NOTAS DE AULA DO

PICME

Programa de Iniciação Científica e Mestrado em Combinatória

http://www.ime.usp.br/~tcco/picme

Anotado por: Henrique Stagni

2^o semestre de 2016

Conteúdo

1 O problema de Kakeya **1**
- 1.1 Conjuntos de Besikovitch 2
- 1.2 Conjunto de Kakeya para Corpos Finitos 2

2 Aplicações do Lema de Schartz-Zippel **3**

3 O Teorema de Mantel para grafos aleatórios **5**

4 Teorema de Erdős-Stone baseado em supersaturação **8**

5 Estabilidade do Teorema de Turán **10**

6 Cintura e número cromático altos **11**
- 6.1 Hipergrafos com cintura e número cromáticos altos 11
- 6.2 Grafos com cintura alta e número cromático alto 14
- 6.3 Número de vértices do grafo $\Gamma_i(n)$ 16

7 Lema Local de Lovász **17**
- 7.1 Primeiro Momento / Cota da união 17
- 7.2 Digrafo de dependência 18
- 7.3 Lema Local de Lovász 19
- 7.4 Demonstração do Lema Local de Lovász 20
- 7.5 Versão algorítmica 21
  - 7.5.1 Ferramentas da prova 22

1 O problema de Kakeya

⋄ ⋄ ⋄ *Aula 1 (16 de Agosto) — Yoshiharu Kohayakawa* ⋄ ⋄ ⋄

1.1 Conjuntos de Besikovitch

Em 1917, Kakeya fez a seguinte pergunta:

> Qual é a menor área de uma região no plano em que podemos girar 360 graus uma agulha de comprimento unitário?

Por "girar", entende-se que deve ser possível transladar e rotacional a agulha para todas as direções. Um exemplo trivial de uma tal região é um disco de raio $\frac{1}{2}$, cuja área é $\frac{1}{4}\pi$. Um deltóite (ver Figura **??**) é um exemplo de uma tal região, de área $\frac{1}{8}\pi$.

De maneira um tanto surpreendente, Besicovitch mostrou que existem regiões cuja área é *arbitrariamente pequena* e que satisfazem as condições da pergunta de Kakeya.

Definimos um *conjunto de Besikovitch/Kakeya* como um conjunto que contém um segmento unitário de qualquer direção. Note que em um conjunto de Besikovitch não é necessário mover o segmento unitário. Dado um conjunto de Besikovitch no plano, é possível *[Pendente]*

Conjectura 1.1. *Todo conjunto de Besikovitch tem dimensão de Hausdorff d.*

[Pendente]

⋄ ⋄ ⋄ *Aula 2 (17 de Agosto) — Yoshiharu Kohayakawa* ⋄ ⋄ ⋄

1.2 Conjunto de Kakeya para Corpos Finitos

Seja $\mathbb{F}$ um corpo finito de tamanho $q = |\mathbb{F}|$. Considere $\mathbb{F}^n$ como um espaço vetorial.

Dizemos que $K \subseteq \mathbb{F}^n$ é um *conjunto de Kakeya* se para todo $\boldsymbol{u} \in \mathbb{F}^n$, existe algum $\boldsymbol{a} \in \mathbb{F}^n$ tal que $\boldsymbol{a} + t\boldsymbol{u} \in K$ para todo $t \in \mathbb{F}$.

Teorema 1.2 (Duir 2009)**.** *Se K é um conjunto de Kakeya, então $|K| \geq \binom{q+n-1}{n}$.*

Observação 1.3. Para n fixo, a cota inferior do Teorema 1.2 corresponde a uma fração positiva do $\mathbb{F}^n$. De fato,

$$\binom{q+n-1}{n} \leq \left(\binom{q+n-1}{n}\right)^n \geq \left(\frac{q}{n}\right)^n = \frac{1}{n^n}|\mathbb{F}^n|.$$

Lema 1.4 (Schartz-Zippel)**.** *Seja $\mathbb{F}$ um corpo finito, $S \subseteq \mathbb{F}$ e $p \in \mathbb{F}[x_1, \dots, x_m]$ um polinômio de grau $\partial p \leq d$. Seja*

$$R = \{\boldsymbol{r} = (r_1, \dots, r_m) \in S^m : p(\boldsymbol{r}) = 0\}$$

Então $|R| \leq d|S|^{m-1}$.

Demonstração. Escreva p como um polinômio sobre x_1, cujos coeficientes são elementos não nulos $p_1, \dots, p_k \in \mathbb{F}[x_2, \dots, x_m]$, i.e.

$$p = \sum_{i=0}^{k} p_i(x_2, \dots, x_m) x_1^i.$$

Seja $R_1 = \{\boldsymbol{r} = (r_1, \dots, r_m) \in R : p_k(r_2, \dots, r_m) = 0\}$. Por indução em m temos

$$\#\{(r_2, \dots, r_m) \in S^{m-1} : p_k(r_2, \dots, r_m) = 0\} \leq (\partial p_k)|S|^{m-2} \leq (d-k)|S|^{m-2}.$$

Portanto $|R_1| \leq |S|(d-k)|S|^{m-2} = (d-k)|S|^{m-1}$. Seja $R_2 = R \setminus R_1$. Se $\boldsymbol{r} = (r1, \ldots, r_m) \in R_2$, então $p_k(r_2, \ldots, r_m) \neq 0$. Portanto $\tilde{p}(x_1) := p(x_1, r_2, \ldots, r_m) \in \mathbb{F}[x_1]$ é não-nulo e tem grau k. Assim, $\#\{r_1 : \tilde{p}(r_1) = 0\} \leq k$. Portanto $|R_2| \leq k|S|^{m-1}$. Logo, $|R| \leq d|S|^{m-1}$. □

Observação 1.5. Note que a cota dada pelo Lema de Schartz-Zippel vale com igualdade se consideramos um polinômio $p' \in \mathbb{F}[x_1]$ com d raízes distintas e o estendemos a um polinômio $p \in \mathbb{F}[x_1, \ldots, x_m]$ (de modo que $x_2, \ldots, x_m$ são variáveis livres em p).

Seja $p(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_m]$ e denote $(x_1, \ldots, x_n)$ por $\boldsymbol{x}$. Escrevemos $\boldsymbol{x} = \sum c_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$, onde a soma é sobre todas as n-uplas de inteiros $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ satisfazendo $\sum_{i=1}^n \alpha_i \leq \partial p$, $\boldsymbol{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ e $c_\alpha \in \mathbb{F}$.

Lema 1.6. *Sejam $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N \in \mathbb{F}^n$ e $N < \binom{d+n}{n}$. Então existe polinômio não-nulo $p(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ com $\partial p \leq d$ tal que $p(\boldsymbol{a}_i) = 0$ para todo $1 \leq i \leq N$.*

Demonstração. Note que existem exatamente $\binom{d+n}{n}$ n-uplas de inteiros $\boldsymbol{\alpha} = (a_i)_{i=1}^n$, $a_i \geq 0$, tais que $\sum_{i=1}^n \alpha_i \leq d$.

Queremos $p = \sum c_{\boldsymbol{\alpha}} x^\alpha$ com $\partial p \leq d$, $p \not\equiv 0$ e $p(\boldsymbol{a}_i) = 0$ para todo $1 \leq i \leq N$. Tais restrições dão origem a um sistema linear homogêneo com $\binom{d+n}{n}$ variáveis mas apenas $N < \binom{d+n}{n}$ equações. Logo, existe $(c_{\boldsymbol{\alpha}}) \neq 0$ que é uma solução para o sistema. □

Demonstração do Teorema 1.2. Suponha, por contradição, que existe $K \subseteq \mathbb{F}^{n-1}$ de Kakeya e $|K| < \binom{q+n-1}{n}$. Pelo Lema 1.6, existe polinômio $p(x_1, \ldots, x_n)$ não-nulo com $\partial p \leq q-1$ e $p(\boldsymbol{a}) = 0$, para todo $\boldsymbol{a} \in K$. Fixe $\boldsymbol{u} \in \mathbb{F}^n \setminus \{0\}$. Como K é de Kakeya, existe $\boldsymbol{a} \in \mathbb{F}^n$ tal que $\boldsymbol{a} + t\boldsymbol{u} \in K$ para todo $t \in \mathbb{F}$. Considere o polinômio $f(t) = p(\boldsymbol{a} + t\boldsymbol{u})$. Temos $\partial f \leq \partial p = d \leq q-1$. Ademais, $f(t) = 0$ para todo $t \in \mathbb{F}$. Segue que f é o polinômio nulo. Em particular, o coeficiente $[t^d]f(t)$ de t^d de f é nulo. Temos

$$\begin{aligned}
[t^d]f(t) = [t^d]p(\boldsymbol{a} + t\boldsymbol{u}) &= [t^d] \sum_{\boldsymbol{\alpha}:\sum \alpha_i \leq d} (\boldsymbol{a} + t\boldsymbol{u})^{\boldsymbol{\alpha}} \\
&= [t^d] \sum_{\boldsymbol{\alpha}:\sum \alpha_i = d} (\boldsymbol{a} + t\boldsymbol{u})^{\boldsymbol{\alpha}} = [t^d] \sum_{\boldsymbol{\alpha}:\sum \alpha_i = d} (\boldsymbol{u})^{\boldsymbol{\alpha}} = \text{“parte homogênea de } p(\boldsymbol{x})\text{”}.
\end{aligned}$$

Seja $\overline{p}(\boldsymbol{x}) = \sum_{\boldsymbol{a}:\sum_{a_i}=d} c_{\boldsymbol{a}} \boldsymbol{x}^{\boldsymbol{\alpha}}$ a parte homogênea de $p(\boldsymbol{x})$. Concluímos que $\overline{p}(\boldsymbol{u}) = 0$ para todo $u \in \mathbb{F}^n$. Mas pelo Lema de Schartz-Zippel temos

$$\{\boldsymbol{r} \in \mathbb{F}^n : \overline{p}(r) = 0\} \leq dq^{n-1} \leq (q-1)q^{n-1} < q^n = |\mathbb{F}|^n,$$

uma contradição. □

◇ ◇ ◇ *Aula 3 (30 de Agosto) — Bruno Cavalar* ◇ ◇ ◇

2 Aplicações do Lema de Schartz-Zippel

Seja X um conjunto finito e $\cdot : X \times X \to X$ uma operação binária sobre X. Estamos interessado em verificar se $\cdot$ é uma operação *associativa*, isto é, se para qualquer tripla $(a, b, c) \in X^3$ vale que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Uma primeira idéia para um algoritmo para verificar se $\cdot$ é associativa consiste em tomar uma tripla $(a, b, c) \in X^3$ uniformemente ao acaso e verificar se (a, b, c) é uma *tripla associativa*, i.e. se $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Infelizmente, o exemplo a seguir mostra que é possível definir uma operação não-associativa $\cdot$ sobre um conjunto X de forma que apenas uma tripla dentre as $|X|^3$ triplas é não-associativa.

Exempplo 2.1. Sejam x, y, a elementos distintos de um conjunto finito X. Defina uma operação $\cdot : X \times X \to X$ fazendo $x \cdot y = x$ e $b \cdot c = a$ para todo par $(b, c) \in X^2$ tal que $(b, c) \neq (x, y)$. Neste caso, temos que a tripla (x, y, y) é não-transitiva pois $x \cdot (y \cdot y) = a$ e $(x \cdot y) \cdot y = x$. Por outro lado, é fácil verificar que para qualquer outra tripla $(\alpha, \beta, \gamma) \neq (x, y, y)$, temos $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma = a$.

O exemplo acima mostra que é possível que apenas uma fração $\frac{1}{|X|^3}$ das triplas testemunhe que $(X, \cdot)$ é não-associativa. Ainda assim, mostraremos que existe um algoritmo com tempo de execução $O(|X|^2)$ que é capaz de determinar com alta probabilidade se $(X, \cdot)$ é associativo. Para isso, usaremos o Lema de Schartz-Zippel, que é enunciado a seguir usando a linguagem de probabilidade.

Lema 2.2 (Schartz-Zippel (versão probabilística))**.** *Seja $p \in K[x_1, \dots, x_m]$ um polinômio de grau $\partial p \leq d$, $S \subseteq K$ um conjunto finito e $\mathbf{x} \in_U S^m$ um vetor escolhido uniformemente ao acaso em S^m. Então*

$$\mathbb{P}(p(x) = 0) \leq \frac{d}{|S|}.$$

Seja $\mathbb{F}$ um corpo finito com $|\mathbb{F}| \geq 6$. Considere o espaço vetorial $\mathbb{F}^X$ de vetores com entradas em $\mathbb{F}$ indexado por elementos de X. Definimos $e : X \to \mathbb{F}^X$, fazendo $e(x)$ ser o vetor que possui entrada 1 na coordenada indexada por x e 0 nas demais coordenadas.

Note que fixado $u \in \mathbb{F}^X$, existem $(u_x)_{x \in X}$ que satisfazem $u = \sum_{x \in X} u_x e(x)$. Definimos uma operação binária $\boxdot : \mathbb{F}^X \times \mathbb{F}^X \to \mathbb{F}^X$ da seguinte forma. Dados $u = \sum_{x \in X} u_x e(x)$ e $v \in \sum_{y \in X} v_y e(y)$, definimos

$$u \boxdot v := \sum_{x,y} \in X u_x v_y e(x) \boxdot e(y) := \sum_{x,y \in X} u_x v_y e(x \cdot y).$$

Proposição 2.3. *$(X, \cdot)$ é associativa se, e somente se, $(\mathbb{F}^X, \boxdot)$ é associativa.*

Demonstração. **(⇐)** Basta notar que se $(X, \cdot)$ possui uma tripla não associativa $(a, b, c) \in X^3$, então a tripla $(e(a), e(b), e(c))$ é não associativa em $\mathbb{F}^X$. De fato,

$$\begin{aligned}
(e(a) \boxdot e(b)) \boxdot e(c) &= e(a \cdot b) \boxdot e(c) \\
&= e((a \cdot b) \cdot c) \\
&\neq e(a \cdot (b \cdot c)) \\
&= e(a) \boxdot e(b \cdot c) \\
&= e(a) \boxdot (e(b) \boxdot e(c)).
\end{aligned}$$

(⇒) Suponha que $(X, \cdot)$ seja associativa. Então para quaisquer $u, v, w \in \mathbb{F}^X$, temos

$$(u \boxdot v) \boxdot w = \sum_{x,y,z \in X} u_x v_y w_z e((x \cdot y) \cdot z) = \sum_{x,y,z \in X} e(x \cdot (y \cdot z)) = u \boxdot (v \boxdot w).$$

□

Agora estamos em condições de descrever um algoritmo que para verificar se $(X,\cdot)$ é associativa.

Algorithm 1 Algoritmo probabilístico para verificar se $(X,\cdot)$ é associativa

1: Para todo $x \in X$, escolha $\alpha_x, \beta_x, \gamma_x \in \mathbb{F}$ uniformemente ao acaso.
2: Faça $u \leftarrow \sum_{x\in X} \alpha_x e(x)$, $v \leftarrow \sum_{x\in X} \beta_x e(x)$, $w \leftarrow \sum_{x\in X} \gamma_x e(x)$.
3: **Se** $u \boxdot (v \boxdot w) \neq (u \boxdot v) \boxdot w$
4: **então devolva** Não-Associativa.
5: **senão devolva** Associativa.

Segue da Proposição 2.3 que se $(X,\cdot)$ é associativa, então o algoritmo acima sempre dá a resposta correta. O resultado abaixo mostra que se $(X,\cdot)$ não é associativa, então o algoritmo dá a resposta correta com alta probabilidade.

Teorema 2.4. *Suponha que $(X,\cdot)$ é não-associativa e sejam u,v,z escolhidos como na linha* 2 *do Algoritmo 1. Então $\mathbb{P}((u,v,w)$ ser associativa$) \leq \frac{1}{2}$.*

Demonstração. Seja $(a,b,c) \in X^3$ uma tripla não-associativa. Podemos supor, sem perda de generalidade, que $\alpha_a, \beta_b, \gamma_c$ são os últimos elementos a serem escolhidos no primeiro passo do algoritmo. Seja $r = (a\cdot(b\cdot c))$. Vamos mostrar que

$$\mathbb{P}((u \boxdot (v \boxdot w))_r \neq ((u \boxdot v) \boxdot w)_r) \leq \frac{1}{2},$$

da onde seguirá o resultado desejado.

Defina $f(\alpha_a, \beta_b, \gamma_c) = (u \boxdot (v \boxdot w))_r \in \mathbb{F}[\alpha_a, \beta_b, \gamma_c]$ e $g(\alpha_a, \beta_b, \gamma_c) = ((u \boxdot v) \boxdot w)_r \in \mathbb{F}[\alpha_a, \beta_b, \gamma_c]$. Observe que

$$f(\alpha_a, \beta_b, \gamma_c) = \sum_{\substack{x,y,z\in X\\ x\cdot(y\cdot z)=r}} \alpha_x \beta_y \gamma_z$$

e que $\alpha_a\beta_b\gamma_c$ aparece no polinômio f com coeficiente 1. Logo $\partial f = 3$. Além disso, como (a,b,c) é não-associativa, segue que $\alpha_a\beta_b\gamma_c$ não aparece no polinômio g (caso contrário, teríamos $(a\cdot b)\cdot c = r$).

Portanto, $f(\alpha_a, \beta_b, \gamma_c) - g(\alpha_a, \beta_b, \gamma_c)$ é um polinômio não-nulo de 3 variáveis e grau 3. Aplicando o Lema 2.2, obtemos

$$\mathbb{P}(f(\alpha_a, \beta_b, \gamma_c) - g(\alpha_a, \beta_b, \gamma_c) = 0) \leq \frac{3}{|F|} \leq \frac{1}{2},$$

como desejado. □

⋄ ⋄ ⋄ *Aula 4 (06 de Agosto) — Marcelo Soares Campos* ⋄ ⋄ ⋄

3 O Teorema de Mantel para grafos aleatórios

Seja $\mathrm{ex}(G,H) = \max\{e(G) : G \not\supset H, v(G) = n\}$. O Teorema de Mantel pode ser escrito da seguinte forma.

Teorema 3.1 (Mantel, 1907).

$$\mathrm{ex}(G, K_3) = \left\lceil \frac{n}{2} \right\rceil \left\lfloor \frac{n}{2} \right\rfloor = \left(\frac{1}{4} + o(1) \right) n^2.$$

Para o grafo aleatório $G(n,p)$ de Erdős-Renyi, definimos

$$\mathrm{ex}(G(n,p), H) = \max\{e(G), G \subset G(n,p), G \not\supset H\}.$$

Queremos provar o seguinte resultado.

Teorema 3.2 (Frankl-Rodl, 1986). *Para $p \gg 1/\sqrt{n}$, $\mathrm{ex}(G(n,p), K_3) = (\frac{1}{4} + o(1))pn^2$ com alta probabilidade.*

Observação 3.3. Para mostrar a desigualdade $\mathrm{ex}(G(n,p), K_3) \geq (\frac{1}{4} + o(1))pn^2$, é suficiente considerar a intersecção de $G(n,p)$ com o grafo $K_{\lfloor n/2 \rfloor \lceil n/2 \rceil}$. De fato, seja $X = e(G(n,p) \cap K_{\lfloor n/2 \rfloor \lceil n/2 \rceil}$. Temos $\mathbb{E}(X) = \frac{1}{4}pn^2$ e $\mathrm{Var}(X) = n\frac{p}{4}(1 - \frac{p}{4})$. Logo, segue da Desigualdade de Chebychev que

$$\mathbb{P}(|X - \mathbb{E}(X)| \geq n) \leq \frac{\mathrm{Var}(X)}{n^2} = \frac{p(1 - \frac{p}{4})}{4n} \to 0,$$

quando $n \to \infty$.

Para demonstrar o Teorema 3.2, vamos precisar do resultado de *supersaturação* abaixo, que afirma que se um grafo G tem uma quantidade de arestas significativamente maior do que $\frac{1}{4}n^2$, então há muitas cópias de triângulos em G.

Lema 3.4 (Supersaturação de triângulos). *Para todo $\varepsilon > 0$, existe $\delta > 0$ tal que se um graf G, $v(G) = n$, satisfaz $e(G) \geq (\frac{1}{4} + \varepsilon)n^2$, então G contém pelo menos $\delta\binom{n}{3}$ triângulos.*

Demonstração. Seja $t = \left\lceil \sqrt{2/\varepsilon} \right\rceil$. Pelo Teorema de Mantel, temos que se H é um grafo com t vértices e com número de arestas $e(H) \geq (\frac{1}{4} + \frac{1}{2}\varepsilon)t^2 \geq \frac{1}{4}t^2 + 1$, então H contém um triângulo. Vamos mostrar que podemos tomar $\delta = \frac{\varepsilon}{2}\binom{t}{3}^{-1}$.

Seja $\mathcal{T} = \binom{V(G)}{t} = \{T \subseteq V(G) : |T| = t\}$. Para qualquer grafo H, definimos a *densidade* $d(H)$ de H como $d(H) = |e(H)|/\binom{v(H)}{2}$. A seguir, biparticionamos $\mathcal{T}$ de acordo com a densidade do grafo induzido por seus elementos. Mais especificamente, definimos

$$\mathcal{R} = \left\{ T \in \mathcal{T} : d(G[T]) > \frac{1}{2} + \frac{\epsilon}{2} \right\} \quad \text{e} \quad \mathcal{S} = \left\{ T \in \mathcal{T} : d(G[T]) \leq \frac{1}{2} + \frac{\varepsilon}{2} \right\}.$$

Note que a densidade $d(G)$ de G pode ser expressa como a média da densidade dos grafos induzidos por membros de $\mathcal{T}$. De fato, temos

$$\frac{\sum_{T \in \mathcal{T}} d(G[T])}{\binom{n}{t}} = \frac{\sum_{T \in \mathcal{T}} e(G[T])}{\binom{t}{2}\binom{n}{t}} = \frac{e(G)\binom{n-2}{t-2}}{\binom{t}{2}\binom{n}{t}} = \frac{e(G)}{\binom{n}{2}} = d(G).$$

Daí, segue que a cardinalidade $\mathcal{R}$ corresponde a uma fração $\frac{1}{2}\varepsilon$ de $\mathcal{T}$. De fato,

$$\binom{n}{t}\left(\frac{1}{2}+\varepsilon\right) \leq \binom{n}{t}d(G) \leq |\mathcal{S}| \cdot \left(\frac{1}{2}+\frac{\varepsilon}{2}\right) + |\mathcal{R}| \cdot 1$$

o que implica $|\mathcal{R}| \geq \frac{\varepsilon}{2}\binom{n}{t}$.

Usamos agora o fato de $G[T]$ conter um triângulo, para todo $T \in \mathcal{R}$. Observamos, também, que cada um desses triângulos pertence a no máximo $\binom{n-3}{t-3}$ conjuntos $T \in \mathcal{R}$. Logo, o número de triângulos em G é pelo menos

$$\frac{|\mathcal{R}|}{\binom{n-3}{t-3}} \geq \frac{\varepsilon\binom{n}{t}}{2\binom{n-3}{t-3}} = \frac{\varepsilon\binom{n}{3}}{2\binom{t}{3}} = \delta\binom{n}{3},$$

como desejado. □

Para provar o Teorema 3.2, precisaremos também do Lema de Containers para triângulos, enunciado abaixo.

Lema 3.5 (Containers para triângulos)**.** *Para todo $\delta > 0$, existe $C > 0$ tal que para todo inteiro n existe uma coleção $\mathcal{G}$ de grafos e uma função $f : \mathcal{P}(E(K_n)) \to \mathcal{G}$ satisfazendo as seguintes propriedades.*

1. *Para todo grafo G livre de triângulos, existe $S \subseteq E(G)$, $|S| \leq Cn^{3/2}$, tal que $E(G) \subseteq f(S)$.*
2. *Para todo $S \subseteq E(K_n)$, o grafo $f(S)$ possui no máximo δn^3 cópias de triângulos.* □

Demonstração do Teorema 3.2. Segue da Observação 3.3, que $\mathrm{ex}(G(n,p),K_3) \geq (\frac{1}{4}+o(1))pn^2$. Para provar a outra desigualdade, mostraremos que para todo $\varepsilon > 0$, a probabilidade de existir algum grafo G livre de triângulos e com pelo menos $m = (\frac{1}{4}+2\varepsilon)pn^2$ arestas contido em $G(n,p)$ é arbitrariamente pequena.

Fixe $\varepsilon > 0$ e seja δ dado como no Lema 3.4. Seja G um grafo livre de triângulos com pelo menos m arestas. Pelo Lema 3.5, existe $S \subseteq E(G)$, $|S| \leq Cn^{3/2}$, tal que $f(S)$ possui no máximo δn^3 triângulos. Segue do Lema 3.4, que $f(S)$ possui no máximo $(\frac{1}{4}+\varepsilon)n^2$ arestas. Agora, notamos que se um tal G estivesse contido em $G(n,p)$, então teríamos $|f(S) \cap E(G(n,p))| \geq m$. Logo, para provarmos o resultado desejado, é suficiente mostrar que $\mathbb{P}(Y \geq 1) \to 0$, onde

$$Y = \#\{S \subseteq E(G(n,p)) : |f(S) \cap E(G(n,p))| \geq m\}.$$

Fixe S e seja $X_S = f(S) \cap E(G(n,p))$. Como $\mathbb{E}(X_S) \leq (\frac{1}{4}+\varepsilon)pn^2$, segue da desigualdade de Chernoff que

$$\mathbb{P}(X_S \geq m - |S|) \leq \exp\{kpn^2\},$$

para algum $k = k(\varepsilon)$, uma vez que $|S| \ll \mathbb{E}(X)$. Logo, temos

$$\mathbb{P}(Y \geq 1) \leq \mathbb{E}(Y) \leq \sum_{s=0}^{Cn^{3/2}} p^s \mathbb{P}(X_S \geq m - |S|) \leq \sum_{s=0}^{Cn^{3/2}} p^s e^{-kpn^2} \leq \sum_{s=0}^{Cn^{3/2}} \left(\frac{epn^2}{2s}\right)^s e^{-kpn^2}.$$

Usando o fato que a função $s \mapsto (epn^2/2s)^s$ atinge seu máximo em $epn^2/4 \ll Cn^{3/2}$, concluímos que, na soma acima, o último termo limita superiormente cada um dos demais. Logo,

$$\mathbb{P}(Y \geq 1) \leq Cn^{3/2} \left(\frac{epn^2}{2Cn^{3/2}} \right)^{Cn^{3/2}} e^{-kpn^2} \to 0,$$

como desejado. □

◇ ◇ ◇ *Aula 5 (20 de Agosto) — Marcelo Tadeu Sales* ◇ ◇ ◇

4 Teorema de Erdős-Stone baseado em supersaturação

Dado um grafo H, defina

$$\mathrm{ex}(n, H) = \max\{e(G) : |V(G)| = n, G \not\supseteq H\}.$$

Exemplos:

1. se $H = K_r$ temos, pelo Teorema de Turan: $\mathrm{ex}(n, K_r) = 1 - \frac{1}{r-1}\frac{n^2}{2}$;
2. $\mathrm{ex}(n, C_4) = O(n^{3/2})$.

Teorema 4.1 (Erdős-Stone-Simonovits). *Para todo $\varepsilon > 0$ e grafo H, com número cromático $\chi(H) \geq 2$, existe $n_0 = n_0(\varepsilon, H)$ tal que para todo $n \geq n_0$,*

$$\mathrm{ex}(n, H) < \left(1 - \frac{1}{\chi(H) - 1} + \varepsilon\right) \frac{n^2}{2}.$$

Observação 4.2. Se $\chi(H) = r$, o grafo de Turán $T(n, r-1)$ mostra que

$$\lim_{n\to\infty} \frac{\mathrm{ex}(n, H)}{n^2} = 1 - \frac{1}{r-1}.$$

Para a demonstração do Teorema 4.1 precisaremos do seguinte resultado de supersaturação, cuja demonstração é análoga a do Lema 3.4 (caso $r = 3$).

Teorema 4.3 (Supersaturação). *Para todo $\varepsilon > 1$ e inteiro $r \geq 2$, existem $\delta > 0$ e n_0 tal que se G é um grafo tal que $|V(G)| \geq n_0$ e $e(G) \geq (1 - \frac{1}{r-1} + \varepsilon)\frac{n^2}{2}$, então G contém pelo menos δn^r cópias de K_r.* □

Um *r-grafo* é um hipergrafo cujas arestas são conjuntos de tamanho r. Dados inteiros $u_1, \ldots, u_r \geq 0$, definimos $K^{(r)}(u_1, \ldots, u_r)$ como um r-grafo cujos vértices são particionados em classes $V_1, \ldots, V_r$, com $|V_i| = u_i$ e tal que $\{x_1, \ldots, x_r\}$ é uma aresta para todo $x_1 \in V_1, \ldots, x_r \in V_r$.

Veremos que o Teorema 4.1 segue como consequência do Teorema 4.3 e do resultado abaixo, que afirma que todo r-grafo com densidade positiva de arestas contém uma cópia de $K^{(r)}(t, \ldots, t)$.

Teorema 4.4 (Erdős). $\mathrm{ex}(n, K^{(r)}(t, \ldots, t)) = o(n^r)$.

Demonstração do Teorema 4.1. Seja H um grafo fixo, com $|V(H)| = t$ e número cromático $r = \chi(H)$. A seguir, denotamos por $K_{t,\ldots,t}$ o grafo r-partido completo cujas classes têm cardinalidade t. Note que $K_{t,\ldots,t} \supseteq H$.

Seja G um grafo e com $|V(G)| = n$ vértices e

$$e(G) \geq \left(1 - \frac{1}{r-1} + \varepsilon\right) n^2$$

Considere o r-grafo F tal que $V(F) = V(G)$ e $\{x_1, \dots, x_r\} \in E(F)$ se, e somente se, os vértices $x_1, \dots, x_r$ induzem um K_r em G. Pelo Teorema 4.3, existem pelo menos δn^r cópias de K_r ($\delta = \delta(\varepsilon)$) em G. Logo $e(F) \geq \delta n^r$. Concluímos, pelo Teorema 4.4 que F contém um $K^{(r)}(t, \dots, t)$, o que implica que $G \supseteq K_{t,\dots,t} \supseteq H$, como desejado. □

Para demonstrar o Teorema 4.4 precisaremos do seguinte lema.

Lema 4.5. *Sejam $A_1, \dots, A_n$ subconjuntos de $[N]$. Suponha que $\sum_{i=1}^n |A_i| = M$. Então para todo $t < n$ existem índices distintos $i_1, \dots, i_t$ tais que*

$$|A_{i_1} \cap \cdots \cap A_{i_t}| \geq \frac{N\left(\frac{M}{N}\right)^t - t^2 n^{t-1} N}{n^t}.$$

Demonstração. TODO □

Demonstração do Teorema 4.4. Façamos por indução em r. Para o caso $r = 2$, fixe $\delta > 0$ e seja G é um grafo com $V(G) = [n]$ e $e(G) \geq \delta n^2$. Queremos mostrar que $K^{(2)}(t,t) \subseteq G$. Para todo $i \in [n]$, seja $A_i = N(i) \subseteq [n]$ os conjunto de vértices adjacentes a i. Sabemos que $\sum_{i=1}^n |A_i| = 2e(G)$. Segue do Lema 4.5 ($r = 2, N = n$) que existem índices $i_1, \dots, i_t$ tais que

$$|A_{i_1} \cap \cdots \cap A_{i_t}| \geq \left(n\left(\frac{2\delta n^2}{n}\right)^t - t^2 n^{t-1} N\right) / n^t = (2\delta)^t - t^2 \geq t,$$

para n suficientemente grande. Daí concluímos que $K^{(2)}(t,t) \subseteq G$.

Agora suponha que $r > 2$ e que o Teorema vale para $r-1$-grafos. Fixe $\delta > 0$ e seja F um r-grafo com $e(F) \geq \delta n^r$. Queremos mostrar que $F \supseteq K^{(r)}(t, \dots, t)$. Defina

$$A_i = \left\{B \in \binom{[n]}{r-1} : (B \cup \{i\}) \in E(F)\right\}.$$

Note que $\sum_{i=1}^n |A_i| = re(G)$. Aplicando o Lema 4.5 ($N = n^{r-1}$ e $M = re(F) \geq r\delta n^r$), obtemos índices $i_1, \dots, i_t$ tais que

$$|A_{i_1} \cap \cdots \cap A_{i_t}| \geq (r^t \delta^t) n^{r-1} - (t^2) n^{r-2} \geq \delta^t n^{r-1},$$

para n suficientemente grande. Logo, por hipótese de indução, o $r-1$ grafo com conjunto de arestas $A_{i-1} \cap \cdots \cap A_{i_t}$ contém uma cópia de $K^{(r-1)}(t, \dots, t)$. Segue da definição dos A_i, que os vértices de tal cópia em conjunto com os vértices $i_1, \dots, i_t$ induzem uma cópia de $K^{(r)}$ em F. □

⋄ ⋄ ⋄ *Aula 6 (27 de Agosto) — Marcelo Tadeu Sales* ⋄ ⋄ ⋄

5 Estabilidade do Teorema de Turán

Sabemos, pelo Teorema de Turán, que todo grafo livre de K_{r+1} de tamanho n possui no máximo $e(T_{n,r})$ arestas, onde $T_{n,r}$ é o grafo r-partido balanceado de n vértices. O resultado abaixo mostra que se o número de arestas de um grafo G livre de K_{r+1} é próximo desse número máximo, então G está próximo de um grafo r-partido.

Teorema 5.1 (Füredi)**.** *Seja $G = (V, E)$ um grafo livre de K_{r+1} e tal que $e(G) \geq e(T_{n,r}) - t$. Então existe subgrafo r-partido $H \subseteq G$ tal que $e(H) \geq e(G) - t$.*

Demonstração. Seja x_1 um vértice de maior grau em G. Defina $V_1^+ = N_G(x_1)$ e $V_1 = V \setminus V_1^+$. Temos

$$|V_1||V_1^+| \geq \sum_{x \in V_1} d(x) = e(V_1, V_1^+) + 2e(V_1).$$

Seja x_2 um vértice de maior grau em $G_1 \coloneqq G[V_1^+]$ e seja $V_2^+ = N_{G_1}(x_2)$. e $V_2 = V_1^+ \setminus V_2^+$. Temos

$$|V_2||V_2^+| \geq \sum_{x \in V_2} d_{G_1}(x) = e(V_2, V_2^+) + 2e(V_2).$$

Em geral, defina x_i como um vértice de maior grau em $G_{i-1} \coloneqq G[V_{i-1}^+]$, $V_i^+ = N_{G_{i-1}}(x_i)$ e $V_i = V \setminus V_i^+$. Temos

$$|V_i||V_i^+| \geq \sum_{x \in V_i} d_{G_{i-1}}(x) = e(V_i, V_i^+) + 2e(V_i).$$

O processo pára em um índice s tal que $V_s^+ = \emptyset$ e temos portanto $V = \dot\bigcup_{i=1}^s V_i$. Como $\{x_1, \ldots, x_s\}$ é um clique em G, devemos ter $s \leq r$.

Ao somarmos a Equação (5) para todo $1 \leq i \leq s$, obtemos

$$\sum_{i=1}^{s} |V_i||V_i^+| \geq \sum_{i=1}^{s} (e(V_i, V_i^+) + e(V_i)) + e(V_i) = e(G) + \sum_{i=1}^{s} e(V_i) \geq e(T_{r,n}) - t + \sum_{i=1}^{s} e(V_i).$$

Por outro lado, também temos

$$\sum_{i=1}^{s} |V_i||V_i^+| = e(K(V_1, \ldots, V_s)) \leq e(T_{r,n}).$$

Combinando as duas últimas equações, concluímos que $\sum_{i=1}^s e(V_i) \leq t$. Logo, um grafo H como no enunciado do Teorema pode ser obtido, a partir de G, ao deletarmos as arestas dentro de cada V_i. □

Corolário 5.2. *Seja $G = (V, E)$ um grafo livre de K_{r+1} e tal que $e(G) \geq e(T_{n,r}) - t$. Então existe uma partição $V = \dot\bigcup_{i=1}^r V_i$ tal que*

$$|E(G) \triangle E(K(V_1, \ldots, V_r))| \leq 3t$$

Corolário 5.3. *Seja H um subgrafo r-partido de G obtido a partir da remoção de t arestas, como no Teorema. Seja $\{V_i\}_{i=1}^r$ uma r-partição (própria) de H. Como $e(H) \geq e(G) - t \geq e(T_{r,n}) - 2t$, podemos adicionar no máximo $2t$, basta adicionar no máximo $2t$ arestas a H para obtermos o grafo completo $K(V_1, \ldots, V_r)$.*

O resultado abaixo mostra que G não só está próximo de um grafo r-partido, mas também está próximo ao grafo r-partido balanceado $T_{n,r}$.

Afirmação 5.4. *Se $r|n$ e $e(K(V_1,\dots,V_r)) \geq e(T_{n,r}) - 2t$, então*

$$E(K(V_1,\dots,V_r)) \triangle E(T_{n,r})| \leq n\sqrt{rt}.$$

Demonstração. Seja $m = n/r$ e sejam $a_1,\dots,a_r$ inteiros tais que $|V_i| = m + a_i$. Note que $\sum_{i=1}^r a_i = 0$ e que $e(T_{n,r}) = \binom{r}{2}m^2$. Por outro lado,

$$e(K(V_1,\dots,V_r)) = \sum_{i\neq j}(m+a_i)(m+a_j) = \sum_{i\neq j} m^2 + (a_i+a_j)m + a_ia_j = \binom{r}{2}m^2 + (r-1)\cancelto{0}{(a_1+\cdots+a_r)}m + \sum_{i\neq j} a_ia$$

Segue da hipótese $e(T_{n,r}) - e(K(V_1,\dots,V_r)) \leq 2t$ que $-\sum_{i\neq j} a_ia_j \leq 2t$. Mas como

$$0 = \left(\sum_{i=1}^r a_i\right)^2 = (a_1^2 + \cdots + a_r^2) + 2\sum_{i\neq j} a_ia_j,$$

temos $(a_1^2 + \cdots + a_r^2)/2 \leq 2t$. Podemos aplicar a desigualdade de Jensen para obter

$$4t \geq a_1^2 + \cdots + a_r^2 \geq \frac{(|a_1| + \cdots + |a_r|)^2}{r},$$

isto é, $|a_1| + \cdots + |a_r| \leq 2\sqrt{rt}$. Concluímos que há no máximo $\sqrt{rt}$ índices i tais que $a_i \geq 0$. Como mover cada tal vértice para outra partição altera no máximo N adjacências, a diferença simétrica entre $E(K(V_1,\dots,V_r))$ e $E(T_{n,r})$ é no máximo $n\sqrt{rt}$. □

6 Cintura e número cromático altos

6.1 Hipergrafos com cintura e número cromáticos altos

◇ ◇ ◇ *Aula 7 (11 de Outubro) — Giulia Maesaka* ◇ ◇ ◇

Seja X um conjunto finito. Dizemos que $(X,\mathcal{M})$ é um *k-grafo*, i.e. um hipergrafo uniforme de tamanho k, se $\mathcal{M} \subseteq \binom{X}{k}$.

Um *circuito* de comprimento p em $(X,\mathcal{M})$ é uma sequência de arestas $M_1,\dots,M_p \in \mathcal{M}$ tal que existe uma sequência de vértices distintos $x_1,\dots,x_p \in X$ satisfazendo $x_i \in M_i \cap M_{(i+1) \bmod p}$ para todo $i = 1,\dots,p$

Denotamos por $\mathrm{g}(X,\mathcal{M})$ a *cintura* do hipergrafo $(X,\mathcal{M})$, isto é, o comprimento de um menor circuito em $(X,\mathcal{M})$.

Um k-grafo $(X,\mathcal{M})$ é a-partido se X admite uma partição $X = \dot\bigcup_{i=1}^a X_i$ tal que $M \cap X_i| \leq 1$ para todo $M \in \mathcal{M}$ e todo $1 \leq i \leq a$.

Teorema 6.1. *Para quaisquer inteiros positivos k, n e p, existe um k-grafo $(X,\mathcal{M})$ tal que*

1. $\mathrm{g}(X,\mathcal{M}) > p$.

2. $\chi(X,\mathcal{M}) > n$.

Seja $(\dot{\bigcup}_{i=1}^{a} X_i, \mathcal{M})$ um k-grafo a-partido e $(Y, \mathcal{N})$ um K-grafo tal que $K = |X_r|$ para algum $r \in [a]$. Dadas bijeções $f_N \colon X_r \to N$ para todo $N \in \mathcal{N}$, definimos a *amalgamação* $(Y, \mathcal{N}) \star (\dot{\bigcup}_{i=1}^{a} X_i, \mathcal{M})$ como o k-grafo a-partido $(\dot{\bigcup}_{i=1}^{a} X_i', \mathcal{M}')$, onde

1. $X_r = Y$ e $X_i' = X_i \times N$ para todo $i \neq r$.
2. $\mathcal{M}' = \{\mathbf{e}(M, N) : M \in \mathcal{M}, N \in \mathcal{N}\}$, onde

$$\mathbf{e}(M,N) = \{(X_i \cap M, N) : i \neq r \text{ and } M \cap X_i \neq \varnothing\} \cup \{f_N(X_r \cap M) : M \cap X_r \neq \varnothing\}.$$

Demonstração do Teorema 6.1. Provamos por indução em p. Para $p = 1$, basta tomar o k-grafo completo $([n(k-1)+1], \binom{n(k-1)+1}{k})$.

Agora assuma $p \geq 2$ e que para todo $p' < p$ e para quaisquer inteiros k e n, existe um k-grafo $(X, \mathcal{M})$ com $\chi(X, \mathcal{M}) > n$ e $\mathrm{g}(X, \mathcal{M}) > p$.

Dados inteiros k e n considere uma sequência $((\dot{\bigcup}_{i=1}^{a} X_i^1, \mathcal{M}^1), \ldots (\dot{\bigcup}_{i=1}^{a} X_i^{a+1}, \mathcal{M}^{a+1}))$ de k-grafos a-partidos tal que

1. $(\dot{\bigcup}_{i=1}^{a} X_i^1, \mathcal{M}^1)$ é um grafo com cintura maior que p e satisfazendo a seguinte propriedade: para todo $W \subseteq [a]$, $|W| = k$, existe $M \in \mathcal{M}^1$ tal que $|M \cap X_i| \neq \varnothing$ para todo $i \in W$. Note que podemos construir um tal grafo com $\binom{a}{k}$ arestas disjuntas.
2. Para todo $1 \leq t \leq a$,

$$(\dot{\bigcup_{i=1}^{a}} X_i^{t+1}, \mathcal{M}^{t+1})) = (Y^{(t)}, \mathcal{N}^{(t)}) \star (\dot{\bigcup_{i=1}^{a}} X_i^{t}, \mathcal{M}^{t})),$$

onde $(Y^t, \mathcal{N}^t)$ é um $|X_t^t|$-grafo com $\chi(Y^t, \mathcal{N}^t) > n$ e $\mathrm{g}(Y^t, \mathcal{N}^t) > p - 1$. (por hipótese de indução, é possível construir um tal grafo) e a operação de amalgação é feita com respeito a bijeções $f_N^{(t)} : X_t^t \to N (N \in \mathcal{N}^t)$ quaisquer.

Seja $G = (\bigcup_{i=1}^{n} i X_i^{a+1}, \mathcal{M}^{a+1})$. Vamos provar que G é o hipergrafo que queremos, isto é, que $\mathrm{g}(G) > p$ e $\chi(G) > n$.

Afirmação 6.2. *Se $(\dot{\bigcup}_{i=1}^{a} X_i, \mathcal{M})$ não tem circuito menor ou igual a p e (Y, N) não tem circuito menor ou igual a $p-1$, então a amalgamação $(\dot{\bigcup}_{i=1}^{a} X_i', \mathcal{M}') := (Y, N) \star (\dot{\bigcup}_{i=1}^{a} X_i, \mathcal{M})$ não tem circuito menor ou igual a p.*

Demonstração. Suponha por absurdo que $((M_1, N_1), \ldots, (M_q, N_q))$ é um circuito em $(\dot{\bigcup}_{i=1}^{a} X_i', \mathcal{M}')$ de tamanho $q \leq p$.

- **Caso 1:** $N_1 = N_2 = \cdots = N_q = N$**.** Neste caso, o grafo induzido por $\{(X_i, N_i) : i \neq r\} \cup f_N(X_r)\}$ é isomorfo a $(\dot{\bigcup}_{i=1}^{a} X_i, M)$, que por hipótese não tem um circuito de tamanho menor ou igual a p.
- **Caso 2: Existe** $i \neq j$ **tal que** $N_i \neq N_j$**.** Sem perda de generalidade, assumimos $i = 1$ e $j = 2$. Note que devemos ter

$$(M_1, N_1) \cap (M_2, N_2) = f_{N_1}(M_1 \cap X_r) = f_{N_2}(M_2 \cap X_r).$$

Se $N_1 = N_q$ também teríamos

$$(M_1, N_1) \cap (M_q, N_q) = f_{N_1}(M_1 \cap X_r),$$

um absurdo, uma vez que o circuito não pode repetir vértices. Logo, devemos ter $N_1 = N_q$.

Seja $(N'_1, N'_2, \ldots, N'_{q'})$ a sequência obtida a partir de $(N_1, N_2, \ldots, N_q)$ ao identificarmos elementos consecutivos iguais. *[Pendente]*.

Logo, $N'_i, N'_{i+1}, \ldots, N'_{i+l}$ é um segmento da sequência $(N'_1, \ldots, N'_{q'})$ com todos os elementos distintos e com $N'_{i+l+1} = N'_i$, $l < q' - 1 \leq q - 1$. Logo, $N'_i, \ldots, N'_{i+l}$ é um circuito em $(Y, \mathcal{N})$ de tamanho $l + 1 \leq q - 1 \leq p - 1$, o que contradiz a hipótese da afirmação. Logo $(\dot\bigcup_{i=1}^{a} X'_i, \mathcal{M}')$ de fato não possui circuitos de tamanho menor ou igual a p.

□

Segue construção da sequência $((\dot\bigcup_{i=1}^{a} X_i^1, \mathcal{M}^1), \ldots (\dot\bigcup_{i=1}^{a} X_i^{a+1}, \mathcal{M}^{a+1}) = G)$ que $\mathrm{g}(G) > p$.

Afirmação 6.3. $\chi(\dot\bigcup_{i=1}^{a} X_i^{a+1}, \mathcal{M}^{a+1}) > n$.

Demonstração. Seja $C\colon \dot\bigcup_{i=1}^{a} X_i^{a+1} \to [n]$ uma coloração de $(\dot\bigcup_{i=1}^{a} X_i^{a+1}, \mathcal{M}^{a+1})$. Temos que provar que existe uma aresta monocromática em $\mathcal{M}^{a+1}$.

Construimos uma sequência de arestas monocromáticas $N_1, \ldots, N_a$, com $N_i \in \mathcal{N}^i$, da seguinte forma. Primeiramente, note que a coloração C restrita aos vértices em $X_a^{a+1} = Y^a$ induz uma coloração de $(Y^a, \mathcal{N}^a)$ com n cores. Como $\chi(Y^a, \mathcal{N}^a) > n$, $\mathcal{N}^a$ deve conter alguma aresta monocromática. Escolhemos N^a como sendo uma tal aresta. Em geral, uma vez escolhidas as arestas N_a, N_{a-1}, N_{i+1}, escolhemos a aresta N_i notando que a coloração C restrita aos vértices

$$\{(v, N_{i+1}, \ldots, N_a) : v \in Y^i\} \subseteq X_i^{a+1}$$

induz uma coloração de $(Y^i, \mathcal{N}^i)$. Como $\chi(Y^i, \mathcal{N}^i) > n$, podemos escolher uma aresta monocromática $N_i \in \mathcal{N}^i$.

Para todo $i = 1 \ldots a$, defina o conjunto

$$Z_i = \{(v, N_{i+1}, \ldots, N_a) : v \in N_i\} \subseteq X_i^{a+1}.$$

Afirmamos que existe uma cópia de $(\dot\bigcup_{i=1}^{a} X_i^1, M^1)$ no grafo $G[Z_1 \cup Z_a]$ induzido por tais conjuntos. De fato, para todo $t = 1 \ldots a$, definimos a função

$$g_t(v) \colon \dot\bigcup_{i=1}^{a} X_i^t \to N_t \cup \{X_i^t \times \{N_t\} : \forall i \neq t\}$$
$$v \mapsto \begin{cases} f_{N_t}^{(t)}(v), & \text{se } v \in X_t^t; \\ (v, N_t), & \text{caso contrário.} \end{cases}$$

É fácil verificar que g_t é um isomorfismo entre $(\bigcup_{i=1}^{a} X_i^t, \mathcal{M}^t)$ e $G[N_t \cup \{X_i^t \times \{N_t\} : \forall i \neq t\}]$. De fato, para todo $M \in M^t$, temos $g_t(M) = \mathbf{e}(M, N_t)$. Seja $g = g_a \circ g_{a-1} \circ \cdots \circ g_1$.

Temos

$$\begin{aligned} g(X_1^1) &= \{(f_{N_1}(v), N_2, \dots, N_a) : v \in X_1^1\} = Z_1 \\ g(X_2^1) &= \{(f_{N_2}(v, N_1), N_3, \dots, N_a) : v \in X_2^2\} \subseteq Z_2 \\ &\vdots \\ g(X_{a-1}^1) &= \{(f_{N_{a-1}}(v, N_1, \dots, N_{a-2}), N_a) : v \in X_{a-1}^1\} \subseteq Z_{a-1} \\ g(X_a^1) &= f_{N_a}(X_a^1, N_1, \dots, N_{a-1}) \subseteq Z_a. \end{aligned}$$

Como cada conjunto Z_i é monocromático e $a = n(k-1)+1$, existe $W \in [a]$, $|W| = k$, tal que para todo $i \in W$, $C(Z_i) = c$ para algum $c \in [n]$. Pela hipótese sobre $(\dot\bigcup X_i^1, \mathcal{M}^1)$ sabemos que existe uma aresta $M \in \mathcal{M}^1$ tal que $M \cap X_i^1 \neq \varnothing$ para todo $i \in W$. Logo, $g(M) \in M^{a_1}$ é tal que $g(M) \subseteq \bigcup_{i \in W} g(X_i^1) \subseteq \bigcup_{i \in W} Z_i$, o que implica que $C(g(M)) = c$, i.e., que $g(M)$ é uma aresta monocromática, como desejado. □

□

◇ ◇ ◇ *Aula 8 (25 de Outubro) — Giulia Maesaka* ◇ ◇ ◇

6.2 Grafos com cintura alta e número cromático alto

Uma *constelação* é um grafo tal que toda componente conexa é uma estrela (um grafo G é uma estrela se $G = K_{1,t}$ para algum t).

Se X é um conjunto finito, denotamos por $K^k(X)$ um grafo completo com peso k em todas arestas e conjunto de vértices igual a X. O comprimento de uma circuito em um grafo com pesos é definido como a soma dos pesos de suas arestas. A cintura $g(G)$ de um grafo com pesos é definida como o comprimento de um menor circuito em G.

Lema 6.4. *Para quaisquer inteiros $i \geq 0$ e $n \geq 1$, existe uma constelação $\Gamma_i(n)$ satisfazendo as seguintes propriedades.*

1. *Existe uma partição $\mathcal{C}_i^n$ de $V(\Gamma_i(n))$ tal que toda parte $X \in \mathcal{C}_i^n$ é um conjunto independente de tamanho $|X| = n$.*

2. *Para todo conjunto independente $M \subset V(\Gamma_i(n))$, existe $X \in \mathcal{C}_i^n$ tal que $X \cap M = \varnothing$.*

3. *Todo circuito do grafo*
$$\Gamma_i^k(n) := \Gamma_i(n) \cup \Big(\bigcup_{X \in \mathcal{C}_i^n} K^k(X) \Big)$$
(obtido a partir de $\Gamma^i(n)$ após tornar o grafo induzido por cada parte $X \in \mathcal{C}_i^n$ em um clique de peso k) que não *está inteiramente contido em uma das partes $X \in \mathcal{C}_i^n$ possui comprimento maior que $2^i(k+1)$.*

Observação 6.5. Podemos tomar $\Gamma_i(1) = K_2$.

Dado um grafo $G = (V, E)$ e bijeções $\phi_X : V \to X$ para todo $X \in \mathcal{C}_i^{|V_i|}$, definimos o grafo

$$\Gamma_i(G) := \Gamma_i(|V|) \cup \left(\bigcup_{\mathcal{C}_i^{|V|}} \phi_X^*(G) \right),$$

onde $\phi^*(G)$ é o grafo com conjuntos de vértices X e tal que ϕ_X é um isomorfismo entre G e $\phi^*(G)$. Ou seja, $\Gamma_i(G)$ é o grafo que é obtido a partir de $\Gamma_i(|V|)$ após tornar o grafo induzido por X isomorfo a G (para toda parte $X \in \mathcal{C}_i^n$).

Teorema 6.6. *Se $\Gamma_i(1) = K_2$, então o grafo $G = \underbrace{\Gamma_i(\Gamma_i(\cdots(\Gamma(1))))}_{n \text{ vezes}}$ tem número cromático pelo menos $(n+1)$, cintura maior que 2^{i+1} e pode ser decomposto em n constelações.*

Demonstração. Por indução em n. A afirmação é válida para $\Gamma_i(1) = K_2$. Para $n \geq 1$, assumimos que a afirmação vale para $G = \underbrace{\Gamma_i(\Gamma_i(\cdots(\Gamma(1))))}_{n \text{ vezes}}$ e consideramos o grafo $\Gamma_i(G)$.

- Suponha por absurdo que $\Gamma_i(G)$ tem uma $(n+1)$-coloração própria. Seja M o conjunto induzido pelos vértices coloridos por uma cor arbitrária c. Como M é um conjunto independente em $\Gamma_i(G)$ e como $\Gamma_i(|V(G)|) \subseteq \Gamma_i(G)$, temos que M também é um conjunto independente em $\Gamma_i(|V(G)|)$. Pelo Lema 6.4, deve existir um $X \in \mathcal{C}^{|V(G)|}$ tal que $X \cap M = \emptyset$, o que implica que os vértices de X tem uma coloração própria com n cores. Mas isso contradiz a hipótese $\chi(G) \geq n+1$, uma vez que o grafo induzido por X é isomorfo a G.

- Suponha por absurdo que $\Gamma_i(G)$ tem um circuito de comprimento menor ou igual a 2^{i+1}. Como $\Gamma_i(G) \subseteq \Gamma_i^1(|V(G)|)$, segue que $\Gamma_i^1(|V(G)|)$ possui um circuito de tamanho no máximo $2^{i+1} = 2^i(1+1)$. Pelo Lema 6.4 um tal circuito deve estar inteiramente contido em alguma parte $X \in \mathcal{C}_i^{|V(G)|}$, o que contradiz a hipótese $g(G) \geq 2^{i+1}$, uma vez que o grafo induzido por X é isomorfo a G.

- Como $\Gamma_i(G) - \Gamma_i(|V(G)|) = \cup_{X \in \mathcal{C}} \phi_X^*(G)$ é um grafo que pode ser decomposto em n constelações (por hipótese de indução), segue que $\Gamma_i(G)$ pode ser decomposto em $n+1$ constelações.

□

Observação 6.7. Grafos que podem ser decompostos em n constelações possuem número cromático no máximo 2^n, uma vez que são a união de n grafos bipartidos.

Demonstração do Lema 6.4. Como já mencionado, podemos tomar $\Gamma_i(1) = K_2$ para todo $i \geq 1$. Veremos que, para todo n, podemos tomar $\Gamma_0(n)$ como n cópias disjuntas de $K_{1,n}$. Formalmente definimos $\Gamma_0(n)$ como o grafo tal que

$$V(\Gamma_0(n)) = \{0,\ldots,n-1\} \cup (\{0,\ldots,n-1\} \times \{0,\ldots,n-1\}) \text{ e}$$
$$E(\Gamma_0(n)) = \{\{i,(i,j)\} : i,j \in \{0,\ldots,n-1\}\}.$$

Considere a partição $\mathcal{C}_0^n = \{C, C_0, \ldots, C_{n-1}\}$ de $V(\Gamma_0(n))$, onde $C = \{0,\ldots,n-1\}$ e $C_i = \{i\} \times \{0,\ldots,n-1\}$. Por construção cada parte em $\mathcal{C}_0^n$ é independente. Além disso, se um conjunto independente M de $\Gamma_0(n)$ contém algum vértice $i \in C$, então $M \cap C_i = \emptyset$. Por fim, o maior circuito de $\Gamma_0^k(n)$ (não contido em alguma das partes) é um triângulo de comprimento $1+1+k > 2^0(k+1)$.

Agora seja $i \geq 1$ e $n \geq 2$ e suponha já construídos $\Gamma_{i'}(n')$ para quaisquer i' e n' tais que $i' < i$ ou $n' < n$. Definimos

$$\Gamma_i(n) = \Gamma_{i-1}(|\mathcal{C}_i^{n-1}|) \cup \bigcup_{X \in \mathcal{C}_{i-1}^{|\mathcal{C}_i^{n-1}|}} \Gamma_i(n-1)_X,$$

isto é, o grafo composto por $\Gamma_{i-1}(|\mathcal{C}_i^{n-1}|)$ e por $|\mathcal{C}_{i-1}^{|\mathcal{C}_i^{n-1}|}|$ cópias de $\Gamma_i(n-1)$. Tais cópias são denotadas por $\Gamma_i(n-1)_X$ para todo $X \in \mathcal{C}_{i-1}^{|\mathcal{C}_i^{n-1}|}$ (e a partição de cada cópia é denotada por $(\mathcal{C}_i^{n-1})_X$).

Para todo $X \in \mathcal{C}_{i-1}^{|\mathcal{C}_i^{n-1}|}$, seja $\psi_X : X \to (\mathcal{C}_i^{n-1})_X$ uma bijeção. Afirmamos que podemos tomar

$$\mathcal{C}_i^n = \{\{z\} \cup \psi_X(z) : \text{ para todo } X \in \mathcal{C}_{i-1}^{|\mathcal{C}_i^{n-1}|} \text{ e } z \in X\}.$$

De fato, suponha que M é um conjunto independente de $\Gamma_i(n)$. Seja $M_1 = M \cap \Gamma_{i-1}(|\mathcal{C}_i^{n-1}|)$ e $M_X = M \cap \Gamma_1(n-1)_X$ para todo X. Por hipótese de indução no grafo $\Gamma_{i-1}(|\mathcal{C}_i^{n-1}|)$, há alguma parte $X \in \mathcal{C}_{i-1}^{|\mathcal{C}_i^{n-1}|}$ tal que $X \cap M_1 = \varnothing$. Mas também podemos aplicar a hipótese de indução no grafo $\Gamma_i(n-1)_X$ e obter que existe $X_2 \in (\mathcal{C}_i^{n-1})_X$ tal que $X_2 \cap M_X = \varnothing$. Seja $z \in X$ tal que $\psi_X(z) = X_2$. Então $(\{z\} \cup X_2)$ é uma parte de $\mathcal{C}_i^n$ com intersecção nula com M.

Resta provar que todo circuito de $\Gamma_i^k(n)$ que *não* está inteiramente contido em uma das partes $X \in \mathcal{C}_i^n$ possui comprimento maior que $2^i(k+1)$. Tomemos um circuito $(x_1, \ldots, x_\ell)$ de comprimento mínimo em $\Gamma_i^k(n)$ que não esteja inteiramente contido em uma parte $X \in \mathcal{C}_i^n$.

- *Caso 1:* $(x_1, \ldots, x_\ell)$ *não usa aresta de* $\Gamma_{i-1}(|\mathcal{C}_i^{n-1}|)$. Neste caso, o circuito está contido em $X \cup \Gamma_i(n-1)$ para algum $X \in \mathcal{C}_{i-1}^{|\mathcal{C}_i^n|}$. Afirmamos que o circuito não pode conter vértices em X. De fato, suponha que exista i tal que $x_i \in X$ e sejam $x_{i-1}, x_{i+1} \in \psi_X(x)$ os vizinhos de x_i no circuito. Como as arestas $x_{i-1}x_i$, x_ix_{i+1} e $x_{i-1}x_{i+1}$ têm todas peso k, segue que $(x_1, \ldots, x_{i-1}, x_{i+1}, x_\ell)$ é um circuito que contradiz a minimalidade de $(x_1, \ldots, x_\ell)$. Logo, $(x_1, \ldots, x_\ell)$ está inteiramente contido em $\Gamma_i(n-1)_X$. Segue da hipótese de indução que $|(x_1, \ldots, x_\ell)| > 2^i(k+1)$.

- *Caso 2:* $(x_1, \ldots, x_\ell)$ *usa uma aresta de* $\Gamma_{i-1}(|\mathcal{C}_i^{n-1}|)$. Seja $(x_1', \ldots, x_\ell')$ o circuito em $\Gamma_{i-1}^k(|\mathcal{C}_i^{n-1}|)$ obtido a partir de $(x_1, \ldots, x_\ell)$ após a remoção dos vértices que não pertencem a $\Gamma_{i-1}(|\mathcal{C}_i^{n-1}|)$. Agora note que o caminho entre x_i' e x_{i+1}' em $(x_1, \ldots, x_\ell)$ tem comprimento pelo menos $2k+1$, uma vez que é necessário arestas de comprimento k para entrar e para sair de $\Gamma_{i-1}(|\mathcal{C}_i^{n-1}|)$. Seja $k' = 2k+1$. Aplicamos a hipótese de indução a $(x_1', \ldots, x_\ell')$ para obter

  $$|(x_1', \ldots, x_\ell')| \geq 2^{i-1}(k'+1) = 2^i(k+1),$$

  o que implica $|(x_1, \ldots, x_\ell)| \geq 2^i(k+1)$, como desejado.

□

6.3 Número de vértices do grafo $\Gamma_i(n)$

Seja $g(i,n)$ o número de partes do grafo $\Gamma_i(n)$. Nesta seção daremos uma cota inferior para $g(i,n)$, (note que esta será uma cota inferior para o número de vértices de $\Gamma_i(n)$).

Para expressar uma cota para $g(i,n)$ de maneira mais concisa, introduzimos as seguintes operações (chamada de *Knuth's up arrow notation*), que são todas associativas a direita.

- $a \uparrow b = a^b = \underbrace{a \times a \times \cdots \times a}_{b \text{ cópias de } a}$.
- $a \uparrow\uparrow b = \underbrace{a \uparrow a \uparrow \cdots \uparrow a}_{b \text{ cópias de } a}$.
- $a \uparrow^{(i)} b = a \underbrace{\uparrow\uparrow \cdots \uparrow}_{i} b = \underbrace{a \underbrace{\uparrow\uparrow \cdots \uparrow}_{i-1} a \underbrace{\uparrow\uparrow \cdots \uparrow}_{i-1} \cdots \underbrace{\uparrow\uparrow \cdots \uparrow}_{i-1} a}_{b \text{ cópias de } a}$.

Segue da definição de $\Gamma_i(n)$ que $g(i,1) = 2$ (para todo $i \geq 0$), $g(0,n) = n+1$ (para todo $n \geq 1$) e que vale a seguinte relação de recorrência:

$$g(i,n) = g(i,n-1) \cdot g(i-1, g(i,n-1)).$$

Vamos verificar por indução que $g(i,n) \geq 2 \uparrow^{(i)} n$. De fato, a desigualdade vale para os casos em que $n = 1$ ou $i = 0$ e, em geral, temos

$$g(i,n) = g(i,n-1) \cdot g(i-1, g(i,n-1)) \geq g(i-1, g(i,n-1)) \geq 2 \uparrow^{(i-1)} g(i,n-1) \geq 2 \uparrow^{(i-1)} 2 \uparrow^{(i)} (n-1)$$

como desejado.

Apesar da construção $\Gamma_i(n)$ ter um número muito grande de vértices, é possível demonstrar a existência de um grafo G de tamanho da ordem k^{2l}, tal que $\chi(G) \geq k$ e $g(G) \geq l$.

7 Lema Local de Lovász

⋄ ⋄ ⋄ *Aula 9 (08 de Novembro) — Bruno Pasqualotto Cavalar* ⋄ ⋄ ⋄

Em uma demonstração que usa o método probabilístico, frequentemente encontramos a seguinte situação: definimos uma coleção de eventos "ruins" $\mathcal{A} = \{A_1, \ldots, A_m\}$ e queremos mostrar que existe algum ponto no espaço de probabilidade que não satisfaz nenhum desses eventos. Isto é, queremos mostrar que que $\mathbb{P}\left(\bigcap_{A \in \mathcal{A}} \overline{A}\right) > 0$ ou equivalentemente $\mathbb{P}\left(\bigcup_{A \in \mathcal{A}} A\right) < 1$.

7.1 Primeiro Momento / Cota da união

Uma primeira tentativa para mostrarmos que $\mathbb{P}\left(\bigcup_{A \in \mathcal{A}} A\right) < 1$ consiste em usar o fato que

$$\mathbb{P}\left(\bigcup_{A \in \mathcal{A}} A\right) \leq \sum_{A \in \mathcal{A}} \mathbb{P}(A).$$

Observação 7.1. A cota acima, chamada de *cota da união*, também pode ser vista como uma aplicação do método do primeiro momento. De fato, seja $X = \sum_{A \in \mathcal{A}} \mathbb{1}_A$ a variável aletaória que conta o número de eventos em $\mathcal{A}$ que ocorrem. Temos

$$\mathbb{P}\left(\bigcup_{A\in\mathcal{A}} A\right) = \mathbb{P}(X>0) \leq \mathbb{E}(X) = \sum_{A\in\mathcal{A}} \mathbb{E}(\mathbb{1}_A) = \sum_{A\in\mathcal{A}} \mathbb{P}(A).$$

Proposição 7.2. *Seja G um hipergrafo k-uniforme com $m < 2^{k-1}$ arestas. Então G é 2-colorível.*

Demonstração. Vamos colorir cada vértice de G com a cor azul ou vermelha de maneira uniforme e independentemente das escolhas de cores dos demais vértices. Para cada aresta e de G definimos o evento A_e = [aresta e é monocromática]. Temos $\mathbb{P}(A_e) = 2/2^k = 2^{1-k}$. Portanto, a probabilidade de existir alguma aresta monocromática é dada por

$$\mathbb{P}\left(\bigcup_{A\in\mathcal{A}} A\right) \leq \sum_{A\in\mathcal{A}} \mathbb{P}(A) \leq m\cdot 2^{1-k} < 1.$$

Segue que existe uma coloração que não deixa nenhuma aresta monocromática. □

7.2 Digrafo de dependência

Dado um digrafo $D=(V,E)$ e um vértice $v\in V$, definimos $N^+(v)=\{w\in v:(v,w)\in E\}$.

Uma coleção de eventos $\mathcal{B}=\{B_1,\dots,B_k\}$ é mutuamente independente se para todo $J\subseteq[k]$ temos $\mathbb{P}\left(\bigcap_{j\in J} B_j\right)=\prod_{j\in J}\mathbb{P}(B_j)$. Note que é possível que $B_1,\dots,B_m$ sejam dois-a-dois independentes mas não sejam mutuamente independentes. Definimos conjuntos de variáveis aleatórias mutuamente independentes de maneira análoga.

Um evento A é *mutuamente independente de* eventos $B_1,\dots,B_k$ se, para quaisquer conjuntos disjuntos $J,J'\subseteq[k]$ temos

$$\mathbb{P}\left(A \mid (\bigcap_{j\in J} B_j)\cap(\bigcap_{j\in \overline{J}} \overline{B_j})\right) = \mathbb{P}(A).$$

Note que é podemos ter A mutuamente independente de $B_1,\dots,B_k$ mesmo quando $A,B_1,\dots,B_m$ não são mutuamente independentes.

Proposição 7.3 (Princípio da independência mútua)**.** *Seja $\mathcal{P}$ um conjunto de variáveis mutuamente independentes e suponha que $\mathcal{A}$ é uma coleção de eventos tal que cada $A\in\mathcal{A}$ é completamente determinado por algum subconjunto $\mathcal{P}_A\subseteq\mathcal{P}$. Então se $A,B_1,\dots,B_k\in\mathcal{A}$ são eventos tais que $\mathcal{P}_A\cap\mathcal{P}_{B_i}=\varnothing$ para todo $i\in[k]$, então A é mutuamente independente de $B_1,\dots,B_k$.* □

Seja $\mathcal{A}$ um conjunto finito de eventos. Um digrafo $D=(\mathcal{A},E)$ é dito um *grafo de dependência* de $\mathcal{A}$ se

para todo $A\in\mathcal{A}$: A é mutuamente independente dos eventos em $\mathcal{A}\setminus(N+(A)\cup A)$.

Note que uma coleção $\mathcal{A}$ pode admitir diversos grafos de dependência.

7.3 Lema Local de Lovász

Lema 7.4 (Lema Local de Lovász Simétrico). *Seja G um grafo de dependência de uma coleção finita $\mathcal{A}$ de eventos. Se existe um número p e um inteiro d satisfazendo*

- $\mathbb{P}(A) \leq p$ *para todo* $A \in \mathcal{A}$;
- $|N^+(A)| \leq d$ *para todo* $A \in \mathcal{A}$;
- $ep(d+1) \leq 1$,

então $\mathbb{P}(\bigcap_{A \in \mathcal{A}} \overline{A}) > 0$.

Adiamos a prova A seguir, mostramos duas aplicações do Lema Local de Lovász Simétrico.

Proposição 7.5. *Seja $G = (V, E)$ um grafo k-uniforme tal que cada aresta intersecta no máximo com outras d arestas. Se $e(d+1) \leq 2^{k-1}$, então G é 2-colorível.*

Demonstração. Colorimos cada vértice de vermelho ou azul aleatoriamente de forma uniforme e independente das escolhas de cores dos demais vértices. Para cada aresta $e \in E$, seja A_e o evento que indica se e é monocromática. Cada A_e é completamente determinado pela cor dos vértices contidos em e. Pelo princípio da independência mútua, temos que o digrafo tal que

$$N^+(A_e) = \{A_f : e \cap f = \varnothing, e \neq f \in E\}$$

é um grafo de dependência de $\{A_e\}_{e \in E}$. O resultado segue do Lema Local de Lovász. □

Teorema 7.6 (Alon, Linial (1989)). *Seja $D = (V, E)$ um grafo dirigido com grau de saída mínimo pelo menos δ e grau de entrada máximo no máximo Δ. Então para todo inteiro $k > 0$ que satisfaz $k \leq \delta/(1 + \ln(1 + \delta\Delta))$, existe um circuito dirigido em D de comprimento divisível por k.*

Demonstração. Podemos supor, sem perda de generalidade, que todo vértice tem grau de saída exatamente δ (uma vez que podemos remover arcos até que tal condição seja satisfeita e encontrar um circuito no grafo resultante).

Seja $\chi : V \to \{0, \ldots, k-1\}$ uma coloração aleatória em que a cor $\chi(v)$ de cada vértice v é escolhida independentemente e com distribuição uniforme. Seja A_v o evento de que não exista $w \in N^+(v)$ tal que $\chi(w) = \chi(v) + 1 \pmod{k}$. Defina

$$I(v) = \{w \in V : N^+(v) \cap (\{w\} \cup N^+(w)) = \varnothing\}.$$

Fixado um vértice v, afirmamos que A_v é mutuamente independente dos eventos em $\{A_w : w \in I(v)\}$. De fato, para todo conjunto $S \subseteq I_v$ temos, pela Lei da Probabilidade Total,

$$\mathbb{P}\left(A_v \cap \bigcap_{w \in S} A_w\right) = \sum_{j=0}^{n-1} \mathbb{P}(\chi(v) = j)\mathbb{P}\left(A_v \cap \bigcap_{w \in S} A_w \mid \chi(v) = j\right)$$

Agora note que, ao nos restringirmos ao espaço em que $\chi(v) = j$, o conjunto de vértices cujas cores determinam A_v e disjunto do conjunto de vértices cujas cores determina

$\bigcap_{w\in S} A_w$. Logo, aplicamos o princípio da independência mútua para obter

$$\begin{aligned}\mathbb{P}\left(A_v \cap \bigcap_{w\in S} A_w\right) &= \sum_{j=0}^{n-1} \mathbb{P}(\chi(v)=j)\mathbb{P}\left(A_v \mid \chi(v)=j\right)\cdot \mathbb{P}\left(\bigcap_{w\in S} A_w \mid \chi(v)=j\right) \\ &= \mathbb{P}(A_v)\cdot \sum_{j=0}^{n-1} \mathbb{P}(\chi(v)=j)\cdot \mathbb{P}\left(\bigcap_{w\in S} A_w \mid \chi(v)=j\right) \\ &= \mathbb{P}(A_v)\cdot \mathbb{P}\left(\bigcap_{w\in S} A_w\right),\end{aligned}$$

como desejado.

Logo, o digrafo dos eventos $\{A_v : v \in V\}$ em que cada evento A_v manda arcos para os eventos A_w tais que $w \notin I(v)$ é um grafo de dependêcia dos eventos $\{A_v : v \in V\}$. Note que, para todo $v \in A_v$, o grau de saída de A_v nesse grafo de dependência é no máximo $\delta + \delta(\Delta - 1) = \delta\Delta$ e que $\mathbb{P}(A_v) = (1 - \frac{1}{k})^\delta$. Como

$$e \cdot (1 - \frac{1}{k})^\delta \cdot (\delta\Delta + 1) \leq e \cdot e^{-\frac{\delta}{k}} \cdot (\delta\Delta + 1) = e^{1-\frac{\delta}{k}}(\delta\Delta + 1) = e^{-\ln(1+\delta\Delta)} \cdot (\delta\Delta + 1) = 1,$$

segue, pelo Lema Local de Lovász Simétrico, existe alguma coloração χ tal que, para todo vértice v existe um vértice $p(v) \in N^+(v)$ tal que $\chi(p(v)) = \chi(v) + 1$.

Fixado um vértice arbitrário $v_1 \in V$, considere a sequência $v_1, v_2, v_3, \ldots$ tal que $v_i = p(v_{i-1})$ $\forall i > 1$. Seja j o menor índice tal que existe $\ell > j$ satisfazendo $v_j = v_\ell$. Então $(v_i, v_{i+1}, \ldots, v_\ell)$ é, claramente, um circuito de comprimento múltiplo de k. □

7.4 Demonstração do Lema Local de Lovász

Nesta seção apresentamos uma prova do Lema 7.7. Para tal, faremos a demonstração da seguinte versão mais geral do Lema 7.7.

Lema 7.7 (Lema Local de Lovász Geral). *Seja $\mathcal{A}$ uma coleção de eventos e $D = (\mathcal{A}, E)$ um grafo de dependência de $\mathcal{A}$. Suponha que exista uma função $x\colon \mathcal{A} \to (0,1)$ tal que*

$$\mathbb{P}(A) \leq x(A) \cdot \prod_{B\in\Gamma(A)} (1 - x(B)).$$

Então

$$\mathbb{P}\left(\cap_{A\in\mathcal{A}} \overline{A}\right) \geq \prod_{A\in\mathcal{A}} (1 - x(A)) > 0.$$

texto

Demonstração do Lema 7.4 (Lema Local de Lovász Simétrico). O resultado é trivial para $d = 0$. Para $d > 0$, basta considerar a função $x\colon \mathcal{A} \to (0,1)$ tal que $x(A) = 1/(d+1) < 1$ para todo $A \in \mathcal{A}$. De fato, temos

$$x(A) \cdot \prod_{B\in N^+(A)} (1 - x(B)) \geq \frac{1}{d+1}\left(1 - \frac{1}{d+1}\right)^d \geq \frac{1}{e(d+1)} \geq p \geq \mathbb{P}(A),$$

isto é, a função x satisfaz a hipótese do Lema 7.7 □

Demonstração do Lema 7.7 (Lema Local de Lovász Geral). Afirmamos que é suficiente provar que todo $S \subseteq \mathcal{A}$ satisfaz

$$\mathbb{P}\left(A \mid \bigcap_{B \in S} \overline{B}\right) \leq x(A) \qquad \text{para todo } A \in \mathcal{A}, A \notin S. \tag{1}$$

(note que para provar a asserção acima, é necessário garantir $\mathbb{P}\left(\bigcap_{B \in S} \overline{B}\right) > 0$) De fato, suponha que todo $S \subseteq \mathcal{A}$ satisfaça (1) e seja $\mathcal{A} = \{A_1, \ldots, A_m\}$. Então

$$\mathbb{P}\left(\bigcap_{i=1}^{m} \overline{A_i}\right) = (1 - \mathbb{P}(A_1)) \cdot (1 - \mathbb{P}(A_1 \mid A_2) \cdots \left(1 - \mathbb{P}\left(A_n \mid \bigcap_{i=1}^{n-1} A_i\right)\right) \geq \prod_{i=1}^{n} (1 - x_i),$$

como desejado.

Provaremos que todo $S \subseteq \mathcal{A}$ satisfaz (1) por indução em $|S|$. Se $S = \varnothing$ então temos, por hipótese, que $\mathbb{P}(A) \leq x(A) \prod_{B \in \Gamma(A)} (1 - x(B))$, da onde segue $\mathbb{P}(A) \leq x(A)$.

Agora suponha $|S| > 1$ e que a desigualdade (1) vale para conjuntos de cardinalidade menor que $|S|$. Seja $S_1 = S \cap \Gamma(A)$ e $S_2 = S \setminus S_1$. Se $S_1 = \varnothing$, então

$$\mathbb{P}\left(A \mid \bigcap_{B \in S} \overline{B}\right) = \mathbb{P}(A) \leq x(A),$$

uma vez que $A \notin S$ e A é mutuamente independente de todos os eventos em S. Suponha agora que $S_1 \neq \varnothing$ e note que

$$\mathbb{P}\left(A \mid \bigcap_{B \in S} \overline{B}\right) = \mathbb{P}\left(A \mid \bigcap_{B \in S_1} \overline{B} \cap \bigcap_{C \in S_2} \overline{C}\right) = \frac{\mathbb{P}\left(A \cap \bigcap_{B \in S_1} \overline{B} \mid \bigcap_{C \in S_2} \overline{C}\right)}{\mathbb{P}\left(\bigcap_{B \in S_1} \overline{B} \mid \bigcap_{C \in S_2} \overline{C}\right)}. \tag{2}$$

O numerador da termo da equação acima pode ser limitado superiormente por

$$\mathbb{P}\left(A \cap \bigcap_{B \in S_1} \overline{B} \mid \bigcap_{C \in S_2} \overline{C}\right) \leq \mathbb{P}\left(A \mid \bigcap_{C \in S_2} \overline{C}\right) = \mathbb{P}(A) \leq x(A) \prod_{B \in \Gamma(A)} (1 - x(B)).$$

Seja $S_1 = \{B_1, \ldots, B_\ell\}$. Temos também

$$\begin{aligned}
\mathbb{P}\left(\bigcap_{B \in S_1} \overline{B} \mid \bigcap_{C \in S_2} \overline{C}\right) &= \mathbb{P}\left(\overline{B_1} \mid \bigcap_{C \in S_2} \overline{C}\right) \cdot \mathbb{P}\left(\overline{B_2} \mid \overline{B_1} \cap \bigcap_{C \in S_2} \overline{C}\right) \cdots \mathbb{P}\left(\overline{B_\ell} \mid \overline{B_1} \cap \cdots \cap \overline{B_{\ell-1}} \cap \bigcap_{C \in S_2} \overline{C}\right) \\
&\geq (1 - x(B_1)) \cdots (1 - x(B_{\ell-1})) \qquad \textit{(por hipótese de indução)} \\
&\geq \prod_{B \in \Gamma(A)} (1 - x(B)).
\end{aligned}$$

Substituindo os limitantes obtidos para o numerador e o denominador do lado direito da equação (2), obtemos o resultado desejado. Concluímos, portanto, que todo $S \subseteq \mathcal{A}$ satisfaz a equação (1). □

7.5 Versão algorítmica

Para conseguir uma versão algoritmica do LLL, Moser e Tardos consideraram um cenário levemente modificado do Lema Local de Lovász, mas que ainda é válido na maior parte das aplicações conhecidas.

Seja $\mathcal{P}$ um conjunto finito de variáveis aleatórias mutuamente independentes num mesmo espaço de probabilidade. Suporemos que todo evento de $\mathcal{A}$ é determinado por um subconjunto dessas variáveis. Diremos que uma atribuição de valores para as variáveis de $\mathcal{P}$ *viola* o evento $A \in \mathcal{A}$ se essa atribuição faz com que A aconteça. Para cada evento $A \in \mathcal{A}$, denote por $\mathrm{vbl}(A)$ um conjunto minimal das variáveis de $\mathcal{P}$ que determina A. Defina também

$$\Gamma(A) := \{B \in \mathcal{A} : \mathrm{vbl}(B) \cap \mathrm{vbl}(A) \neq \varnothing\},$$

e $\Gamma^+(A) := \Gamma(A) \cup A$.

Seja D o digrafo com conjunto de vértices $\mathcal{A}$ e tal que a vizinhança de um evento A é $\Gamma(A)$. Como A é mutuamente independente de todos os eventos em $\mathcal{A} \setminus (\Gamma(A) \cup \{A\})$, temos que D é um digrafo de dependência para $\mathcal{A}$. O celebrado algoritmo de Moser-Tardos é como segue.

Algorithm 2 Algoritmo de Moser-Tardos

para todo $P \in \mathcal{P}$ **faça** $v_P \leftarrow$ uma valoração aleatória de P **enquanto** $\exists A \in \mathcal{A} : A$ é violado quando $(P = v_P : \forall P \in \mathcal{P})$ **faça** escolha arbitrariamente um evento violado $A \in \mathcal{A}$ **para todo** $P \in \mathrm{vbl}(A)$ **faça** $v_P \leftarrow$ uma nova valoração aleatória de P **devolva** $(v_P)_{P\in\mathcal{P}}$

Cada vez que um evento A é escolhido na linha 4 dizemos que ele foi *reamostrado*. Note que a eficiência do método depende de que i) o número de reamostragens não seja muito grande; ii) valores aleatórios para cada variável $P \in \mathcal{P}$ possam ser eficientemente amostrados; iii) verificar (e encontrar) a ocorrência de um evento também possa ser feito eficientemente. A versão construtiva do LLL de Moser e Tardos trata do primeiro problema.

Teorema 7.8 (Moser e Tardos). *Seja $\mathcal{P}$ um conjunto finito de variáveis aleatórias mutuamente independentes num mesmo espaço de probabilidade e $\mathcal{A}$ uma coleção finita de eventos determinados por essas variáveis. Se existe uma função $x : \mathcal{A} \to (0,1)$ tal que*

$$\mathbb{P}(A) \leq x(A) \prod_{B\in\Gamma(A)} (1 - x(B)) \quad \textit{para todo } A \in \mathcal{A},$$

então existe uma atribuição de valores às variáveis de $\mathcal{P}$ que não viola nenhum dos eventos de $\mathcal{A}$. Além disso, o número esperado de reamostragens do evento $A \in \mathcal{A}$ que o algoritmo aleatório acima faz é no máximo $\frac{x(A)}{1-x(A)}$. Portanto, o número total de amostragens esperado é $\sum_{A\in\mathcal{A}} \frac{x(A)}{1-x(A)}$.

7.5.1 Ferramentas da prova

Seja $C : \mathbb{N} \to \mathcal{A}$ uma função que lista os eventos na ordem em que são reamostrados. Se o algoritmo termina, C é parcialmente definido, apenas até o número total de reamostragens. Chamamos C de *registro* do algoritmo.

Uma *árvore testemunha* $\tau = (T, \sigma_T)$ é uma árvore finita enraizada T juntamente com um rotulamento $\sigma_T : V(T) \to \mathcal{A}$ dos seus seus vértices por eventos tal que os filhos de um vértice $u \in V(T)$ recebem rótulos de $\Gamma^+(\sigma_T(u))$. Se filhos distintos de um mesmo vértice sempre recebem rótulos distintos dizemos que a árvore testemunha é *própria*. Denotaremos $V(\tau) := V(T)$ e para todo $v \in V(\tau)$ escrevemos $[v] := \sigma_T(v)$.

- Dado um registro C, associaremos com cada passo de reamostragem t uma árvore testemunha $\tau_C(t)$ que servirá como justificativa para a necessidade desse passo.
- Definimos $\tau_C^{(t)}(t)$ como uma árvore com apenas um vértice raíz isolado rotulado com $C(t)$.
- Então, "voltando no tempo" pelo registro, para cada $i = t-1, t-2, \dots, 1$ distinguimos dois casos:
    1. Se existe um vértice $v \in \tau_C^{(i+1)}(t)$ tal que $C(i) \in \Gamma^+([v])$, então escolhemos entre todos os tais vértices aquele que tem maior distância da raíz, e colocamos um novo filho u para v que rotulamos $C(i)$, obtendo a árvore $\tau_C^{(i)}(t)$.
    2. Caso contrário, definimos $\tau_C^{(i)} := \tau_C^{(i+1)}(t)$.
- Dizemos que uma árvore testemunha τ *ocorre* no registro C se existe $t \in \mathbb{N}$ tal que $\tau_C(t) = \tau$.

Lema 7.9. *Seja τ uma árvore testemunha e C o registro (aleatório) produzido pelo algoritmo.*

1. *Se τ ocorre em C, então τ é próprio.*
2. *A probabilidade de τ aparecer em C é no máximo $\prod_{v \in V(\tau)} \mathbb{P}([v])$.*