célula R.
- Caso contrário, subdivida R em quatro quadrantes de igual tamanho. Nos quadrantes 1 e 3, f_i vale 1 e nos quadrantes 2 e 4, f_i vale -1.

Vamos provar um resultado bem geral donde segue imediatamente que $\langle f_i, f_j \rangle = 0$ para todo $i \neq j$.

Definição 3.1. *Dados inteiros $0 \leq a, b \leq m+1$, seja $G_{a,b}$ o grid obtido dividindo-se $[0, 1]^2$ em retângulos de tamanho $2^{-a} \times 2^{-b}$. Uma função $f : [0, 1]^2 \to \mathbb{R}$ é* (a, b)-checkered *se para toda célula R de $G_{a,b}$,*

- *Se $P \cap R \neq \emptyset$ então $f = 0$ em toda a célula R.*
- *Caso contrário, existe $c = c(R) \in \{-1, 0, 1\}$ tal que nos quadrantes 1 e 3, f vale c e nos quadrantes 2 e 4, f vale $-c$.*

Lema 3.1. *Se f é (a, b)-checkered e g é (a', b')-checkered, com $a' < a$ e $b < b'$ então fg é (a, b')-checkered.*

Demonstração. Primeiramente observamos que cada célula T de $G_{a,b'}$ é a intersecção de um único par de células $R \in G_{a,b}, S \in G_{a',b'}$. Se $T = R \cap S \neq \emptyset$ então $f(R) = f(S) = \{0\}$ e, logo, $f(T) = \{0\}$.

O caso mais interessante ocorre quando $R = S = \emptyset$ e $c(R) \neq 0 \neq c(S)$. Observe que o valor de f nos quadrantes 1 e 2 de T é o oposto do valor de f nos quadranes 3 e 4 de T. Analogamente, o valor de g nos quadrantes 2 e 3 de T é o oposto do valor de g nos quadrantes 1 e 4 de T. Fica claro que a célula T satisfaz as condições necessárias para que fg seja (a, b')-checkered. Como isso deve valer para toda célula $T \in G_{a,b'}$, temos que fg é (a, b')-checkered. □

É trivial verificar que toda função (a, b)-checkered tem integral nula (sob a região $[0, 1]^2$). Note que $G_i = G_{i,m+1-i}$ e, portanto, f_i é $(i, m+1-i)$-checkered. Segue dessas observações e do lema 3.1 que $\langle f_i, f_j \rangle = 0$ para todo $i \neq j$. Concluímos que

$$\int F^2 = \int \Big(\sum_{i=0}^{m+1} f_i \Big)^2 = \sum_{i=0}^{m+1} \int f_i^2 \leq \sum_{i=0}^{m+1} 1 = m + 2.$$

A segunda parte do método das funções ortogonais pede para que estimemos $\langle F, D\rangle$ por baixo. Novamente, provaremos um resultado mais geral que será imediatamente aplicado.

Lema 3.2. *Dada uma função f, (a,b)-checkered, seja S o conjunto de todos os centros de massa dos primeiros quadrantes das células de $G_{a,b}$. Então,*

$$\int fD = \frac{n}{4^{a+b+2}} \sum_{p\in S} f(p).$$

Demonstração. Vamos calcular a integral acima para cada célula $R \in G_{a,b}$. Se $P \cap R$ é não-vazio então a integral sobre R é 0. Caso contrário, seja R_1 o primeiro quadrante de R. Para cada $q = q_1 \in R_1$, sejam q_2, q_3 e q_4 os pontos correspondentes a q_1 nos demais quadrantes. Seja p o centro de massa de R_1 ($p \in S$). Temos

$$\begin{aligned}\int_{q\in R} f(q)D(q)dq &= \int_{q\in R_1} f(q)\big(D(q) - D(q_2) + D(q_3) - D(q_4)\big)dq \\ &= f(p)\int_{q\in R_1} n\cdot \operatorname{area}[q_1,q_2,q_3,q_4]dq \qquad (2)\\ &= nf(p)\Big(\frac{\operatorname{area} R}{4}\Big)^2 = nf(p)4^{-a-b-2}.\end{aligned}$$

A primeira igualdade segue das propriedades de f. A segunda igualdade segue diretamente da definição da função D, notando que $P\cap R = \emptyset$ implica que os termos $|P \cap B_{q_i}|$ se cancelam na soma $D(q) - D(q_2) + D(q_3) - D(q_4)$. A área do retângulo formado pelos pontos q_i é igual a área de R_1 que é equivalente a $1/4$ da área de R; disso segue a terceira igualdade.

A partir de (2) concluímos a demonstração do lema. □

Para as funções f_i, basta tomar $a = i$ e $b = m+1-i$ e $n = 2^m$ no lema 3.2. Observe que para $p \in S$, temos $f_i(p) > 0$ sempre que a célula que contém p, digamos $R \in G_i$, é tal que $R \cap P = \emptyset$. Como o número de células de G_i é $2n$ e P possui n pontos, pelo menos n células são vazias, logo

$$\int f_i D = \frac{2^m}{4^{m+3}} \sum_{p\in S} f_i(p) \geq \frac{2^m n}{4^{m+3}} = 2^{-6},$$

e portanto, $\langle F, D\rangle \geq 2^{-6}(m+2) = \Omega(\log n)$. Usando o método das funções ortogonais (veja a desigualdade (1)), provamos o teorema 3.1 para o caso $d = 2$, já que

$$\int_{[0,1]^2} D(\mathbf{q})^2 d\mathbf{q} = \Omega(\log n).$$

4 Grafos e Teoria de Ramsey

4.1 Alguns Resultados de Teoria de Ramsey

Nesta seção provaremos alguns resultados cuja motivação vem da seguinte pergunta de Erdős e Hajnal: "É verdade que para todo grafo H, existe $\varepsilon(H) > 0$ tal que para todo grafo G que é H-livre, devemos ter um clique ou um conjunto independente de tamanho $> n^{\varepsilon(H)}$?". Dizemos que um grafo é H-livre se este não contém uma cópia induzida de H.

No artigo [2], são mostrados alguns resultados de teoria de Ramsey relacionados a torneios e também é proposta uma formulação, equivalente a pergunta de Erdős e Hajnal, envolvendo torneios. A pergunta é efetivamente respondida positivamente para uma classe especial de grafos.

Definição 4.1. *Se para um grafo H a resposta à pergunta de Erdős e Hajnal é positiva então dizemos que H* possui a propriedade EH.

Definição 4.2. *Dado um grafo G com conjunto de vértices $[n] \stackrel{df}{=} \{1, \ldots, n\}$ e grafos $\{F_i\}_{i=1}^n$, formamos o grafo $G(F_1, \ldots, F_n)$ substituindo cada vértice $i \in [n]$ por F_i e ligando todas as cópias dos vértices de F_i com as cópias dos vértices de F_j se e somente se $\{i, j\} \in E(G)$.*

Teorema 4.1. *Sejam H e F grafos possuindo a propriedade EH e $V(H) = \{v_1, \ldots, v_k\}$. Então o grafo $H(F, v_2, \ldots, v_k)$ também possui a propriedade EH.*

Demonstração. Denotamos por $\hom(G) = \max\{\alpha(G), \omega(G)\}$, ou seja, o tamanho do maior conjunto homogêneo de G (um clique ou conjunto independente). Suponha que H e F sejam como no enunciado. Seja $H_0 = H - v_1$. Por simplicidade, denote $H(F) = H(F, v_2, \ldots, v_k)$. Seja G um grafo $H(F)$-livre com n vértices e suponha que $\hom(G) < n^{\varepsilon(H)\delta}$. Vamos tentar obter uma contradição, dado que $\delta > 0$ é suficientemente pequeno.

Estamos supondo que n é suficientemente grande. Em particular, $m \stackrel{\text{df}}{=} \lceil n^\delta \rceil > k$. Pela definição de $\varepsilon(H)$, todo m-conjunto $U \subset V(G)$ deve induzir pelo menos um subgrafo isomorfo a H, caso contrário, encontraríamos um conjunto homogêneo de tamanho $m^{\varepsilon(H)} > \hom(G)$, o que é absurdo. Então, G possui pelo menos $\binom{n}{m} / \binom{n-k}{m-k}$ cópias induzidas de H. Para cada uma dessas cópias, fixe a imersão de H em G correspondente.

Como o número de imersões de H_0 em G é limitado superiormente por $n(n-1)\cdots(n-k+2)$, deve haver uma imersão $H_0 \hookrightarrow G$ que pode ser extendida para uma imersão $H \hookrightarrow G$ em pelo menos

$$M \stackrel{\text{df}}{=} \binom{n}{m} \Big/ \left\{ \binom{n-k}{m-k} n(n-1)\cdots(n-k+2) \right\}$$

maneiras diferentes. Em outras palavras, há $k-1$ vértices $v_2', \ldots, v_k' \in V(H)$ e um M-conjunto $W \subset V(G)$ tal que para todo $w \in W$, a função f definida por $f(v_1) = w, f(v_i) = v_i'$ para $i = 2, \ldots, k$ é uma imersão $H \hookrightarrow G$.

Considere o grafo $G[W]$. Se este grafo não for F-livre então G possui uma cópia induzida de $H(F)$. Basta lembrar da definição do grafo $H(F)$ e observar que se $W' \subset W$ é tal que $G[W']$ é uma cópia isomorfa a F então, pela construção de W, $G[W' \cup \{v'_2, \ldots, v'_k\}] \cong H(F)$.

Como F possui a propriedade EH, concluimos que

$$\hom(G[W]) \geq |W|^{\varepsilon(F)} \geq M^{\varepsilon(F)}.$$

Por outro lado,

$$n^{\varepsilon(H)\delta} > \hom(G) \geq \hom(G[W]).$$

Com algumas contas simples, determinamos que se

$$\delta < \frac{\varepsilon(F)}{\varepsilon(H) + k\varepsilon(F)},$$

chegamos a uma contradição. □

Corolário 4.1. *Dados $H, F_1, \ldots, F_k$ grafos com a propriedade EH e $V(H) = \{v_1, \ldots, v_k\}$ então o grafo $H(F_1, \ldots, F_k)$ também possui a propriedade EH.*

Definição 4.3. *Definimos como* torneio *um grafo dirigido $T = (V, A)$, onde para todo $\{u, v\} \in \binom{V}{2}$, temos $|\{uv, vu\} \cap A| = 1$. Um torneio com uma ordem linear ($<$) nos vértices é chamado de* torneio ordenado *e é denotado por $(T, <)$. Dizemos que um torneio $(T, <)$ é um* subtorneio ordenado *de $(T', <')$ se existe uma função injetiva $f : V(T) \hookrightarrow V(T')$ que preserva a ordem e adjacência, ie,*

(i) $f(u) <' f(v)$ *sse* $u < v$

(ii) $(f(u), f(v)) \in E(T')$ *sse* $(u, v) \in E(T)$.

Lema 4.1. *Sejam $t > n > 1$ dois inteiros positivos e seja $S = \{a_1, \ldots, a_{tn}\}$ um tn-conjunto. Seja $g : S \to [t]$ uma função tal que para todo $p \in [t]$, temos $|\{i : g(a_i) = p\}| = n$. Ademais, seja $f : S \to [n]$ uma função aleatória cujo valor de cada a_i é escolhido independente e uniformemente. Seja E o evento em que existem $1 \leq i_1 < i_2 < \cdots < i_n \leq tn$ tais que $g(a_{i_j}) \neq g(a_{i_k})$ para todo $j \neq k$ e $f(a_{i_j}) = j$ para todo $j \in [n]$.*

A probabilidade de que E não *valha é no máx.*

$$\sum_{q=0}^{n-1} \binom{tn}{q} \frac{n^{q(n-1)}(n-1)^{tn-nq}}{n^{tn}} \leq \left(\frac{4et}{n}\right)^n e^{-t}.$$

Demonstração. Vamos estimar o número de funções f para as quais o evento E falha. Dada uma tal f, seja i_1 o menor inteiro (se existir) tal que $f(a_{i_1}) = 1$. Supondo que $i_1 < i_2 \cdots < i_{j-1}$ já foram definidos de forma que $f(a_{i_s}) = s$ para todo $s < j$ e que os valores $g(a_{i_s})$ de são todos distintos. Seja $i_j > i_{j-1}$ o menor inteiro (se existir) tal que $f(a_{i_j}) = j$ e $g(a_{i_j}) \neq g(a_{i_s})$ para todo $s < j$. Note que, como E falha para f, este processo deve se encerrar após a definição de $q \leq n - 1$ índices.

Observe que o valor de q elementos de f é fixado (a saber, $f(i_s) = s$ para $s = 1, \ldots, q$). Também é simples verificar que o valor de f fica restrito a $n-1$ possíveis valores em quase todo o domínio. Em particular, os únicos valores de k para os quais f poderia assumir qualquer valor de $[n]$ estão contidos no conjunto $X \stackrel{\text{df}}{=} \left(\cup_{s\in[q]}\{k \mid g(a_k) = g(a_{i_s})\}\right) \setminus \{i_1, \ldots, i_q\}$. Para demonstar este fato, suponha $x \in X$ tal que x pode assumir qualquer valor de $[n]$. Observe que não podemos se $x < i_1$ pois isso contraria a construção do conjunto de índices (pois não podemos ter $g(x) = 1$). De forma análoga concluimos que $x \not> i_q$ e, para todo $s = 1, \ldots, q-1$, se $i_s < x < i_{s+1}$ então $g(x)$ não pode valer $s+1$.

Como $|X| = q(n-1)$, o número de funções f para as quais E falha é limitada superiormente por

$$T \stackrel{\text{df}}{=} \sum_{q=0}^{n-1} \binom{tn}{q} n^{q(n-1)} (n-1)^{tn-qn},$$

pois há $\binom{tn}{q}$ maneiras de escolher i_s, $s = 1, \ldots, q$ tais que $f(i_s) = s$. O total de funções é dado por n^{tn}, logo

$$\mathbf{P}[\overline{E}] \leq T/n^{tn} \leq \left(\frac{4et}{n}\right)^n e^{-t},$$

como queríamos. □

Teorema 4.2. *Para todo torneio ordenado $(T, <)$, existe um torneio T' tal que para toda ordem $<'$ de T' o torneio ordenado $(T, <)$ é um subtorneio de $(T, <')$. Ademais, se T tem n vértices então existe um T' com a propriedade acima com $O(n^3 \log^2 n)$ vértices.*

Definição 4.4. *Um* Plano Projetivo Finito *é um hipergrafo $\mathcal{P} = (X, \mathcal{L})$ onde X é um conjunto finito de pontos e $\mathcal{L}$ é um conjunto de linhas, que respeitam os seguintes axiomas:*

1. *existe $F \subset X$ com $|F| = 4$ tal que $|L \cap F| \leq 2$ para todo $L \in \mathcal{L}$;*
2. *para todo $L_1, L_2 \in \mathcal{L}$, temos $|L_1 \cap L_2| = 1$;*
3. *para todo par de pontos distintos $x_1, x_2 \in X$ existe uma única linha $L \in \mathcal{L}$ tal que $x_1, x_2, \in L$.*

Dizemos que tal plano projetivo é de ordem n *quando $|X| = |\mathcal{L}| = n^2 + n + 1$ e, para todo $L \in \mathcal{L}$, $|L| = n + 1$.*

Demonstração. Fixe $(T, <)$ um torneio em n vértices, digamos $[n]$, cuja ordem linear é a ordem natural. Seja $c > 3$ uma constante e $t - 1$ a menor potência de primo tal que $t > cn \log n$ (o TNP nos garante que $t = (1 + o(1))cn \log n$). É sabido que para toda potência de primo p^k, existe um plano projetivo finito de ordem p^k. Sendo assim, seja $\mathcal{P} = (X, \mathcal{L})$ um plano projetivo finito de ordem $t - 1$.

Associe a cada ponto $p \in X$ um conjunto S_p de n elementos, com os conjuntos S_p dois-a-dois disjuntos. Os vértices de T' são $V(T') = \cup_{p\in X} S_p$. Note que $|V(T')| <$

nt^2. Para cada linha $L \in \mathcal{L}$, sorteie uma função aleatória $f_L : \cup_{p\in L} S_p \to [n]$. Os sorteios são independentes para cada linha. Para definir a orientação dos arcos do torneio, sejam $u, v \in \cup_{p\in L} S_p$. Se $u \in S_p$ e $v \in S_{p'}$ com $p \neq p'$ e $f_L(u) \neq f_L(v)$, então (u, v) é arco de T' se e somente se $(f_L(u), f_L(v))$ é arco de T'. Se u e v não forem dessa forma, oriente de maneira arbitrária.

Vamos provar que com probabilidade tendendo a 1 (quando n tende a infinito), T' contém uma cópia ordenada de T em qualquer ordem. Fixe uma ordem $<'$ para T'. Estimaremos a probabilidade de que, nesta ordem, não encontramos $(T, <)$ como subtorneio ordenado. Para cada linha $L \in \mathcal{L}$, $<'$ induz uma ordem para os tn vértices de $\cup_{p\in L} S_p$. Seja $S_L = (a_1, \ldots, a_{tn})$ tal ordem; defina $g_L(a_i) = p$ se e somente se $a_i \in S_p$. Observe que S_L, g_L, f_L estão nas condições do lema 4.1.

Suponha que o evento E do lema 4.1 valha para S_L, g_L, f_L. Então existm índices $i_1 < \cdots < i_n$ tais que $f_L(a_{i_s}) = s$ para todo $s \in [n]$ e para todo $j \neq k$, a_{i_j} e a_{i_k} vêm de conjuntos S_p e $S_{p'}$ distintos. Mas então $(T'[\{a_{i_1}, \ldots, a_{i_n}\}], <') \cong (T, <)$. Portanto, a probabilidade de que $(T', <')$ não contém $(T, <)$ em *nenhum* conjunto S_L é limitada superiormente por

$$\Big\{\Big(\frac{4et}{n}\Big)^n e^{-t}\Big\}^{(t-1)^2+t} = \exp\big\{-(1+o(1))c^3n^3\log^3 n\big\}.$$

O número de ordens para T' é dado por

$$\{(n((t-1)^2+t)\}! \leq \exp\{-(1+o(1))3c^2n^3\log^3 n\}$$

e, como $c > 3$, a probabilidade de que T' não contém $(T, <)$ em alguma ordem $<'$ é $o(1)$, completando a prova. □

O resultado acima não é muito longe do melhor possível. Em [2] também é provado que para qualquer $(T, <)$ com n vértices, se T' é um torneio com menos de $n^2/(\sqrt{3}e^2)$ vértices então há uma ordem $<'$ tal que $(T', <')$ não contém $(T, <)$.

5 Reconstruindo Subconjuntos de $\mathbb{Z}_n$

Definição 5.1. *Seja n um inteiro positivo e seja $X \subseteq \mathbb{Z}_n$. O k-*deck *de X é a função definida em todo multiconjunto Y de $\mathbb{Z}_n$ de tamanho k por*

$$d_{X,k} = |\{i \in \mathbb{Z}_n \mid \mathrm{supp}(Y + i) \subseteq X\}|,$$

onde $\mathrm{supp}(Y)$ é o conjunto dos elementos de Y desconsiderando-se a multiplicidade. Observe que, como estamos falando de multiconjuntos, a exigência de que Y tenha tamanho k pode ser relaxada para tamanho $\leq k$ sem perda de generalidade.

Definição 5.2. *Dizemos que o conjunto X é* reconstrutível a partir do k-deck de X *se podemos deduzir X (a menos de translação) a prtir do seu k-deck, ou seja,*

$$d_{W,k} \equiv d_{X,k} \textit{ implica } W = X + i \textit{ para algum } i \in \mathbb{Z}_n.$$

Mais geralmente, dizemos que uma função é reconstrutível a partir do k-deck de X se seu valor é uma função de $d_{X,k}$.

5.1 O caso em que n é primo

Lema 5.1. *Para todo $k \leq n$, qualquer conjunto $A \subseteq \mathbb{Z}_n$ e qualquer multiconjunto $\{i_1, \ldots, i_k\}$ de $\mathbb{Z}_n$, podemos reconstruir $|(A - i_1) \cap \cdots \cap (A - i_k)|$ a partir do k-deck de A.*

Demonstração. Observe que $f(A) = |(A-i_1)\cap\cdots\cap(A-i_k)|$ é igual a $d_{A,k}(\{i_1, \ldots, i_k\})$ já que um elemento x é contado por $f(A)$ se e somente se $x + i_j \in A$ para $j \in [k]$, ou seja, sse x é contado em $d_{A,k}$. Portanto, f é uma função de $d_{A,k}$, logo é reconstrutível a partir do k-deck de A. □

Definição 5.3. (função característica) *Para um conjunto S fixado, denotamos por $\chi_S(x)$ a função que vale 1, caso $x \in S$ e 0, caso contrário.*

Teorema 5.1. *Se p é primo então todo subconjunto de $\mathbb{Z}_p$ é reconstrutível a partir de seu 3-deck.*

Demonstração. Uma matriz $\mathbf{M}$ é chamada *circulante* se existem inteiros $\{a_i \mid i \in \mathbb{Z}_n\}$ tais que a i-ésima linha de $\mathbf{M}$ é $(a_i, a_{i+1}, \ldots, a_{i+n-1})$. Denotamos por $\mathbf{Z}$ a matriz circulante fundamental (a matriz circulante cuja primeira linha é $(0, 1, 0, \ldots, 0)$). A matriz $\mathbf{Z}$ é tal que cada potência $\mathbf{Z}^i$ consiste de um deslocamento cíclico de i casas em toda linha da matriz $\mathbf{Z}$.

Considere conjuntos $A, B \subseteq \mathbb{Z}_p$ que tenham o mesmo 3-deck. Associamos ao conjunto A a matriz (circulante) $\mathbf{M}_A$, definida por $(\mathbf{M}_A)_{ij} = \chi_A(j - i)$. É simples verificar que

$$\mathbf{M}_A = \sum_{j \in A} \mathbf{Z}^j.$$

Como os auto-valores de $\mathbf{Z}$ são exatamente as raízes p-ésimas da unidade, denotadas por ζ^k, para $k = 0, \ldots, p-1$ (onde $\zeta = e^{2\pi \mathbf{i}/p}$) e seus auto-vetores são $\zeta^k(1, \zeta, \ldots, \zeta^{p-1})$, para $k = 0, \ldots, p-1$ então os auto-valores de $\mathbf{M}_A$ são $\sum_{j \in A} \zeta^{jk}$, para $k = 0, \ldots, p-1$.

Dividimos então a prova em dois casos. Caso $\mathbf{M}_A$ seja não-singular, seja $\mathbf{\Lambda}$ a sua inversa (também circulante) cuja primeira linha é $\boldsymbol{\lambda}$. Defina $\mathbf{M}_B$ de forma análoga a $\mathbf{M}_A$ e considere $\mathbf{C} = \mathbf{\Lambda}\mathbf{M}_B$, cuja primeira linha é $\mathbf{c}$. Vamos provar que $\mathbf{C} = \mathbf{Z}^k$ para algum k. Por definição, temos

$$\begin{aligned}
\sum_{i=0}^{p-1} c_i^2 &= \sum_{i=0}^{p-1} \Big(\sum_{j=0}^{p-1} \lambda_j \cdot \chi_B(j - i) \Big)^2 \\
&= \sum_{0 \leq j,k < p} \lambda_j \lambda_k \sum_{i=0}^{p-1} \chi_B(j - i)\chi_B(k - i) \\
&= \sum_{0 \leq j,k < p} \lambda_j \lambda_k |(B - j) \cap (B - k)|.
\end{aligned}$$

A segunda igualdade segue de $\chi_B(j-i)\chi_B(k-i) = 1 \Leftrightarrow j-i, k-i \in B \Leftrightarrow -i \in (B-j)\cap(B-k)$. Usando o lema 5.1 sabemos que $|(B-j)\cap(B-k)|$ pode ser obtido a partir do 2-deck de B (e, portanto, do 3-deck também). Aplicando a mesma idéia vista acima, verificarmos que

$$\sum_{i=0}^{p-1} c_i^3 = \sum_{0\leq j,k,l<p} \lambda_j\lambda_k\lambda_l|(B-j)\cap(B-k)\cap(B-l)|.$$

Tal expressão também é reconstrutível a partir do 3-deck de B.

Por hipótese, o 3-deck de A e B são iguais, logo, $\sum c_i^2 = \sum(\mathbf{\Lambda M}_A)_{1i}^2 = \sum \mathbf{I}_{1i}^2 = 1$ e, analogamente $\sum c_i^3 = 1$. Tais condições implicam que $\mathbf{c} = \mathbf{e}_k$ para algum k. Caso contrário, temos $c_i \in [0,1)$ e $1 = \sum_{c_i\neq 0} c_i^2 > \sum_{c_i\neq 0} c_i^3$. Concluimos que $\mathbf{M}_B = \mathbf{M}_A\mathbf{Z}^k$ e, portanto, B é uma translação de A.

Resta o caso em que $\mathbf{M}_A$ é singular. Observe que $\emptyset \subset \mathbb{Z}_p$ é o único subconjunto tal que $d_{\emptyset,1} \equiv 0$. Podemos supor que $\emptyset \neq A \subseteq \mathbb{Z}_p$. Como os auto-valores de $\mathbf{M}_A$ são os p valores $\alpha_i = q(\zeta^i)$, para $i = 0,\ldots,p-1$, com $q(x) = \sum_{j\in A} x^j$, devemos ter algum $\alpha_i = 0$ para $\mathbf{M}_A$ ser singular.

Sabemos que $\alpha_0 = |A| > 0$. O polinômio mínimo de ζ^i, $i \in (0,p)$, é $m_p(x) = 1 + x + \cdots + x^{p-1}$. Temos $q(\zeta^i) = 0$ somente se $m_p \mid q$, o que ocorre somente se $A = \mathbb{Z}_p$. É evidente que $d_{A,1}$ vale sempre p sse $A = \mathbb{Z}_p$, ou seja, A é reconstrutível a partir de seu 3-deck. □

5.2 A abordagem para o caso geral

Nesta seção abordaremos a reconstrução de $\mathbb{Z}_n$ para um n qualquer. Os grupos considerados serão sempre abelianos e $\mathbb{Z}_n$ é o grupo aditivo dos inteiros módulo n.

Definição 5.4. *Seja Γ um grupo de permutação sobre um conjunto Ω. Dizemos que dois conjuntos $X, Y \subseteq \Omega$ são* isomorfos *se $X = gY$ para algum $g \in \Gamma$.*

Definição 5.5. *O k-*deck *de X é a função definida em multiconjuntos de Ω por*

$$d_{X,k}(Y) = |\{g \in \Gamma \mid \mathrm{supp}(gY) \subseteq X\}|.$$

Dizemos que Γ é reconstrutível a partir de seu k-deck *se $d_{X,k} \equiv d_{Y,k}$ implica que X e Y são isomorfos.*

Definição 5.6. *Uma* ação de um grupo *G sobre um conjunto X é um mapa $\phi : G\times X \to X$ para o qual valem*

1. *$\phi(e,x) = x$, onde e é a identidade de G;*
2. *$\phi(g,\phi(h,x)) = \phi(gh,x)$ para quaisquer $g,h \in G$.*

Para não sobrecarregar a notação podemos usar simplesmente $g \cdot (h \cdot x) = gh \cdot x$ para representar a propriedade 2, por exemplo.

Definição 5.7. *Um* group ring *é o conjunto de todas as somas finitas $\sum_x a_x x$, com todos os x pertencentes a um grupo G e todos os a_x pertencentes a um corpo $\mathbb{F}$. Denotamos tal conjunto por $\mathbb{F}G$.*

O método empregado em [3] consiste em considerar não apenas os subconjuntos de um grupo G, mas todas as funções $f : G \to \mathbb{Q}$ sob a ação de G dada por $g \cdot f(x) = f(g^{-1}x)$. Claramente este conjunto de funções pode ser identificado com o group ring $\mathbb{Q}G$ através do mapa $f \leftrightarrow \sum_{x \in G} x f(x)$.

Definição 5.8. *Se $f \in \mathbb{Q}G$ e $k \geq 1$, o* k-deck *de f é a função definida em multiconjuntos de G por*

$$d_{f,k}(Y) = \sum_{g \in G} \prod_{x \in gY} f(x).$$

Dizemos que f é reconstrutível a partir de seu k-deck *se $d_{f,k} \equiv d_{f',k}$ implica que $f = g \cdot f'$ para algum $g \in G$.*

Definição 5.9. *Definimos $r_{\mathbb{Q}}(G)$ como sendo o menor inteiro k tal que toda função $f : G \to \mathbb{Q}$ é reconstrutível a partir de seu k-deck.*

Definição 5.10. *Se para $f, f' \in \mathbb{Q}G$ temos $d_{f,k} \equiv d_{f',k}$ porém não existe $g \in G$ tal que $f = g \cdot f'$ então chamamos f' de um k-impostor de f.*

Podemos mapear todo conjunto $S \subseteq G$ à função $\chi_S \in \mathbb{Q}G$ e, portanto, qualquer cota superior para $r_{\mathbb{Q}}(G)$ é uma cota superior para o menor k tal que G é reconstrutível a partir de seu k-deck.

Seja $Q_n = \mathbb{Q}[x]/\langle x^n - 1 \rangle$. A aritmética de Q_n é bem simples: se associarmos a cada $p \in Q_n$ um vetor de $\mathbb{Q}^n$ da maneira canônica, multiplicar p por x^i equivale a um deslocamento cíclico de i casas no vetor correspondente. É simples verificar que $\mathbb{Q}\mathbb{Z}_n \cong Q_n$ e que a ação de $\mathbb{Z}_n$ sobre $\mathbb{Q}\mathbb{Z}_n$ é isomorfa a ação de $\mathbb{Z}_n$ sobre Q_n dada por $i \cdot \alpha = x^i \alpha$. Basta observar que se $i \in \mathbb{Z}_n$ e $f \in \mathbb{Q}\mathbb{Z}_n$ então $(i \cdot f)(x) = f(x - i)$, que corresponde a um deslocamento cíclico de i casas no vetor correspondente a f.

Uma maneira de investigar Q_n é através da transformada discreta de Fourier, o qual consideraremos em §5.4. Isto requer que trabalhemos num domínio maior, já que a transformada de Fourier lida com complexos.

Definição 5.11. *Dados dois elementos de Q_n defina o seu* produto estrela *como sendo*

$$\Big(\sum_{j=0}^{n-1} a_j x^j\Big) \star \Big(\sum_{j=0}^{n-1} b_j x^j\Big) = \sum_{j=0}^{n-1} a_j b_j x^j.$$

Observe que $\star$ é comutativa, associativa e distributiva sobre a soma de elementos de Q_n. Dado um multiconjunto $I = \{i_1, \ldots, i_r\}$, defina

$$\alpha^I = (x^{i_1}\alpha) \star \cdots \star (x^{i_r}\alpha).$$

Uma combinação linear de tais expressões, ie, $p(\alpha) = \sum_{I \in \mathcal{I}} \lambda_I \alpha^I$ é chamada de $\star$-polinômio. *O* grau *de p é definido como $\max_{I \in \mathcal{I}} |I|$.*

Por simplicidade, suponha $\alpha = \sum_{0 \leq j < n} a_j x^j$. Definimos o mapa linear $S : Q_n \to \mathbb{Q}$ por $S(\alpha) = \sum_j a_j$. Definimos para um multiconjunto I a função $S_I(\alpha) = S(\alpha^I)$. Temos

$$S_{\{i_1,\ldots,i_r\}}(\alpha) = \sum_{0 \leq j < n} a_{j-i_1} \cdots a_{j-i_r}.$$

Uma composição do tipo $S \circ p$ com p um $\star$-polinômio é denominada uma $\star$-expressão. *O* grau *de uma $\star$-expressão $S \circ p$ é dada pelo grau de p.*

Definição 5.12. *Dados ideais $M, N \subset Q_n$ definimos seu* $\star$-produto *$M \star N$ como sendo o ideal*

$$M \star N = \langle M, N, \{m \star n \mid m \in M, n \in N\} \rangle.$$

A k-ésima $\star$-potência *de M é definida indutivamente como $M^{\star 1} = M$ e $M^{\star(k+1)} = M \star M^{\star k}$ para $k \geq 1$.*

Na prova do teorema principal (teo. 5.4) mostraremos que dado $\alpha \in Q_n$, é possível obter um $\star$-polinômio p tal que $p(\alpha) = 1 \in Q_n$ e, além disso, tal p tem grau razoavelmente baixo, digamos, no máximo l. Depois mostraremos que os valores de $\star$-expressões de grau no máximo k são reconstrutíveis a partir de seu k-deck. Isto permitirá provar, com um pouco de trabalho, que se $\beta \in Q_n$ é tal que $d_{\beta,3l} \equiv d_{\alpha,3l}$ então temos $p(\beta) = x^i$ para algum $i \in \{0, \ldots, n-1\}$ e, posteriormente, mostrar que $\beta = x^i \alpha$.

5.3 As $\star$-expressões

Lema 5.2. *Suponha que $k \geq 1$ é um inteiro e $\alpha, \beta \in C_n$ são tais que $d_{\alpha,k} \equiv d_{\beta,k}$. Se $f = \sum_{I \in \mathcal{I}} \lambda_I S_I$ é uma $\star$-expressão de grau no máximo k então $f(\alpha) = f(\beta)$.*

Demonstração. Claramente basta mostrar o resultado para $f = S_I$ com $I = \{i_1, \ldots, i_r\}$, $r \leq k$. Temos

$$\begin{aligned} f(\alpha) &= \sum_{0 \leq j < n} a_{j-i_1} \cdots a_{j-i_r} \\ &= d_{\alpha,r}(\{-i_1, \ldots, -i_r\}) \\ &= d_{\beta,r}(\{-i_1, \ldots, -i_r\}) \\ &= f(\beta). \end{aligned}$$

A segunda igualdade segue da definição 5.8, observando que α deve ser encarado como um elemento de $\mathbb{Q}\mathbb{Z}_n$ e, portanto, $\alpha(i)$ *não* é o valor do polinômio α em $i \in \mathbb{Z}_n$, mas sim a i-ésima coordenada de α, ou seja, a_i. □

Lema 5.3. *Suponha que $\alpha \in Q_n$ satisfaça $S_{\{0,0\}}(\alpha) = S_{\{0,0,0\}}(\alpha) = 1$. Então $\alpha = x^i$ para algum $i \in \{0, \ldots, n-1\}$.*

Demonstração. Basta verificar que $S_{\{0,0\}}(\alpha) = \sum_j a_j^2$ e $S_{\{0,0,0\}}(\alpha) = \sum_j a_j^3$ e aplicar o resultado utilizado na demonstração do teorema 5.1. □

Lema 5.4. *Sejam p e q dois $\star$-polinômios e f uma $\star$-expressão. Então $p \circ q$ é um $\star$-polinômio de grau no máximo $\operatorname{grau}(p)\operatorname{grau}(q)$ e $f \circ p$ é uma $\star$-expressão de grau no máximo $\operatorname{grau}(f)\operatorname{grau}(p)$.*

Demonstração. Contas bem diretas. □

Proposição 5.1. *Suponha que $\alpha \in Q_n$ e que existe um $\star$-polinômio p tal que $p(\alpha) = 1$. Se $\operatorname{grau}(p) \leq k$ e $\beta \in Q_n$ tem o mesmo $3k$-deck de α então $\beta = x^i\alpha$ para algum $i \in \mathbb{Z}_n$.*

Demonstração. Seja $u = p(\beta)$. O lema 5.4 nos garante que a composta $S_{\{0,0,0\}} \circ p$ é uma $\star$-expressão de grau no máximo $3k$. Pelo lema 5.2 temos $S_{\{0,0,0\}}(u) = f(\beta) = f(\alpha) = S_{\{0,0,0\}}(1) = 1$. Analogamente, $S_{\{0,0\}}(u) = 1$ e, do lema 5.3, concluímos que $u = x^i$ para algum $i \in \mathbb{Z}_n$. Para todo $j \in \mathbb{Z}_n$ defina a função $g_j : \gamma \mapsto \langle x^j p(\gamma), \gamma\rangle$. Observe que cada g_j é uma $\star$-expressão de grau $k+1$ pois, se $p(\gamma) = \sum_{I\in\mathcal{I}} \lambda_I \gamma^I$ então, definindo

$$q(\gamma) = \sum_{I\in\mathcal{I}} \lambda_I(\gamma^{I+j} \star \gamma) = \sum_{I\in\mathcal{I}} \lambda_I \gamma^{(I+j)\cup\{0\}},$$

temos $g_j = S \circ q$. Se $(b_k)_{k\in\mathbb{Z}_n}$ são os coeficientes de β e $(a_k)_{k\in\mathbb{Z}_n}$ os de α então

$$b_{i+j} = \langle x^j x^i, \beta\rangle = \langle x^j p(\beta), \beta\rangle = g_j(\beta) = g_j(\alpha) = \langle x^j p(\alpha), \alpha\rangle = \langle x^j, \alpha\rangle = a_j, \quad (3)$$

donde $g_j(\beta) = g_j(\alpha)$ é conseqüência do lema 5.2. A equação (3) nos fornece $\beta = x^i\alpha$. □

Teorema 5.2. *Seja $\alpha \in Q_n$ e $J = \langle\alpha\rangle$. Se $J^{\star k} = Q_n$ então não há $3k$-impostores para α.*

Demonstração. Como $1 \in Q_n$ e $J^{\star k} = Q_n$, existe um $\star$-polinômio p de grau no máximo k tal que $p(\alpha) = 1$. Pela proposição 5.1 qualquer β com $d_{\beta,3k} \equiv d_{\alpha,3k}$ deve ser da forma $\beta = x^i\alpha$ para $i \in \mathbb{Z}_n$. □

5.4 Transformadas de Fourier

Utilizaremos a transformada discreta de Fourier, denotada por $\mathcal{F} : C_n \to \mathbb{C}^n$ para analisar a rapidez com a qual as iteradas $\langle\alpha\rangle^{\star k}$ chegam a Q_n (quando chegarem). Isso será feito olhando-se para $\mathcal{F}(\langle\alpha\rangle^{\star k})$.

Proposição 5.2. *O mapa $\mathcal{F}$ definido como $\mathcal{F}(\alpha) = (\alpha(\zeta^k))_{k\in\mathbb{Z}_n}$ — onde $\zeta = e^{2\pi\mathbf{i}/n}$ — é um isomorfismo de anel (onde a multiplicação de $\mathbb{C}^n$ é feita coordenada a coordenada). A inversa de $\mathcal{F}$ é dada por*

$$\mathcal{F}^{-1}(z_0, \ldots, z_{n-1}) = \frac{1}{n} \sum_{j\in\mathbb{Z}_n} \Big(\sum_{r\in\mathbb{Z}_n} z_r \zeta^{-rj} \Big) x^j. \tag{4}$$

Definição 5.13. *Definimos, para $S \subseteq \mathbb{Z}_n$, os conjuntos $Z_S = \{(f_i)_{i\in\mathbb{Z}_n} \mid f_i = 0$ para todo $i \in S\}$ e $NZ_S = Z_{\mathbb{Z}_n\setminus S} = \{(f_i)_{i\in\mathbb{Z}_n} \mid f_i = 0$ para todo $i \notin S\}$.*

Recordaremos alguns fatos básicos sobre ideais de C^n e $\mathbb{C}^n$ que serão úteis para os próximos resultados.

Proposição 5.3. *Os anéis C^n e $\mathbb{C}^n$ são domínimos principais (Euclidianos, de fato). Os ideais de C^n são indexados pelos subconjuntos T do conjunto de raízes n-ésimas da unidade $\{\zeta^i \mid i \in \mathbb{Z}_n\}$. O ideal correspondente a T é $M_T = \langle\prod_{\zeta^i\in T}(x - \zeta^i)\rangle$. Os ideais de $\mathbb{C}^n$ são indexados pelos subconjuntos S do conjunto $\{0, \ldots, n-1\}$. A S corresponde o ideal Z_S, definido acima. A transformada de Fourier mapeia o ideal M_T ao ideal $Z_{\{j|\zeta^j\in T\}}$.*

A razão pela qual os elementos de Q_n são mais facilmente reconstrutíveis do que os elementos de C_n deve-se ao fato da estrutura dos ideais de Q_n ser muito mais interessante que a dos ideais de C_n. Antes de revermos os fatos, precisamos de algumas notações.

Definição 5.14. *Seja $D(n) = \{d \mid d$ divide $n\}$ e seja $F = \mathbb{Q}[\zeta]$ o corpo de decomposição de $x^n - 1$ sobre os racionais. O n-ésimo polinômio ciclotômico é definido como*

$$\Phi_n(x) = \prod_{(j,n)=1} (x - \zeta^j).$$

Para todo $D \subseteq D(n)$ definimos $\Phi_D = \prod_{d\in D} \Phi_d$.

Definição 5.15. *Se $D \subseteq D(n)$, definimos $S(D) = \{j \in \mathbb{Z}_n \mid (n, j) = n/d$ para algum $d \in D\}$ e $S^c(D) = \mathbb{Z}_n \setminus S(D) = \{j \in \mathbb{Z}_n \mid n/(n, j) \notin D\}$.*

Proposição 5.4. *Os polinômios ciclotômicos possuem as seguintes propriedades.*

1. *Para todo $n \geq 1$, o polinômio Φ_n tem coeficientes inteiros, é irredutível em $\mathbb{Q}[x]$ e tem grau $\phi(n)$.*
2. *Os automorfismos de $\mathrm{Gal}(F \mid \mathbb{Q})$ são os mapas $\zeta \mapsto \zeta^i$, com $i \in \mathbb{Z}_n^* = \{j \in \mathbb{Z}_n \mid (j, n) = 1\}$.*

3. *Os polinômios $\{\Phi_d \mid d \in D(n)\}$ são relativamente primos dois a dois.*

4. *Para qualquer $D \subseteq D(n)$, os vetores $\chi_{S(D)}$ e $\chi_{S^c(D)}$ estão em $\mathcal{F}(Q_n)$. A transformada de Fourier do ideal $\langle \Phi_D \rangle \subseteq Q_n$ é $\mathcal{F}(Q_n) \cap Z_{S(D)}$.*

Demonstração. Os primeiros fatos podem ser encontrados em qualquer livro que aborda o assunto. O último merece destaque. É simples verificar que para todo $x \in \mathbb{Z}_n^*$, o mapa $\psi : j \in S(D) \mapsto xj$ é uma bijeção de $S(D)$. Qualquer automorfismo $\sigma_i \in \mathrm{Gal}(F \mid \mathbb{Q})$, com $\sigma_i(\zeta) = \zeta^i$ mantém fixo os termos de $\mathcal{F}^{-1}(\chi_{S(D)})$, ou seja,

$$\sigma_i\Big(\sum_{k \in S(D)} \zeta^{k(-j)}\Big) = \sum_{k \in S(D)} \sigma_i(\zeta^{k(-j)}) = \sum_{k \in S(D)} \zeta^{ik(-j)} = \sum_{k \in S(D)} \zeta^{k(-j)},$$

onde a última igualdade segue do fato que $k \mapsto ik$ é uma bijeção de $S(D)$. Pela teoria de Galois, os coeficientes de $\mathcal{F}^{-1}(\chi_{S(D)})$ são racionais. Para o vetor $\chi_{S^c(D)}$, segue um raciocínio análogo, já que $k \in S^c(D) \mapsto ik$ é uma bijeção de $S^c(D)$.

Para a segunda parte, verifica-se prontamente que $\mathcal{F}(\langle \Phi_D \rangle) \subseteq \mathcal{F}(Q_n) \cap Z_{S(D)}$ observando que todo $j \in S(D)$ é da forma $j = kn/d$ com $k \in \mathbb{Z}_n^*$ e que $\zeta^j = \exp\{2\pi \mathbf{i} k/d\}$ é uma raiz primitiva d-ésima da unidade (pois $(i,k) = 1$). Para mostrar a inclusão reversa, tome $f \in \mathcal{F}(Q_n) \cap Z_{S(D)}$ e seja $\alpha = \mathcal{F}^{-1}(f)$. Como $f \in \mathcal{F}(Q_n)$ é evidente que $\alpha \in Q_n$ e como $f \in Z_{S(D)}$, para cada $d \in D$ devemos ter $\alpha(\zeta^{n/d}) = 0$. Mas o polinômio mínimo de $\zeta^{n/d} = e^{2\pi \mathbf{i}/d}$ é Φ_d, logo $\Phi_d \mid \alpha$. Pela propriedade 3, concluimos que $\Phi_D \mid \alpha$ e então $\alpha \in \langle \Phi_D \rangle$. □

Lema 5.5. *Sejam I, J ideais com $I = \langle \Phi_D \rangle$ e $J = \langle \Phi_E \rangle$, sendo $D, E \subseteq D(n)$. A transformada de Fourier do ideal $I \star J$ é dada por*

$$\mathcal{F}(I \star J) = \mathcal{F}(Q_n) \cap NZ_S, \tag{5}$$

onde $S = S^c(D) \cup S^c(E) \cup \big(S^c(D) + S^c(E)\big)$.

Demonstração. É simples verificar que, definindo o $\star$-produto de elementos de $\mathbb{C}^n$ como [†]

$$(z_i)_{i \in \mathbb{Z}_n} \star (w_i)_{i \in \mathbb{Z}_n} = n\Big(\sum_{j+k=i} z_j w_k\Big)_{i \in \mathbb{Z}_n},$$

temos $\mathcal{F}(\alpha \star \beta) = \mathcal{F}(\alpha) \star \mathcal{F}(\beta)$.

Pela propriedade 4, da proposição 5.4, temos $\chi_{S^c(D)} \in \mathcal{F}(I)$ e $\chi_{S^c(E)} \in \mathcal{F}(J)$. O elemento $\mathcal{F}\big(\mathcal{F}^{-1}(\chi_{S^c(D)}) \star \mathcal{F}^{-1}(\chi_{S^c(E)})\big) = \chi_{S^c(D)} \star \chi_{S^c(E)}$ deve, evidentemente,

[†] A semelhança com multiplicação de polinômios em C_n não é coincidência. O mapa $\mathcal{F}$ é um isomorfismo que leva a operação de multiplicação de polinômios em C_n ao produto componente a componente de $\mathbb{C}^n$ ou, de forma análoga, o produto $\star$ em $\mathbb{C}^n$ ao produto componente a componente (produto $\star$) em C_n.

pertencer a $I \star J$ e, sendo assim, $\chi_{S^c(D)} + \chi_{S^c(E)} + (\chi_{S^c(D)} \star \chi_{S^c(E)}) \in I \star J$.

É simples verificar que $\operatorname{supp}\big(\chi_{S^c(D)} + \chi_{S^c(E)} + (\chi_{S^c(D)} \star \chi_{S^c(E)}\big) = S$, logo, pela proposição 5.3, verificamos que, quando $I \star J$ é um ideal de C_n, a imagem $\mathcal{F}(I \star J)$ deve ser um ideal que contém NZ_S; nos restringindo aos racionais, temos $\mathcal{F}(I \star J) \supset \mathcal{F}(Q_n) \cap NZ_S$.

Para a inclusão reversa, observe que para todo $i \notin S$ e $a \in \mathcal{F}(I), b \in \mathcal{F}(J)$ todo termo da soma $\sum_{j+k=i} a_j b_k$ é zero (pois $i \notin S^c(D) + S^c(E)$), ou seja, $(a \star b)_i = 0$. Além disso, $a_i = b_i = 0$ pois $i \in S(D) \cap S(E)$. Com isso concluimos que $\mathcal{F}(I \star J) = \mathcal{F}(Q_n) \cap NZ_S$. □

Corolário 5.1. *Se $I_1 = \langle \Phi_{D_1} \rangle, \ldots, I_r = \langle \Phi_{D_r} \rangle$ são ideais, então*

$$\mathcal{F}(I_1 \star \cdots \star I_r) = \mathcal{F}(Q_n) \cap NZ_S,$$

com $S = \bigcup_{j=1}^{r} S^c(D_j) \cup \big(\bigcup_{T \subset [r]} \bigoplus_{k \in T} S^c(D_k)\big)$.

Demonstração. O caso $r = 2$ é apenas o lema anterior. A prova segue por indução da seguinte forma. $I_1 \star \ldots I_r$ é um ideal de Q_n e já sabemos que ele é gerado por $\langle \Phi_D \rangle$ para algum conjunto $D \subseteq D(n)$. Temos, pelo lema 5.5, $\mathcal{F}\big((I_1 \star \cdots \star I_r) \star I_{r+1}\big) = \mathcal{F}(Q_n) \cap NZ_{S'}$, com $S' = S^c(D) \cup S^c(D_{r+1}) \cup (S^c(D) + S^c(D_{r+1}))$. Porém, pela propriedade 4, da proposição 5.4 temos $\mathcal{F}(I_1 \star \cdots \star I_r) = \mathcal{F}(Q_n) \cap Z_{S(D)} = \mathcal{F}(Q_n) \cap NZ_{S^c(D)}$. Por outro lado, pela hipótese de indução temos $\mathcal{F}(I_1 \star \cdots \star I_r) = \mathcal{F}(Q_n) \cap NZ_S$ e segue que $S = S^c(D)$. Substituindo, obtemos

$$S' = S \cup S^c(D_{r+1}) \cup (S + S^c(D_{r+1})) = \bigcup_{j=1}^{r+1} S^c(D_j) \cup \Big(\bigcup_{T \subset [r+1]} \bigoplus_{k \in T} S^c(D_k) \Big).$$

□

Definição 5.16. *Dizemos que um elemento $\alpha \in Q_n$ é d-*periódico *se $x^d \alpha = \alpha$, com $n > d \in D(n)$. Dizemos que um ideal $I \subset Q_n$ é periódico se todos os seus elementos são d-periódicos.*

Ainda não discutimos o caso de elementos d-periódicos $\alpha \in Q_n$. Toda $\star$-potência de α é d-periódica e a soma de elementos d-periódicos também é d-periódica. Isso mostra que todo elemento de $\langle \alpha \rangle^{\star k}$ é d-periódico e, portanto, $1 \notin \langle \alpha \rangle^{\star k}$.

Lema 5.6. *O elemento Φ_D é periódico sse existe um primo $p \mid n$ tal que p^m é a maior potência de p que divide n e $\{p^m e \mid p \nmid e, e \mid n\} \subseteq D$.*

Demonstração. Seja $\pi_{n,d} = 1 + x^d + \cdots + x^{n-d}$, onde $d \in D(n)$. Observe que $\alpha = x^d \alpha$ sse $\pi_{n,d} \mid \alpha$. Além disso, como $x^n - 1 = (x^d - 1)\pi_{n,d}$, pela proposição 5.4, temos $\pi_{n,d} = \Phi_{\{e \mid e \in D(n), e \nmid d\}}$.

Suponha que Φ_D seja d-periódico. Então Φ_D é e-periódico para todo $d \mid e \in D(n) \setminus \{n\}$. Em particular, Φ_D é (n/p)-periódico para algum primo $p \mid n$. Então $\pi_{n,n/p} = \Phi_{\{e \mid e \in D(n), e \nmid n/p\}}$ divide Φ_D. Portando, $\{e \mid e \in D(n), e \nmid n/p\} = \{p^m e \mid p \nmid e, e \mid n\} \subseteq D$. □

Lema 5.7. *Se n é ímpar então $\mathbb{Z}_n^* \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^*) = \mathbb{Z}_n$. Se n é par então $\mathbb{Z}_n^* \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^*) \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^* + \mathbb{Z}_n^*) = \mathbb{Z}_n$.*

Demonstração. Seja $n = p_1^{r_1} \cdots p_m^{r_m}$ a fatoração de n. Pelo teorema Chinês do resto, associamos bijetivamente a cada $a \in \mathbb{Z}_n$, uma n-upla em $\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_1^{r_m}}$. As n-uplas correspondentes a elementos de $\mathbb{Z}_n \setminus \mathbb{Z}_n^*$ são aquelas em que pelo menos uma coordenada é nula. Se n é ímpar então, como $\mathbb{Z}_{p_i^{r_i}}^* + \mathbb{Z}_{p_i^{r_i}}^* = \mathbb{Z}_{p_i^{r_i}}$, fica claro que $\mathbb{Z}_n^* \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^*) = \mathbb{Z}_n$. Por outro lado, temos $\mathbb{Z}_{2^k}^* + \mathbb{Z}_{2^k}^* = 2\mathbb{Z}_{2^k}$. Se $i \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$ então $(i, n) > 1$. Se i for par, é simples ver que $i \in \mathbb{Z}_n^* + \mathbb{Z}_n^*$. Caso contrário $i - 1$ é par e, portanto, $i - 1 \in \mathbb{Z}_n^* + \mathbb{Z}_n^*$. Como $1 \in \mathbb{Z}_n^*$, temos $i \in \mathbb{Z}_n^* + \mathbb{Z}_n^* + \mathbb{Z}_n^*$. □

Teorema 5.3. *Se $\alpha \in Q_n$ e n tem $m = \omega(n)$ fatores primos distintos então ou α é periódico ou $\langle\alpha\rangle^{\star 3m} = Q_n$.*

Demonstração. Suponha que α não é periódico. Então, como todo ideal de Q_n é gerado pelo produto de polinômios ciclotômicos, pelo lema 5.6 segue que $\langle\alpha\rangle = \langle\Phi_D\rangle$ para algum $D \subset D(n)$ tal que, para todo primo $p \in D(n)$, existe $f_p \in D(n)$ com $f_p \notin D$ e $p \nmid (n/f_p)$. Observe que o conjunto $S' = \{n/f_p \mid p \text{ primo que divide } n\}$ está contido em $S^c(D)$. Além disso, $|S'| \leq m$ e o mdc de todos os elementos de S' é 1 por construção. Pelo teorema de Bézout, todo elemento de $\mathbb{Z}_n$ pode ser expresso como uma combinação linear de elementos de S' com coeficientes em $\mathbb{Z}_n$.

Seja $i \in \mathbb{Z}_n$ representado como $\sum_{s \in S'} c_s s$, com cada $c_s \in \mathbb{Z}_n$. Pelo lema 5.4, cada c_s é expresso como soma de no máximo 3 elementos de $\mathbb{Z}_n^*$, o que mostra que todo elemento de $\mathbb{Z}_n$ pode ser expresso como soma de no máximo $3m$ termos de $S^c(D)$, já que qualquer produto rs com $r \in S^c(D)$ e $s \in \mathbb{Z}_n^*$ está em $S^c(D)$. Aplicando o corolário 5.1 a $\langle\alpha\rangle^{\star 3m}$ teremos $S = \bigcup_{T \subseteq [r]} \bigoplus_{j \in T} S^c(D) = \mathbb{Z}_n$ e, portanto, $\mathcal{F}(\langle\alpha\rangle^{\star 3m}) \supseteq \mathcal{F}(Q_n)$. Logo, $\langle\alpha\rangle^{\star 3m} = Q_n$. □

Uma observação deve ser feita (não comentada no artigo original). Se $n \notin D$ ou então se existem dois elementos relativamente primos em $S^c(D)$, o conjunto S' pode ter seu tamanho reduzido para ≤ 2, o que prova uma cota bem melhor do que $3m$ para uma boa parte dos elementos de Q_n.

5.5 O Resultado Principal

Proposição 5.5. *Se $\alpha \in Q_n$ não é periódico e $\omega(n) = m$ então não há $9m$-impostores de α.*

Demonstração. Pelo teorema 5.3 sabemos que $1 \in \langle\alpha\rangle^{\star 3m}$, ou seja, existe um $\star$-polinômio p de grau $\leq 3m$ com $p(\alpha) = 1$. A proposição 5.1 nos diz que não há $9m$-impostores de α. □

Teorema 5.4. *Nenhum elemento de Q_n tem $9m$-impostores, onde $m = \omega(n)$. Efetivamente, todo subconjunto de $\mathbb{Z}_n$ é reconstrutível a partir de seu $9m$-deck.*

Demonstração. A proposição 5.5 lida com os elementos não periódicos de Q_n. Podemos detectar a periodicidade de um elemento a partir de seu 2-deck. Com efeito, $S_{\{0,d\}}(\alpha) = \langle\alpha, x^d\alpha\rangle$ e $S_{\{0,0\}}(\alpha) = \langle\alpha, \alpha\rangle = \|\alpha\|^2$. Como $\|x^d\alpha\| = \|\alpha\|$, por Cauchy-Schwarz, temos $|S_{\{0,d\}}(\alpha)| \leq S_{\{0,0\}}(\alpha)$ com igualdade sse $\alpha = x^d\alpha$. Além disso, se $\alpha = (a_0, \ldots, a_{n-1})$ é periódico e seu período mínimo é d, podemos construir o $9m$-deck de $\alpha' = (a_0, \ldots, a_{d-1}) \in Q_d$ a partir do $9m$-deck de α em Q_n (basta tomar $d_{\alpha',9m}(I) = d_{\alpha,9m}(I)$).

Se $\alpha, \beta \in Q_n$ são dois elementos com mesmo período minimal d e mesmo $9m$-deck então seus elementos induzidos α', β' também tem mesmo $9m$-deck. Como α' e β' não são periódicos e $\omega(d) \leq m$, pela proposição 5.5, não pode haver $9m$-impostores de α, portanto, $\beta' = x^{i'}\alpha'$ para algum $i' \in \mathbb{Z}_d$. Isso implica que $\beta = x^i\alpha$ para todo $i \equiv i' \pmod{d}$. □

6 Evitando Seqüências Monocromáticas com Intervalos Particulares [4]

Neste estudo, abordaremos algumas generalizações do teorema de Van der Waerden em progressões aritméticas. Podemos, por exemplo, fixar um conjunto S de inteiros positivos e nos perguntar se, para toda coloração de $\mathbb{N}$ com r cores, sempre podemos encontrar uma PA de k termos cuja razão é um elemento de S.

Chamamos um conjunto S de *r-grande* se, para toda r-coloração de $\mathbb{N}$, há PAs cuja razão está em S de tamanho arbitrariamente grande. Chamamos S de *grande* se S é r-grande para todo $r \geq 1$. Além de progressões aritméticas, consideraremos o seguinte tipo de seqüência.

Definição 6.1. *Seja $S \subseteq \mathbb{N}$. Uma seqüência de inteiros positivos $\{x_1, \ldots, x_k\}$ é uma* S-difseqüência *se $x_i - x_{i-1} \in S$ para $2 \leq i \leq k$.*

Definição 6.2. *Um conjunto de inteiros positivos S é chamado* r-acessível *se sempre que $\mathbb{N}$ é r-colorido, há S-difseqüências de tamanho arbitrariamente longo. Se S é r-acessívelpara todo $r \geq 1$ chamamos S de* acessível.

Definição 6.3. *Se S não é acessível, o* grau de acessibilidade *de S, denotado por $\mathrm{DA}(S)$ é o maior valor r tal que S é r-acessível.*

Denotamos por $f(S,k;r)$ o maior valor de n (se existir) tal que para toda r-coloração de $[1,n]$ há uma S-difseqüência monocromática com k termos. A família de todos os conjuntos r-acessíveis será denotada por $\mathcal{A}_r$ e $\mathcal{A} = \bigcap_r \mathcal{A}_r$ é a família de todos os conjuntos acessíveis. Analogamente, $\mathcal{L}_r$ é a família de todos os conjuntos r-grandes e $\mathcal{L}$ é a família dos conjuntos grandes.

Lema 6.1. *Seja $c \geq 0$, $r \geq 2$ e S um conjunto de inteiros positivos. Se para toda $(r-1)$-coloração de S encontramos $(S+c)$-difseqüências de tamanho arbitrariamente grande em S então $S + c \in \mathcal{A}_r$.*

Demonstração. Seja $S = \{s_i \mid i \in \mathbb{N}\}$ e assuma que toda $(r-1)$-coloração de S admite $(S+c)$-difseqüências de tamanho arbitrariamente grande. Seja χ uma r-coloração de $\mathbb{N}$. Vamos provar por indução em k que há $(S+c)$-difseqüências monocromáticas com k termos.

A base da indução ($k = 1$) é trivial. Suponha $k \geq 1$ e que, sob a coloração χ, existe uma $(S+c)$-difseqüência $X = \{x_1, \ldots, x_k\}$. Podemos assumir que X tem cor vermelha. Considere $A = \{x_k + s_i + c \mid s_i \in S\} = S + x_k + c$. Se algum membro de A é vermelho, encontramos uma $(S+c)$-difseqüência de tamanho $k+1$. Caso contrário, temos uma $(r-1)$-coloração de A, que é apenas um deslocamento do conjunto S. Nossa hipótese inicial nos grante que há difseqüências de tamanho arbitrariamente longo em A. □

Lema 6.2. *Seja S um conjunto de inteiros positivos. Se $f(S,k;r) = M$ então $f(jS,k;r) = j(M-1)+1$.*

Demonstração. Como $f(S,k;r) = M$, para qualquer coloração χ de $T = \{i \cdot j + 1 \mid i = 0, \ldots, M-1\}$ devemos ter uma jS-difseqüência monocromática de k termos. Basta definir $\chi' : [1,M] \to \{0,1\}$ como $\chi'(i) = \chi((i-1)j+1)$ e verificar que qualquer S-difseqüência monocromática (sob χ') $x_1, \ldots, x_k \in [1,M]$ induz a seqüência $\{(x_i - 1)j + 1\}$, que é monocromática em $[1, j(M-1)+1]$ sob a coloração χ.

Por outro lado, seja χ uma r-coloração de $[1, M-1]$ que evite S-difseqüências monocromáticas. Defina a r-coloração χ' do intervalo $[1, j(M-1)]$ por

$$\chi'(n) = \chi\Big(\Big\lceil \frac{n}{j} \Big\rceil\Big).$$

Suponha por contradição que $\chi'(x'_1) = \cdots = \chi'(x'_k)$, com $x'_i - x'_{i-1} \in jS$. Pela maneira como χ' é definida, tomando $x_i = \lceil x'_i / j \rceil$ temos que $x_i - x_{i-1} \in S$ e $\chi(x_1) = \cdots = \chi(x_k)$, o que é absurdo. □

Teorema 6.1. *Seja $a \in \mathbb{N} \setminus \{1,3\}$ e*

$$S = \{(a-1)a^j \mid j = 0, 1, \ldots\} \cup \{(a-1)^2 a^j \mid j = 0, 1, \ldots\}.$$

Então $2 \leq \mathrm{DA}(S) \leq a$. Além disso, $f(S,k;2) \leq a^k - a + 1$ para todo $k \geq 1$.

Demonstração. Para mostrar que $\mathrm{DA}(S) \leq a$ vamos mostrar uma $(a+1)$-coloração de $\mathbb{N}$ que evita S-difseqüências monocromáticas de 2 termos. Defina $\chi : \mathbb{N} \to \mathbb{Z}_{a+1}$ de forma que $\chi(x) = \bar{x}$. Suponha que $\chi(y) = \chi(z)$ e $z - y \in S$. Por definição, temos $(a+1) \mid (z-y)$. Sendo assim, ou $(a+1) \mid (a-1)a^j$ ou $(a+1) \mid (a-1)^2 a^j$ para algum $j \geq 0$. Se p é um primo que divide $a+1$ então p não divide a, mas então $p \mid (a-1)^2$. Como $\mathrm{mdc}(a+1, a-1) \leq 2$, devemos ter $p = 2$ e $a+1 = 2^k$. Segue que $a-1 = 2(2^{k-1}-1)$ e, portanto, $k \leq 2$, mas isso contradiz o fato de que $a \notin \{1, 3\}$.

Vamos completar a prova mostrando que toda coloração $\alpha : [1, a^k - a + 1] \to \{0, 1\}$ contém uma S-difseqüência monocromática. O resultado seguirá por indução em k. Obviamente, ele vale para $k = 1$. Assuma $k \geq 2$ e que o resultado vale para $k-1$. Seja $X = \{x_1, \ldots, x_{k-1}\}$ uma S-difseqüência monocromática, digamos com cor 0, contida em $[1, a^{k-1} - a + 1]$. Considere o conjunto $A = \{x_{k-1} + (a-1)a^i \mid i = 0, \ldots, k-1\}$. Observe que $A \subseteq [1, a^k - a + 1]$. Se existe $y \in A$ cuja cor é 0 então $X \cup \{y\}$ é uma S-difseqüência monocromática de k termos. Caso contrário, A é uma S-difseqüência monocromático com k termos. □

Corolário 6.1. *Se* $S = \{2^i \mid i \geq 0\}$ *então* $\mathrm{DA}(S) = 2$ *e*

$$8(k-3) + 1 \leq f(S, k; 2) \leq 2^k - 1,$$

para todo $k \geq 3$*.*

Tomando $a = 2$ no teorema 6.1 verificamos que $\mathrm{DA}(S) = 2$ e que a cota superior está correta. Para a cota inferior podemos utilizar indução em k.

Lema 6.3. *Sejam* $m \geq 2$ *e* $i \geq 1$ *com* $\mathrm{mdc}(i, m) = 1$*. Seja* $S = \{x \in \mathbb{N} \mid x \equiv i \pmod{m}\}$*. Então* $S \notin \mathcal{A}_2$*.*

Demonstração. Seja $\chi : \mathbb{N} \to \{0, 1\}$ definida de forma que $\chi(x) = 0$ se e somente se x é múltiplo de m. Seja X uma S-difseqüência qualquer de m termos sendo x_1 o primeiro termo. Se $x_1 \equiv j \pmod{m}$ então a seqüência, módulo m, é $j, j+i, \ldots, j+(m-1)i$. Observe que, como $\mathrm{mdc}(i, m) = 1$, todos esses m valores são distintos e, portanto, devemos ter um múltiplo de m e $m-1$ não-múltiplos de m em X, ou seja, X não pode ser monocromática sob χ. □

A partir do lema acima é simples verificar que se $a \geq 3$ então $T = \{a^i \mid i \geq 0\} \notin \mathcal{A}_2$. Basta verificar que $T \subseteq \{x \mid x \equiv 1 \pmod{a-1}\}$ e aplicar o lema.

É simples mostrar que $\mathcal{A}_2 \neq \mathcal{L}_2$. Para tal fim, tome $S = \{2\} \cup (2\mathbb{N}+1)$. Pelo lema 6.1 verificamos que $S \in \mathcal{A}_2$. Para verificar que $S \notin \mathcal{L}_2$, é só tomar $m = 4$ no

Teorema 6.2. *Se* S *é um conjunto* 2*-grande então, para cada inteiro positivo* m*, há uma infinidade de múltiplos de* m *em* S*.*

Demonstração. Basta mostrar que, para todo m, existe um múltiplo de m em S (e assim segue que há um múltiplo de $m^2, m^3, \ldots$ e, portanto, uma infinidade de múltiplos de m). Suponha que S não contenha múltiplos de um inteiro positivo m. Defina $\chi : \mathbb{N} \to \{0, 1\}$ tal que

$$\chi(n) = 0 \Leftrightarrow n \bmod 2m \in \{1 \bmod 2m, \ldots, m \bmod 2m\}.$$

Suponha que S seja 2-grande e tome uma PA $X = \{x, x + d, \ldots, x + nd\}$, com $d \in S$ monocromática sob a coloração χ. Pela definição de χ, temos $\chi(n+2m) = \chi(n)$ para todo n. Logo, se $d \equiv i \pmod{2m}$, com $0 < i < 2m$, então $x, x + i, \ldots, x + ni$ é uma seqüência monocromática.

Suponha $i < m$. Como $x \bmod 2m$ pertence a um dos intervalos $[1, m]$ ou $[m + 1, 2m]$, é evidente que dando um "salto" de i elementos a frente de $x \bmod 2m$ devemos permanecer no mesmo intervalo. Como i é pequeno demais para pular o intervalo de tamanho m contendo a cor $1 - \chi(x)$, todos os m saltos devem ocorrer dentro do intervalo, o que é impossível mesmo se $i = 1$. Se $i > m$, podemos imaginar que os saltos são feitos para trás, pulando $2m - i < m$ elementos, um caso simétrico ao tratado acima. □

Lema 6.4. *Se $r \geq 1$ e S não contém múltiplos de r então $S \notin \mathcal{A}_r$.*

Demonstração. Considere a r-coloração $\chi : \mathbb{N} \to \mathbb{Z}_r$ dada por $\chi(n) = n \bmod r$. Tal coloração evita qualquer S-difseqüência monocromática com dois termos. □

Teorema 6.3. *Seja $m \geq 2$ e $S_m = \mathbb{N} \setminus m\mathbb{N}$. Então $\mathrm{DA}(S_m) = m - 1$.*

Demonstração. A partir do lema 6.4 é imediato que $\mathrm{DA}(S_m) \leq m - 1$. Para provar a desigualdade no sentido contrário, seja χ qualquer $(m - 2)$-coloração de S_m. Como cada elemento de S_m pertence a uma das classes de congruência $[1, m - 1]$ e há apenas $m - 2$ cores, devem haver uma cor c e $i, j \in \mathbb{Z}_m (i \neq j)$ tais que $\chi^{-1}(\{c\})$ contém infinitos elementos congruentes a i e infinitos elementos congruentes a j. Pela definição de S_m, ordenando $\chi^{-1}(\{c\})$, obtemos uma S_m-difseqüência monocromática já que a diferença entre termos consecutivos da seqüência é um inteiro da forma $am \pm (i - j) \in S_m$. □

6.1 Translações do Conjunto de Primos

Denotamos por P o conjunto de todos os primos. Estaremos interesados em verificar quando uma translação $P + t$ é acessível. Fica claro pelo lema 6.4 que se $t \geq 0$ é par então $P + t$ não pode ser acessível já que não há múltiplos de $2t + 2$ em $P + t$. Não é sabido se alguma translação par de P é 2-acessível, no entanto, toda translação ímpar de P é acessível, como veremos nesta seção.

Seja $\mathbf{b} = (b_1, \ldots, b_k) \in \mathbb{Z}^k$, $p \in P$ e $x \in \mathbb{R}^+$. Definimos

$$\pi(x; \mathbf{b}) = \#\{n \mid 1 < n + b_i \leq x \text{ é primo para todo } i \in [1, k]\};$$
$$\rho(p; \mathbf{b}) = \#\{b_i \bmod p \mid i \in [1, k]\};$$
$$\sigma(\mathbf{b}) = \prod_{p \in P} \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\rho(p; \mathbf{b})}{p}\right);$$
$$Q = \{n \mid 1 < n + b_i \leq x, i \in [1, k]\};$$
$$T(x; \mathbf{b}) = \sum_{n \in Q} \prod_{i=1}^{k} \frac{1}{\log(n + b_i)}.$$

Teorema 6.4. (Balog) *Sejam $k \in \mathbb{Z}^+$, $x \in \mathbb{R}^+$ suficientemente grande, t um inteiro não-negativo fixado e*

$$B = \left\{ \left(0, q_1 + t, \ldots, \sum_{i=1}^{k-1} (q_i + t)\right) \mid q_i \in P \cap [k, x/2k] \text{ para todo } i \in [1, k-1] \right\}.$$

Defina $Z = \{\mathbf{b} \in B \mid\}$. Então

$$\sum_{\mathbf{b} \in Z} |\pi(x; \mathbf{b}) - \sigma(\mathbf{b}) T(x; \mathbf{b})| \ll_k \frac{x^k}{\log^{2k} x} \tag{6}$$

Teorema 6.5. (Primos em Progressões Aritméticas – Dirichlet) *Seja $k > 0$ e $\mathrm{mdc}(a, k) = 1$. Defina $\pi_a(x) = \#\{p \mid p \in P, p \leq x, p \equiv a \pmod{k}\}$. Então*

$$\pi_a(x) \sim \frac{x}{\varphi(k) \log x} \text{ quando } x \to \infty,$$

onde φ é a função de Euler.

Definição 6.4. *Seja $p \in P$. Denominamos um conjunto de polinômios $\mathcal{P} \subseteq \mathbb{Z}[y]$ de* p-admissível *se existe um inteiro h tal que p não divide nenhum $f(h)$ com $f \in \mathcal{P}$. Se $\mathcal{P}$ é p-admissível para todo primo p então chamamos $\mathcal{P}$ de* admissível.

Lema 6.5. *Seja $k \geq 2$ e $t \geq 1$ ímpar. Para $\mathbf{z} = (z_1, \ldots, z_{k-1}) \in \mathbb{Z}^{k-1}$, defina o conjunto*

$$Y_{\mathbf{z}} = \left\{ y + \sum_{j=1}^{i-1} (z_j + t) \Big| 1 \leq i \leq k \right\} \subset \mathbb{Z}[y] \text{ e seja}$$

$$M = \{\mathbf{q} \mid q_i \in P \cap (k, x/2k], \text{para } i \in [1, k) \text{ e } Y_{\mathbf{q}} \text{ admissível}\}$$

para $x \in \mathbb{R}^+$ suficientemente grande. Então $|M| \gg_k x^{k-1} / \log^{k-1} x$.

Demonstração. Se $p > k$ então é simples ver que $Y_{\mathbf{q}}$ é p-admissível. Basta observar que há no máximo k classes de congruência $\pmod p$ em $Y_{\mathbf{q}}$, logo há uma classe de congruência $j \in \mathbb{Z}_p$ tal que para $y = 0$ temos $j \notin Y_{\mathbf{q}}$. [†] Tomando $y = p - j$ podemos garantir que $0 \notin Y_{\mathbf{q}}$.

Suponha então que $p \leq k$ e sejam $r_1 = 2, r_2 = 3, \ldots, r_d$ todos os primos $\leq k$. Tome h não múltiplo de nenhum r_i. Temos que $r_i | h+q_1+t$ se e somente se $q_1 \equiv -h-t \pmod{r_i}$. Podemos escolher inteiros $a_i \in [1, r_i - 1]$ tais que $a_i \not\equiv -h - t \pmod{r_i}$ (lembrando que t e h são ímpares, verificamos prontamente que $a_1 = 1$). Sendo $m = r_1 \times \cdots \times r_d$, pelo Teorema Chinês do Resto, sabemos que existe um inteiro $c_1 \in [0, m-1]$ tal que $c_1 \equiv a_i \pmod{r_i}$ para todo $i = 1, \ldots, d$. Ademais, $\mathrm{mdc}(c_1, m) = 1$, caso contrário algum r_i divide c_1, o que é absurdo.

Pelo Teorema de Dirichlet (teo. 6.5), o número de escolhas possíveis para q_1 (congruentes a $c_1 \bmod m$) é assintoticamente

$$\frac{1}{\varphi(m)} \cdot \frac{x/2k}{\log(x/2k)} = \frac{1}{2k\varphi(m)} \cdot \frac{x}{\log x - \log 2k} > \frac{1}{2k\varphi(m)} \cdot \frac{x}{\log x}.$$

Fixado q_1, o processo de escolha de q_2 é análogo e, consecutivamente, determinamos valores para $q_1, \ldots, q_{k-1}$. Ao fim as escolhas garantem que nenhum r_i divide qualquer elemento de $Y_{\mathbf{q}}$, como desejávamos. Notando que $\varphi(m)$ é uma constante que só depende de k verificamos que

$$|M| \gg_k \left(\frac{x}{\log x}\right)^{k-1}.$$

□

Usando o teorema 6.4 e o lema 6.5 temos o seguinte resultado.

Lema 6.6. *Para $k \geq 2$, $t \geq 1$ ímpar e $x \in \mathbb{R}^+$ suficientemente grande, defina*

$$W = \Big\{(p, q_1, \ldots, q_{k-1}) \mid p \in P, q_i \in P \cap (k, x/2k)\Big\} \text{ e}$$

$$S = \Big\{(p, q_1, \ldots, q_{k-1}) \in W \mid p + \sum_{j=1}^{i}(q_j + t) \leq x \text{ é primo para } i = 1, \ldots, k-1\Big\}.$$

Então $|S| \gg_k x^k / \log^{2k-1} x$.

Demonstração. Usaremos a notação do teorema 6.4 e do lema 6.5. Em particular, M é definido exatamente como no lema 6.5 e $\mathbf{b} = \mathbf{b}(\mathbf{q}) = \big(0, q_1 + t, \ldots, \sum_{j=1}^{k-1}(q_j + t)\big)$. Para aplicar o teorema 6.4, devemos obter cotas para ρ, σ e T.

[†] Estamos abusando da notação, na verdade nos referimos aos elementos de $Y_{\mathbf{q}}$ módulo p.

É evidente que ao restringirmos a soma (6) aos $\mathbf{b}$ tais que $\sigma(\mathbf{b}) > 0$ ainda podemos usar a cota do teorema (já que cada termo da soma é não-negativo).

Sabe-se que $\sigma(\mathbf{b}) < \infty$. Vamos mostrar que para todo $\mathbf{q} = (q_1, \ldots, q_{k-1}) \in M$ temos $\sigma(\mathbf{b}) > 0$. Para termos $\sigma(\mathbf{b}) = 0$ é necessário que para algum $p \in P$ tenhamos $\rho(p; \mathbf{b}) = p$. Se isso ocorre, $\{b_1 \bmod p, \ldots, b_k \bmod p\}$ é o conjunto de todos os resíduos módulo p. Mas isso contraria a hipótese de que $Y_{\mathbf{q}}$ é admissível. Usando a desigualdade trivial $\rho(p, \mathbf{b}) \leq k$, temos a seguinte cota

$$\sigma(\mathbf{b}) \geq \prod_{p \leq k} \frac{1}{p}\Big(1 - \frac{1}{p}\Big)^{-k} \prod_{p > k} \Big(1 - \frac{k}{p}\Big)\Big(1 - \frac{1}{p}\Big)^{-k} = \sigma_k, \tag{7}$$

uma constante que só depende de k. Vamos mostrar que $\sigma_k > 0$.

O primeiro produtório de (7) é positivo, portanto precisamos mostrar a convergência do produtório infinito. Seja $1 + a_p = (1 - 1/p)^{-k}(1 - k/p)$. Vamos utilizar a desigualdade $1 + x > \exp\{x - x^2/2\}, (0 < x \leq 1)$ observando que para algum p_0, temos $a_p \leq 1$ para todo $p > p_0$ e então

$$\prod_{p > p_0} (1 + a_p) > \prod_{p > p_0} \exp\Big\{a_p - \frac{1}{2}a_p^2\Big\} = \exp\Big\{\sum_{p > p_0} a_p - \frac{1}{2}\sum_{p > p_0} a_p^2\Big\}. \tag{8}$$

É simples verificar que se $\sum_p |a_p|$ converge então $\sum_p a_p$ e $\sum_p a_p^2$ também convergem e o lado direito de (8) é positivo.

Pelo teorema binomial temos

$$a_p = \frac{(1 - k/p) - (1 - 1/p)^k}{(1 - 1/p)^k} = \frac{\sum_{j=2}^{k} (-1)^{k-j+1}\binom{k}{i} p^{-i}}{(1 - 1/p)^k}, \text{ logo}$$

$$|a_p| \leq \frac{\sum_{j=2}^{k} \binom{k}{i} p^{-i}}{(1 - 1/p)^k} \leq \frac{p^{-2}\sum_{j=2}^{k} \binom{k}{i}}{(1 - 1/2)^k} < \frac{4^k}{p^2},$$

e como $\sum_p p^{-2}$ converge, concluímos que $\sum_p |a_p|$ converge. A partir de (7) provamos que para todo $\mathbf{b} \in M$, temos $\sigma(\mathbf{b}) \geq \sigma_k > 0$.

A cota para $T(x, \mathbf{b})$ segue de

$$\begin{aligned}\#\{n \mid 1 < n + b_i \leq x, i \in [1, k]\} = (x - b_k) + O(1) &= x - \sum_{j=1}^{k-1}(q_i + t) + O(1) \\ &> x - k\frac{x}{2k} - kt + O(1) = \frac{x}{2} + O(1),\end{aligned}$$

pois k e t são constantes que podem ser absorvidas pelo $O(1)$. Isso nos dá

$$T(x, \mathbf{b}) > \Big(\frac{x}{2} + O(1)\Big)\frac{1}{\log^k x}. \tag{9}$$

A partir do teorema 6.4 inferimos que

$$\sum_{\mathbf{q}\in M}\big|\#\{n \mid n+b_i \text{ é primo para } i\in[1,k]\}-\sigma(\mathbf{b})T(x,\mathbf{b})\big| \ll_k \frac{x^k}{\log^{2k} x}. \tag{10}$$

Observe que $b_1 = 0$ e $S \supset \{(n,\mathbf{q}) \mid n+b_i \text{ é primo para } i\in[1,k], \mathbf{b}=\mathbf{b}(\mathbf{q}), \mathbf{q}\in M\}$. Utilizando as cotas (7), (9), (10) e o lema 6.5 temos

$$\begin{aligned}
|S| &\geq \sum_{\mathbf{q}\in M}\#\{n \mid n+b_i \text{ é primo para } i\in[1,k]\}\\
&\gg_k \sum_{\mathbf{q}\in M}\sigma(\mathbf{b})T(x,\mathbf{b}) - O\Big(\frac{x^k}{\log^{2k} x}\Big)\\
&\gg_k \sigma_k|M|\Big(\frac{x}{2}+O(1)\Big)\frac{1}{\log^k x} - O\Big(\frac{x^k}{\log^{2k} x}\Big)\\
&\gg_k \sigma_k\Big(\frac{x}{\log x}\Big)^{k-1}\Big(\frac{x}{2}+O(1)\Big)\frac{1}{\log^k x} - O\Big(\frac{x^k}{\log^{2k} x}\Big)\\
&\gg_k \frac{x^k}{\log^{2k-1} x},
\end{aligned}$$

para todo x suficientemente grande. □

Teorema 6.6. *Para todo $t \geq 1$ ímpar P contém $(P+t)$-difseqüências arbitrariamente grandes. Ademais, $P+t \in \mathcal{A}_2$*

Demonstração. A primeira parte segue da aplicação direta do lema 6.6. A segunda parte segue da primeira associada ao lema 6.1. □

Referências

[1] B. Chazelle, *The discrepancy method: randomness and complexity*. Cambridge University Press, 2000.

[2] N. Alon, J. Pach, and J. Solymosi, "Ramsey-type theorems with forbidden subgraphs.," *Combinatorica*, vol. 21, no. 2, pp. 155–170, 2001.

[3] A. J. Radcliffe and A. D. Scott, "Reconstructing subsets of $\mathbb{Z}_n$," *J. Comb. Theory Ser. A*, vol. 83, no. 2, pp. 169–187, 1998.

[4] B. M. Landman and A. Robertson, "Avoiding monochromatic sequences with special gaps," *Arxiv Preprint*, 2003.