SINOPSE DAS AULAS

MAC5775 MÉTODOS PROBABILÍSTICOS EM COMBINATÓRIA E EM TEORIA DA COMPUTAÇÃO I

PRIMEIRO SEMESTRE DE 2018

Notas de aula produzidas por

1. . . . ,
2. . . . ,
3. . . . e
4. . . . .

Data: 2018/8/20, 3:54pm

Sumário

1

Parte 1. PRIMEIROS CONTATOS COM O MÉTODO PROBABILÍSTICO 3

1. ... 3

1.1. Aula 05 de março de 2018 3

1.2. Aula 07 de março de 2018 6

1.3. Aula 12 de março de 2018 9

1.4. Aula 14 de março de 2018 13

1.5. Aula 19 de março de 2018 - Incidência de Pontos e Retas 16

1.6. Aula 21 de março de 2018 20

2. O método do segundo momento 24

2.1. Aula 05 de maio de 2018 24

2.2. Aula 04 de abril de 2018: Subgrafos pequenos em $G(n,p)$ 29

2.3. Aula 09 de Abril de 2018: O Teorema de Rödl 34

2.4. Aula 11 de abril de 2018 42

2.5. Aula 23 de abril de 2018 45

3. Probabilidades exponencialmente pequenas 48

3.1. Aula 25 de abril de 2018: Probabilidades exponencialmente pequenas 48

3.2. Aula 07 de maio de 2018 50

3.3. Aula 09 de maio de 2018 53

3.4. Aula 14 de maio de 2018 57

3.5. Aula 16 de maio de 2018 60

3.6. Aula 05 de maio de 2018 64

Parte 2. MAIS APLICAÇÕES 68

Parte 3. TÓPICOS AVANÇADOS 69

3.7. Aula 6 de junho de 2018 69

4. Lema Local de Lovász 70

4.1. Aula 11 de junho de 2018: Lema Local de Lovasz Algoritmico 71

5. Complexidade de circuitos 77

5.1. Aula 13 de junho de 2018: Cotas inferiores para complexidade monótona 77

5.2. Aula 18 de junho de 2018: Complexidade monótona e circuitos de profundidade limitada 79

5.3. Aula 20 de Junho de 2018: Circuitos de profundidade limitada (continuação) 81

Parte 4. BIBLIOGRAFIA 86

Referências 86

Parte 1. PRIMEIROS CONTATOS COM O MÉTODO PROBABILÍSTICO

§1. ...

1.1. Aula 05 de março de 2018. [1]

1.1.1. *Provas por contagem.*

Exemplo 1. Vamos chamar de *dovetail shuffling* (também conhecido como *riffle shuffling*) o processo de dividir um baralho comum de 52 cartas em dois montes do mesmo tamanho e entrelaçar as cartas desses montes de forma arbitrária. Pergunta: quatro dovetail shufflings são suficientes para se obter qualquer ordenação das cartas?

Executar um dovetail shuffling corresponde a escolher um subconjunto de 26 posições de uma lista de 52 disponíveis; essas posições escolhidas recebem as cartas do primeiro monte (em ordem) e as outras 26 posições recebem as cartas do segundo monte (também em ordem). Portanto, existem $\binom{52}{26}$ diferentes dovetail shufflings. Atingimos, assim, no máximo $\binom{52}{26}^4$ diferentes permutações do baralho original após quatro dovetail shufflings.

Usando os limitantes $\binom{52}{26} \leq 2^{52}$ e $52! \geq (\frac{52}{e})^n$, temos

$$\binom{52}{26}^4 \leq (2^4)^{52} < \left(\frac{52}{e}\right)^{52} \leq 52!\,,$$

pois $2^4 = 16 < \frac{52}{3} < \frac{52}{e}$.

Portanto, a resposta é *não*.

Exemplo 2. Consideremos agora funções booleanas. Se $f : \{0,1\}^n \to \{0,1\}$ é uma função booleana, sabemos que é possível expressar f como uma fórmula booleana em n variáveis, usando apenas parênteses e os operadores $\neg$, $\wedge$ e $\vee$. Por exemplo, podemos facilmente codificar f na formal normal disjuntiva (FND) da seguinte forma: para cada $(a_1, \ldots, a_n) \in f^{-1}(1)$, definimos uma conjunção cujos literais são x_i se $a_i = 1$ e $\neg x_i$ se $a_i = 0$, para $i = 1, \ldots, n$, sendo a fórmula para f uma disjunção dessas conjunções. Claramente, tal codificação em FND pode ter comprimento $\Theta(n2^n)$. Pergunta: é possível codificar toda função booleana com uma fórmula de comprimento no máximo n^{2018}?

Uma função booleana em n variáveis atribui, para cada um dos 2^n vetores de n bits, um valor em $\{0,1\}$; são, portanto, 2^{2^n} possíveis escolhas para f. Por outro lado, usando apenas os $n+5$ símbolos "$\neg$", "$\wedge$", "$\vee$", "(", ")", $x_1, \ldots, x_n$, existem no máximo $(n+5)^m$ fórmulas de comprimento m.

[1] Notas produzidas por Gabriel Ferreira Barros e Tiago Royer.

Temos que

$$2^{2^n} > (n+5)^m$$

quando

$$\frac{2^n}{\ln_2(n+5)} > m.$$

Se escolhermos $m = n^{2018}$, veremos que o lado esquerdo cresce mais rápido do que o lado direito. Portanto, para n suficientemente grande, teremos mais funções booleanas do que fórmulas de comprimento n^{2018} para representá-las. Assim, a resposta é *não*.

Exemplo 3. Um *hipergrafo* é um par (V, E) com $E \subseteq 2^V$. Um k-grafo é um hipergrafo em que toda hiperaresta $e \in E$ possui cardinalidade k.

Dizemos que o hipergrafo H possui a *propriedade* B ou, equivalentemente, que H é 2-*colorível* se existe uma coloração $c : V \to [2]$ tal que nenhuma aresta é monocromática (isto é, c não é constante em nenhuma aresta).

Defina o número $m(n)$ por

$$m(n) = \min\{|E|\colon\ H = (V, E) \text{ é um } n\text{-grafo que não é 2-colorível }\}.$$

Sabe-se que $m(n) = \Omega(\sqrt{n/\ln n}2^n)$ [7] e que $m(n) < n^2 2^n$ [3]. Erdős and Lovász conjecturam que $m(n) = \Theta(n2^n)$ [4].

Temos $m(1) = 1$ (qualquer 1-aresta é monocromática) e $m(2) = 3$ (um triângulo possui três arestas e não é 2-colorível; os grafos com menos arestas são todos 2-coloríveis). Analisemos $m(3)$.

Para obter um limitante superior, considere o plano de Fano (Figura 2). Os vértices do hipergrafo correspondente são os pontos do plano, e as hiperarestas são as linhas (indicadas pelas seis linhas retas e pelo círculo).

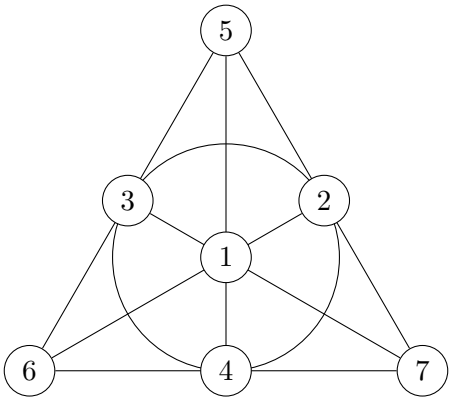

FIGURA 1. Plano de Fano.

Afirmamos que o plano de Fano não é 2-colorível. De fato, por simetria podemos assumir que os vértices 2 e 3 possuem a mesma cor, e o vértice 4 possui uma cor diferente. Agora, para qualquer cor que escolhamos para o vértice 1, as cores dos demais vértices serão forçadas, e em ambos os casos terminaremos com uma aresta monocromática. Portanto, o plano de Fano não é 2-colorível, o que mostra que $m(3) \leq 7$.

Mostraremos agora que $m(3) > 6$. Seja $H = (V, E)$ um 3-grafo com $|E| \leq 6$. Consideremos dois casos.

Primeiro caso: $|V| \leq 6$. Sem perda de generalidade, podemos assumir que $|V| = 6$. Escolha três vértices de V ao acaso, pinte-os de uma mesma cor e pinte os outros três de outra cor. Existem $\binom{6}{3} = 20$ possíveis colorações, e cada aresta só fica monocromática em duas dessas escolhas. Assim, existem no máximo $2|E| \leq 12$ colorações "proibidas", e esse número é menor que o número total de colorações. Portanto, alguma dessas colorações não deixa nenhuma aresta monocromática.

Segundo caso: $|V| > 6$. Considere o grafo bipartido G cujos vértices são $V \cup E$ e há uma aresta entre $v \in V$ e $e \in E$ se $v \in e$. Cada $e \in E$ é tocado por exatamente três arestas, portanto o número de arestas de G é igual a $3|E| \leq 18$. Como $|V| \geq 7$, o grau médio (em G) dos vértices $v \in V$ é menor ou igual a $18/|V| < 3$, o que implica que ao menos um vértice v está em no máximo duas hiperarestas de H. Como estas duas hiperarestas cobrem no máximo cinco vértices de H (incluindo v), existe um vértice u tal que nenhuma hiperaresta contém ambos u e v. Agora, construa o hipergrafo H' identificando u e v; H' ainda é um 3-grafo, e, por indução, é 2-colorível. Basta então copiar as cores para o grafo H original (u e v terão a mesma cor).

Portanto, $m(3) = 7$.

Uma busca computacional realizada por Östergård mostrou que $m(4) = 23$ [9].

Proposição 4. *Seja $m(n)$ como definido acima. Então*

$$m(n) \geq 2^{n-1}.$$

Demonstração. Seja $H = (V, E)$ um n-grafo com $|E| < 2^{n-1}$. Vamos mostrar que H é 2-colorível.

Pinte cada vértice de uma cor de maneira independente, com ambas as cores tendo a mesma probabilidade. A probabilidade de uma aresta fixa $e \in E$ ficar monocromática é $\frac{2}{2^n} = 2^{1-n}$. Logo, a probabilidade de alguma aresta $e \in E$ ficar monocromática é no máximo $2^{1-n}|E| < 1$, e o procedimento descrito acima pinta H corretamente com probabilidade positiva.

Isso significa que H é 2-colorível. □

1.2. **Aula 07 de março de 2018.** ...[2]

Definição 5. *Uma tupla* $(\Omega, \mathbb{P})$ *é um* espaço de probabilidade finito *se* $|\Omega| < \infty$ *e* $\mathbb{P} : 2^\Omega \to [0,1]$ *é uma função que satisfaz*

(1) $\mathbb{P}(\varnothing) = 0$*;*

(2) $\mathbb{P}(\Omega) = 1$*;*

(3) Para todo $A, B \subseteq \Omega$ *tais que* $A \cap B = \varnothing$ *vale que* $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)$.

Um conjunto $A \subseteq \Omega$ *é chamado* evento.

Observação 6. Se $A, B \subseteq \Omega$ então $\mathbb{P}(A \cup B) \leq \mathbb{P}(A) + \mathbb{P}(B)$. Em geral, se $(A_\lambda)_{\lambda \in \Lambda}$ são eventos em Ω, então

$$\mathbb{P}\left(\bigcup_\lambda A_\lambda\right) \leq \sum_{\lambda \in \Lambda} \mathbb{P}(A_\lambda).$$

Essa desigualdade é chamada "cota da união", ou às vezes "desigualdade de Boole."

1.2.1. *Caso uniforme.*

Se $A = \{a_\lambda : \lambda \in \Lambda\}$, então $\mathbb{P}(A) = \sum_{\lambda \in \Lambda} \mathbb{P}(a_\lambda)$. Se $\mathbb{P}(\omega) = 1/|\Omega|$ para todo $w \in \Omega$, chamamos o espaço $(\Omega, \mathbb{P})$ de espaço de probabilidade *uniforme*. Neste caso, $\mathbb{P}(A) = |A|/|\Omega|$ para todo $A \subseteq \Omega$.

Exemplo 7. Considere o espaço de probabilidade $(\Omega, \mathbb{P})$ onde $\Omega = \{0,1\}^n$, $n \geq 1$, e $\mathbb{P}$ uniforme. Assim, $\mathbb{P}((x_i)_{i=1}^n) = 1/(2^n)$ para todo $(x_i)_{i=1}^n \in \{0,1\}^n$.

Exemplo 8. Considere o espaço de probabilidade $(\Omega, \mathbb{P})$ onde $\Omega = S_n$, $n \geq 1$, e $\mathbb{P}$ uniforme. Assim, $\mathbb{P}(\sigma) = 1/n!$ para todo $\sigma \in S_n$.

Exemplo 9. Considere o espaço de probabilidade $(\Omega, \mathbb{P})$ onde $\Omega = S_{52}$ e $\mathbb{P}$ uniforme. Isto é, $(\Omega, \mathbb{P})$ é uma permutação uniforme do baralho de 52 cartas. Quanto é $\mathbb{P}(\sigma(1) < \sigma(2))$? A resposta correta é $1/2$. Essa resposta é intuitivamente verdadeira porque a distribuição é uniforme. Para provar formalmente o resultado, basta observar que existe uma bijeção entre $A = \{\sigma \in S_n : \sigma(1) < \sigma(2)\}$ e $B = \{\sigma \in S_n : \sigma(2) < \sigma(1)\}$. Deste modo, temos $|A| = |B| = n!/2$.

1.2.2. *Eventos independentes.*

Definição 10. *Dois eventos* $A, B \subseteq \Omega$ *são* independentes *se* $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$. *Mais geralmente, os eventos* $A_1, \ldots, A_k \subseteq \Omega$ *são* independentes *se, para todo* $i_1 < i_2 < \cdots < i_\ell$ *e* $\ell \geq 2$ *vale que* $\mathbb{P}(A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_\ell}) = \mathbb{P}(A_{i_1})\mathbb{P}(A_{i_2}) \ldots \mathbb{P}(A_{i_\ell})$. *Finalmente, os eventos* $A_1, \ldots, A_n \subseteq \Omega$ *são* k-a-k independentes *se, para todo* $i_1 < i_2 < \cdots < i_k$*, os eventos* $A_{i_1}, \ldots, A_{i_k}$ *são independentes.*

[2] Notas produzidas por Bruno Pasqualotto Cavalar e Marcelo Tadeu Sales. Aula de 07/03/2018.

Exemplo 11. Considere o espaço de probabilidade uniforme sobre S_n, $n \geq 3$. Considere também os seguintes eventos nesse espaço de probabilidade:

- $A = \{\sigma(1) = 1\}$;
- $B = \{\sigma(1) = 2\}$;
- $C = \{\sigma(2) = 2\}$;
- $D = \{\sigma(2) < 3\}$.

A tabela a seguir indica a relação de dependência entre os eventos.

	A	B	C	D
A	Não	Não	Não	Sim
B		Não	Não	Sim
C			Não	Sim sse $n = 3$
D				Não

Daqui em diante, escrevemos $x \in_U \Omega$ para denotar que x é escolhido uniformemente ao acaso dentro de Ω.

Exemplo 12. Seja $x_i \in_U \{0, 1\}$, para $i = 1, \ldots, n$. Suponha que as n escolhas são independentes. Segue que $\mathbb{P}[(x_i)_{i=1}^n = (a_i)_{i=1}^n] = 1/(2^n)$ para qualquer $(a_i)_{i=1}^n \in \{0, 1\}^n$ fixo. Observe que a amostragem de $x = (x_i)_{i=1}^n$ segue a distribução $(\Omega, \mathbb{P}) = (\{0, 1\}^n, \text{uniforme})$.

Exemplo 13. Tome $X_1 \in_U \mathbb{Z}_2$ e $X_2 \in_U \mathbb{Z}_2$ e defina $X_3 := X_1 + X_2$. Temos que X_1, X_2 e X_3 são 2-a-2 independentes, mas não são independentes, pois X_3 é completamente determinado pela escolha de X_1 e X_2.

Exemplo 14 (Secretary/Hiring Problem)**.** No problema da contratação, Bob entrevista n candidatos, um por vez, e escolhe apenas um deles. No entanto, a cada entrevista Bob é forçado a contratar ou rejeitar, e não pode voltar atrás na sua decisão. Suponha que cada candidato possui um número que indica a sua qualidade, e que Bob quer contratar o candidato de maior número. Suponha também que a ordem relativa dos números dos candidatos forma uma permutação aleatória uniforme. Qual é uma boa estratégia para garantir que Bob irá contratar o candidato de maior número? Aqui vamos analisar a estratégia de corte r, denotada por E_r.

A estratégia E_r vê os primeiros r candidatos, e depois escolhe o primeiro candidato que tiver número maior do que o máximo dos primeiros r candidatos. Seja σ a permutação que indica a ordem relativa dos números dos candidatos. Fazendo abuso de notação, escreveremos que $\sigma(i) = \max$ se o número máximo estiver na posição i. Observe que, se $\sigma(i) = \max$ para $i \in [r]$, então E_r não escolhe o máximo. Por outro lado, se $\sigma(i) = \max$ para $i > r$, então E_r escolhe o máximo se, e somente se, o máximo dos primeiros $i - 1$ candidatos estiver entre os

primeiros r candidatos. Como a permutação é escolhida uniformemente ao acaso, isso acontece com probabilidade $r/(i-1)$.

Disto segue que

$$\begin{aligned}
\mathbb{P}[E_r \text{ escolhe o máximo}] &= \sum_{i=1}^{n} \mathbb{P}[E_r \text{ escolhe o máximo} \,|\, \sigma(i) = \max]\mathbb{P}[\sigma(i) = \max] \\
&= \sum_{i=r+1}^{n} \mathbb{P}[E_r \text{ escolhe o máximo} \,|\, \sigma(i) = \max]\mathbb{P}[\sigma(i) = \max] \\
&= \sum_{i=r+1}^{n} \frac{r}{i-1} \cdot \frac{1}{n} \\
&= \frac{r}{n} \sum_{i=r+1}^{n} \frac{1}{i-1} \\
&\sim \frac{r}{n} \ln \frac{n}{r}.
\end{aligned}$$

Como $x \ln(1/x)$ é maximizado para $x = 1/e$, segue que $\mathbb{P}[E_r \text{ escolhe o máximo}] \sim 1/e \approxeq 0.37$ para $r = n/e$.

Exemplo 15 (Grafos aleatórios)**.** Denotamos por $G(n,p)$ o *grafo aleatório binomial* em que cada aresta aparece independentemente com probabilidade p. Seja E_1 o evento de $G(n,1/2)$ ser bipartido e E_2 o evento de $G(n,1/2)$ ser conexo. Sem perda de generalidade, suponha que $V(G(n,p)) = [n]$.

Vamos provar primeiro que o grafo aleatório $G(n,1/2)$ não é bipartido com alta probabilidade. Para todo $k = 1, 2, \ldots, \lfloor n/3 \rfloor$, defina $V_k := \{3k-2, 3k-1, 3k\}$. Seja também A_k o evento de não ocorrer o triângulo de vértices V_k em $G(n,1/2)$. Como $V_i \cap V_j = \varnothing$ para todo $i \neq j$, segue que os eventos A_i e A_j são independentes para todo $i \neq j$. Observe também que $\mathbb{P}[A_k] = 2^{-3}$. Note ainda que, se $G(n,1/2)$ é bipartido, então não pode ocorrer A_k para todo $k = 1, 2, \ldots, \lfloor n/3 \rfloor$. Segue que

$$\mathbb{P}[E_1] \leq \prod_{k=1}^{\lfloor n/3 \rfloor} \mathbb{P}[\neg A_k] = 2^{-3\lfloor n/3 \rfloor} = o(1).$$

Portanto, com alta probabilidade o grafo aleatório $G(n,1/2)$ não é bipartido.

Vamos provar agora que $G(n,1/2)$ é conexo com alta probabilidade. Observe que, se $G(n,1/2)$ é desconexo, então existem dois vértices $x_i, x_j \in V(G(n,1/2))$ tais que não existe caminho de comprimento dois entre v_i e v_j. Isso acontece com probabilidade igual a $2^{-2(n-2)}$. Portanto, pela cota da união segue que

$$\mathbb{P}[\neg E_2] \leq \binom{n}{2} 2^{-2(n-2)} \sim 8\frac{n^2}{4^n} = o(1).$$

Isso mostra que $G(n, 1/2)$ é conexo com alta probabilidade.

1.3. **Aula 12 de março de 2018.** [3]

1.3.1. *Variáveis aleatórias e esperança.*

Definição 16. *Seja* $(\Omega, \mathbb{P})$ *um espaço de probabilidade finito tal que* $\mathbb{P} : 2^\Omega \to [0, 1]$. *Uma* variável aleatória *(real) é uma função* $f : \Omega \to \mathbb{R}$.

Definição 17. *A* esperança *da variável aleatória* f, *denotada* $\mathbb{E}(f)$, *é igual a*

$$\sum_{\omega \in \Omega} \mathbb{P}(\omega) f(\omega).$$

Observação 18. Se $\mathbb{P}$ é uniforme, então

$$\mathbb{E}(f) = |\Omega|^{-1} \sum_{\omega \in \Omega} f(\omega) = \text{ Avg}(f).$$

Definição 19. *Seja* $A \subseteq \Omega$. *A* função indicadora *de* A *é* $\mathcal{I}_A : \Omega \to \mathbb{R}$ *dada por*

$$\mathcal{I}_A(\omega) = \begin{cases} 1, & \text{se } \omega \in A \\ 0, & \text{se } \omega \notin A \end{cases}$$

(Notação alternativa: $\mathbb{1}_A$, $[A]$, χ_A, *etc.)*

Observação 20. $\mathbb{E}(\mathcal{I}_A) = \mathbb{P}(A)$.

Teorema 21. Linearidade da esperança.

Sejam f, g *variáveis aleatórias sobre* $(\Omega, \mathbb{P})$ *e* $\alpha \in \mathbb{R}$. *Então*

(i) $\mathbb{E}(f + g) = \mathbb{E}(f) + \mathbb{E}(g)$

(ii) $\mathbb{E}(\alpha f) = \alpha \mathbb{E}(f)$

Exemplo 22. Considere $\Omega = \{0, 1\}^n$ com $n \geq 1$ e $\mathbb{P}$ uniforme. Seja $x = (x_i)_{i=1}^n \in \{0, 1\}^n$ e a variável aleatória f_1 definida por $f_1(x) = \sum_{i=1}^n x_i = \#$ bits 1 do vetor x. Então

$$\mathbb{E}(f_1) = \sum_{x \in \{0,1\}^n} \mathbb{P}(x) f(x) = 2^{-n} \sum_{k=0}^{n} \binom{n}{k} k = 2^{-n} \sum_{k=1}^{n} \frac{n}{k} \binom{n-1}{k-1} k = 2^{-n} n 2^{n-1} = \frac{n}{2}.$$

Esse mesmo resultado pode ser obtido com o auxílio de funções indicadoras dadas pelos eventos $A_i = \{x \in \{0, 1\}^n : x_i = 1\}$. Note que $\forall x \in \Omega$

$$f_1(x) = \sum_{i=1}^{n} \mathcal{I}_{A_i}(x)$$

[3] Notas produzidas por Rodrigo Enju e André Nakazawa.

e consequentemente, pela linearidade da esperança,

$$\mathbb{E}(f_1) = \sum_{i=1}^{n} \mathbb{E}(\mathcal{I}_{A_i}) = \sum_{i=1}^{n} \mathbb{P}(A_i) = \frac{n}{2},$$

pois segue da uniformidade de $\mathbb{P}$ que $\mathbb{P}(A_i) = \frac{1}{2}$ $\forall i \in [n]$.

Observação 23. *Contagem dupla.* O resultado do exemplo anterior confirma a relação

$$\sum_{k=0}^{n} \binom{n}{k} k = n2^{n-1}.$$

Exemplo 24. *Coelhos sobreviventes.* Considere a seguinte situação, temos n coelhos e n caçadores. Cada caçador escolhe independentemente um coelho com probabilidade uniforme e atira. Os coelhos que não foram escolhidos por nenhum caçador são ditos sobreviventes. Então, podemos definir uma variável aleatória f_2 como o número de coelhos sobreviventes.

O espaço de probabilidade desta situação é

$$[n]^{[n]} = \{t : [n] \to [n]\}$$

com distribuição uniforme.

Seja A_i o evento em que o coelho i sobrevive. Temos que

$$f_2 = \sum_{i=1}^{n} \mathcal{I}_{A_i}.$$

Como a probabilidade do coelho i sobreviver é

$$\mathbb{P}(A_i) = \left(1 - \frac{1}{n}\right)^n$$

e tal probabilidade tende para $1/e$ quando n tende para infinito, segue que

$$\mathbb{E}(f_2) = \sum_{i=1}^{n} \mathbb{E}(\mathcal{I}_{A_i}) = \sum_{i=1}^{n} \mathbb{P}(A_i) \to n\frac{1}{e} = \frac{n}{e}.$$

Exemplo 25. *Número de máximos sucessivos.* Dada uma sequência $x_1, \cdots, x_n$ de n números inteiros distintos, dizemos que um elemento x_i é *left-to-right maxima* (LtR max) se $x_i \geq x_j$ sempre que $i \geq j$. Queremos estimar o número de LtR maxes em sequências de n números. Para isso, considere $\pi \in_U S_n$ e seja f_3 o número de LtR maxes em $\pi(1), \cdots, \pi(n)$. Tomemos o evento $A_i = \{\pi \in S_n : \pi(i) \text{ é um LtR max}\}$, então

$$f_3 = \sum_{i=1}^{n} \mathcal{I}_{A_i}.$$

A probabilidade do evento A_i é igual à probabilidade do i-esimo elemento ser o maior dentre os i primeiros elementos de π. Como π é uma permutação uniforme, a probabilidade de i ser o maior elemento de $(\pi(1), \cdots, \pi(i))$ é $1/i$. Assim,

$$\mathbb{E}(f_3) = \sum_{i=1}^{n} \mathbb{P}(A_i) = 1 + \frac{1}{2} + \cdots + \frac{1}{n} = H_n.$$

Então segue de $\log(n+1) \leq H_n \leq \log(n) + 1$ que $H_n = \Theta(\log n)$.

Exemplo 26. *Número de comparações no algoritmo Quicksort.* Considere o algoritmo Quicksort determinístico que ao receber uma entrada $x_{\pi(1)}, \cdots, x_{\pi(n)}$ de n elementos distintos devolve $x_1 < \cdots < x_n$ como saída, sendo que $\pi \in_U S_n$. Queremos estimar f_4 o número de comparações efetuadas pelo algoritmo. Tal resultado será desenvolvido em notas posteriores.

1.3.2. *Mais aplicações.*

Observação 27. Dado um grafo G qualquer, denotamos por $V(G)$ o conjunto de seus vértices e por $E(G)$ o conjunto de suas arestas. Ademais, escrevemos G^N para expressar que $|V(G)| = N$.

(1) Subgrafo bipartido grande

Teorema 28. *Seja $G = G^{2n}$, para $n \geq 1$. Existe uma bipartição balanceada com mais do que $|E(G)|/2$ arestas entre os conjuntos.*

Demonstração. Escolhemos $A \subseteq V(G)$, com $|A| = n$, uniforme ao acaso. Consideremos a bipartição A, B, com $V(G) = A \cup B$. Seja X o número de arestas entre A e B. Para cada $e \in E(G)$, seja $F_e = \{e \text{ é uma aresta entre } A \text{ e } B\}$. Então

$$X = \sum_{e \in E(G)} \mathcal{I}_{F_e}$$

Temos que

$$\mathbb{P}(F_e) = \frac{2\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{2\binom{2n-2}{n-1}}{\frac{2n(2n-1)}{n(n-1)}\binom{2n-2}{n-2}} = \frac{\frac{n-1}{2n-1}\frac{n}{n-1}\binom{2n-2}{n-2}}{\binom{2n-2}{n-2}} = \frac{n}{2n-1} > \frac{n}{2n} = \frac{1}{2}.$$

Portanto

$$\mathbb{E}(X) = \sum_{e \in E(G)} \mathbb{P}(F_e) > \frac{|E(G)|}{2}.$$

□

(2) Conjuntos independentes

Seja G um grafo, $S \subseteq V(G)$ é dito *independente* (ou estável) se $\nexists\, e \in E(G)$ com $e \subseteq S$. Definimos $\alpha(G) = max\{|S| : S \subseteq V(G)\}$.

Teorema 29 (Turán)**.** *Seja $G = G^n$, com $n \geq 1$, e $m = |E(G)|$. Então*

$$\alpha(G) \geq \frac{n^2}{2m+n}.$$

Lema 30. *Para todo grafo G vale que*

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{d(v)+1},$$

onde $d(v)$ é o grau do vértice $v \in V(G)$.

Demonstração. (Lema 30). Seja $V(G) = [n]$, sem perda de generalidade, e $\pi \in_U S_n$. Considere que $\pi(i)$ é bom se todos os vizinhos de $\pi(i)$ estão à direita de $\pi(i)$, isto é, $\pi(i) < \pi(j)$ $\forall j \in [n]$ tal que $\{\pi(i), \pi(j)\} \in E(G)$. Seja $B = \{i \in [n] : \pi(i) \text{ é bom}\}$. Note que B é independente, pois se $\{\pi(i), \pi(j)\} \in E(G)$ com $\pi(i) < \pi(j)$, então $\pi(j) \notin B$, ou seja, $\{\pi(i), \pi(j)\} \not\subseteq B$. Fixando $\pi \in S_n$ temos que

$$|B| = \sum_{1 \leq i \leq n} \mathcal{I}_{\{\pi(i) \text{ é bom}\}}.$$

Logo

$$\mathbb{E}(|B|) = \sum_{1 \leq i \leq n} \mathbb{P}\{\pi \in S_n : \pi(i) \text{ é bom}\} = \sum_{1 \leq i \leq n} \frac{1}{d(\pi(i))+1} = \sum_{i \in [n]} \frac{1}{d(i)+1},$$

e consequentemente existe $\pi \in S_n$ tal que

$$|B| \geq \sum_{i \in [n]} \frac{1}{d(i)+1}.$$

Então, da independência de B segue que

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{d(v)+1}.$$

□

Teorema 31. Desigualdade de Jensen. *Seja X uma variável aleatória e f uma função convexa. Então $f(\mathbb{E}(X)) \leq \mathbb{E}(f(X))$.*

Demonstração. (Teorema 29). Pelo lema 30, temos que

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{d(v)+1}$$

Seja $X \in_U \{d(v) : v \in V(G)\}$ e

$$f(x) = \frac{1}{x+1}.$$

Como f é convexa,

$$\mathbb{E}(f(X)) = \frac{1}{n} \sum_{v \in V(G)} \frac{1}{d(v)+1} \geq \frac{1}{\bar{d}+1} = f(\bar{d}) = f(\mathbb{E}(X)),$$

sendo

$$\bar{d} = Avg(d) = \frac{1}{n} \sum_{v \in V(G)} d(v) = \frac{2m}{n}.$$

Logo

$$\alpha(G) \geq n \frac{1}{\bar{d}+1} = \frac{n^2}{2m+n}.$$

□

1.4. **Aula 14 de março de 2018.** [4]

1.4.1. *Uma aplicação geométrica.*

Definição 32. *Seja L um conjunto de retas do plano. Denotamos por $V(L)$ (ou simplesmente por V, quando L está subentendido pelo contexto) o conjunto de interseções de retas em L. Dizemos que L é uma configuração de retas em posição geral se ele satisfaz as seguintes condições:*

(1) Para cada ponto $v \in V(L)$, há exatamente duas retas que passam por v em L;

(2) Não há duas retas paralelas distintas em L;

(3) Não há retas verticais em L.

Definição 33. *Seja L uma configuração de retas em posição geral. Dado $v \in V$, definimos o nível de v em L, denotado por $\ell(v)$, como o número de interseções da semi-reta vertical de origem v com retas de L que não passam por v.*

Dada uma configuração de retas em posição geral L, considere as convenções:

- $V_k = \{v \in V : \ell(v) = k\}$.
- $V_{\leq k} = \bigcup_{0 \leq i \leq k} V_k$.
- $t_k(L) = |V_k|$; $t_{\leq k}(L) = |V_{\leq k}|$.
- $t_k(n) = max\{t_k(L) : |L| = n\}$; $t_{\leq k}(n) = max\{t_{\leq k}(L) : |L| = n\}$.

Observação 34. Note que $t_k(n) \leq n - k - 1$. Daí, $t_{\leq k}(n) \geq (n-1) + ... + (n-k-1) = (k+1)(2n-k-2)/2 = \Omega(nk)$.

[4] Notas produzidas por Thiago Estrela e Ângelo Lovatto.

Teorema 35 (Clarkson - Shor)**.** *Temos:*

$$t_{\leq k} \leq 3(k+1)n.$$

Demonstração. Seja $R = L_p$ um subconjunto aleatório de L obtido incluindo-se cada $\ell \in L$ de modo independente com probabilidade p. Seja $X = t_0(R)$. Note que, para qualquer $M \subseteq L$, tem-se $t_0(M) \leq |M|-1 \leq |M|$ (Observação 34). Assim:

$$\mathbb{E}(X) = \mathbb{E}(T_0(R)) \leq \mathbb{E}(|R|) = np.$$

Para cada $v \in V(L)$, considere o evento $A_v = \{v \in V_0(R)\}$. A_v ocorre se e somente se ambas as retas que determinam a interseção v estão em R e nenhuma das retas que interceptam a semi-reta vertical de origem v em L estão em R. Portanto, temos

$$t_0(R) = \sum_{v \in V(L)} \mathbb{1}_{A_v},$$

$$\mathbb{P}(A_v) = p^2(1-p)^{\ell_L(v)},$$

294 onde $\ell_L(v)$ é o nível de v em L. Assim,

$$\begin{aligned}
np = \mathbb{E}(|R|) &\geq \mathbb{E}(t_0(R)) \\
&= \sum_{v \in V(L)} \mathbb{E}(\mathbb{1}_{A_v}) && \text{(linearidade da esperança)} \\
&= \sum_{v \in V(L)} \mathbb{P}(A_v) \\
&= \sum_{v \in V(L)} p^2(1-p)^{\ell_L(v)} \\
&\geq \sum_{v \in V_{\leq k}(L)} p^2(1-p)^{\ell_L(v)} \\
&\geq \sum_{v \in V_{\leq k}(L)} p^2(1-p)^{k} && (\ell_L(v) \leq k) \\
&= t_{\leq k}(L)p^2(1-p)^k.
\end{aligned}$$

Logo,

$$t_{\leq k}(L) \leq \frac{n}{p(1-p)^k}.$$

295 Tomando $p = 1/(k+1)$, segue que

$$\frac{n}{p(1-p)^k} = \frac{n}{\frac{1}{k+1}(1-\frac{1}{k+1})^k} \leq en(k+1),$$

$$\therefore t_{\leq k}(L) \leq 3n(k+1).$$

□

1.4.2. *Número de comparações do Quicksort.* O algoritmo Quicksort recebe uma sequência $(x_1, \ldots, x_n)$ de números como entrada e separa seus elementos, exceto x_1, em duas sequências: uma contendo os elementos menores que x_1 e outra com os elementos maiores ou iguais a x_1. Em ambas, a ordem dos elementos permanece a mesma da sequência de entrada. Cada uma é então ordenada por uma aplicação recursiva do mesmo método. A recursão termina quando as sequências são trivialmente pequenas (1 ou nenhum elemento).

Embora o algoritmo possa precisar de $O(n^2)$ passos para completar a ordenação, na prática Quicksort é bem eficiente, como mostra o seguinte teorema.

Teorema 36. *Suponha $x_1 < x_2 < \cdots < x_n$. Seja π uma permutação aleatória escolhida uniformemente ao acaso entre todas as permutações da sequência $(1, \ldots, n)$. Em outras palavras, $\pi \in_\cup S_n$. Seja $T(\pi) = \#$ comparações no Quicksort com entrada*

$$x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}.$$

Então $\mathbb{E}(T) \leq 2n \ln n$.

Demonstração. Seja $T_i = T_i(\pi) = \#$ comparações quando $x_{\pi(i)}$ é o pivô. Por exemplo, temos sempre que $T_1 = n - 1$. Em geral, podemos interpretar T_i de acordo com a seguinte sequência:

$$x_1, \ldots, \mathbf{x_j}, x_{j+1}, x_{j+2}, x_{j+3}, \underline{\mathbf{x_{j+4}}} = x_{\pi(i)}, x_{j+5}, \mathbf{x_{j+6}}, \ldots, x_n.$$

A sequência mostra os elementos ordenados, onde os que estão em negrito marcam os pivôs escolhidos antes de $x_{\pi(i)}$, ou seja, os elementos com índices $\pi(1), \ldots, \pi(i-1)$. Note que T_i é igual ao número de elementos não marcados entre $x_{\pi(i)}$ e o elemento em negrito mais próximo, em ambas as direções. Informalmente, T_i é exatamente a quantidade de elementos que $x_{\pi(i)}$ "enxerga", se os em negrito forem considerados opacos.

Claramente, $T(\pi) = \sum_{i=1}^n T_i$, pois cada elemento é pivô exatamente uma vez. Por linearidade da esperança, temos que $\mathbb{E}(T(\pi)) = \sum_{i=1}^n \mathbb{E}(T_i)$.

Para calcular $\mathbb{E}(T_i)$, consideraremos o algoritmo executando de volta no tempo, ou seja, começamos com todos os elementos já marcados como pivôs. Geramos então a sequência aleatória π da seguinte maneira: em cada passo de tempo i, começando com $i = n$ até 1, escolhemos um dos elementos em negrito uniformemente ao acaso e atribuímos seu índice a

$\pi(i)$, simultaneamente desmarcando tal elemento como pivô. A quantidade T_i é o número de elementos que $x_{\pi(i)}$ enxerga nesse momento.

Note que no passo de tempo i, antes de sortear $\pi(i)$, restam exatamente i pivôs na sequência. Cada um dos $n-i$ elementos não marcados enxerga no máximo 2 em negrito. Portanto o número de pares (não marcado, marcado) cujos membros enxergam um ao outro é no máximo $2(n-i)$. Em média, um dos i elementos em negrito enxerga no máximo $\frac{2(n-i)}{i}$ elementos, e portanto $\mathbb{E}(T_i) \leq \frac{2(n-i)}{i}$. Logo, temos

$$\begin{aligned}\mathbb{E}(T(\pi)) &= \sum_{i=1}^{n} \mathbb{E}(T_i) \leq \sum_{i=1}^{n} \frac{2(n-i)}{i} \\ &= 2n \sum_{i=1}^{n} \frac{1}{i} - 2n = 2nH_n - 2n \\ &\leq 2n \ln n.\end{aligned}$$

□

1.5. **Aula 19 de março de 2018 - Incidência de Pontos e Retas.** [5]

1.5.1. *Plano Projetivo Finito.*

Definição 37. *Seja $|X| < \infty$, $\mathcal{L} \subseteq \wp(X)$. A dupla $(X, \mathcal{L})$ é plano projetivo se:*

(1) $\exists F \subseteq X : |F| = 4$ *e* $|F \cap L| \leq 2, \forall L \in \mathcal{L}$;

(2) $\forall L, L' \in \mathcal{L}$, $L \neq L'$ *temos* $|L \cap L'| = 1$;

(3) $\forall x, x' \in X, x \neq x', \exists! \, L \in \mathcal{L}$ *com* $\{x, x'\} \subseteq L$;

Podemos chamar o conjunto X de Pontos e o conjunto $\mathcal{L}$ de Retas, para uma ideia intuitiva

Fato 38. *Da definição de plano projetivo finito pode ser deduzido:*

(1) $\forall L, L' \in \mathcal{L}$ *temos* $|L| = |L'|$;

(2) ***def**: A **ordem** de um plano projetivo finito é* $|L| - 1, L \in \mathcal{L}$;

(3) Se um plano projetivo finito tem ordem n:

- $\forall x \in X$ *existem exatamente* $n+1$ *retas* $L \in \mathcal{L}$ *com* $x \in L$;
- $\forall L \in \mathcal{L}, |L| = n+1$;
- $|X| = n^2 + n + 1$ *e* $|\mathcal{L}| = n^2 + n + 1$;

[5] Notas produzidas por Rafael Zuolo e Gabriel Lasso

1.5.2. *Existência e Exemplo.* Seja q uma potência de primo, então um plano projetivo finito de ordem n pode ou não existir:

n	2	3	4	5	6	7	8	9	10	11	12	$\cdots$	q
$\exists!$	sim	sim	sim	sim	não	sim	sim	sim	não	sim	em aberto	$\cdots$	sim

Note que mesmo se tratando de conjuntos finitos, não se sabe se existe ou não um PPF de ordem $n = 12$. Para $n = 2$, chamamos o PPF de **fano**:

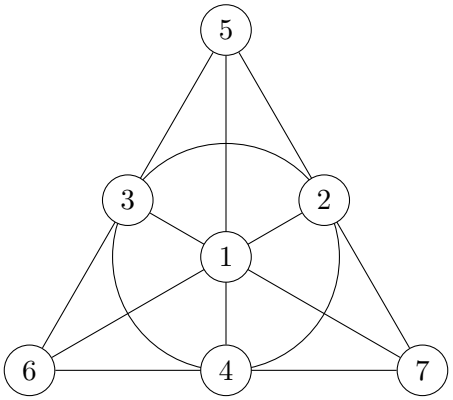

FIGURA 2. Fano.

Para meditar em casa: é possível desenhar o fano no $\mathbb{R}^2$ com retas?

Definição 39. ***Incidência****: É um par* (x, L) *com* $x \in L$*;*

Podemos representar a incidência como um grafo bipartido, onde uma partição representa o conjunto de pontos, a outra o conjunto de retas, e uma aresta liga um ponto x a uma reta L se existe a incidência (x, L):

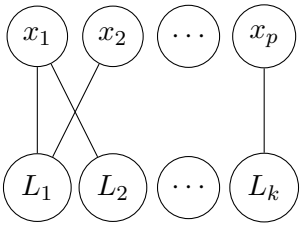

FIGURA 3. Grafo bipartido das incidências

Note que esse grafo de incidência não pode ter C^4, pois dois pontos não podem determinar duas retas distintas.

O número de incidência no plano projetivo finito de ordem n é:

$$|\mathcal{L}|(n+1) = (n^2 + n + 1)(n+1) = O(n^3)$$

1.5.3. *Agora em* $\mathbb{R}^2$. Seja $X \subseteq \mathbb{R}^2, |X| < \infty$, e $\mathcal{L}$ uma coleção de retas em $\mathbb{R}^2$. O quão grande pode ser o número de incidências (x, L)? Utilizando o fato do grafo de incidências ser livre de C^4, podemos obter um limite superior:

Teorema 40. *Seja $B = B(n, m; t)$ um grafo bipartido $m \times n$ com t arestas. Se $C^4 \nsubseteq B$, então:*

$$t \leq \min\{n\sqrt{m} + m; m\sqrt{n} + n\}$$

Demonstração.

$$\frac{m^2}{2} \geq \binom{m}{2} \geq \sum_i \binom{d_i}{2} \geq n\binom{\overline{d_i}}{2}$$

pela desigualdade de Jensen, onde $\overline{d_i}$ é o grau médio de B:

$$n\binom{\overline{d_i}}{2} = n\binom{t/n}{2} \geq \frac{n}{2}(\frac{t}{n} - 1)^2 \Longrightarrow$$
$$\Longrightarrow \frac{t}{n} - 1 \leq \sqrt{\frac{m^2}{n}} \Longrightarrow t \leq m\sqrt{n} + n$$

Analogamente para n, portanto t é o mínimo das duas expressões deduzidas. □

Tando no plano projetivo finito como em $\mathbb{R}^2$, se temos N pontos e N retas, então o número de incidências $\#inc = O(N^{\frac{3}{2}})$.

No plano projetivo finito essa aproximação é justa, mas e em $\mathbb{R}^2$?

Pergunta para refletir: Existe $X \subseteq \mathbb{R}^2, |X| = n$, tal que seja válido ao mesmo tempo:

- $\forall$ reta determinada por X contém $o(n)$ pontos?;
- O número de retas determinadas por X é $o(n^2)$?;

1.5.4. *O Teorema de Szemeredi e Trotter.* Seja $P \subseteq \mathbb{R}^2, \mathcal{L}$ retas em $\mathbb{R}^2$.

Definição 41. $I(P, \mathcal{L}) := \#\{(x, L) : x \in P, L \in \mathcal{L}, x \in L\}$ $I(m, n) = \max\{I(P, \mathcal{L}) : |P| = m, |\mathcal{L}| = n\}$

Considerando o grafo bipartido $P \times \mathcal{L}$ e usando o fato que ele não contém C^4, deduzimos que:

$$I(m, n) \leq \min\{m\sqrt{n} + m; n\sqrt{m} + m\}$$

Caso m=n, então $I(n, n) = O(n^{\frac{3}{2}})$.

O teorema de Sz-Tr mostra que $I(n, n) = O(n^{\frac{4}{3}})$ e é justo.

Proposição 42. $I(n, n) = \Omega(n^{\frac{4}{3}})$

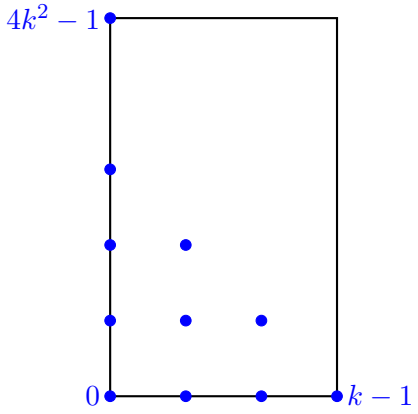

FIGURA 4. Construção de pontos para $I(n,n) = \Omega(n)^{\frac{4}{3}}$

Demonstração. Considere $X = \{0, \cdots, k-1\} \times \{0, \cdots, 4k^2-1\}$, ou seja, $n = |X| = 4k^3$.

Faça $\mathcal{L} = \{y = ax + b : a = 0, 1, \cdots, 2k-1; b = 0, \cdots, 2k^2-1\}$.

Note que $0 \leq ax + b \leq (2k-1)(k-1) + 2k^2 - 1 = 4k^2 - O(k) < 4k^2$.

$\therefore I(P, \mathcal{L}) \geq |\mathcal{L}|k = (4k^3)k = 4k^4$, mas $n^{\frac{4}{3}} = (4k^3)^{\frac{4}{3}} \leq 4k^4 \leq I(P, \mathcal{L})$ □

Teorema 43.

$$I(m,n) \leq 4(mn)^{\frac{2}{3}} + 4m + n$$

Prova será apresentada mais a frente, aguarde.

1.5.5. *Número de Cruzamentos.*

Definição 44. *Seja $G = (V, E)$ um grafo, $e(G) = |E(G)|$, $v(G) = |V(G)|$.*

Denomina-se $cr(G) = \min\{$ cruzamentos necessários para desenhar G no plano $\}$.

Se G pode ser desenhado no plano sem cruzamentos então $e(G) \leq 3v(G) - 6$. Segue que, dado $G = G^n$, $cr(G) \geq e(G) - (3n-6)$.

Obs: Se $e(G) = \alpha n, \alpha > 3$ então $cr(G) \geq e(G) - 3n = (\alpha - 3)n$. Por exemplo, se $\alpha = \ln n$, então $cr(G) \geq (\ln n - 3)n \sim n \ln n$.

Teorema 45 (Ajtai, Chvátal, Newborn & Szemerédi '82, Leighton '84)**.** *Seja $G = G^n, e(G) \geq 4n$, então $cr(G) \geq \frac{e(G)^3}{64n^2}$.*

Observe que se $e(G) = n(\ln n)$, pelo teorema acima temos $cr(G) \geq \frac{n(\ln^3 n)}{64} = \Omega(n(\ln^3 n))$

Demonstração. Seja $H = G[V_p]$, subgrafo aleatório induzido dos vértices de G, onde $0 < p \leq 1$ é um parâmetro a ser determinado depois. Seja $t = cr(G)$.

Temos $cr(H) \geq e(H) - 3v(H)$, assim, $\mathbb{E}(cr(H)) \geq \mathbb{E}(e(H)) - 3\mathbb{E}(v(H)) = e(G)p^2 - 3np$, mas $\mathbb{E}(cr(H)) \leq tp^4$, pois dado um desenho de G com t cruzamentos, para o mesmo cruzamento estar em H cada um dos 4 vértices devem estar em H.

Desses dois limitantes de $\mathbb{E}(cr(H))$, deduzimos que $t \geq e(G)p^{-2} - 3np^{-3}$. Tomando $p = \frac{4n}{e(G)}$, ficamos com $t \geq (\frac{e(G)}{4n})^2 - 3n(\frac{e(G)}{4n})^2 = \frac{e(G)^3}{64n^2}$. □

Corolário 46. $\forall G = G^n, cr(G) \geq \frac{e(G)^3}{64n^2} - n$

Demonstração. Se $e(G) \geq 4n$, vale, claramente.

Se $e(G) < 4n$, então $\frac{e(G)^3}{64n^2} < n$, que vale por vacuidade. □

1.5.6. *Demonstração do Szemerédi e Trotter.*

Demonstração. Seja $P = P^m, \mathcal{L} = \mathcal{L}^n$. Monte um grafo G tal que: $V(G) = P$ e $E(G) = \{\{x, y\}\ in \binom{V(G)}{2}\}$ tal que x e y são pontos consecutivos de uma reta L, para toda $L \in \mathcal{L}$. Por exemplo, se uma reta L contém k_L pontos, então L definirá $k_L - 1$ arestas em G.

Note que $\binom{n}{2} \geq cr(G) \geq \frac{e(G)^3}{64m^2} - m$ pelo teorema 45 e seu corolário. Assim, como o número de incidência $t = I(P, \mathcal{L}) = e(G) + n$, pois incidência na reta $L = k_L$, deduzimos: $n^2 \geq \binom{n}{2} \geq \frac{(t-n)^3}{64m^2} - m \implies (t - n) \leq (64n^2m^2 + 64m^3)^{\frac{1}{3}}$, assim:

$$t \leq 4(nm)^{\frac{2}{3}} + 4m + n$$

□

1.6. **Aula 21 de março de 2018.** [6]

1.6.1. *O corolário de Szemerédi e Trotter.* Seja $P = P^m \subseteq \mathbb{R}^2$, $k \geq 2$. Defina $\mathcal{L} = \mathcal{L}_{\geq k} = \{L : L$ reta em $\mathbb{R}^2$ com $|L \cap P| \geq k\}$. Seja $n = |\mathcal{L}|$. As incidências entre pontos e retas podem ser representadas pelo grafo bipartido onde uma das bipartições contém as retas de $\mathcal{L}$ e a outra, os pares não ordenados dos pontos de P ($\binom{m}{2}$ no total). Existe uma aresta de $\{x, y\}$ para um $L \in \mathcal{L}$ se e somente se $\{x, y\}$ está contido em L. Com essa construção, vemos que $n\binom{k}{2} \leq \sum_L \binom{|L \cap P|}{2} \leq \binom{m}{2}$. Logo,

$$n \leq \frac{\binom{m}{2}}{\binom{k}{2}} = \frac{m(m-1)}{k(k-1)} \leq \frac{2m^2}{k^2}$$

[6] Notas produzidas por Ângelo Lovatto e Thiago Estrela

Corolário 47 (Szemerédi e Trotter)**.** *Para todo $P = P^m \subseteq \mathbb{R}^2$, o número n de retas em $\mathbb{R}^2$ que contém pelo menos k pontos de P é limitado por*

$$n = O\left(\frac{m^2}{k^3} + \frac{m}{k}\right)$$

Demonstração. (Corolário 47)

Consideramos as incidências entre P e $\mathcal{L}$, limitadas pelo Teorema de Szemerédi e Trotter, logo

$$kn \leq I(P, \mathcal{L}) \leq 4(mn)^{2/3} + 4m + n$$

Assim,

$$n(k-1) \leq 4(mn)^{2/3} + 4m$$

Caso 1: $m \leq (mn)^{2/3}$

Neste caso, $n(k-1) \leq 8(mn)^{2/3}$.

$$\begin{aligned} n &\leq \frac{8(mn)^{2/3}}{k-1} \\ &\leq \frac{16(mn)^{2/3}}{k} \\ n^{1/3} &\leq \frac{2^4 m^{2/3}}{k} \\ n &\leq \frac{2^{12} m^2}{k^3} \end{aligned}$$

Caso 2: $m > (mn)^{1/3}$

Temos

$$\begin{aligned} n(k-1) &\leq 8m \\ n &\leq \frac{8m}{k-1} \\ &\leq \frac{16m}{k} \end{aligned}$$

□

Teorema 48 (Beck '83)**.** *Existe constante absoluta $c > 0$ para a qual o seguinte vale: $\forall P = P^n \in \mathbb{R}^2$*

ou (i) $\exists$ reta L tal que $|L \cap P| \geq cn$

ou (ii) P determina $\geq cn^2$ retas distintas

Demonstração. (Teorema 48)

Fixe $P = P^n$. Seja $\mathcal{L}$ o conjunto de retas determinadas por P (i.e. $\mathcal{L} = \mathcal{L}_{\geq 2}$). Dizemos que $L \in \mathcal{L}$ é uma $\underline{t\text{-reta}}$ ($t \geq 1$) se

$$2^t \leq |L \cap P| < 2^{t+1}$$

418 Se $\{x, y\} \subseteq P$, $x \neq y$, então x e y são t-conexos se a reta determinada por x e y é uma t-reta. Pelo Corolário 47, o número de t-retas é

$$O\left(\frac{n^2}{2^{3t}} + \frac{n}{2^t}\right)$$

419 Uma t-reta contém $< \binom{2^{t+1}}{2} = O\left(2^{2t}\right)$ pares de pontos de P. Logo,

$$\begin{aligned} \#\text{ pares } \{x, y\}\ t\text{-conexos} &= O\left(\left(\frac{n^2}{2^{3t}} + \frac{n}{2^t}\right) 2^{2t}\right) \\ &= O\left(\frac{n^2}{2^t} + 2^t n\right) \end{aligned}$$

Seja C uma constante grande e $T = \{t : C \leq 2^t \leq n/C\} = \{t_0, t_0 + 1, \ldots, t_1\}$. Temos

$$2^{t_0 - 1} < C \therefore 2^{t_0} = O(C)$$

$$2^{t_1 + 1} > n/C \therefore 2^{t_1} = \Omega(n/C)$$

Vamos dizer que o par $\{x, y\} \subseteq P$, $x \neq y$, é T-conexo se $\{x, y\}$ é t-conexo para algum $t \in T$. Temos

$$\#\text{ pares } \ T\text{-conexos} = O\left(\sum_{t \in T}\left(\frac{n^2}{2^t} + 2^t n\right)\right)$$

420

$$\begin{aligned} \sum_{t \in T}\left(\frac{n^2}{2^t} + 2^t n\right) &\leq 2\frac{n^2}{2^{t_0}} + 2(2^{t_1} n) \\ &\leq \left(\frac{2}{C}\right) n^2 + 2\frac{n}{C} n \\ &= \frac{4}{C} n^2 \end{aligned}$$

Escolhendo C grande o suficiente, deduzimos que há $\geq \frac{n^2}{4}$ pares que não são T-conexos. Suponha que $\{x, y\} \subseteq P$, $x \neq y$, determina L que não é T-reta e

$$|L \cap P| > 2^{t_1} = \Omega\left(\frac{n}{C}\right)$$

Mas tal reta satisfaz (i) acima e o resultado segue.

Suponha portanto que as retas L determinadas pelos pares $\{x, y\}$ que não são T-conexos são

todas tais que

$$|L \cap P| < 2^{t_0} = O(C)$$

Concluímos que esses $\geq n^2/4$ pares determinam

$$\geq \frac{n^2/4}{\binom{C}{2}} \geq \frac{n^2}{2C^2}$$

421 retas distintas. Isso satisfaz (ii) acima e o resultado segue.

422 □

1.6.2. *Quicksort(Continuação).* Sejam $x_1 < \cdots < x_n$ números reais e $\pi \in_\cup S_n$. A entrada do algoritmo será

$$x_{\pi(1)}, \ldots, x_{\pi(n)}$$

O quicksort que consideraremos recebe uma sequência e define o primeiro elemento como o pivô, separando os outros em dois grupos: $\sigma = \{x_{\pi(i)} : x_{\pi(i)} < x_{\pi(1)}\}$ e $\tau = \{x_{\pi(i)} : x_{\pi(i)} > x_{\pi(1)}\}$, dentro dos quais a ordem relativa entre os elementos é mantida. Ou seja, a sequência passa a ser

$$\sigma, x_{\pi(1)}, \tau$$

Faremos a análise de caso médio desse algoritmo. Pomos

$$T(\pi) = \#\text{ comparações com a entrada } \pi$$

Podemos caracterizar as distribuições de σ e τ da seguinte maneira: escolha $m \in_\cup \{0, 1, \ldots, n-1\}$, escolha $\sigma \in_\cup S_m$ e $\tau \in_\cup S_{n-1-m}$. Fato: σ e τ são independentes. Temos

$$T(\pi) = T(\sigma) + T(\tau) + n - 1$$

$$\therefore \mathbb{E}(T(\pi)) = \mathbb{E}(T(\sigma)) + \mathbb{E}(T(\tau)) + n - 1$$

423 Mostraremos então que $\mathbb{E}(T(\pi)) = \Theta(n \ln n)$.

424 *Demonstração.* Denote $\mathbb{E}(T(\pi))$ por μ_n ($n = |\pi|$). Reescrevemos a igualdade como

$$\begin{aligned} \mu_n &= \frac{1}{n} \sum_{m=0}^{n-1} (\mu_m + \mu_{n-m-1}) + n - 1 \\ &= \frac{2}{n} \sum_{0 \leq m < n} \mu_m + n - 1 \qquad \forall n \geq 1 \end{aligned}$$

425 e definimos $\mu_0 = 0$.

Temos então a seguinte fórmula para $n \geq 1$:

$$n\mu_n = 2 \sum_{0 \leq m < n} \mu_m + n(n-1)$$

Quando $n \geq 2$, temos que:

$$(n-1)\mu_{n-1} = 2 \sum_{0 \leq m < n-1} \mu_m + (n-1)(n-2)$$

$$n\mu_n - (n-1)\mu_{n-1} = 2\mu_{n-1} + 2(n-1)$$

$$\therefore n\mu_n = (n+1)\mu_{n-1} + 2(n-1)$$

426 Dividindo os dois lados por $n(n+1)$,

$$\begin{aligned} \frac{\mu_n}{n+1} &= \frac{\mu_{n-1}}{n} + \frac{2(n-1)}{n(n+1)} \\ &= \frac{\mu_{n-1}}{n} + 2\left(\frac{2}{n+1} - \frac{1}{n}\right) \end{aligned}$$

427 Denote $\mu_i/(i+1)$ por a_i ($a_1 = \mu_1/2 = 0$). Reescrevemos a igualdade como

$$\begin{aligned} a_n &= a_{n-1} + \frac{4}{n+1} - \frac{2}{n} \\ &= \left(\frac{4}{n+1} - \frac{2}{n}\right) + \left(\frac{4}{n} - \frac{2}{n-1}\right) + \cdots + \left(\frac{4}{3} - \frac{2}{2}\right) + a_1 \\ &= 4\left(H_{n+1} - \frac{1}{2} - 1\right) - 2\left(H_n - 1\right) \\ &= \frac{2}{n+1} + 2H_{n+1} - 4 \end{aligned}$$

428

$$\begin{aligned} \therefore \mu_n = (n+1)a_n &= 2(n+1)H_{n+1} + 2 - 4(n+1) \\ &= 2(n+1)(H_{n+1} - 1) - 2n \\ &= \Theta(n \ln n) \end{aligned}$$

429 □

430 §2. O método do segundo momento

431 2.1. **Aula 05 de maio de 2018.** [7]

[7] Notas produzidas por Gabriel Lasso e Rafael Zuolo

2.1.1. *Segundo momento.* Se X é uma variável aleatória e $\mu = \mathbb{E}(X)$, definimos

$$Var(X) = \mathbb{E}((X-\mu)^2)$$

$$\sigma = \sqrt{Var(X)}$$

Fato 49. $Var(X) = \mathbb{E}(X^2) - \mu^2$

Demonstração.

$$Var(X) = \mathbb{E}((X-\mu)^2)$$

$$= \mathbb{E}(X^2 - 2\mu X + \mu^2)$$

$$= \mathbb{E}(X^2) - 2\mu^2 + \mu^2$$

$$= \mathbb{E}(X^2) - \mu^2$$

□

Lema 50. *(Desigualdade de Markov) Se X é uma v.a. não negativa, então para todo $A \geq 1$, vale*

$$\mathbb{P}(X \geq A\mu) \leq \frac{1}{A}$$

Demonstração. Para todo $t \geq 0$, temos:

$$t\mathbb{P}(X \geq t) \leq \mathbb{E}(X)$$

$$\mathbb{P}(X \geq t) \leq \frac{\mathbb{E}(X)}{t}$$

Fazendo $t = A\mu$ temos o resultado □

Lema 51. *(Desigualdade de Chebychev) Se X é uma v.a., então para todo $A \geq 1$, vale*

$$\mathbb{P}(|X-\mu| \geq A\sigma) \leq \frac{1}{A^2}$$

Demonstração. Considere $Y = (X-\mu)^2 \geq 0$.

$$\mathbb{P}(|X-\mu| \geq t) = \mathbb{P}((X-\mu)^2 \geq t^2) = \mathbb{P}(Y \geq t^2)$$

Por Markov:

$$\mathbb{P}(Y \geq t^2) \leq \frac{\mathbb{E}(Y)}{t^2} = \frac{Var(x)}{t^2}$$

Fazendo $t = A\sigma$ chegamos ao resultado. □

2.1.2. *Um caso importante.* Se temos uma v.a. que é soma de outras v.a.:

$$X = \sum_{i=0}^{n} X_i$$

$$\mu = \mathbb{E}(X) = \sum_{i=0}^{n} \mathbb{E}(X_i)$$

Temos

$$Var(X) = \mathbb{E}(X^2) - \mathbb{E}(X^2)$$

$$Var(X) = \sum_{i,j} (\mathbb{E}(X_i X_j) - \mathbb{E}(X_i)\mathbb{E}(X_j))$$

Definição 52. *Chamamos* $\mathbb{E}(X_i X_j) - \mathbb{E}(X_i)\mathbb{E}(X_j)$ *de covariância de* X_i *e* X_j *e denotamos por* $cov(X_i, X_j)$.

$$Var(X) = \sum_{i=1}^{n} Var(X_i) + \sum_{i \neq j} cov(X_i, X_j)$$

Definição 53. X_i *e* X_j *são independentes se* $cov(X_i, X_j) = 0$.

Se os X_is são 2 a 2 independentes, então $Var(X) = \sum Var(X_i)$

Muitas vezes os X_i são variáveis indicadoras com $X_i \equiv Ber(p_i)$.

Nesse caso,

$$Var(X_i) = \mathbb{E}(X_i)^2 - \mathbb{E}(X_i)^2$$

$$= \mathbb{E}(X_i) - \mathbb{E}(X_i)^2$$

$$= p_i - p_i^2 \leq p_i = \mathbb{E}(X_i)$$

Assim,

$$Var(X) \leq E(X) + \sum_{i \neq j} cov(X_i, X_j)$$

2.1.3. *Um teorema de Hardy e Ramanujan.*

Definição 54. *Se* $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$ *com* p_i *primo e* a_i *inteiro positivo, então:*

- $\omega(n) = r = \#$*divisores primos distintos de* n.
- $\Omega(n) = a_1 + a_2 + ... + a_r = \#$*divisores primos de* n*, contando sua multiplicidade.*
- $d(n) = (1 + a_1)(1 + a_2)...(1 + a_r) = \#$*divisores de* n.
- $\pi(n) = \#$*primos menores ou iguais a* n.

Estamos interessados no espaço $[N]$ com a distribuição uniforme. A função $\omega : [N] \to \mathbb{R}$ é uma variável aleatória para um n escolhido uniformemente ao acaso em $[N]$.

Temos:

$$\omega(n) = \sum_{p \leq N \ p \text{ primo}} X_p(n)$$

onde

$$X_p(n) = \begin{cases} 1 \text{ se } p|n \\ \\ 0 \text{ caso contrário} \end{cases}$$

Fato 55. $\mathbb{E}(\omega) = \ell og \ell og N + O(1)$

Demonstração.

$$\mathbb{E}(\omega) = \sum_{p \leq N \ p \text{ primo}} \mathbb{E}(X_p)$$

$$\mathbb{E}(\omega) = \sum_{p \leq N \ p \text{ primo}} \mathbb{P}(p|n)$$

$$\mathbb{E}(\omega) = \sum_{p \leq N \ p \text{ primo}} \frac{\#\text{múltiplos de } p \text{ menores ou iguais a } N}{N}$$

$$\mathbb{E}(\omega) = \sum_{p \leq N \ p \text{ primo}} \frac{\lfloor \frac{N}{p} \rfloor}{N}$$

$$\mathbb{E}(\omega) = \sum_{p \leq N \ p \text{ primo}} \frac{\frac{N}{p} - (\frac{N}{p} - \lfloor \frac{N}{p} \rfloor)}{N}$$

$$\mathbb{E}(\omega) = \sum_{p \leq N \ p \text{ primo}} \frac{1}{p} + o(\frac{1}{N})$$

$$\mathbb{E}(\omega) = \ell og \ell og N + o(1)$$

$$\text{(Usando o fato que } \sum_{p \leq N \ p \text{ primo}} \frac{1}{p} = \ell og \ell og N + o(1))$$

□

Teorema 56. *(Hardy, Ramanujan)*

$\forall A > 0 \exists N_0$ *tal que* $\forall N > N_0$

$$\mathbb{P}(|\omega(n) - \ell og \ell og N| \geq A\sqrt{\ell og \ell og N}) \leq \frac{2}{A^2}$$

Ademais, de $b = b(N) \to \infty$,

$$\lim_{N \to \infty} \mathbb{P}(|\omega(n) - \ell og \ell og N| \geq B\sqrt{\ell og \ell og N}) = 0$$

Demonstração. Vamos calcular a variância de ω:

$$Var(\omega) \leq \mathbb{E}(\omega) + \sum_{p \neq q \text{ primos}} cov(X_p, X_q)$$

Fixe $p \neq q$. Temos:

$$cov(X_p, X_q) = \mathbb{E}(X_p X_q) - \mathbb{E}(X_p)\mathbb{E}(X_q)$$

$$= \mathbb{P}(X_p X_q) - \mathbb{P}(X_p)\mathbb{P}(X_q)$$

$$= \frac{\lfloor \frac{N}{pq} \rfloor}{N} - \frac{\lfloor \frac{N}{p} \rfloor}{N} \frac{\lfloor \frac{N}{q} \rfloor}{N}$$

$$\leq \frac{\lfloor \frac{N}{pq} \rfloor}{N} - \left(\frac{1}{p} - \frac{1}{N}\right)\left(\frac{1}{q} - \frac{1}{N}\right)$$

$$\leq \frac{1}{pq} - \left(\frac{1}{pq} - \frac{1}{pN} - \frac{1}{qN} + \frac{1}{N^2}\right)$$

$$\leq \frac{1}{N}\left(\frac{1}{p} + \frac{1}{N}\right)$$

Assim, temos que

$$\sum_{p \neq q \text{ primos}} cov(X_p, X_q) \leq \sum_{p \leq N \text{ primo}} \sum_{q \leq N, q \neq p \text{ primo}} \frac{1}{N}\left(\frac{1}{p} + \frac{1}{q}\right)$$

$$\leq \frac{1}{N} \sum_{p \leq N \text{ primo}} \left(\frac{1}{p} \sum_{q \leq N \text{ primo}} 1 + \sum_{q \leq N \text{ primo}} \frac{1}{q}\right)$$

$$= \frac{1}{N}\left(\sum_{p \leq N \text{ primo}} \frac{1}{p} \sum_{q \leq N \text{ primo}} 1 + \sum_{q \leq N \text{ primo}} \frac{1}{q} \sum_{p \leq N \text{ primo}} 1\right)$$

$$= \frac{2\pi(N)}{N}\left(\sum_{p \leq N \text{ primo}} \frac{1}{p}\right)$$

$$= \frac{2(1 + o(1))\frac{N}{\ell ogN}}{N}(\ell og\ell ogN + O(1))$$

$$= O(\frac{\ell og\ell ogN}{\ell ogN}) = o(1)$$

Assim, $Var(\omega) = \ell og\ell ogN + o(1)$ e $\sigma = \sqrt{(\ell og\ell ogN)} + o(1)$.

Agora basta aplicar Chebyshev e chegamos no resultado desejado. □

Erdös e Kac provaram também que

$$\lim_{N \to \infty} \mathbb{P}(\omega(n) \geq \ell og\ell ogN + t\sqrt{\ell og\ell ogN}) = \frac{1}{\sqrt{2\pi}} \int_t^\infty e^{-x^2/2} dx \forall t \in \mathbb{R}$$

Isto é, ω tende a ter uma ditribuição normal.

Fato 57. $\mathbb{E}(|\omega(n) - \Omega(n)|) = O(1)$

Disso segue que o teorema de H.R. também vale com ω substituído por Ω.

2.2. **Aula 04 de abril de 2018: Subgrafos pequenos em $G(n,p)$.** [8]

Formalmente, definimos $G(n,p)$ como sendo o espaço de probabilidade $(\mathcal{G}, \mathbb{P})$, em que $\mathcal{G}$ é o conjunto de todos os grafos sobre $[n]$, e se $G \in \mathcal{G}$ então $\mathbb{P}(G)$ é definido como

$$\mathbb{P}(G) = p^{e(G)}(1-p)^{\binom{n}{2}-e(G)}.$$

Informalmente, os grafos de $G(n,p)$ são gerados tomando $[n]$ como o conjunto de vértices e o conjunto das arestas é um subconjunto aleatório de $\binom{[n]}{2}$, em que cada aresta é incluida no conjunto com probabilidade p, de maneira independente.

Observe que, embora $G(n,p)$ seja um espaço de probabilidade, nos referiremos a $G(n,p)$ como sendo o grafo aleatório em si; isto é, escreveremos "seja $G = G(n,p)$" para significar que G é um grafo de $\mathcal{G}$ escolhido aleatoriamente de acordo com a distribuição $\mathbb{P}$. Embora tecnicamente isto seja um abuso de notação, cometeremos ente abuso sistematicamente doravante.

O grafo aleatório $G(n,p)$ é também chamado de *grafo aleatório de Erdős–Rényi* ou de *grafo aleatório binomial*.

Mais geralmente, dado um grafo $\Gamma = (V, E)$, podemos definir o *subgrafo aleatório binomial* Γ_p de Γ como sendo um grafo aleatório em que V é o conjunto de vértices e E_p é o conjunto de arestas; isto é, cada aresta de E aparece no grafo com probabilidade p. Teremos, então, que $G(n,p) = (K^n)_p$.

Sejam H e G dois grafos. Definiremos $\#\{H \hookrightarrow G\}$ como sendo o número de funções injetivas $f : V(H) \to V(G)$ que preservam arestas; isto é, se $\{u,v\}$ é uma aresta de H, então $\{f(u), f(v)\}$ é uma aresta de G. (Tais injeções são também chamadas de *homomorfismos* de H em G.) Em outras palavras, estamos contando as cópias rotuladas de H em G, não necessariamente induzidas.

Estamos interessados na v.a. $X_H(G(n,p)) = \#\{H \hookrightarrow G(n,p)\}$.

Temos

$$X_H = \sum_f X_f,$$

onde X_f é a função indicadora do evento

$$\{f : V(H) \to V(G(n,p)) \mid f \text{ é homomorfismo}\}$$

e a soma é sobre todas as injeções $f : V(H) \hookrightarrow V(G(n,p))$. X_f será 1 se $\{f(u), f(v)\}$ for uma aresta de $G(n,p)$ para cada uma das $e(H)$ arestas $\{u,v\}$ de H; assim, $\mathbb{E}(X_f) = p^{e(H)}$. Existem

[8] Notas produzidas por Felix Liu e Tiago Royer.

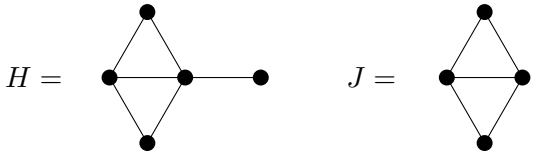

FIGURA 5. Grafos H e J dos exemplos 58 e 59.

$n(n-1)(n-2)\dots(n-v(H)+1) = (n)_{v(H)}$ possíveis homomorfismos de H em $G(n,p)$, e, portanto,

$$\mathbb{E}(X_H) = (n)_{v(H)}p^{e(H)}.$$

Exemplo 58. Considere o grafo H da figura 5. Suponha que $p \ll n^{-5/6}$. Neste caso,

$$\mathbb{E}(X_H) = (n)_5 p^6 \sim n^5 p^6 \ll 1;$$

portanto, pela desigualdade de Markov, a probabilidade de um grafo $G(n,p)$ conter H é assintóticamente zero. Neste caso, dizemos que quase todo $G(n,p)$ não contém H como subgrafo.

Exemplo 59. Suponha agora que $n^{-5/6} \ll p \ll n^{-4/5}$. Observe que neste caso, $\mathbb{E}(X_H) \gg 1$; e $\mathbb{E}(X_H)$ tende a infinito conforme n cresce.

Se considerarmos agora o grafo J da figura 5, pelo mesmo raciocínio temos $\mathbb{E}(X_J) \ll 1$, e então quase todo $G(n,p)$ não contém J como subgrafo. Como J é, por sua vez, um subgrafo de H, isso nos permite concluir que quase todo $G(n,p)$ também não contém H, muito embora o número esperado de cópias de H em $G(n,p)$ tenda a infinito.

Podemos generalizar o exemplo acima da seguinte maneira: defina $m(H)$ por

$$m(H) = \max\left\{\frac{e(J)}{v(J)} : J \subseteq H, v(J) > 0\right\}.$$

Temos então a seguinte afirmação.

Proposição 60. *Seja H um grafo com pelo menos uma aresta. Se $p \ll n^{-1/m(H)}$, então*

$$\lim_{n\to\infty} \mathbb{P}(G(n,p) \supset H) = 0.$$

Demonstração. Seja J um subgrafo de G que maximiza $\frac{e(J)}{v(J)}$. Repetindo o argumento acima, temos

$$\begin{aligned}\mathbb{P}(G(n,p) \supset H) &\leq \mathbb{P}(G(n,p) \supset J)\\ &= \mathbb{P}(X_J \geq 1)\end{aligned}$$

$$\leq \mathbb{E}(X_J)$$
$$\sim n^{v(J)}p^{e(J)}$$
$$\ll n^{v(J)}n^{-e(J)/m(H)} = 1. \qquad \square$$

Queremos obter resultados na outra direção, isto é, que garantam que o grafo H apareça em quase todo grafo $G(n,p)$. Conforme o exemplo 59 mostra, simplesmente calcular a esperança não é suficiente para extrair esse tipo de informação; portanto, iremos calcular a variância de X_H também.

Defina $\Phi_H = \Phi_H(n,p)$ por

$$\Phi_H(n,p) = \min\{\mathbb{E}(X_J) \mid J \subseteq H, e(J) > 0\}.$$

Proposição 61. *Suponha que $e(H) > 0$. São equivalentes:*

- $np^{m(H)} \to \infty$.
- $n^{v(J)}p^{e(J)} \to \infty$ *para todo grafo* $J \subseteq H$ *com pelo menos um vértice.*
- $\mathbb{E}(X_J) \to \infty$ *para todo grafo* $J \subseteq H$ *com pelo menos um vértice.*
- $\Phi_H \to \infty$.

Como $X_H = \sum_f X_f$, temos

$$\mathrm{Var}(X_H) \leq \mathbb{E}(X_H) + \sum_{f \neq g} \mathrm{Cov}(X_f, X_g).$$

Defina $\Delta_H = \sum_{f \neq g} \mathbb{E}(X_f X_g)$; observe que Δ_H é maior ou igual à soma das covariâncias na expressão para $\mathrm{Var}(X_H)$. Temos o seguinte limitante para Δ_H.

Lema 62. *Sejam Δ_H e Φ_H como definidos acima. Então*

$$\Delta_H \leq \frac{\mathbb{E}(X_H)^2}{\Phi_H} 2^{2v(H)} v(H)!\, v(H).$$

Demonstração. Seja V o conjunto de vértices de $G(n,p)$ e sejam U e F, respectivamente, o conjunto de vértices e arestas de H. Se $f : U \hookrightarrow V$ é uma injeção, denotaremos por H_f a cópia rotulada de H em K^n correspondente a f. Temos, por exemplo, que $H_f \subseteq G(n,p)$ se e só se $X_f = 1$.

Para que tenhamos $X_f X_g = 1$, precisamos ter tanto $H_f \subseteq G(n,p)$ quanto $H_g \subseteq G(n,p)$; ou seja, todas as arestas de $E(H_f) \cup E(H_g)$ precisam aparecer no grafo. Portanto,

$$\begin{aligned}\Delta_H &= \sum_{f \neq g} p^{|E(H_f) \cup E(H_g)|} \\ &= \sum_{f \neq g} p^{2e(H) - |E(H_f) \cap E(H_g)|} \\ &= p^{2e(H)} \sum_{f \neq g} p^{-|E(H_f) \cap E(H_g)|}.\end{aligned}$$

Defina $J_{f,g} = f^{-1}(H_f \cap H_g)$. Temos, por exemplo, $e(J_{f,g}) = |E(H_f) \cap E(H_g)|$. Assim,

$$\Delta_H = p^{2e(H)} \sum_{f \neq g} p^{-e(J_{f,g})}.$$

O subgrafo $J_{f,g}$ de H pode assumir o mesmo valor para diferentes valores de f e g. No somatório que define Δ_H, agruparemos os pares de funções (f,g) que resultam no mesmo grafo $J_{f,g}$. Defina

$$W_J = \{(f,g) \mid J_{f,g} = J\};$$

temos

$$\begin{aligned}\Delta_H &= p^{2e(H)} \sum_{J \subseteq H} \sum_{(f,g) \in W_J} p^{-e(J)} \\ &= p^{2e(H)} \sum_{J \subseteq H} p^{-e(J)} |W_J|.\end{aligned}$$

Agrupando os subgrafos J pelo número de vértices e introduzindo o fator $(n)_k (n)_k^{-1}$ temos

$$\begin{aligned}\Delta_H &= p^{2e(H)} \sum_{k=1}^{v(H)} \sum_{\substack{J \subseteq H \\ v(J)=k}} p^{-e(J)} |W_J| \\ &= p^{2e(H)} \sum_{k=1}^{v(H)} \sum_{\substack{J \subseteq H \\ v(J)=k}} p^{-e(J)} (n)_k^{-1} (n)_k |W_J| \\ &= p^{2e(H)} \sum_{k=1}^{v(H)} \sum_{\substack{J \subseteq H \\ v(J)=k}} \mathbb{E}(X_J)^{-1} |W_J| (n)_k \\ &\leq \frac{p^{2e(H)}}{\Phi_H} \sum_{k=1}^{v(H)} \sum_{\substack{J \subseteq H \\ v(J)=k}} |W_J| (n)_k.\end{aligned}$$

Podemos limitar o valor de $|W_J|$ da seguinte maneira. Suponha que $v(J) = k$. Existem $(n)_{v(H)}$ possíveis escolhas para f. Sabemos que $g(V(H))$ precisa intersectar $f(V(H))$ em exatamente k vértices. Existem $\binom{v(H)}{k}$ formas de escolher os k vértices de $V(H)$ que g mapeará para $f(V(H))$. Há $(v(H))_k$ formas de associar esses k vértices aos de $f(V(H))$; e $(n - v(H))_{v(H)-k}$ formas de associar os demais vértices para fora de $f(V(H))$. Dessa maneira, cobrimos todos os possíveis pares (f, g) tais que $J_{f,g} = J$, mas, potencialmente, também incluimos pares tais que $J_{f,g} \neq J$. Isso nos dá apenas um limitante superior para $|W_J|$:

$$|W_J| \leq (n)_{v(H)} \binom{v(H)}{k} (v(H))_k (n - v(H))_{v(H)-k}.$$

Usando este limitante, temos

$$\begin{aligned}
\Delta_H &\leq \frac{p^{2e(H)}}{\Phi_H} \sum_{k=1}^{v(H)} \sum_{\substack{J \subseteq H \\ v(J)=k}} (n)_{v(H)} \binom{v(H)}{k} (v(H))_k (n - v(H))_{v(H)-k} (n)_k \\
&\leq \frac{p^{2e(H)}}{\Phi_H} \sum_{k=1}^{v(H)} \sum_{\substack{J \subseteq H \\ v(J)=k}} (n)_{v(H)} 2^{v(H)} (v(H))_k (n - v(H))_{v(H)-k} (n)_k \\
&\leq \frac{p^{2e(H)}}{\Phi_H} \sum_{k=1}^{v(H)} \sum_{\substack{J \subseteq H \\ v(J)=k}} (n)_{v(H)} 2^{v(H)} v(H)! \, (n - v(H))_{v(H)-k} (n)_k \\
&\leq \frac{p^{2e(H)}}{\Phi_H} \sum_{k=1}^{v(H)} \sum_{\substack{J \subseteq H \\ v(J)=k}} (n)_{v(H)} 2^{v(H)} v(H)! \, (n)_{v(H)} \\
&\leq \frac{p^{2e(H)}}{\Phi_H} \sum_{k=1}^{v(H)} (n)_{v(H)} 2^{2v(H)} v(H)! \, (n)_{v(H)} \\
&= \frac{(p^{e(H)} (n)_{v(H)})^2}{\Phi_H} 2^{2v(H)} v(H)! \, v(H) \\
&= \frac{\mathbb{E}(X_H)^2}{\Phi_H} 2^{2v(H)} v(H)! \, v(H).
\end{aligned}$$

□

Proposição 63. *Seja H um grafo com pelo menos uma aresta. Se $p \gg n^{-1/m(H)}$, então* $\lim_{n\to\infty} \mathbb{P}(G(n,p) \supset H) = 1$.

Demonstração. Sabemos que

$$\lim_{n\to\infty} \mathbb{E}(X_H) = \infty.$$

Então, para todo n grande o bastante,

$$\mathbb{P}(X_H = 0) \leq \mathbb{P}(|X_H - \mathbb{E}(X_H)| \geq \mathbb{E}(X_H)).$$

Usando Chebyshev (e os lemas anteriores), temos

$$\begin{aligned}\mathbb{P}(X_H = 0) &\leq \frac{\mathrm{Var}(X_H)}{\mathbb{E}(X_H)^2} \\ &\leq \frac{\mathbb{E}(X_H) + \Delta_H}{\mathbb{E}(X_H)^2} \\ &\leq \frac{1}{\mathbb{E}(X_H)} + O\left(\frac{1}{\Phi_H(n,p)}\right).\end{aligned}$$

Como $\lim_{n\to\infty} \Phi_H(n,p) = \infty$, o resultado segue. □

As proposições 60 e 63 podem ser resumidas da seguinte maneira:

$$\lim_{n\to\infty} \mathbb{P}(G(n,p) \supset H) = \begin{cases} 0, & \text{se } p \ll n^{-1/m(H)}; \\ 1, & \text{se } p \gg n^{-1/m(H)}. \end{cases}$$

Dizemos, neste caso, que $n^{-1/m(H)}$ é a *função limiar* para $H \subseteq G(n,p)$.

2.3. **Aula 09 de Abril de 2018: O Teorema de Rödl.** [9]

Sejam $n > k \geq \ell \geq 1$ naturais e considere um conjunto $\mathcal{A} \subseteq \binom{[n]}{k}$. Dizemos que o conjunto $\mathcal{A}$ é uma (n,k,ℓ)-*cobertura* de $[n]$ se para todo $B \in \binom{[n]}{\ell}$ existe $A \in \mathcal{A}$ tal que $B \subseteq A$. Em particular, uma $(n,k,1)$-cobertura é uma coleção de k-uplas em que todo elemento de $[n]$ está contido em pelo menos uma k-upla.

De modo similar, dizemos que $\mathcal{A}$ é um (n,k,ℓ)-*empacotamento* se para todo $A, B \in \mathcal{A}$ temos que $|A \cap B| < \ell$. Uma definição análoga é a de que para qualquer $B \in \binom{[n]}{\ell}$ existe no máximo um elemento $A \in \mathcal{A}$ tal que $B \subseteq A$. Desta definição temos que um $(n,k,1)$-empacotamento é apenas uma família disjunta de conjuntos de $\mathcal{A}$.

Aqui estaremos interessados no problema extremal relacionado com essas famílias. Defina

$$M(n,k,\ell) = \min\{|\mathcal{A}|\colon \mathcal{A} \text{ é uma } (n,k,\ell)\text{-cobertura}\}$$

como o tamanho da menor (n,k,ℓ)-cobertura de $[n]$. Analogamente, defina

$$m(n,k,\ell) = \max\{|\mathcal{A}|\colon \mathcal{A} \text{ é um } (n,k,\ell)\text{-empacontamento}\}$$

como o tamanho do maior (n,k,ℓ)-empacotamento de $[n]$. Queremos estimar esses dois valores.

Uma maneira simples de obter uma estimativa é usando contagem dupla. Seja $\mathcal{A}$ uma cobertura e S o número de pares (A,B) com $A \in \mathcal{A}$ e $B \in \binom{[n]}{\ell}$ e $B \subseteq A$. Podemos contar S de duas formas. A primeira é fixando um conjunto A e contando o número de $B \subseteq A$. Esse número

[9] Nota de aula por Bruno Pasqualotto Cavalar e Marcelo Tadeu Sales. Aula de 09/04/2018

é exatamente o número de subconjuntos de tamanho ℓ de A, de onde obtemos

$$S = |\mathcal{A}| \cdot \binom{k}{\ell}.$$

A segunda forma é fixando um conjunto B e contando o número de $A \in \mathcal{A}$ tais que $B \subseteq A$. Como $\mathcal{A}$ é uma (n, k, ℓ)-cobertura, temos que para todo B existe pelo menos um $A \in \mathcal{A}$ tal que $B \subseteq A$. Assim obtemos que

$$S \geq \binom{n}{\ell}.$$

Onde concluímos que

$$|\mathcal{A}| \geq \frac{\binom{n}{\ell}}{\binom{k}{\ell}},$$

para toda cobertura A. Consequentemente, temos que

$$M(n, k, \ell) \geq \frac{\binom{n}{\ell}}{\binom{k}{\ell}}.$$

Fazendo exatamente o mesmo para empacotamentos, obtemos que

$$m(n, k, \ell) \leq \frac{\binom{n}{\ell}}{\binom{k}{\ell}}.$$

Em 1963, Erdős e Hanani conjecturaram que essas estimativas estão assintoticamente corretas.

Conjectura 64 (Erdős e Hanani, '63)**.** *Sejam $k \geq \ell \geq 1$ naturais. Então*

$$\lim_{n\to\infty} M(n, k, \ell)\binom{k}{\ell}\binom{n}{\ell}^{-1} = \lim_{n\to\infty} m(n, k, \ell)\binom{k}{\ell}\binom{n}{\ell}^{-1} = 1.$$

Essa conjectura foi provada em 1985 por Rödl, que provou o seguinte teorema.

Teorema 65 (Rödl, '85)**.** *Dados $k \geq \ell \geq 1$ naturais e $\varepsilon > 0$, existe n_0 tal que para todo $n \geq n_0$ temos*

$$(1-\varepsilon)\frac{\binom{n}{\ell}}{\binom{k}{\ell}} \leq m(n, k, \ell) \leq \frac{\binom{n}{\ell}}{\binom{k}{\ell}} \leq M(n, k, \ell) \leq (1+\varepsilon)\frac{\binom{n}{\ell}}{\binom{k}{\ell}}.$$

Nessa e nas próximas aulas veremos uma demonstração desse Teorema baseada na demonstração original. Como veremos, essa demonstração usará do primeiro e do segundo momento de uma maneira bem engenhosa.

Começaremos introduzindo um problema um pouco mais geral que o Teorema 65. Dados n, r, seja $\mathcal{H} \subseteq \binom{[n]}{r}$ um hipergrafo r-uniforme. Um hipergrafo nada mais é do que um par $\mathcal{H} = (V, E)$

onde $E \subseteq \mathcal{P}(V)$. Em nosso contexto $V = [n]$ e E são subconjuntos de $[n]$ de tamanho r. Por essa justificativa, denotamos $\mathcal{H}$ pelo conjunto de arestas. Um hipergrafo r-uniforme também é chamado de r-grafo. É fácil ver que 2-grafos são simplesmente grafos.

Dizemos que um conjunto $\mathcal{C} \subseteq \mathcal{H}$ de arestas é uma *cobertura* se para todo vértice $x \in V(\mathcal{H})$ existe aresta $C \in \mathcal{C}$ tal que $x \in C$. Da mesma forma, dizemos que um conjunto $\mathcal{C}$ é um *empacotamento* de $\mathcal{H}$ se para todo vértice x existe no máximo uma aresta em $\mathcal{C}$ contendo x, isto é, se todas as arestas de $\mathcal{C}$ são disjuntas. Note aqui que neste caso o conceito de empacotamento coincide com o de emparelhamento.

Defina o número de cobertura de um r-grafo $\mathcal{H}$ por

$$\beta(\mathcal{H}) := \min\{|\mathcal{C}|\colon \mathcal{C} \text{ é uma cobertura de } \mathcal{H}\}.$$

Também defina o número de empacotamento de um r-grafo $\mathcal{H}$ por

$$\nu(\mathcal{H}) := \max\{|\mathcal{C}|\colon \mathcal{C} \text{ é um empacotamento de } \mathcal{H}\}.$$

Por uma contagem dupla análoga a feita na situação anterior obtemos que

$$\nu(\mathcal{H}) \leq \frac{n}{r} \leq \beta(\mathcal{H}).$$

Assim seria interessante provar que essas estimativas são fortes, isto é, que vale

$$\beta(\mathcal{H}) = (1 + o(1))\frac{n}{r}$$
$$\nu(\mathcal{H}) = (1 + o(1))\frac{n}{r}.$$

Se isso fosse verdade para todo r-grafo, então Teorema 65 seria um corolário desse resultado. De fato, sejam $N > k \geq \ell \geq 1$ inteiros e suponha que queremos estimar $M(N, k, \ell)$ e $m(N, k, \ell)$. Então construa um hipergrafo $\mathcal{H}_{EH}$ onde os vértices são os subconjuntos de tamanho ℓ de $[N]$ e as arestas são dadas por

$$E(\mathcal{H}_{EH}) = \left\{ \binom{K}{\ell} : K \subseteq [N],\, |K| = k \right\},$$

isto é, um conjunto de vértices é uma aresta se este conjunto consiste de todos os subconjuntos de tamanho ℓ de um conjunto de tamanho k. Isso nos permite traçar uma bijeção entre as arestas de $\mathcal{H}_{EH}$ e os conjuntos de $\binom{[N]}{k}$.

Uma cobertura de $\mathcal{H}_{EH}$ consiste em um conjunto de arestas $\mathcal{C}$ que contém, em sua união, todos os vértices de $\mathcal{H}_{EH}$. Podemos associar cada aresta de $\mathcal{C}$ com um subconjunto de tamanho

k de $[N]$. Essa bijeção nos dá um conjunto $\mathcal{A} \subseteq \binom{[N]}{k}$. Como cada vértice de $\mathcal{H}_{EH}$ está contido em uma aresta, segue que todo subconjunto de tamanho ℓ está contido em um subconjunto de tamanho k em $\mathcal{A}$. Logo $\mathcal{A}$ é uma (N, k, ℓ)-cobertura. Assim

$$M(N, k, \ell) = \beta(\mathcal{H}_{EH}).$$

Da mesma forma, podemos associar um empacotamento $\mathcal{C}$ de $\mathcal{H}_{EH}$ com um (N, k, ℓ)-empacotamento $\mathcal{A}$ de $[N]$ e portanto

$$m(N, k, \ell) = \nu(\mathcal{H}_{EH}).$$

Assim teríamos que $M(N, k, \ell)$ e $m(N, k, \ell)$ são assintóticamente iguais a

$$\frac{n}{r} = \frac{\binom{N}{\ell}}{\binom{k}{\ell}},$$

como queríamos.

Infelizmente, não existem esperanças de que este fato seja verdadeiro. Vários contra-exemplos podem ser dados. Por exemplo, considere $\mathcal{H}$ como o r-grafo em que as arestas são todos os subconjuntos de tamanho r que contém 1. É fácil ver que

$$\beta(\mathcal{H}) \approx \frac{n}{r-1}$$
$$\nu(\mathcal{H}) = 1.$$

É necessário colocar alguma hipótese sobre $\mathcal{H}$. Felizmente, a conjectura de Erdős e Hanani nos dá uma dica sobre o tipo de hipótese necessária: $\mathcal{H}_{EH}$ é regular!

Fixado um vértice $x \in V(\mathcal{H}_{EH})$ queremos calcular $d(x)$. Note que x na verdade é um subconjunto de $[n]$ de tamanho ℓ e uma aresta que contém x corresponde a um subconjunto de tamanho k que contém x. Portanto $d(x)$ é igual ao número de subconjuntos de $[n]$ de tamanho k que contém o subconjunto ℓ. É fácil ver que esse número é igual a $\binom{n-\ell}{k-\ell}$ e logo $\mathcal{H}_{EH}$ é regular.

Vamos então tentar esse cenário. Suponha que $\mathcal{H}$ é um grafo D-regular. Primeiro vamos mostrar que é apenas necessário resolver o problema para coberturas.

Exercicio 66. Seja $\mathcal{H}$ um r-grafo conexo e $\varepsilon > 0$ tal que $\beta(\mathcal{H}) \leq (1+\varepsilon)\frac{n}{r}$, então $\nu(\mathcal{H}) \geq (1-\varepsilon r)\frac{n}{r}$. Da mesma forma, se $\nu(\mathcal{H}) \geq (1-\varepsilon)\frac{n}{r}$, então $\beta(\mathcal{H}) \leq (1+\varepsilon r)\frac{n}{r}$.

Solução. Seja $\mathcal{C}$ uma cobertura de $\mathcal{H}$ de tamanho $\beta(\mathcal{H})$. Para um vértice $i \in [n]$, seja x_i o número de arestas $C \in \mathcal{C}$ tal que $i \in C$. Vamos contar o número de pares (i, C), onde $i \in [n]$,

$C \in \mathcal{C}$ são tais que $i \in C$. Uma contagem dupla fixando os vértices primeiro e depois as arestas nos dá que

$$\sum_{i=1}^{n} x_i = |\mathcal{C}| \cdot r \leq (1+\varepsilon)n$$

Note que por $\mathcal{C}$ ser uma cobertura, temos que $x_i \geq 1$ para todo i. Seja $I \subseteq [n]$ os índices em que $x_i > 1$. Para todo $i \in I$, seja $\{C_{i1}, \ldots, C_{ix_1}\}$ todas as arestas de $\mathcal{C}$ contendo i. Construa uma coleção $\mathcal{C}'$ dada por

$$\mathcal{C}' = \mathcal{C} \setminus \left(\bigcup_{i=1}^{n} \{C_{i2}, \ldots, C_{ix_i}\} \right).$$

Essa nova coleção sastifaz duas condições: A primeira é que todo vértice aparece em no máximo uma aresta de $\mathcal{C}'$, tornando $\mathcal{C}'$ um empacotamento. A segunda é que

$$|\mathcal{C}'| \geq \beta(\mathcal{H}) - \varepsilon n \geq (1 - \varepsilon r)\frac{n}{r}.$$

Portanto $\nu(\mathcal{H}) \geq (1-\varepsilon r)\frac{n}{r}$. A outra afirmação segue de maneira similar. □

Vamos achar agora probabilisticamente uma cobertura para um r-grafo D-regular. Seja $\mathcal{H}_p$ o r-grafo obtido por selecionar cada aressta de $\mathcal{H}$ independentemente com probabilidade p. Esse conjunto de arestas de $\mathcal{H}_p$ cobrem um conjunto de vértices $S \subseteq [n]$. Para cada vértice em $[n] \setminus S$ considere uma aresta em que está contido e chame de $\mathcal{A}$ esse conjunto de arestas. Então $\mathcal{C} = \mathcal{H}_p \cup \mathcal{A}$ é uma cobertura de $\mathcal{H}$. É fácil ver que

$$|\mathcal{C}| \leq |\mathcal{H}_p| + (n - |S|).$$

Assim precisamos apenas estimar o tamanho de $[n] \setminus S$ e de $\mathcal{H}_p$.

Seja X a variável aleatória que conta o número de arestas de $\mathcal{H}_p$ e Y a variável aleatória que conta o número de vértices não cobertos em $\mathcal{H}_p$. Estamos interessados em $\mathbb{E}(X+Y)$. Uma conta simples mostra que

$$\mathbb{E}(X) = pe(\mathcal{H}),$$

e por uma contagem temos que

$$e(\mathcal{H}) = \frac{Dn}{r}.$$

Assim concluímos que

$$\mathbb{E}(X) = \frac{pDn}{r}.$$

Para estimarmos Y note que um vértice não é coberto por $\mathcal{H}_p$ se todas as arestas incidente nele nao foram escolhidas. Logo

$$\mathbb{E}(Y) = \sum_{i=1}^{n} \mathbb{P}(i \text{ não ser coberto}) = \sum_{i=1}^{n} (1-p)^D \leq ne^{-pD}.$$

Linearidade da esperança nos dá

$$\mathbb{E}(X+Y) = \mathbb{E}(X) + \mathbb{E}(Y) \leq \frac{pDn}{r} + ne^{-pD}.$$

Para otimizarmos o valor, queremos escolher p em que essa função seja mínima. Cálculo nos mostra que isso é atingido quando $p = \frac{\ln r}{D}$. Portanto

$$\mathbb{E}(X+Y) \leq (\ln r + 1)\frac{n}{r}.$$

Isso significa que existe uma cobertura de um r-grafo D-regular com $(n \ln r)/r$ arestas, o que é um pouco mais do que o desejado. Infelizmente, o próximo exemplo mostra que ser D-regular não é suficiente.

Exemplo 67. Considere a seguinte construção feita por Frankl. Seja $\mathcal{H}$ um 3-grafo de $n = 9k$ vértices. Particionemos os vértices em $2k+1$ conjuntos $A_0, A_1, \ldots, A_{2k}$. Faça $|A_0| = 3k$ e $|A_1| = \ldots = |A_{2k}| = 3$. Considere como arestas todas as triplas contendo exatamente um elemento de A_0 em dois elementos de algum A_i.

Vamos primeiro checar que $\mathcal{H}$ é regular. Fixe um vértice $x \in A_0$. Para $1 \leq i \leq 2k$ existem exatamente $\binom{3}{2} = 3$ arestas contendo x e elementos de A_i. Logo o número de arestas contendo x é $3 \cdot 2k = 6k$. Agora fixe um vértice $x \in A_i$ para $i \neq 0$. Toda aresta contendo x tem q conter um outro elemento de A_i. Existem duas possibilidades. Selecionada uma possibilidade o terceiro elemento é arbitrario em A_0. Isso nos dá $2 \cdot 3k = 6k$ arestas contendo x e logo $\mathcal{H}$ é regular.

Seja agora $\mathcal{C}$ uma cobertura de $\mathcal{H}$. Como $\mathcal{C}$ tem de cobrir todos os A_i's para $i \neq 0$, precisaremos de pelo menos duas arestas para cada A_i (Uma aresta só usa dois elementos de A_i). Portanto será necessário pelo menos $2 \cdot 2k = 4k$ arestas e $|\mathcal{C}| \geq 4k$. Isso implica que

$$\beta(\mathcal{H}) \geq 4k = \frac{4}{3}\left(\frac{9k}{3}\right) = \frac{4n}{3r}.$$

Então é necessário algo a mais do que apenas ser D-regular. O próximo exercício mostra que se o grafo $\mathcal{H}$ for gerado aleatoriamente, então com alta probabilidade ele admite uma cobertura assintóticamente perfeita.

Exercicio 68. Seja r um inteiro e $D := D(n)$ uma função tal que $D \geq 2\ln n$. Seja $\mathcal{H}(n,p)$ o r-grafo aleatório cujo conjunto de arestas é escolhido independentemente e com probabilidade p em $\binom{[n]}{r}$. Então

$$\lim_{n\to\infty} \mathbb{P}\left(\beta(\mathcal{H}(n,p)) = (1+o(1))\frac{n}{r}\right) = 1,$$

para $p \geq D/\binom{n-1}{r-1}$.

Solução. Vamos mostrar o seguinte fato,

$$\lim_{n\to\infty} \mathbb{P}\left(\alpha(\mathcal{H}(n,p)) < \frac{n}{D^{1/r}}\right) = 1,$$

isto é, $\mathcal{H}(n,p)$ quase certamente não possui um conjnuto independente de tamanho $n/D^{1/r}$.

Seja X a variável aleatória que conta o número de conjuntos de tamanho m de $[n]$ que são independentes. Uma conta nos mostra que

$$\mathbb{E}(X) = \binom{n}{m}(1-p)^{\binom{m}{r}} \leq \binom{n}{m}e^{-p\binom{m}{r}} \leq \left(\frac{en}{m}\right)^m e^{-p\binom{m}{r}}.$$

Assim se $m = n/D^{1/r}$ temos

$$\begin{aligned}
\mathbb{E}(X) &\leq (eD)^{n/(rD^{1/r})} e^{-p\binom{n/D^{1/r}}{r}} \\
&\leq \exp\left(\frac{2n\ln D}{rD^{1/r}} - \frac{D\binom{n/D^{1/r}}{r}}{\binom{n-1}{r-1}}\right) \\
&\leq \exp\left(\frac{2n\ln D}{rD^{1/r}} - \frac{n}{2r}\right) \\
&\leq \exp\left(-\frac{n}{4r}\right),
\end{aligned}$$

pois $D \to \infty$ quando $n \to \infty$. Logo por Markov

$$\lim_{n\to\infty} \mathbb{P}\left(\alpha(\mathcal{H}(n,p)) > \frac{n}{D^{1/r}}\right) \leq \mathbb{P}(X > 1) \leq \mathbb{E}(X) \leq \exp\left(-\frac{n}{4r}\right) \to 0,$$

quando $n \to \infty$.

Note também que com probabilidade 1, o r-grafo $\mathcal{H}(n,p)$ é conexo. Seja Y a variável aleatória que conta o número de vértices isolados de $\mathcal{H}(n,p)$. Então

$$\mathbb{E}(Y) = n(1-p)^{\binom{n-1}{r-1}} \leq ne^{-p\binom{n-1}{r-1}} \leq ne^{-D} \leq ne^{-2\ln n} = \frac{1}{n}.$$

Assim, por Markov,

$$\mathbb{P}(Y > 1) \leq E(X) \leq \frac{1}{n} \to 0,$$

quando $n \to \infty$.

Assim, com alta probabilidade temos que $\mathcal{H}(n,p)$ é conexo e possui $\alpha(\mathcal{H}(n,p)) \leq n/D^{1/r}$. Agora construa uma cobertura recursivamente. Inicialmente temos $\mathcal{H}_0 = \mathcal{H}(n,p)$ e $\mathcal{C}_0 = \varnothing$. No i-ésimo passo escolhemos uma aresta f de $\mathcal{H}_{i-1}$ e fazemos $\mathcal{C}_i = \mathcal{C}_{i-1} \cup \{f\}$ e $\mathcal{H}_i = \mathcal{H}_{i-1}[V(\mathcal{H}_{i-1}) \setminus f]$. Caso não seja possível escolher essa aresta f interrompemos o processo e para cada vértice de $\mathcal{H}_{i-1}$ adicionamos uma aresta que contém este vértice à $\mathcal{C}_{i-1}$. Essa aresta, apesar de não existir em $\mathcal{H}_{i-1}$, existe em $\mathcal{H}(n,p)$ ($\mathcal{H}(n,P)$ é conexo). Assim no final obteremos uma cobertura $\mathcal{C}$.

Suponha que o processo descrito acima pare no k-ésimo passo. Em cada rodada o processo retira uma aresta do conjunto de vértices do hipergrafo. Assim o processo dura no máximo $\frac{n}{r}$ rodadas e logo $k \leq n/r$. Ainda mais, porque o processo para no k-ésimo passo temos que $\mathcal{H}_{k-1}$ é um conjunto independente. Portanto $|\mathcal{H}_{k-1}| \leq n/D^{1/r}$. Logo

$$|\mathcal{C}| \leq k + |\mathcal{H}_{k-1}| \leq \frac{n}{r} + \frac{n}{D^{1/r}} = (1+o(1))\frac{n}{r},$$

com alta probabilidade. □

Algo interessante pode ser retirado do último exemplo. Note que o grau em típico de um vértice nesse $\mathcal{H}(n,p)$ é em torno de

$$p\binom{n-1}{r-1} = D.$$

Além disso note o número típico de arestas comum a dois vértices nesse grafo é em torno de

$$p\binom{n-2}{r-2} = O(D/n) = o(D).$$

E esse último elemento é suficiente para resolver o problema.

Dados um r-grafo $\mathcal{H}$, definimos o *cograu* $d(x,y)$ como o número de arestas em $\mathcal{H}$ que contém $\{x,y\}$. Defina

$$\Delta_1(\mathcal{H}) = \max\{d(x) : x \in V\}$$

como o maior grau de $\mathcal{H}$ e

$$\Delta_2(\mathcal{H}) = \max\{d(x,y) : x,y \in V\}$$

como o maior cograu de $\mathcal{H}$.

Dizemos que um r-grafo $\mathcal{H}$ satisfaz a propriedade $R(K,D,\delta)$ se

(1) $\Delta_1(\mathcal{H}) \leq KD$.

(2) Para pelo menos $(1-\delta)n$ vértices em $\mathcal{H}$ vale que $d(x) = (1 \pm \delta)D$.

(3) $\Delta_2(\mathcal{H}) \leq \delta D$.

O seguinte resultado é devido a Frank, Rödl e Pippenger.

Teorema 69 (Frankl, Rödl, Pippenger)**.** *Para todo inteiro $r \geq 2$ e reais $\varepsilon > 0$, $K \geq 1$, existem $\delta := \delta(r,K,\varepsilon)$ e $D_0 := D_0(r,K,\varepsilon)$ tal que para todo $n \geq D \geq D_0$ o seguinte vale.*

Todo r-grafo $\mathcal{H}$ convexo com a propriedade $R(K,D,\delta)$ é tal que

$$\beta(\mathcal{H}) \leq (1+\varepsilon)\frac{n}{r}.$$

Um comentário: no exemplo dado por Frankl, a condição do cograu falha. De fato, se considerarmos dois vértices no mesmo A_i com $i \neq 0$, temos que o seu cograu é $3k$ enquanto o grafo é $6k$ regular. Nas próximas aulas focaremos em demonstrar o Teorema 69.

2.4. **Aula 11 de abril de 2018.** [10]

Definição 70. *Sejam V um conjunto (finito) de vértices e $\mathcal{H} \subseteq \binom{V}{r}$, $r \geq 2$, um r-grafo. O* grau máximo *de $\mathcal{H}$, denotado por $\Delta(\mathcal{H})$, é dado por $\Delta(\mathcal{H}) = \max\{d(x) : x \in V\}$, onde $d(x) = d_{\mathcal{H}}(x)$ é o grau de x em $\mathcal{H}$. O* cograu máximo *de $\mathcal{H}$, por sua vez, é $\Delta^{(2)}(\mathcal{H})$ definido como $\Delta^{(2)}(\mathcal{H}) = \max\{d(x,y) : x,y \in V, x \neq y\}$, sendo que, dados x, y distintos, $d(x,y) = d_{\mathcal{H}}(x,y)$ é o cograu de x e y em $\mathcal{H}$.*

Observação 71. Ao dizer que $\mathcal{H} \subseteq \binom{V}{r}$ é r-grafo, recorremos a um abuso de notação. Formalmente, temos que $(V,\mathcal{H})$ é r-grafo, mas confundimos $\mathcal{H}$ e $E(\mathcal{H})$ por motivos de facilidade.

[10] Notas produzidas por André Nakazawa e Gabriel Barros.

Definição 72. *Sejam* $|V| = n$, $r \geq 2$, $\mathcal{H} \subseteq \binom{V}{r}$, $\delta > 0$, $k \geq 1$, $D \geq 1$. *Dizemos que* $\mathcal{H}$ *é* (δ, k, D)-pseudoaleatório *se:*

(i) $\Delta(\mathcal{H}) \leq kD$,

(ii) existem $\geq (1-\delta)n$ *vértices* $x \in V$ *tais que* $d(x) = (1 \pm \delta)D$,

(iii) $\Delta^{(2)}(\mathcal{H}) \leq \delta D$.

Teorema 73 (Frankl, Rödl & Pippenger)**.** *Para todo* $r \geq 2$, $k \geq 1$ *e* $\alpha > 0$, *existem* $\gamma > 0$, $n_0 \geq 1$ *e* $D_0 \geq 1$ *tais que, para todo* $\mathcal{H} \subseteq \binom{V}{r}$ (γ, k, D)*-pseudoaleatório com* $|V| = n \geq n_0$ *e* $D \geq D_0$, *tem-se*

$$\operatorname{cov}(\mathcal{H}) \leq (1+\alpha)\frac{n}{r}.$$

Definição 74. *Sejam* V *um conjunto (finito) de vértices,* $\mathcal{H} \subseteq \binom{V}{r}$, *com* $r \geq 2$, *um* r*-grafo e* $U \subseteq V$. *Denotamos por* $\mathcal{H} - U$ *o* r-grafo induzido por $V \setminus U$, *isto é,* $\mathcal{H} - U = \mathcal{H}[V \setminus U] = \{E \in \mathcal{H} : E \subseteq V \setminus U\}$.

Lema 75 (Nibbling Lemma)**.** *Para todo* $r \geq 2$, $K \geq 1$, $\varepsilon > 0$ *e* $\delta' > 0$, *existem* $\delta_{NL} > 0$, $n_{NL}^{(0)}$ *e* $D_{NL}^{(0)}$ *tais que, para todo* $\mathcal{H} \subseteq \binom{V}{r}$ (δ_{NL}, K, D)*-pseudoaleatório com* $|V| = n \geq n_{NL}^{(0)}$ *e* $D \geq D_{NL}^{(0)}$, *existe* $\mathcal{C} \subseteq \mathcal{H}$ *com as seguintes propriedades:*

(i) $|\mathcal{C}| = (1 \pm \delta')(\varepsilon n/r)$,

(ii) $|V(\mathcal{H}')| = (1 \pm \delta')ne^{-\varepsilon}$, *onde* $\mathcal{H}' = \mathcal{H} - V(\mathcal{C})$, *e*

(iii) $\mathcal{H}'$ *é* (δ', K', D')*-pseudoaleatório, onde* $K' = Ke^{\varepsilon(r-1)}$ *e* $D' = De^{-\varepsilon(r-1)}$.

Adiemos a prova do Lema 75 para o final da seção e consideremos agora a prova do Teorema 73.

Demonstração do Teorema 73. Dados $r \geq 2$, $k \geq 1$ e $\alpha > 0$, escolhemos δ, t e ε de modo que $0 < \delta, t^{-1} \ll \varepsilon \ll \alpha$. Mais precisamente, seja $\varepsilon > 0$ tal que

$$\frac{\varepsilon}{1 - e^{-\varepsilon}(1+\varepsilon^2)} + \varepsilon < 1 + \alpha;$$

seja $t \geq 1$ um inteiro tal que

$$(e^{-\varepsilon}(1+\varepsilon^2))^t < \frac{\varepsilon}{r};$$

e seja $0 < \delta \leq \varepsilon^2$ tal que

$$(1+\delta)\frac{\varepsilon}{1 - e^{-\varepsilon}(1+\varepsilon^2)} + \varepsilon < 1 + \alpha.$$

Seja $\mathcal{H} \subseteq \binom{V}{r}$ um hipergrafo (γ, k, D)-pseudoaleatório qualquer com $|V| = n \geq n_0$ e $D \geq D_0$, onde γ, n_0 e D_0 serão determinados adiante. O teorema é provado aplicando t vezes o Lema 75,

a partir de $\mathcal{H}_0 := \mathcal{H}$, obtendo sucessivamente

$$\mathcal{C}_0 \subseteq \mathcal{H}_0, \mathcal{H}_1 := \mathcal{H}_0 - V(\mathcal{C}_0), \ldots, \mathcal{C}_{t-1} \subseteq \mathcal{H}_{t-1}, \mathcal{H}_t := \mathcal{H}_{t-1} - V(\mathcal{C}_{t-1}).$$

731 A fim de que cada tal aplicação seja possível, é necessário que cada $\mathcal{H}_i$ ($0 \leq i \leq t-$
732 1) seja (δ_i, K_i, D_i)-pseudoaleatório, com δ_i, K_i, D_i e $|V(\mathcal{H}_i)|$ assumindo valores adequados.
733 Definimos $\delta_t := \delta$. Dados r, $K = K_{t-1} := ke^{\varepsilon(t-1)(r-1)}$, ε e $\delta' = \delta_t$, o lema nos dá δ_{NL}, $D^{(0)}_{NL}$
734 e $n^{(0)}_{NL}$, e a conclusão do lema vale para todo hipergrafo $(\delta'_{NL}, K_{t-1}, \geq D^{(0)}_{NL})$-pseudoaleatório com
735 pelo menos $n^{(0)}_{NL}$ vértices, onde δ'_{NL} é qualquer real tal que $0 < \delta'_{NL} \leq \delta_{NL}$. Definimos

$$\begin{aligned}
\delta_{t-1} &:= \min\{\delta_{NL}, \delta_t e^{-\varepsilon(r-1)}\},\\
D^{(0)}_{t-1} &:= \max\{D^{(0)}_{NL}, e^{\varepsilon(r-1)}\},\\
n^{(0)}_{t-1} &:= \max\{n^{(0)}_{NL}, 2e^{\varepsilon}(1-\delta_t)^{-1}\}.
\end{aligned}$$

736 De maneira análoga, para $i = t-2, t-3, \ldots, 0$, definimos

$$\begin{aligned}
K_i &:= ke^{\varepsilon i(r-1)},\\
\delta_i &:= \min\{\delta_{NL}(r, K_i, \varepsilon, \delta_{i+1}), \delta_{i+1}e^{-\varepsilon(r-1)}\},\\
D^{(0)}_i &:= \max\{D^{(0)}_{NL}(r, K_i, \varepsilon, \delta_{i+1}), D^{(0)}_{i+1}e^{\varepsilon(r-1)}\},\\
n^{(0)}_i &:= \max\{n^{(0)}_{NL}(r, K_i, \varepsilon, \delta_{i+1}), n^{(0)}_{i+1}e^{\varepsilon}(1-\delta_t)^{-1}\}.
\end{aligned}$$

737 Assim, pomos $\gamma = \delta_0$, $n_0 = n^{(0)}_0$, e $D_0 = D^{(0)}_0$.

Agora mostremos que

$$\mathcal{C} := \bigcup_{i=0}^{t-1} \mathcal{C}_i \cup \mathcal{C}_t$$

738 satisfaz $|\mathcal{C}| \leq (1+\alpha)n/r$, onde $\mathcal{C}_t \subseteq \mathcal{H}_t$ é uma cobertura qualquer de $\mathcal{H}_t$. Notemos que $\mathcal{C}$ é uma
739 cobertura de $\mathcal{H}$. Como $\max\{\delta_i : 0 \leq i \leq t\} = \delta \leq \varepsilon^2$, temos que

$$|V(\mathcal{H}_t)| = n\prod_{i=1}^{t}[e^{-\varepsilon}(1 \pm \delta_i)] \leq n(e^{-\varepsilon}(1+\delta))^t \leq n(e^{-\varepsilon}(1+\varepsilon^2))^t \leq n\frac{\varepsilon}{r}.$$

740 Então,

$$|\mathcal{C}| \leq \sum_{i=0}^{t-1}|\mathcal{C}_i| + |V(\mathcal{H}_t)| \leq \sum_{i=0}^{t-1}\left[\frac{\varepsilon|V(\mathcal{H}_i)|}{r}(1+\delta_{i+1})\right] + \frac{\varepsilon}{r}n \leq \frac{\varepsilon}{r}(1+\delta)\sum_{i=0}^{t-1}|V(\mathcal{H}_i)| + \frac{\varepsilon}{r}n,$$

741 onde

$$\sum_{i=0}^{t-1}|V(\mathcal{H}_i)| \leq n\sum_{i=0}^{t-1}(e^{-\varepsilon}(1+\varepsilon^2))^i \leq \frac{n}{1-e^{-\varepsilon}(1+\varepsilon^2)}.$$

Logo,

$$|\mathcal{C}| \leq \frac{\varepsilon}{r}(1+\delta)\frac{n}{1-e^{-\varepsilon}(1+\varepsilon^2)} + \frac{\varepsilon}{r}n \leq \frac{n}{r}\left((1+\delta)\frac{\varepsilon}{1-e^{-\varepsilon}(1+\varepsilon^2)} + \varepsilon\right) < \frac{n}{r}(1+\alpha),$$

e portanto $\mathrm{cov}(\mathcal{H}) \leq (1+\alpha)n/r$. □

2.5. **Aula 23 de abril de 2018.** [11]

Nesta aula, provamos o Lema 75, da Aula de 11 de abril de 2018 (*Nibbling Lemma*).

Demonstração do Lema 75. Ao longo da prova, sempre que necessário, vamos supor que n e D são suficientemente grandes. Vamos denotar por δ_1, δ_2, ... números reais que tendem a 0 quando $\delta_{NL} \to 0$, $n \to \infty$ e $D \to \infty$. Assim, com escolhas apropriadas de δ_{NL}, $n_{NL}^{(0)}$ e $D_{NL}^{(0)}$, garantimos que, para cada δ_i, valha $\delta_i < \delta'$.

Seja $\mathcal{C} = \mathcal{H}_p$ um subconjunto aleatório de arestas de $\mathcal{H}$, com $p = \varepsilon/D$. Vamos provar que, com probabilidade positiva, valem as três propriedades (i), (ii) e (iii). Temos que

$$r|\mathcal{H}| = \sum_{v\in V} d(v) = (1-\delta_{NL})n(1\pm\delta_{NL})D \pm \delta_{NL}nKD = (1\pm\delta_1)nD.$$

Logo,

$$\mathbb{E}(|\mathcal{C}|) = p|\mathcal{H}| = (1\pm\delta_1)\frac{\varepsilon n}{r}.$$

Como $\mathrm{Var}(|\mathcal{C}|) = (1-p)p|\mathcal{H}| \leq \mathbb{E}(|\mathcal{C}|)$ ($|\mathcal{C}|$ tem distribuição binomial), temos, pela Desigualdade de Chebyshev, para $\lambda > 0$ arbitrário, que

$$\mathbb{P}(||\mathcal{C}| - \mathbb{E}(|\mathcal{C}|)| > \lambda\mathbb{E}(|\mathcal{C}|)) < \frac{\mathrm{Var}(|\mathcal{C}|)}{\lambda^2(\mathbb{E}(|\mathcal{C}|))^2} \leq \frac{1}{\lambda^2(1\pm\delta_1)\varepsilon n/r} \to 0$$

quando $n \to \infty$. Portanto, para $\delta_2 > 0$ adequado,

$$\mathbb{P}\left(|\mathcal{C}| \neq (1\pm\delta_2)\frac{\varepsilon n}{r}\right) < \frac{1}{3}. \tag{1}$$

Consideremos agora a propriedade (ii). Para cada $v \in V$, seja X_v a v.a. indicadora do evento "$v \in V(\mathcal{H}')$". Notemos que $|V(|\mathcal{H}'|)| = \sum_{v\in V} X_v$. No caso em que $d(v) = (1\pm\delta_{NL})D$, temos que

$$\mathbb{E}(X_v) = \mathbb{P}(X_v = 1) = (1-p)^{d(v)} = (1-p)^{(1\pm\delta_{NL})D},$$

e, como

$$e^{-\varepsilon(1+\delta_{NL})(1-\varepsilon/D)^{-1}} \leq (1-p)^{(1+\delta_{NL})D} \leq (1-p)^{(1\pm\delta_{NL})D} \leq (1-p)^{(1-\delta_{NL})D} \leq e^{-\varepsilon(1-\delta_{NL})},$$

[11] Notas produzidas por Gabriel Barros e REVISOR?.

concluímos que $\mathbb{E}(X_v) = e^{-\varepsilon}(1 \pm \delta_3)$. Há no máximo δ_{NL} vértices v tais que $d(v) \neq (1 \pm \delta_{NL})D$. Assim, observando que $0 \leq \mathbb{E}(X_v) \leq 1$ para todo $v \in V$, obtemos

$$\mathbb{E}(|V(\mathcal{H}')|) = ne^{-\varepsilon}(1 \pm \delta_4).$$

751 Temos que $\mathrm{Var}(|V(\mathcal{H}')|) \leq \mathbb{E}(|V(\mathcal{H}')|) + \sum_{v \neq w} \mathrm{Cov}(X_v, X_w)$. Ademais,

$$\begin{aligned}
\mathrm{Cov}(X_v, X_w) &= \mathbb{E}(X_v X_w) - \mathbb{E}(X_v)\mathbb{E}(X_w) \\
&= (1-p)^{d(v)+d(w)-d(v,w)} - (1-p)^{d(v)+d(w)} \\
&\leq (1-p)^{-d(v,w)} - 1 \leq \left(1 - \frac{\varepsilon}{D}\right)^{-\delta_{NL}D} - 1 \leq \delta_5.
\end{aligned}$$

752 Assim, $\mathrm{Var}(|V(\mathcal{H}')|) \leq \mathbb{E}(|V(\mathcal{H}')|) + \delta_5 n^2 \leq \delta_6(\mathbb{E}(|V(\mathcal{H}')|))^2$, e, por Chebyshev,

$$\mathbb{P}\left(|V(\mathcal{H}')| \neq (1 \pm \delta_7)\mathbb{E}(|V(\mathcal{H}')|) = (1 \pm \delta_8)ne^{-\varepsilon}\right) < \frac{1}{3}. \tag{2}$$

753 Finalmente, consideremos a propriedade (*iii*). Há pelo menos $(1 - \delta_9)n$ vértices v tais que

754 (A) $d(v) = (1 \pm \delta_{NL})D$, e

755 (B) todas as $d(v)$ arestas E com $v \in E$, a menos de no máximo $\delta_{10}D$ delas, satisfazem

$$|\{F \in \mathcal{H} : v \notin F, F \cap E \neq \varnothing\}| = (1 \pm \delta_{11})(r-1)D \tag{3}$$

De fato, temos, por hipótese, que no máximo $\delta_{NL}n \leq \delta_9 n/2$ vértices w tem $d(w) \neq (1 \pm \delta_{NL})D$. Observemos que, se uma aresta E com $v \in E$ é tal que todo $w \in E$ tem $d(w) = (1 \pm \delta_{NL})D$, então E satisfaz (3), pois, neste caso, temos

$$(1 \pm \delta_{NL})(r-1)D - \binom{r-1}{2}\delta_{NL}D \leq |\{F \in \mathcal{H} : v \notin F, F \cap E \neq \varnothing\}| \leq (1 \pm \delta_{NL})(r-1)D$$

756 (na desigualdade da esquerda, usamos o fato de que $d(w, w') < \delta_{NL}D$ para todo par $w \neq w'$).
757 Portanto, as arestas E com $v \in E$ em que não vale (3) contêm algum w com $d(w) \neq (1 \pm \delta_{NL})D$.
758 O número de arestas de $\mathcal{H}$ contendo algum w com $d(w) \neq (1 \pm \delta_{NL})D$ é no máximo $\delta_{NL}nKD$.
759 E, por contagem dupla, o número de vértices contidos em mais do que $\delta_{10}D$ tais arestas é no
760 máximo $\delta_{NL}nKDr/(\delta_{10}D) \leq \delta_9 n/2$, para escolhas adequadas de δ_9 e δ_{10}.

Basta que mostremos que, para a maioria dos vértices v que satisfazem (A) e (B), se v está em $V(\mathcal{H}')$, então vale que $d_{\mathcal{H}'}(v)$ é conforme a propriedade (*iii*). Fixemos um tal vértice v . Uma aresta E com $v \in E$ *sobrevive* se toda aresta F tal que $v \notin F$ e $F \cap E \neq \varnothing$ não está em $\mathcal{C}$. Dizemos que E é *boa* se satisfaz 3. Para cada aresta E com $v \in E$, seja Y_E a v.a. indicadora de

"E sobrevive". Seja $Z_v = \sum_{v \in E} Y_E$. Notemos que, se $v \in V(\mathcal{H}')$, então $d_{\mathcal{H}'}(v) = Z_v$. Temos que

$$\mathbb{E}(Z_v) = (1 \pm \delta_{NL} \pm \delta_{10})D(1-p)^{(1\pm\delta_{11})(r-1)D} \pm \delta_{10}D = e^{-\varepsilon(r-1)}D(1 \pm \delta_{12}).$$

761 E

$$\begin{aligned}\mathrm{Var}(Z_v) &\leq \mathbb{E}(Z_v) + \sum_{E \neq E'} \mathrm{Cov}(Y_E, Y_{E'}) \\ &\leq \mathbb{E}(Z_v) + 2\delta_{10}D^2(1 \pm \delta_{NL}) + \sum_{\substack{E \neq E' \\ E,E' \text{ boas}}} \mathrm{Cov}(Y_E, Y_{E'}).\end{aligned}$$

Fixemos uma aresta boa E. A condição sobre os cograus nos dá que, em $\sum_{E' \text{ boa}} \mathrm{Cov}(Y_E, Y_{E'})$, o número de parcelas tais que $|E \cap E'| > 1$ é no máximo $(r-1)\delta_{NL}D$. Para cada E', seja $t(E, E')$ o número de arestas de $\mathcal{H}$ que intersectam E e E' e não contêm v. A condição sobre os cograus nos dá também que $t(E, E') \leq (r-1)^2\delta_{NL}D$. Assim, para as arestas E' tais que $E \cap E' = \{v\}$,

$$\mathrm{Cov}(Y_E, Y_{E'}) \leq (1-p)^{-t(E,E')} - 1 \leq (1-p)^{-(r-1)^2\delta_{NL}D} - 1 \leq \delta_{13},$$

e portanto, para cada aresta boa E fixa,

$$\sum_{E' \text{ boa}} \mathrm{Cov}(Y_E, Y_{E'}) \leq (r-1)\delta_{NL}D + D(1+\delta_{NL})\delta_{13} \leq \delta_{14}D.$$

762 Segue que

$$\begin{aligned}\mathrm{Var}(Z_v) &\leq \mathbb{E}(Z_v) + 2\delta_{10}D^2(1 \pm \delta_{NL}) + (1+\delta_{NL})\delta_{14}D^2 \\ &\leq \mathbb{E}(Z_v) + \delta_{15}D^2 \leq \delta_{16}(\mathbb{E}(Z_v))^2.\end{aligned}$$

Portanto, por Chebyshev,

$$\mathbb{P}\left(Z_v \neq (1 \pm \delta_{18})e^{-\varepsilon(r-1)}D\right) < \delta_{17},$$

763 e, por Markov,

$$\mathbb{P}\left(|\{v : v \text{ satisfaz (A) e (B) e } Z_v \neq (1 \pm \delta_{18})e^{-\varepsilon(r-1)}D\}| > 3\delta_{17}n\right) < \frac{1}{3}. \tag{4}$$

764 Concluímos por (1), (2) e (4), usando a cota da união, que as propriedades (i), (ii) e (iii)
765 valem com probabilidade positiva.

766 □

3.1. Aula 25 de abril de 2018: Probabilidades exponencialmente pequenas. [12]

Dados três pontos $x, y, z \in \mathbb{R}^n$, denotamos por $\angle(x, y, z)$ o ângulo centrado em x determinado pelos pontos y e z.

Definição 76. *Dizemos que $X \subseteq \mathbb{R}^n$ é* obtuso *se existem pontos $x, y, z \in X$ tais que $\angle(x, y, z) > \pi/2$.*

Seja $g(n) := \max\{|X| : X \subseteq \mathbb{R}^n \text{ e } X \text{ não é obtuso}\}$.

Proposição 77. *Vale que $g(n) \geq 2^n$.*

Demonstração. Considere $\Omega_n = \{0, 1\}^n \subseteq \mathbb{R}^n$. Temos que não existem $x, y, z \in \Omega_n$ tais que $\angle(x, y, z) > \pi/2$. De fato, se $x, y, z \in \Omega_n$, temos que

$$\langle z - x, y - x \rangle = \|z - x\| \, \|y - x\| \cos\theta,$$

e $\langle z - x, y - x \rangle \geq 0$, pois

$$\langle z - x, y - x \rangle = |A \smallsetminus (B \cup C)| + |(B \cap C) \smallsetminus A| \,,$$

onde $A = \operatorname{supp} x$, $B = \operatorname{supp} y$ e $C = \operatorname{supp} z$. Portanto, $\cos\theta \geq 0$, implicando que $\theta \leq \pi/2$. □

Erdös provou em (aproximadamente) 1950 que $g(n) \leq 2^n$.

Vamos agora considerar uma noção análoga.

Definição 78. *Dizemos que $X \subseteq \mathbb{R}^n$ é* agudo *se toda tripla de pontos $x, y, z \in X$ é tal que $\angle(x, y, z) < \pi/2$.*

Seja $f(n) := \max\{|X| : X \subseteq \mathbb{R}^n \text{ e } X \text{ é agudo}\}$. Em 1962, Danzer e Grünbaum provaram o seguinte resultado sobre $f(n)$.

Proposição 79 (Danzer e Grünbaum (1962))**.** *Para todo $n \geq 1$, temos que $f(n) \geq 2n - 1$.*

Além disso, fizeram a seguinte conjectura.

Conjectura 80 (Danzer e Grünbaum (1962))**.** *Para todo $n \geq 1$, vale que $f(n) \leq 2n - 1$.*

Em 1983, Erdös e Füredi provaram que a conjectura é falsa, usando probabilidades exponencialmente pequenas.

[12] Notas produzidas por Bruno Pasqualotto Cavalar e REVISOR?.

Teorema 81 (Erdös e Füredi (1962))**.** *Para todo $n \geq 1$ existe $X \subseteq \mathbb{R}^n$ agudo que satisfaz $|X| \geq \lfloor (1/2)(2/\sqrt{3})^n \rfloor$.*

Demonstração. Escolhemos $a_1, a_2, \ldots, a_{2m} \in_U \Omega_n$ independentemente, onde $m = \lfloor (1/2)(2/\sqrt{3})^n \rfloor$. Fixe $\alpha, \beta, \gamma \in [2m]$. Sejam $A = \operatorname{supp} a_\alpha$, $B = \operatorname{supp} a_\beta$ e $C = \operatorname{supp} a_\gamma$. Observe que $\angle(a_\alpha, a_\beta, a_\gamma) \leq \pi/2$. Ademais, quando $a_\alpha \neq a_\beta \neq a_\gamma \neq a_\alpha$, vale que $\angle(a_\alpha, a_\beta, a_\gamma) = \pi/2$ se, e somente se,

$$\langle a_\beta - a_\alpha, a_\gamma - a_\alpha \rangle = |A \smallsetminus (B \cup C)| + |(B \cap C) \smallsetminus A| = 0.$$

Isto é, se e só se $B \cap C \subseteq A \subseteq B \cup C$. Segue que

$$\mathbb{P}[\angle(a_\alpha, a_\beta, a_\gamma) = \pi/2] \leq \mathbb{P}[B \cap C \subseteq A \subseteq B \cup C] = (3/4)^n.$$

Seja R o número de pares $(\alpha, \{\beta, \gamma\})$ tais que $\alpha, \beta, \gamma \in [2m]$, $\alpha \neq \beta \neq \gamma \neq \alpha$ e $\angle(a_\alpha, a_\beta, a_\gamma) = \pi/2$. Temos

$$\mathbb{E}[R] \leq \binom{2m}{3} 3 \left(\frac{3}{4}\right)^n \leq 4m^3 \left(\frac{3}{4}\right)^n \leq 4m \left(\frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^n\right)^2 \left(\frac{3}{4}\right)^n = m.$$

Portanto, existe escolha dos a_i $(1 \leq i \leq 2m)$ com $R \leq m$. Fixe tais a_i e removea dessa lista os vértices dos ângulos retos. Sobram $\geq m$ elementos formando um conjunto agudo.[13] □

Observe que acima usamos o método da alteração. Para obter uma prova sem o método da alteração, podemos fazer do seguinte modo. Seja $a_1, \ldots, a_M \in_U \Omega_n$. Se $3\binom{M}{3}\left(\frac{3}{4}\right)^n < 1$, então existe uma escolha de $a_1, \ldots, a_M$ como queremos. Isto pode ser satisfeito com $M = (4/3)^{n/3}$, o que é mais fraco do que o resultado obtido acima.

Recentemente, Gerencsér e Harangi (2017) fortaleceram esse resultado, provando que $f(n) \geq 2^{n-1} - 1$. Isto é assintoticamente ótimo, visto que $f(n) \leq 2^n - 1$.

Em 1983, Erdös e Füredi consideraram a seguinte generalização do problema anterior.

Definição 82. *Dizemos que $X \subseteq \mathbb{R}^n$ é* θ-conjunto *se toda tripla de pontos $x, y, z \in X$ é tal que $\angle(x, y, z) < \theta$.*

Teorema 83. *Para todo $\varepsilon > 0$ existe $\delta > 0$ tal que para todo $n \geq 1$ existe $X \subseteq \mathbb{R}^n$ que é $(\pi/3 + \varepsilon)$-conjunto com $|X| \geq (1 + \delta)^n$.*

3.1.1. *Algumas desigualdades exponenciais.* Seja $X_i \widetilde{\mathrm{Be}}(p_i)$, com $i \in [n]$, e suponha que os X_i são independentes. Seja $X = \sum_i X_i$. Temos que $\mu := \mathbb{E}[X] = \sum_i p_i$. Nesse caso, valem as seguintes desigualdades.

[13] Observe que os a_i sobreviventes são distintos!

Teorema 84 (Desiguadades de Chernoff)**.**

$$\mathbb{P}[X \geq \mu + t] \leq \exp\left\{-\frac{t^2}{2(\mu + t/3)}\right\}, \qquad t \geq 0; \tag{5}$$

$$\mathbb{P}[X \leq \mu - t] \leq \exp\left\{-\frac{t^2}{2\mu}\right\}, \qquad t \geq 0; \tag{6}$$

$$\mathbb{P}[X \geq (1+\varepsilon)\mu] \leq \exp\left\{-\frac{\varepsilon^2\mu}{3}\right\}, \qquad 0 < \varepsilon < 3/2; \tag{7}$$

$$\mathbb{P}[x \leq (1-\varepsilon)\mu] \leq \exp\left\{-\frac{\varepsilon^2\mu}{2}\right\}, \qquad \varepsilon > 0; \tag{8}$$

$$\mathbb{P}[x \geq t] \leq \exp\{-t\}, \qquad t \geq 7\mu; \tag{9}$$

$$\mathbb{P}[x \geq \mu + t] \leq \exp\left\{-\frac{2t^2}{n}\right\}, \qquad t \geq 0; \tag{10}$$

$$\mathbb{P}[x \leq \mu - t] \leq \exp\left\{-\frac{2t^2}{n}\right\}, \qquad t \geq 0. \tag{11}$$

3.2. **Aula 07 de maio de 2018.** [14]

Consideremos uma VA X não-negativa. Temos que,

$$\forall u > 0, \mathbb{P}(X \geq \mu + t) = \mathbb{P}(e^{uX} \geq e^{u(\mu+t)}),$$

pois e^{uX} é crescente, e por Markov,

$$\mathbb{P}(e^{uX} \geq e^{u(\mu+t)}) \leq e^{-u(\mu+t)}\mathbb{E}(e^{uX}).$$

Portanto,

$$\forall u > 0, \mathbb{P}(X \geq \mu + t) \leq e^{-u(\mu+t)}\mathbb{E}(e^{uX}).$$

Analogamente,

$$\forall u < 0, \mathbb{P}(X \leq \mu - t) = \mathbb{P}(e^{uX} \geq e^{u(\mu-t)}),$$

e, por Markov,

$$\mathbb{P}(e^{uX} \geq e^{u(\mu-t)}) \leq e^{-u(\mu-t)}\mathbb{E}(e^{uX}).$$

Portanto

$$\forall u < 0, \mathbb{P}(X \leq \mu - t) \leq e^{-u(\mu-t)}\mathbb{E}(e^{uX}).$$

Onde

$$\mathbb{E}(e^{uX}) = \mathbb{E}(1 + uX + \frac{1}{2!}(uX)^2 + \cdots) =$$

[14] Notas produzidas por Ângelo Lovatto e Rodrigo Enju

$$= \mathbb{E}\left(\sum_{k\geq 0}\frac{u^k}{k!}X^k\right) = \sum_{k\geq 0}\frac{u^k}{k!}\mathbb{E}(X^k).$$

Observação 85. $\mathbb{E}(X^k)$ é o k-ésimo momento de X, e $\mathbb{E}(e^{uX})$ é a função geradora de momentos de X (ou transformada de Laplace).

3.2.1. *Soma de VAs independentes.* Seja X uma VA, tal que

$$X = \sum_{i=1}^{n} X_i,$$

com $X_i \sim Be(p_i)$, onde $\mathbb{P}(X_i = 1) = p_i$ e $\mathbb{P}(X_i = 0) = 1 - p_i$, e X_i independentes.

Então, para esta VA, a função geradora de momentos é da forma

$$\mathbb{E}(e^{uX}) = \mathbb{E}\left(e^{u\sum_{i=1}^{n} X_i}\right) =$$

$$= \mathbb{E}(\prod_{i=1}^{n} e^{uX_i}) = \prod_{i=1}^{n}\mathbb{E}(e^{uX_i}) =$$

$$= \prod_{i=1}^{n}(1 - p_i + p_i e^u).$$

Supondo que $p_i = p$ para todo i, então $X \sim Bi(n, p)$.

Neste caso, $\mathbb{E}(e^{uX}) = (1 - p + pe^u)^n$.

Assim,

$$\forall u > 0, \mathbb{P}(X \geq \mu + t) \leq e^{-u(\mu+t)}(q - p + pe^u)^n$$

Como X é binomial, então se $\mu + t = n$, então a probabilidade é extamente p^n, e se $\mu + t > n$, a probabilidade é zero. Supomos então que $\mu < \mu + t < n$. Tome

$$e^u = \frac{(\mu + t)(1 - p)}{(n - \mu - t)p} > 1.$$

Substituindo este e^u no limitante de $\mathbb{P}(X \geq \mu + t)$, obtemos

$$\mathbb{P}(X \geq \mu + t) \leq \left(\frac{\mu}{\mu + t}\right)^{\mu+t}\left(\frac{n - \mu}{n - \mu - t}\right)^{n-\mu-t},$$

para todo $0 \leq t \leq n - \mu$ (Chernoff 1952, e independentemente Okamoto, 1958).

Procuremos uma simplificação para a expressão. Tome

$$\varphi(x) = \begin{cases} (1 + x)\ln(1 + x) - x & \text{se } x \geq -1 \\ \infty & \text{se } x < -1. \end{cases}$$

Seja

$$f(x) = \frac{x^2}{2}$$

$$h(x) = \frac{x^2}{2\left(1 + \frac{x}{3}\right)}$$

$$(*) \begin{cases} \varphi(x) \geq f(x) & \forall -1 \leq x \leq 0 \\ \varphi(x) \geq h(h) & \forall x \geq 0 \end{cases}$$

Ademais,

$$\ln\left(\left(\frac{\mu}{\mu+t}\right)^{\mu+t}\left(\frac{n-\mu}{n-\mu-t}\right)^{n-\mu-t}\right) = -\mu\varphi\left(\frac{t}{\mu}\right) - (n-\mu)\varphi\left(\frac{-t}{n-\mu}\right).$$

Assim,

$$\mathbb{P}(X \geq \mu + t) \leq \exp\left\{-\mu\varphi\left(\frac{t}{\mu}\right) - (n-\mu)\varphi\left(\frac{-t}{n-\mu}\right)\right\}.$$

Se considerarmos uma VA $Y = n - X$, então é fácil ver que vale

$$\mathbb{P}(X \leq \mu - t) \leq \exp\left\{-\mu\varphi\left(\frac{-t}{\mu}\right) - (n-\mu)\varphi\left(\frac{t}{n-\mu}\right)\right\}, \forall 0 \leq t \leq \mu.$$

Como $\varphi(x) \geq 0 \forall x \geq 0$, então temos

$$\mathbb{P}(X \geq \mu + t) \leq \exp\left\{-\mu\varphi\left(\frac{t}{\mu}\right)\right\},$$

$$\mathbb{P}(X \leq \mu - t) \leq \exp\left\{-\mu\varphi\left(\frac{-t}{\mu}\right)\right\},$$

Usando (*), obtemos

$$\begin{aligned} \mathbb{P}(X \geq \mu + t) &\leq \exp\left\{-\mu h(t/\mu)\right\} \\ &= \exp\left\{-\mu\frac{t^2/\mu^2}{2(1+t/3\mu)}\right\} \\ &= \exp\left\{-\frac{t^2}{2(\mu+t/3)}\right\}. \end{aligned}$$

Ademais,

$$\mathbb{P}(X \leq \mu - t) \leq \exp\left\{-\mu f(-t/\mu)\right\}$$

$$= \exp\left\{-\mu t^2/2\mu^2\right\}$$
$$= \exp\left\{-t^2/2\mu\right\}$$

847 Em geral, é comum usar $t = \varepsilon\mu$. Neste caso, temos

$$\mathbb{P}(X \leq \mu(1-\varepsilon)) \leq e^{-\varepsilon^2\mu/2}, \forall 0 \leq \varepsilon \leq 1.$$

$$\begin{aligned}\mathbb{P}(X \geq \mu + t) &\leq \exp\left\{-\frac{\varepsilon^2\mu^2}{2\mu(1+\varepsilon/3)}\right\} \\ &= \exp\left\{-\frac{\varepsilon^2\mu}{2(1+\varepsilon/3)}\right\} \\ &\leq \exp\left\{-\frac{\varepsilon^2\mu}{3}\right\}, \text{ se } 0 \leq \varepsilon \leq \frac{3}{2}.\end{aligned}$$

848 Agora, vamos considerar o caso geral, em que $X_i \sim Be(p_i)$. Tome

$$p = \frac{1}{n}\sum_{i=1}^{n} p_i.$$

849 E seja $Y \sim Bi(n,p)$. Temos

$$\begin{aligned}\mathbb{E}(e^{uX}) &= \prod_{i=1}^{n}(1 - p_i + p_i e^u) \\ &= \prod_{i=1}^{n}(1 + p_i(e^u - 1))\end{aligned}$$

850 Então, por Jensen (considerando uma função $f(x) = \log(1+xt)$), temos que

$$\begin{aligned}\prod_{i=1}^{n}(1 + p_i(e^u - 1)) &\leq (1 + p(e^u - 1))^n \\ &= \mathbb{E}(e^{uY}).\end{aligned}$$

851 ## 3.3. **Aula 09 de maio de 2018.** [15]

852 3.3.1. *Desigualdade de Janson.* Seja $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ um conjunto finito e $0 \leq p_1, \ldots, p_n \leq 1$.

[15] Notas produzidas por Felix Liu e Gabriel Lasso.

Nesta seção, definimos $\Gamma_{p_1,\dots,p_n}$ como sendo o espaço de probabilidade $(\mathcal{P}(\Gamma), \mathbb{P})$, onde para $F \subseteq \Gamma$ definimos

$$\mathbb{P}(F) = \left(\prod_{\gamma_i \in F} p_i\right)\left(\prod_{\gamma_i \notin F} (1-p_i)\right).$$

Informalmente, podemos considerar que F é obtido de $\Gamma_{p_1,\dots,p_n}$ tomando cada elemento γ_i com probabilidade independente p_i. Por conveniência, também chamaremos de $\Gamma_{p_1,\dots,p_n}$ um conjunto obtido dessa distribuição.

Definição 86. *Dada uma função $f : \mathcal{P}(\Gamma) \to \mathbb{R}$, dizemos que f é*

- *crescente, se $f(A) \leq f(B)$ para todo $A \subseteq B \subseteq \Gamma$; e*
- *decrescente, se $f(A) \geq f(B)$ para todo $A \subseteq B \subseteq \Gamma$.*

Definição 87. *Seja $\mathcal{F} \subseteq \mathcal{P}(\Gamma)$. Dizemos que $\mathcal{F}$ é*

- *crescente, se $A \in \mathcal{F}$ e $A \subseteq B$ implica que $B \in \mathcal{F}$ para todo $A, B \subseteq \Gamma$; e*
- *decrescente, se $A \in \mathcal{F}$ e $A \supset B$ implica que $B \in \mathcal{F}$ para todo $A, B \subseteq \Gamma$; e*

Teorema 88 (Fortuin, Kasteleyn, Ginibre/Harris)**.** *Sejam X_1 e X_2 VAs, ambas crescentes ou ambas decrescentes. Então X_1 e X_2 são positivamente correlacionadas, ou seja*

$$\mathbb{E}(X_1 X_2) \geq \mathbb{E}(X_1)\mathbb{E}(X_2).$$

Note que se $\mathcal{F} \subseteq \mathcal{P}(\Gamma)$ é uma família crescente, então $\mathbb{1}_{\{A \in \mathcal{F}\}}$ é uma função crescente. Analogamente, se $\mathcal{F}$ é decrescente, então $\mathbb{1}_{\{A \in \mathcal{F}\}}$ também é decrescente. Dessas observações, segue o seguinte corolário.

Corolário 89. *Se $\mathcal{F}, \mathcal{G} \subseteq \mathcal{P}(\Gamma)$ são ambos crescentes ou ambos decrescentes, então*

$$\mathbb{P}(\Gamma_{p_1,\cdots,p_n} \in \mathcal{F} \cap \mathcal{G}) \geq \mathbb{P}(\Gamma_{p_1,\cdots,p_n} \in \mathcal{F})\mathbb{P}(\Gamma_{p_1,\cdots,p_n} \in \mathcal{G}).$$

Exemplo 90. Podemos considerar $G(n,p)$ como sendo o grafo cujo conjunto de vértices é $[n]$ e cujas arestas são obtidas de $\binom{[n]}{2}_{p,\dots,p}$. Sejam $\mathcal{F} = \{\chi(G(n,p) \geq 3)\}$ e $\mathcal{G} = \{G(n,p) \text{ é hamiltoniano}\}$. Então vale que $\mathbb{P}(\mathcal{F} \cap \mathcal{G}) \geq \mathbb{P}(\mathcal{F})\mathbb{P}(\mathcal{G})$.

Dados dois conjuntos A, F, definimos a variável aleatória $I_A = \mathbb{1}_{\{A \subseteq F\}}$. Sejam $\mathcal{S} \subseteq \mathcal{P}(\Gamma)$ e $X = \sum_{A \in \mathcal{S}} I_A$. Segue o seguinte corolário.

Corolário 91. *É verdade que*

$$\mathbb{P}(X = 0) \geq \exp\left\{-\frac{\mathbb{E}(X)}{1 - \max_i p_i}\right\}$$

Demonstração. Observe que, dado $F = \Gamma_{p_1,\dots,p_n}$, $X(F) = 0$ se e somente se $\forall A \in \mathcal{S}, A \not\subseteq F$. Assim, também podemos afirmar que

$$\{X = 0\} = \bigcap_{A\in\mathcal{S}} \{A \not\subseteq \Gamma_{p_1,\dots,p_n}\}.$$

Então

$$\mathbb{P}(X = 0) = \mathbb{P}\left(\bigcap_{A\in\mathcal{S}} \{A \not\subseteq \Gamma_{p_1,\dots,p_n}\}\right).$$

Por 88, segue que

$$\mathbb{P}(X = 0) \geq \prod_{A\in\mathcal{S}} \mathbb{P}(A \not\subseteq \Gamma_{p_1,\dots,p_n}) = \prod_{A\in\mathcal{S}} (1 - \mathbb{P}(A \subseteq \Gamma_{p_1,\dots,p_n})) = \prod_{A\in\mathcal{S}} (1 - \prod_{i\in A} p_i).$$

E então

$$\begin{aligned}\mathbb{P}(X = 0) &\geq \prod_{A\in\mathcal{S}} \exp\left\{-\frac{\prod_{i\in A} p_i}{1 - \prod_{i\in A} p_i}\right\} \\ &\geq \prod_{A\in\mathcal{S}} \exp\left\{-\frac{\mathbb{E}(I_A)}{1 - \max_{i\in A} p_i}\right\} = \exp\left\{-\frac{\sum_{A\in\mathcal{S}} \mathbb{E}(I_A)}{1 - \max_{i\in A} p_i}\right\} = \exp\left\{-\frac{\mathbb{E}(X)}{1 - \max_{i\in A} p_i}\right\}.\end{aligned}$$

□

Seja

$$\overline{\Delta} = \sum_{\substack{A,B\in\mathcal{S} \\ A\cap B\neq\varnothing}} \sum \mathbb{E}(I_A I_B) = \sum_{A\in\mathcal{S}} \mathbb{E}(I_A) + \sum_{\substack{A,B\in\mathcal{S} \\ A\cap B\neq\varnothing, A\neq B}} \sum \mathbb{E}(I_A I_B) = \mathbb{E}(X) + 2\Delta,$$

onde $\Delta = \frac{1}{2} \sum \sum_{A,B\in\mathcal{S}, A\cap B\neq\varnothing, A\neq B} \mathbb{E}(I_A I_B)$.

Teorema 92 (Janson '90)**.** *Para todo $0 \leq t \leq \mu$, é verdade que*

$$\mathbb{P}(X < \mu - t) \leq \exp\left\{-\varphi\left(\frac{-t}{\mu}\right)\frac{\mu^2}{\overline{\Delta}}\right\} \leq \exp\left\{-\frac{t^2}{2\overline{\Delta}}\right\}.$$

Teorema 93 (Janson, Łuczak e Rucinski '90)**.** *As seguintes desigualdades são verdadeiras.*

(1) $\mathbb{P}(X = 0) \leq \exp\{-\mu + \Delta\}$*; e*

(2) $\mathbb{P}(X = 0) \leq \exp\left\{-\frac{\mu^2}{\mu+2\Delta}\right\} = \exp\left\{-\frac{\mu^2}{\overline{\Delta}}\right\}$.

Exemplo 94. Revisitemos a questão dos subgrafos de $G(n,p)$ (2.2).

Anteriormente, concluímos que, dado um grafo H,

$$\lim_{n\to\infty} \mathbb{P}(H \subseteq G(n,p)) = \begin{cases} 0, \text{ se } p << n^{-\frac{1}{m(H)}}; \\ 1, \text{ se } p >> n^{-\frac{1}{m(H)}}; \end{cases}$$

onde $m(H) = \max\left\{\frac{e(J)}{v(J)} : J \subseteq H, v(J) > 0\right\}$.

Pelas desigualdades que vimos nesta seção, podemos encontrar cotas para $\mathbb{P}(H \not\subseteq G(n,p))$.

Sejam G e H dois grafos, onde $|V(G)|= n$. A cada função injetora $f : V(H) \to V(G)$ podemos associar um conjunto $S_f = \{f(u)f(v) : uv \in E(H)\} \subseteq \binom{V(G)}{2}$. Para que f seja um homomorfismo de H em G, basta que $S_f \subseteq E(G)$. Tomando $\mathcal{S}_H = \{S_f : f : V(H) \to V(G), f \text{ é injetora}\}$ e $I_S = \mathbb{1}_{\{S\subseteq E(G)\}}$, temos que $X_H = \sum_{S\in\mathcal{S}_H} I_S$ é o número de homomorfismos de H presentes em G. Assim, temos que $\mathbb{P}(H \not\subseteq G(n,p)) = \mathbb{P}(X_H = 0)$.

Definimos $\Phi_H = \Phi(n,p) = \min\{\mathbb{E}(X_J) : J \subseteq H\}$. Seja então $J \subseteq H$ tal que $\mathbb{E}(X_J) = \Phi_H$. Claramente, $\mathbb{P}(H \not\subseteq G(n,p)) \geq \mathbb{P}(J \not\subseteq G(n,p))$. Considerando $\Gamma = \binom{[n]}{2}$, $m = \binom{n}{2}$ e $p_1 = \cdots = p_m = p$, podemos aplicar a desigualdade em 91, de onde obtemos que

$$\mathbb{P}(H \not\subseteq G(n,p)) \geq \mathbb{P}(J \not\subseteq G(n,p)) \geq \exp\left\{-\frac{\mathbb{E}(X_J)}{1-p}\right\} = \exp\left\{-\frac{1}{1-p}\Phi_H\right\}.$$

Obtendo assim uma cota inferior. Para uma cota superior, podemos aplicar uma desigualdade de 93, obtendo

$$\mathbb{P}(H \not\subseteq G(n,p)) \leq \exp\left\{-\frac{(\mathbb{E}(X_H))^2}{\overline{\Delta}}\right\}.$$

Como neste caso

$$\overline{\Delta} = \sum_{\substack{S_{f'},S_{f''}\in\mathcal{S}_H \\ S_{f'}\cap S_{f''}\neq\varnothing}}\sum \mathbb{E}(I_{S_{f'}} I_{S_{f''}}) \leq c_H \frac{(\mathbb{E}(X_H))^2}{\Phi_H};$$

temos que

$$\mathbb{P}(H \not\subseteq G(n,p)) \leq \exp\{-c_H\Phi_H\}.$$

3.3.2. *Desigualdade de McDiarmid.* Dados conjuntos $A_1, \ldots, A_n$, dizemos que uma função $f : \prod_{k=1}^n A_k \to \mathbb{R}$ é $(c_k)_{k=1}^n$-lipschitz se $|f(X) - f(X')|\leq c_k$ sempre que X e X' diferem apenas na k-ésima coordenada.

Teorema 95 (Desigualdade de McDiarmid)**.** *Sejam $X_1, \ldots, X_n$ v.a.s independentes, seja f uma função $(c_k)_{k=1}^n$-lipschitz; e seja Y a v.a. dada por $Y = f(X_1, \ldots, X_n)$. Então para todo $t > 0$,*

(1) $\mathbb{P}(Y - \mathbb{E}(Y) \geq t) \leq \exp\left\{-\frac{2t^2}{\sum c_k^2}\right\}$; *e*

(2) $\mathbb{P}(Y - \mathbb{E}(Y) \leq -t) \leq \exp\left\{-\frac{2t^2}{\sum c_k^2}\right\}$.

A desigualdade de McDiarmid é também conhecida como *bounded differences inequality.*

Exemplo 96. Seja $f(x) = \sum x_k$ e considere $X_i \sim \text{Be}(p)$ v.a.s independentes. Então $Y \sim \text{Bi}(n,p)$; e obtemos $\mathbb{P}(Y \geq \mathbb{E}(Y) + t) \leq \exp\left\{-\frac{2t^2}{n}\right\}$.

Exemplo 97 (Número cromático de grafos aleatórios)**.** Seja $V = [n]$ e $\Gamma = \binom{V}{2}$. Cada $x \in \{0,1\}^\Gamma$ está associado a um grafo G_x, a saber, aquele tal que $x_e = 1 \Leftrightarrow e \in E(G_x)$.

Com essa representação, podemos analisar parâmetros de grafos na forma de funções $f : \{0,1\}^\Gamma \to \mathbb{R}$. Por exemplo, tome $f(x) = \chi(G_x)$. Neste caso, f é 1-lipschitz, uma vez que adicionar ou remover uma única aresta num dado grafo altera seu número cromático em no máximo 1.

Seja g um parâmetro de grafos. Dizemos que g é concentrado em um intervalo de largura s se existe u tal que $\lim_{n\to\infty} \mathbb{P}(u \leq g(G(n,p)) \leq u+s) = 1$, onde $u = u(n,p)$ e $s = s(n,p)$.

Teorema 98 (Shamir e Spencer '87)**.** *Para todo $p = p(n)$, $\chi(G(n,p))$ é concentrado em um intervalo de largura $\omega\sqrt{n}$, para todo $\omega \to \infty$ com $n \to \infty$.*

Com a codificação que temos para grafos, obtemos de McDiarmid que

$$\mathbb{P}(|Y - \mathbb{E}(Y)| \geq t) \leq 2\exp\left\{-\frac{2t^2}{\binom{n}{2}}\right\}.$$

Isso não nos fala muito: para que a exponencial tenda a zero, precisamos que $t^2 >> n^2$.

Considere a seguinte codificação alternativa. Associe a cada vértice k o conjunto $A_k = \mathcal{P}(\{\{i,k\} : i < k\})$, de todos os conjuntos possíveis de arestas entre k e algum vértice anterior. Existe uma relação biunívoca entre $x \in \prod A_k$ e $G_x = G([n], E)$: basta tomar $E = \bigcup x_k$. Observe que $f(x) = \chi(G_x)$ continua sendo uma função 1-lipschitz, uma vez que diferir em uma única coordenada equivale a adicionar ou remover arestas todas vizinhas a um mesmo vértice. Por McDiarmid, obtemos

$$\mathbb{P}(|\chi(G(n,p)) - \mu| \geq t) \leq 2\exp\left\{-\frac{2t^2}{n-1}\right\},$$

cujo lado direito tende a zero com $\frac{t}{\sqrt{n}} \to \infty$.

3.4. **Aula 14 de maio de 2018.** [16]

Problema básico: $\chi(G(n, \frac{1}{2})) = ?$

Fato 99. *Sabemos (pelo método do 1º momento) que $\chi(G(n,\frac{1}{2})) \geq (\frac{1}{2} + o(1))\dfrac{n}{\log_2(n)}$, pois $\alpha(G(n,\frac{1}{2})) \leq (2 + o(1))\log_2(n)$.*

Teorema 100 (Grimmett & McDiarmid '75)**.** $\chi(G(n,\frac{1}{2})) \leq (1 + o(1))\dfrac{n}{\log_2(n)}$.

[16] Notas produzidas por Rafael Zuolo e André Nakazawa

Teorema 101 (Bollobás '88)**.**

$$\chi(G(n,1/2)) \;=\; (1/2+o(1))\frac{n}{\log_2(n)}$$

938 *Ademais, se* $0<p<1$ *é constante, então*

$$\chi(G(n,p)) \;=\; (1/2+o(1))\frac{n}{\log_b(n)},$$

939 *onde* $b=\dfrac{1}{1-p}$.

940 *Demonstração.* (Teorema 101): aplicação de martingais.

$$\textit{Objetivo: } \chi(G(n,1/2)) \le (1/2+o(1))\frac{n}{\log_2(n)}.$$

941 Basicamente, queremos provar que, para todo $\varepsilon>0$,

$$\mathbb{P}(\alpha(G(n,1/2))<(2-\varepsilon)\log_2(n)) \ll 2^{-n^{2+o(1)}}.$$

942 Seja X_k o número de conjuntos independentes de cardinalidade k em $G(n,1/2)$. Temos $\mu_k =$
943 $\mathbb{E}(X_k)=\binom{n}{k}2^{-\binom{k}{2}}$. Se $k\ll\sqrt{n}$, então, pela fórmula de Stirling temos que

$$\mu_k = n^k\frac{\prod_{j=0}^{k-1}(1-j/n)}{(1+o(1))(k/e)^k\sqrt{2\pi k}}2^{-k(k-1)/2} \sim \left(\frac{1}{(2\pi k)^{\frac{1}{2k}}}\frac{en}{k}2^{-(k-1)/2}\right)^k = \bar{\mu}(k),$$

944 pois $\prod_{j=0}^{k-1}(1-j/n)\sim 1$. Suponha $x\in\mathbb{R}$ tal que $\bar{\mu}(x)^{1/x}=1$. Então, como $(2\pi x)^{\frac{1}{2x}}=1+o(1)$,
945 segue que

$$n=(1+o(1))\frac{x}{e}2^{(x-1)/2}=(1+o(1))2^{(x-1)/2+\log_2(x/e)}=(2^{\frac{1}{2}})^{x(1+o(1))}.$$

946 Assim, $x=(2+o(1))\log_2(n)$. Ademais, temos

$$\frac{\mu_k}{\mu_{k-1}}=\frac{\binom{n}{k}}{\binom{n}{k-1}}2^{-\binom{k}{2}+\binom{k-1}{2}}=\frac{n-k+1}{k}\frac{1}{2^{k-1}}$$

947 Se $k\sim(2+o(1))\log_2(n)$, então

$$\frac{\mu_k}{\mu_{k-1}}\sim\frac{n}{k}\frac{2}{2^k}\sim\frac{n}{2\log_2(n)}\frac{2}{n^{2+o(1)}}=n^{-1+o(1)}.$$

948 Seja $k_0=k_0(n)$ tal que $\mu_{k_0-1}\ge 1>\mu_{k_0}$. Teríamos $\mu_{k_0}\ge n^{-1+o(1)}$ e, assim, $\mu_{k_0-4}\ge n^{3+o(1)}$.
949 Definimos $k=k(n)=k_0-4$. Temos $k\sim 2\log_2(n)$.

950 **Lema 102.** $\mathbb{P}(X_k=0)=\mathbb{P}(\alpha(G(n,1/2))<k)\le exp\{-\dfrac{n^2}{32(\log_2(n))^4}\}$.

Demonstração. Usando Janson: $\mathbb{P}(X_k = 0) \leq \exp\{-\mu_k^2/\bar{\Delta}\}$ onde, tomando $V = V(G(n, 1/2))$,

$$\bar{\Delta} = \sum_{\substack{A\subseteq V\\|A|=k}} \sum_{\substack{B\subseteq V\\|B|=k\\\binom{A}{2}\cap\binom{B}{2}\neq\varnothing}} \mathbb{E}(I_A I_B)$$

em que, dado $A \subseteq V$, definimos $I_A = \{A \text{ é independente}\}$. Seja

$$\Delta = \frac{1}{2} \sum_{\substack{A\subseteq V\\|A|=k}} \sum_{\substack{A\neq B\subseteq V\\|B|=k\\\binom{A}{2}\cap\binom{B}{2}\neq\varnothing}} \mathbb{E}(I_A I_B).$$

951 Temos $\bar{\Delta} = \mu_k + 2\Delta$.

Fato 103.

$$\Delta = \left(\frac{1}{2} + o(1)\right) \mu_k^2 \frac{k^4}{n^2}$$

Demonstração.

$$2\Delta = \sum_{\substack{A\subseteq V\\|A|=k}} \sum_{\substack{A\neq B\subseteq V\\|B|=k\\\binom{A}{2}\cap\binom{B}{2}\neq\varnothing}} \mathbb{P}(I_A I_B = 1) = \sum_{\substack{A\subseteq V\\|A|=k}} \sum_{i=2}^{k-1} \binom{k}{i}\binom{n-k}{k-i} 2^{-(2\binom{k}{2}-\binom{i}{2})} = \binom{n}{k} 2^{-\binom{k}{2}} \Delta^*,$$

952 tomando $\Delta^* = \sum_{2\leq i<k} \binom{k}{i}\binom{n-k}{k-i} 2^{-\binom{k}{2}+\binom{i}{2}}$.

Assim, temos

$$\frac{\Delta^*}{\mu_k} = \sum_{2\leq i<k} \frac{\binom{k}{i}\binom{n-k}{k-i}}{\binom{n}{k}} 2^{\binom{i}{2}}$$

. Considere $g(i) = \dfrac{\binom{k}{i}\binom{n-k}{k-i}}{\binom{n}{k}} 2^{\binom{i}{2}}$, de modo que $\dfrac{\Delta^*}{\mu_k} = \sum_{2\leq i<k} g(i)$. Temos

$$g(2) = \frac{\binom{k}{2}\binom{n-k}{k-2}}{\binom{n}{k}} 2^{\binom{2}{2}} = \frac{\binom{k}{2}}{\frac{n(n-1)}{k(k-1)}} \frac{\binom{n-k}{k-2}}{\binom{n-2}{k-2}} \sim \frac{k^4}{n^2}$$

e

$$g(k-1) = \frac{\binom{k}{k-1}\binom{n-k}{k-(k-1)}}{\binom{n}{k}} 2^{\binom{k-1}{2}} = \frac{k(n-k)}{\binom{n}{k}} \frac{2^{-(k-1)}}{2^{-\binom{k}{2}}} = (2 + o(i)) \frac{kn2^{-k}}{\mu_k}.$$

953 Observe que $g(i)$ é convexo.

954 **Fato 104.** $\max\{g(i) : 2 \leq i < k\} = \max\{g(2), g(k-1)\}$

Demonstração. Temos que $\frac{g(3)}{g(2)}$, $\frac{g(4)}{g(3)}$, $\frac{g(n-3)}{g(n-2)}$ e $\frac{g(n-2)}{g(n-1)}$ são $O(\frac{k^2}{n})$, sendo que $\frac{k^2}{n} < 1$ para n suficientemente grande. Ademais, se $5 \leq i \leq k-4$, temos

$$\frac{g(i+1)g(i-1)}{g(i)^2} = 2\left(\frac{k-i}{k-i+1}\right)^2 \frac{i}{i+1}\frac{n-2k+i}{n-2k+i+1} \geq 17/16 > 1.$$

□

Portanto, $g(2) \sim \frac{(2\log_2 n)^4}{n^2}$ e $g(k-1) \sim \frac{n2^{-(2+o(1))\log_2 n}}{n^3+o(1)} = n^{-4+o(1)}$.

Segue então que $\frac{\Delta^*}{\mu_k} = (1+o(1))g(2)$ tendo $max\{g(i) : 2 \leq i < k\} = g(2)$ e $(k/n^2)g(2) = o(1)$, donde concluímos $\Delta = \left(\frac{1}{2}+o(1)\right)\mu_k^2\frac{k^4}{n^2}$. □

Por Janson, $\mathbb{P}(\alpha(G(n.1/2)) < k) = \mathbb{P}(X_k = 0) \leq exp\{-\frac{\mu_k^2}{\mu_k+2\Delta}\}$ Como $\mu_k << 2\Delta$,

$$exp\{-\frac{\mu_k^2}{\mu_k+2\Delta}\} = exp\{-\frac{\mu_k^2}{(1+o(1))2\Delta}\} = exp\{-\frac{(1+o(1))n^2}{k^4}\} \leq exp\{-\frac{n^2}{17(\log_2 n)^4}\},$$

concluindo o Lema. □

Se $m = \left\lfloor \frac{n}{(\ln n)^2} \right\rfloor$, então $k = k(m) = k_0(m) - 4 = (2+o(1)\log_2 m) = (2+o(1))\log_2(n)$. Seja $B_W = \{\alpha(G(n,1/2)[W]) < k(m)\}$, $W \subseteq V = V(G(n,1/2))$ com $|W| = m$. Temos que

$$\mathbb{P}(B_W) \leq exp\{-\frac{m^2}{17(\log_2 m)^4}\} = e^{-n^{2+o(1)}}.$$

Assim,

$$\mathbb{P}(\exists W \in V, |W| = m; \alpha(G(n,1/2)[W]) < k(m)) \leq \binom{n}{m} e^{-n^{2+o(1)}} \leq 2^n e^{-n^{2+o(1)}} = o(1).$$

Seja $G = G^n$ tal que para todo $W \subseteq V(G)$ com $|W| = m$, $\alpha(G[W]) \geq k(m)$. Vimos que $G(n,1/2)$ é um tal G com probabilidade $1-o(1)$. Ademais, temos

$$\chi(G) \leq \frac{n}{k(m)} + m = \frac{n}{(2+o(1))\log_2 n} + \frac{n}{(\log_2 n)^2} = \frac{n}{(2+o(1))\log_2(n)}.$$

□

3.5. **Aula 16 de maio de 2018.** [17]

3.5.1. *Prova do teorema de Bollobás via diferenças limitadas.* A demonstração via diferenças limitadas faz uso do seguinte lema crucial:

[17] Notas produzidas por Ângelo Lovatto e Rodrigo Enju

964 **Lema 105.** *Para $k = k(n)$, temos*

$$\mathbb{P}(\alpha(G(n,1/2)) < k) \leq e^{-n^{2+o(1)}}$$

965 *Demonstração.* (Lema 105)

966 Seja $\mu_k = \binom{n}{k} 2^{-\binom{k}{2}}$ a esperança do número de conjuntos independentes de $G(n,1/2)$ com k

967 elementos. Seja $Y_k = \#$ conjuntos independentes com k elementos. Queremos mostrar que

$$\mathbb{P}(Y_k = 0) \leq e^{-n^{2+o(1)}},$$

968 ou seja, quase certamente $\alpha(G(n,1/2)) \geq k$. Observe que $\mu_k = \mathbb{E}(Y_k) \geq n^{3+o(1)}$.

969 Se Y_k fosse Lipchitz, a prova estaria concluída, porém, note que cada grafo em $G = G^n$ é um

970 ponto de $\{0,1\}^{\binom{n}{2}}$, que não tem diferenças limitadas.

971 Bollobás então considera a variável aleatória

$$Z_k = \max\{|\mathcal{F}|\text{: } \mathcal{F}\text{família de k-conjuntos independentes 2-a-2 pares disjuntos}\}.$$

972 Esta variável aleatória é 1-Lipschitz.

973 Queremos mostrar que $\lambda = \mathbb{E}(Z_k) \geq n^{2+o(1)}$. Note que se isto vale, então por McDiarmid, o

974 lema 105 vale.

975 De fato, $\lambda = \mathbb{E}(Z_k) \geq cn^2/(\log_2 n)^4$. □

Fato 106.

$$\lambda = \mathbb{E}(Z_k) \geq c\frac{n^2}{(log_2 n)^4}$$

976 *Demonstração.* (Fato 106)

977 Pomos

$$\Delta = \frac{1}{2} \sum_{\substack{A^k \\ |A\cap B|\geq 2}} \sum_{B^k \neq A} \mathbb{E}(\mathbb{1}_A \mathbb{1}_B) \sim \frac{1}{2}\mu^2 \frac{k^4}{n^2},$$

978 onde $\mu = \mu_k$.

979 Seja $\mathbb{1} = \mathbb{1}^k$ uma família de k-conjuntos independentes em $G(n,1/2)$. Seja também

$$\mathcal{P} = \{\{A,B\} : A,B \in \mathbb{1}^k, A \neq B, |A \cap B| \geq 2\}.$$

980 Seja $0 < q < 1$ e considere $\mathbb{1}' = \mathbb{1}_q \subseteq \mathbb{1}$. Seja

$$\mathcal{P}' = \{\{A,B\} : A,B \in \mathbb{1}_q, A \neq B, |A \cap B| \geq 2\}.$$

Para cada dois conjuntos de $\mathbb{1}'$ com 2 ou mais elementos em comum, podemos remover um dos conjuntos, obtendo uma família de conjuntos disjuntos. Portanto, temos

$$Z_k \geq |\mathbb{1}'| - |\mathcal{P}'|.$$

Temos que $\mathbb{E}(|\mathbb{1}'|) = \mu_k q$. Ademais, $\mathbb{E}(|\mathcal{P}'|) = \Delta q^2$, pois note que $\Delta = \mathbb{E}(|\mathcal{P}|)$, e cada elemento sobrevive com probabilidade q, logo cada par sobrevive com probabilidade q^2. Então

$$\Delta q^2 \sim \frac{1}{2}\mu^2 \frac{k^4}{n^2} q^2.$$

Assim, $\mathbb{E}(Z_k) \geq \mathbb{E}(|\mathbb{1}'|) - \mathbb{E}(|\mathcal{P}'|) = \mu_k q - \Delta q^2 = (\mu_k - \Delta q)q$

Tomamos $q = \mu_k / 2\Delta \ll 1$. Concluímos que

$$\begin{aligned} \mathbb{E}(Z_k) = \mathbb{E}(Z_k) &\geq q\frac{\mu_k}{2} = \frac{\mu_k^2}{4\Delta} \\ &\sim \frac{\mu_k^2}{(2\mu_k^2 k^2/n^2)} \\ &= \frac{1}{2}\frac{n^2}{k^2} \sim \frac{1}{32}\frac{n^2}{(\log_2(n))^4}. \end{aligned}$$

□

3.5.2. *Concentração de χ e ω.*

(1) Concentração de ω.

Seja $0 < p < 1$ fixo. Existe uma função inteira $r = r_p(n)$ tal que

$$\lim_{n\to\infty} \mathbb{P}(r - 1 \leq \omega(G(n,p)) \leq r) = 1.$$

Ou seja, ω está concentrado em dois valores.

Observação 107. $r \sim 2\log_b(n), b = 1/p$.

Vamos observar que provamos algo um pouco mais fraco. Seja k_o tal que $\mu_{k_0} - 1 \geq 1 \geq \mu_{k_0}$ e $k = k_0 - 4$. Temos que

$$\mathbb{P}(\omega < k) \to 0 (n \to \infty).$$

Isto é, $\omega \geq k$ quase sempre. Por outro lado, $\mu_{k_0+1} = n^{-1+o(1)}$, logo $\mu_{k_0} \leq n^{-1+o(1)}$. Assim,

$$\mathbb{P}(\omega \geq k_0 + 1) \to 0 (n \to \infty).$$

Concluímos que $k_0 - 4 \leq \omega \leq k_0$ vale com probabilidade tendendo a 1, conforme $n \to \infty$.

(2) Concentração de χ.

Seja a VA X a concentração com largura $\mathbb{1} = \mathbb{1}(n,p)$, se existe $u = u(n,p)$ tal que

$\lim_{n\to\infty} \mathbb{P}(u \le X(G(n,p)) \le u+s) = 1.$

Teorema 108. *(Shamir e Spencer, 1987)*

Suponha $p = p(n) = n^{-\alpha}$, onde $0 < \alpha < 1$ é uma constante.

(i) Se $0 < \alpha < 1/2$, então $\chi(G(n,p))$ está concentrado em largura $s = n^{-\alpha+1/2}\omega(n)$, para uma função ω que tende para ∞ quando $n \to \infty$.

(ii) Se $1/2 < \alpha < 1$, então $\chi(G(n,p))$ está concentrado em um intervalo com $s = \lfloor (2\alpha+1)/(2\alpha-1) \rfloor$ inteiros.

Observação 109. Para $\alpha > 1/2$, de fato $\chi(G(n,p))$ é concentrado em dois valores (Tuczale (91), Alon e Krivelevich (97)).

Demonstração. (Teorema 108) - Técnica de Frieze/Tuczale.

Seja $\omega = \omega(n) \to \infty$ arbitrário. Seja $u = u(n)$ o menor inteiro tal que $\mathbb{P}(\chi(G(n,p)) \le u) \ge 1/\omega$. Dado $G = G^n$, seja $f(G)$ o tamanho mínimo de um conjunto de vértices $W \subseteq V(G)$ tal que $\chi(G-W) \le u$. Então tomamos $Z = f(G(n,p))$.

Observe que f é 1-Lipschitz em relação à codificação $G \leftrightarrow x \in \prod_{k=2}^{n} A_k$.

Assim,

$$\mathbb{P}(|Z - \mathbb{E}(Z)| \ge t) \le 2e^{-2t^2/n}.$$

Temos

$$\frac{1}{\omega} \le \mathbb{P}(\chi(G(n,p)) \le u) \le \mathbb{P}(Z=0) \le 2e^{-2\mu^2/2},$$

onde $\mu = \mathbb{E}(Z)$. Assim, reordenando os termos, temos que $\mu < \omega n^{1/2}$ para n grande.

Portanto,

$$\mathbb{P}(Z \ge 2\omega n^{1/2}) \le e^{-\frac{2(n^{1/2}\omega)^2}{n}} \to 0,$$

pois $\omega(n) \to \infty$ $(n \to \infty)$. E assim, $\mathbb{P}(\chi(G(n,p)-W) \le u$ para algum $|W| < 2n^{1/2}\omega) = 1 - o(1)$. Segue que $\mathbb{P}(u \le \chi(G(n,p))) \le u + 2n^{1/2}\omega) = 1 + o(1)$, pois podemos colorir cada vértice de W com uma nova cor.

E o lema a seguir mostra W pode ser colorido com até s cores, logo $\mathbb{P}(u \le \chi(G(n,p))) \le u+s) = 1 + o(1)$. □

Lema 110. *Quase certamente, $G(n,p)$ é tal que para todo $W \subseteq V(G(n,p))$, com $|W| \le 2n^{1/2}\omega$, temos que $\chi(G(n,p)[W]) \le s$, onde s é tal como no teorema 108.*

3.6. **Aula 05 de maio de 2018.** [18]

3.6.1. *Lema da aula passada.* Na última aula provamos que o número cromárico de $G(n,p)$, com $p = n^{-}\alpha$, $0 < \alpha < 1$ constante, é concentrado com largura s, onde

- $s = n^{1/2-\alpha}\omega$ se $\alpha < \frac{1}{2}$
- $s = \lfloor \frac{2\alpha+1}{2\alpha-1} \rfloor$ se $\alpha > \frac{1}{2}$

com $\omega \to \infty$ e $W \subseteq V(G(n,p)), |W| \leq \omega\sqrt{n}$.

Para isso, ficou faltando provar o seguite lema, que provaremos agora:

Lema 111. *Suponha $p = n^{-}\alpha$, $0 < \alpha < 1$ constante e $\omega \to \infty$.*

Quase todo $G(n,p)$ tem a seguinte propriedade:

- *$\forall W \subseteq V = V(G(n,p))$ com $|W| \leq \omega\sqrt{n}$, $\delta(G[W]) \leq s-1$, onde:*
  - *(1) Se $\alpha < \frac{1}{2}$, $s = 3n^{1/2-\alpha}\omega$*
  - *(2) Se $\alpha > \frac{1}{2}$ e $\omega \leq \ell ogn$, $s = \lfloor \frac{2\alpha+1}{2\alpha-1} \rfloor$*

Demonstração. Vamos estimar a quantidade esperada de $W \subseteq V$ com $|W| \leq \omega\sqrt{n}$ e $\delta(G[W]) \geq s$ e mostrar que esse número é $o(1)$.

Tal número é:

$$\leq \sum_{s<t\leq\omega\sqrt{n}} \binom{n}{t}\binom{\binom{t}{2}}{st/2} p^{st/2}$$

$$\leq \sum_{t} \left(\frac{en}{t}\right)^t \left(\frac{et^2/2}{st/2}p\right)^{st/2}$$

$$= \sum_{t} \left(\frac{en}{t}\frac{e^{s/2}t^{s/2}}{s^{s/2}}n^{-\alpha s/2}\right)^t$$

$$= \sum_{t} \left(\frac{en}{t}\frac{e^{s/2}t^{s/2}}{s^{s/2}}n^{-\alpha s/2}\right)^t$$

$$= \sum_{t} \left(e\frac{e}{2}^{s/2} n^{1-\alpha s/2} t^{s/2-1}\right)^t$$

Seja $b(t) = e\frac{e}{2}^{s/2} n^{1-\alpha s/2} t^{s/2-1}$

$b(t)$ cresce com t, pois $s \geq 3$.

Para $t_0 = \omega/\sqrt{n}$, temos:

$$b(t_0) = e\left(\frac{e}{2}\right)^{\frac{s}{2}} \omega^{\frac{s}{2}-1} n^{1-\alpha\frac{s}{2}+\frac{1}{2}(\frac{s}{2}-1)}$$

$$= e\left(\frac{e}{2}\right)^{\frac{s}{2}} \omega^{\frac{s}{2}-1} n^{\frac{1}{2}-(\alpha-\frac{1}{2})\frac{s}{2}}$$

[18] Notas produzidas por Gabriel Lasso e Rodrigo Enju

- Suponha que $\alpha > \frac{1}{2}$

  Temos

$$\frac{1}{2} - (\alpha - \frac{1}{2})\frac{s}{2} < 0 \iff$$
$$\frac{1}{2} < (\alpha - \frac{1}{2})\frac{s}{2} \iff$$
$$1 < (\alpha - \frac{1}{2})s \iff$$
$$2 < (2\alpha - 1)s \iff$$
$$s > \frac{2}{(2\alpha - 1)}$$

  Tomando o menor $s \in \mathbb{N}$ tal que $s > \frac{2}{(2\alpha-1)}$, temos

$$s = \lfloor \frac{2}{2\alpha - 1} + 1 \rfloor = \lfloor \frac{2\alpha + 1}{2\alpha - 1} \rfloor$$

  Como $\omega < \ell ogn$, para algum $\varepsilon > 0$ vale que $b(\omega\sqrt{n}) \leq n^{-\varepsilon} \to 0$.

  Assim, como

$$b(s) \leq b(s+1) \leq ... \leq b(\omega\sqrt{n}) = n^{-\varepsilon}$$

  Vale que

$$\sum_{s<t\leq\omega\sqrt{n}} b(t)^t \leq \sum_{s<t\leq\omega\sqrt{n}} n^{-\varepsilon t} \leq 2b(s)^s \leq 2n^{-\varepsilon s} = o(1)$$

- Suponha agora que $\alpha < \frac{1}{2}$

  Temos

$$b(t_0) = \frac{e}{\omega}\left(\frac{e\omega}{2}\right)^{\frac{s}{2}} n^{\frac{1}{2}+(\frac{1}{2}-\alpha)\frac{s}{2}}$$

  Se $s = 3n^{1/2-\alpha}\omega$, então

$$b(t_0) = \frac{e}{\omega}\left(\frac{e}{3}\right)^{\frac{s}{2}} n^{\frac{1}{2}}$$

  Tomando o ℓog dos dois lados:

$$\ell ogb(t_0) = \ell og\frac{e}{\omega} - \frac{s}{2}\ell og\left(\frac{3}{e}\right) + \frac{1}{2}\ell ogn \to -\infty$$

  Logo $b(t_0) \to 0$ e, pelo mesmo motivo do caso anterior, $\sum_t b(t)^t = o(1)$.

□

3.6.2. *Martingais.* **Preliminares**

Um espaço de probabidade é uma tripla $(\Omega, \mathcal{F}, \mathbb{P})$ tal que:

- Ω é um conjunto chamado espaço amostral.
- $\mathcal{F}$ é uma σ-álgebra sobre Ω, isto é, $\mathcal{F}$ é uma coleção de subconjuntos de Ω tal que:

(1) $\varnothing \in \mathcal{F}$

(2) $A \in \mathcal{F} \Rightarrow \Omega \setminus A \in \mathcal{F}$ (Fechado por complemento)

(3) $\{E_i\}_{i\in\mathbb{N}} \subseteq \mathcal{F} \Rightarrow \bigcup_i E_i \in \mathcal{F}$ para toda coleção enumerável de elementos de $\mathcal{F}$ $\{E_i\}_{i\in\mathbb{N}}$ (Fechado por união enumerável).

Obs: É fácil mostrar que o fecho por interseção é equivalente ao fecho por união.

- $\mathbb{P}$ é uma função $\mathcal{F} \to \mathbb{R}^+$ respeitando:

(1) $\mathbb{P}(\varnothing) = 0$.

(2) $\mathbb{P}(\bigcup_i E_i) = \sum_i \mathbb{P}(E_i)$ para toda coleção enumerável de elementos de $\mathcal{F}$ $\{E_i\}_{i\in\mathbb{N}}$ disjuntos dois a dois.

(3) $\mathbb{P}(\Omega) = 1$.

Para nós, na vasta maioria dos casos, $|\Omega| < \infty$ e $\mathcal{F} = 2^\Omega$.

Vamos supor nessa seção que $|\Omega| < \infty$.

Se $\mathcal{F}$ é uma σ-álgebra, os membros não vazios minimais de $\mathcal{F}$ formam uma partição de Ω. Reciprocamente, dada uma partição de Ω, podemos definir uma σ-álgebra $\mathcal{F}$ associada a essa partição.

Portanto podemos identificar σ-álgebras sobre Ω com partições de Ω.

Seja X uma variável aleatória e $\mathcal{F}$ uma σ-álgebra sobre Ω. Dizemos que X é $\mathcal{F}$ **mensurável** se X é constante nos blocos da partição associada à $\mathcal{F}$.

Seja X uma variável aleatória e $\mathcal{F}$ uma σ-álgebra sobre Ω. Definimos a esperança conficional $\mathbb{E}(X|\mathcal{F})$ como a variável aleatória $\mathcal{F}$ mensurável tal que

$\mathbb{E}(X|\mathcal{F})(\omega)$ = esperança de X no espaço condicional B_λ onde $\omega \in B_\lambda$ e $(B_\lambda)_{\lambda\in\Lambda}$ é a partição associada à Ω.

Note que $\mathbb{E}(X) = \mathbb{E}(\mathbb{E}(X|\mathcal{F}))$.

Se Y é uma σ-álgebra, definimos $\sigma(Y)$ como sendo a σ-álgebra associada à partição $(Y^{-1}(x))_{x\in\mathbb{R}}$.

Finalmente, $\mathbb{E}(X|Y) = \mathbb{E}(X|\sigma(Y))$

Um **filtro** é uma sequência $(\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2, ...)$ tal que $\{\varnothing, \Omega\} = \mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq ...$

Se $(P_i)_{i\in\mathbb{N}}$ são as partições associadas, então dizemos que P_i refina P_{i-1}.

Fixe um filtro $(\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2, ...)$.

Um **martingal** é uma sequência de variáveis aleatórias $(X_i)_{i\in\mathbb{N}}$ tal que $\mathbb{E}(X_i|\mathcal{F}_{i-1}) = X_{i-1}$.

Uma **sequência de diferenças de martingais (sdm)** é uma sequência de variáveis aleatória $(Y_i)_{i\in\mathbb{N}\setminus\{0\}}$ tal que Y_i é $\mathcal{F}_i$ mensurável e $\mathbb{E}(Y_i|\mathcal{F}_{i-1}) = 0$.

Observação 112. Seja $(X_0, X_1, ...)$ um martingal. Então $(Y_1 = X_1 - X_0, Y_2 = X_2 - X_1, ...)$ é uma sdm.

Demonstração. Fixe i.

Como X_i e X_{i-1} são $\mathcal{F}$ mensuráveis (X_{i-1} é $\mathcal{F}_{i-1}$ mensurável, o que é maus forte), então Y_i também é $\mathcal{F}$ mensurável.

$$\mathbb{E}(Y_i|\mathcal{F}_{i-1}) =$$

$$\mathbb{E}(X_i - X_{i-1}|\mathcal{F}_{i-1}) =$$

$$\mathbb{E}(X_i|\mathcal{F}_{i-1}) - \mathbb{E}(X_{i-1}|\mathcal{F}_{i-1}) =$$

$$X_{i-1} - X_{i-1} = 0$$

□

Observação 113. Se X_0 é uma constante e $(Y_1, Y_2, ...)$ é uma sdm, então $(X_0, X_0 + Y_1, X_0 + Y_1 + Y_2, ...)$ é um martingal.

Demonstração. Fixe i.

$$\mathbb{E}(X_i|\mathcal{F}_{i-1}) =$$

$$\mathbb{E}(X_{i-1} + Y_i|\mathcal{F}_{i-1}) =$$

$$\mathbb{E}(X_{i-1}|\mathcal{F}_{i-1}) + \mathbb{E}(Y_i|\mathcal{F}_{i-1}) =$$

$$\mathbb{E}(X_{i-1}|\mathcal{F}_{i-1}) = X_{i-1}$$

□

3.7. Aula 6 de junho de 2018. [19]

3.7.1. *Circuitos 0 (mod k).*

Definição 114. *Seja $D = (V, E)$, com $V \neq \varnothing$,* grafo dirigido (digrafo) *e $E \subseteq V \times V$. Vamos sempre considerar grafos dirigidos sem laços nesta seção, isto é, $\forall v \in V, (v, v) \notin E$. Definimos, para D digrafo e $x \in V$:*

$$d^+(x) = \textit{grau de saída de } x = |\{(x, y) \in E : y \in V\}|$$

$$d^-(x) = \textit{grau de entrada de } x = |\{(y, x) \in E : y \in V\}|$$

$$\Delta^+(D) = max_{x \in V}\{d^+(x)\}$$

$$\Delta^-(D) = max_{x \in V}\{d^+(x)\}$$

$$\delta^+(D) = min_{x \in V}\{d^-(x)\}$$

$$\delta^-(D) = min_{x \in V}\{d^-(x)\}$$

E dizemos que D é d-regular para algum $d \in \mathbb{N}$ se $\Delta^+(D) = \Delta^-(D) = \delta^+(D) = \delta^-(D) = d$.

Teorema 115 (Alon & Linial. 1989)**.** *Seja D um digrafo e $k \geq 2$, inteiro. Se*

$$e(\Delta^-(D)\delta^+(D) + 1)(1 - 1/k)^{\delta^+(D)} \leq 1$$

então D contém um circuito de comprimento $\equiv 0 \mod k$.

Observação 116. Fixe $k = 2$, e suponha D digrafo d-regular. Se $d \geq 8$, então, segue do Teorema 115 que D contém um circuito (de comprimento) par. Ademais, sabe-se que podemos impor restrições mais fracas a d. Friedland mostrou que $d \geq 7$ é suficiente e, posteriormente, Thomassen conseguiu provar o mesmo resultado para $d \geq 3$.

Observação 117. Em 1975, Lovász questionou a existência de um k tal que todo digrafo D com $\delta^+(D) \geq k$ contivesse um circuito par. A inexistência de tal k foi provada por Thomassen em 1985, com a demonstração de que para qualquer escolha de k existe um D com $\delta^+(D) \geq k$ tal que D não contém circuito par. Todavia, também foi mostrado por Thomassen que, para $D = D^n$, se $\delta^+(D) \geq \lfloor \log_2 n \rfloor + 1$ então podemos garantir que D contém circuito par.

Corolário 118. *Para todo digrafo D e $k \geq 2$, se*

$$\Delta^-(D) \leq \frac{1}{e\delta^+(D)}((\frac{k}{k-1})^{\delta^+(D)} - e)$$

[19] Notas produzidas por André Nakazawa e REVISOR?

então D contém um circuito de comprimento $\equiv 0 \mod k$.

Corolário 119. *Todo digrafo D d-regular contém circuito de comprimento $\equiv 0 \mod k$, para todo k tal que*

$$2 \leq k \leq \frac{d}{1+\ln(d^2+1)}.$$

Lema 120. *Seja D um grafo dirigido, e $k \geq 2$, inteiro. Suponha que existe uma função $f : V(D) \to \mathbb{Z}/k\mathbb{Z}$ tal que para todo vértice $v \in V = V(D)$ existe um vértice $u \in \Gamma^+(v) = \{u \in V : (v,u) \in E\}$ com $f(u) = f(v)+1 \mod k$. Então D contém um circuito de comprimento $\equiv 0 \mod k$.*

Demonstração. Considere uma sequência de vértices $s = (v_i)_{i\geq 0}$ tal que $v_0 \in V$ é um vértice qualquer e para todo $i > 0$ tem-se $v_i \in \Gamma^+(v_{i-1})$ e $f(v_i) = f(v_{i-1})+1 \mod k$. Como V é finito, existem $0 \leq i < j$ tais que $v_i = v_j$, logo, tomando j mínimo, temos que $\mathcal{C} = (v_i, v_{i+1}, \cdots, v_j)$ é circuito em D. Além disso, o comprimento de $\mathcal{C}$ é $\equiv 0 \mod k$ pois, caso contrário, teríamos $f(v_i) \neq f(v_j) \mod k$ pela construção de s. □

Demonstração. (Teorema 115). Sem perda de generalidade, tomamos $\delta^+(D) = \Delta^+(D)$. Escolhemos $f : V(D) \to \mathbb{Z}/k\mathbb{Z}$ ao acaso, com $f(v) \in_u \mathbb{Z}/k\mathbb{Z}$ independente entre todos os vértices $v \in V$. Para todo $v \in V$ considere o evento $A_v = \{f(u) \neq f(v)+1 \mod k, \forall u \in \Gamma^+(v)\}$, que impediria a aplicação do Lema anterior. Pela uniformidade da escolha de f temos que

$$\mathbb{P}(A_v) = \mathbb{P}(f(u) \neq f(v)+1 \mod k)^{|\Gamma^+(v)|} = (1-1/k)^{\delta^+(D)}.$$

Seja G o grafo de dependência para os eventos $A_v, v \in V$. Como para todo $v \in V$ temos que A_v é independente de A_u se $u \in U_v$, onde

$$U_v = \{u \in V \setminus \{v\} : (\{u\} \cup \Gamma^+(u)) \cap \Gamma^+(v) = \varnothing\},$$

segue que $\Delta^+(G) \leq \Delta^-(D)\delta^+(D)$, pois para todo $v \in V$

$$|(V \setminus \{v\}) \setminus U_v| \leq \left|\Gamma^+(v)\right| + \left|\bigcup_{w\in\Gamma^+(v)} \Gamma^-(w) \setminus \{v\}\right| \leq \Delta^-(D)\delta^+(D),$$

onde $\Gamma^-(v) = \{u \in V : (u,v) \in E\}$. Logo, pelo Corolário 2 do LLL conclui-se o resultado do Teorema. □

§4. Lema Local de Lovász

4.1. **Aula 11 de junho de 2018: Lema Local de Lovasz Algoritmico.** [20]

4.1.1. *Um fato importante.*

Fato 121 (Princípio da Independência Mútua)**.** *Seja $\mathcal{P}$ um conjunto finito de variáveis aleatórias mutuamente independentes num mesmo espaço de probabilidade. Suponha que todo evento de $\mathcal{A}$ é determinado por um subconjunto dessas variáveis. 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*

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

Então A é mutuamente independente de todos os eventos em $\mathcal{A} \setminus (\Gamma(A) \cup \{A\})$. Em outras palavras, o digrafo $D = (\mathcal{A}, E)$ com conjunto de arestas $E := \{(A, B) : A \in \mathcal{A}, B \in \Gamma(A)\}$ é um digrafo de dependência para $\mathcal{A}$. Note que nesse caso o digrafo é simétrico e, portanto, podemos também falar de um grafo de dependência*.* □

4.1.2. *Cenário geral.*

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 $\Gamma(A)$. Pelo Princípio da Independência Mútua (Fato 121), temos que A é mutuamente independente de

[20] Notas produzidas por Bruno Pasqualotto Cavalar e Gabriel Ferreira Barros.

todos os eventos em $\mathcal{A} \setminus (\Gamma(A) \cup \{A\})$ e D é um digrafo de dependência para $\mathcal{A}$. O celebrado algoritmo de Moser-Tardos é como segue.

Algoritmo 1: Algoritmo de Moser-Tardos

1 **para todo** $P \in \mathcal{P}$ **faça**

2 $\quad v_P \leftarrow$ uma valoração aleatória de P (de acordo com sua distribuição);

3 **enquanto** $\exists A \in \mathcal{A} : A$ *é violado quando* $(P = v_P : \forall P \in \mathcal{P})$ **faça**

4 $\quad$ escolha um evento violado $A \in \mathcal{A}$ de acordo com alguma regra qualquer fixada;

5 $\quad$ **para todo** $P \in \mathrm{vbl}(A)$ **faça**

6 $\quad\quad v_P \leftarrow$ uma nova valoração aleatória de P (de acordo com sua distribuição);

7 **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 é muito grande; ii) valores aleatórios para cada variável $P \in \mathcal{P}$ podem ser eficientemente amostrados; iii) verificar (e encontrar) a ocorrência de um evento também pode ser feito eficientemente. A versão construtiva do LLL de Moser e Tardos trata do primeiro problema.

Teorema 122 (Moser e Tardos [6])**.** *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 $\sum_{A \in \mathcal{A}} \frac{x(A)}{1-x(A)}$.

4.1.3. *A prova.* Antes de provarmos o Teorema 122, precisaremos definir alguns conceitos.

Definição 123. *Seja $C : \mathbb{N} \to \mathcal{A}$ uma função que lista os eventos na ordem em que são reamostrados no algoritmo. Se o algoritmo termina, C é parcialmente definido, apenas até o número total de reamostragens. Chamamos C de* registro *do algoritmo.*

Definição 124. *Uma* árvore-testemunha *$\tau = (T, \sigma_\tau)$ é uma árvore finita enraizada T juntamente com um rotulamento $\sigma_\tau : V(T) \to \mathcal{A}$ tal que se u é filho de v em T então $\sigma_\tau(u) \in \Gamma^+(\sigma_\tau(v))$.*

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* $v \in V(\tau)$ *definimos* $[v] := \sigma_\tau(v)$.

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 $i = t-1, t-2, \ldots, 1$ 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 $\tau = \tau_C(t)$. Para todo vértice $v \in V(\tau)$, denotemos por $d(v)$ a profundidade de v. Definamos também $q(v)$ como o maior $q \in \mathbb{N}$ tal que v está contido em $\tau_C^{(q)}(t)$. Note que, por construção, $C(q(v)) = [v]$.

Lema 125. *Sejam C o registro produzido pelo algoritmo e τ uma árvore-testemunha que ocorre em C. Vale que*

(1) Se vértices $u, v \in V(\tau)$ são tais que $d(u) = d(v)$, então $\mathrm{vbl}([u]) \cap \mathrm{vbl}([v]) = \varnothing$.

(2) A árvore-testemunha τ é própria.

(3) As árvores-testemunha que ocorrem em C são duas-a-duas distintas.

Demonstração. Primeiro, vamos provar os itens i) e ii). Seja τ uma árvore testemunha que ocorre em C. Para algum $t \in \mathbb{N}$, temos $\tau = \tau_C(t)$.

Sejam $u, v \in V(\tau)$. Note que se $q(u) < q(v)$ e $\mathrm{vbl}([u]) \cap \mathrm{vbl}([v]) \neq \varnothing$, então $d(u) > d(v)$, pois na construção de $\tau_C(t)$ o vértice u é colocado como filho de v ou de algum outro vértice com profundidade maior. Desse modo, se $d(u) = d(v)$ então $\mathrm{vbl}([u]) \cap \mathrm{vbl}([v]) = \varnothing$, o que prova o item i). Disto temos que os rótulos dos filhos de um mesmo vértice formam um conjunto independente no grafo de dependência. Em particular, segue que τ é própria. Isso prova o item ii).

Observe agora que, se duas árvores-testemunha tem raízes distintas, então elas são obviamente diferentes; caso contrário, basta notar que, se t_i é o i-ésimo instante de tempo no qual $C(t_i) = A$, então $\tau_C(t_i)$ contém i vértices rotulados com o evento A. Isso prova o item iii). □

Denotemos agora por N_A a variável aleatória que conta o número de vezes que o evento $A \in \mathcal{A}$ foi reamostrado. Defina também $\mathcal{T}_A$ como o conjunto das árvores-testemunha próprias cujas

raízes são rotuladas com o evento A. Pelo Lema 125, temos que

$$N_A = \sum_{\tau \in \mathcal{T}_A} \mathbb{1}[\tau \text{ ocorre em } C],$$

pois a cada aparecimento do evento A no registro C está associada uma única árvore-testemunha distinta de $\mathcal{T}_A$ que ocorre em C. Logo,

$$\mathbb{E}[N_A] = \sum_{\tau \in \mathcal{T}_A} \mathbb{P}[\tau \text{ ocorre em } C]. \tag{12}$$

Deste modo, para limitar $\mathbb{E}[N_A]$ basta limitar $\mathbb{P}[\tau \text{ ocorre em } C]$ para $\tau \in \mathcal{T}_A$. É disso que trata o próximo lema.

Lema 126. *Seja $\tau \in \mathcal{T}_A$ e C o registro (aleatório) produzido pelo algoritmo. Temos que*

$$\mathbb{P}[\tau \text{ ocorre em } C] \leq \prod_{v \in V(\tau)} \mathbb{P}[[v]].$$

Demonstração. Considere o seguinte algoritmo, que chamamos de *τ-verificação*. Em ordem de profundidade decrescente (na mesma profundidade a ordem pode ser arbitrária), visitamos todos os vértices de τ e, para cada $v \in V(\tau)$, atribuímos uma nova valuação aleatória às variáveis em $\mathrm{vbl}([v])$ (independentemente e de acordo com a distribuição de cada variável) e verificamos se a valuação resultante viola o evento $[v]$. Se todos os eventos forem violados, dizemos que a τ-verificação *passou*. Claramente, a τ-verificação passa com probabilidade exatamente $\prod_{v \in V(\tau)} \mathbb{P}[[v]]$. Aqui argumentaremos que o evento de τ ocorrer em C está contido no evento de a τ-verificação passar. Claramente, isso é suficiente para provar o lema.

Para conseguirmos fazer essa análise, consideramos uma leve modificação do algoritmo que em nada altera o seu comportamento. Considere uma tabela cujas colunas são indexadas pelas variáveis de $\mathcal{P}$. Para cada $P \in \mathcal{P}$, a coluna P contém uma sequência infinita $eft(P^{(0)}, P^{(1)}, P^{(2)}, \dots ight)$ de amostras independentes de P, tomadas de acordo com sua distribuição. Toda vez que o algoritmo (o algoritmo de Moser-Tardos ou a τ-verificação) for reamostrar a variável P, basta pegar o próximo valor da coluna P que ainda não foi utilizado. O que mostraremos é que, quando a tabela é a mesma para os dois algoritmos, se τ ocorre em C então a τ-verificação passa.

Suponhamos então que τ ocorre em C, isto é, $\tau = \tau_C(t)$ para algum $t \in \mathbb{N}$. Para todo $P \in \mathcal{P}$ e $v \in V(\tau)$ defina

$$S(P, v) := \{w \in V(\tau) : d(w) > d(v), P \in \mathrm{vbl}([w])\}.$$

Fixemos agora $v \in V(\tau)$. Afirmamos que quando a τ-verificação visita o vértice v e reamostra as variáveis de $\mathrm{vbl}([v])$, a tabela dá o valor $P^{(|S(P,v)|)}$ para $P \in \mathrm{vbl}([v])$. De fato, como a τ-verificação visita os vértices em ordem decrescente de profundidade, antes de visitar o vértice v cada $P \in \mathrm{vbl}([v])$ foi reamostrado exatamente quando os vértices de $S(P, v)$ eram visitados. Além disso, do item 1 do Lema 125 temos que o vértice v é o único com profundidade $d(v)$ que depende das variáves em $\mathrm{vbl}([v])$.

Observemos agora que, quando o algoritmo de Moser-Tardos escolhe o evento $[v]$ no passo $q(v)$ para reamostrar suas variáveis, o evento $[v]$ está violado. Afirmamos que, logo antes dessa reamostragem, a cada $P \in \mathrm{vbl}([v])$ também está atribuído o valor $P^{(|S(P,v)|)}$. Note que, na τ-verificação, depois de as variáveis em $\mathrm{vbl}([v])$ serem reamostradas, a tabela dá exatamente esse valor para cada $P \in \mathrm{vbl}([v])$. Portanto, se a afirmação é verdadeira, teremos que o evento $[v]$ estava violado depois da reamostragem da τ-verificação. Como v é arbitrário, isso é suficiente para concluir que a τ-verificação passou. Basta, portanto, provar a afirmação.

Note agora que, pela própria construção de $\tau_C(t)$, temos que

$$S(P, v) = \{w \in V(\tau) : q(w) < q(v), P \in \mathrm{vbl}([w])\}.$$

Portanto, antes do passo de reamostragem $q(v)$ do algoritmo de Moser-Tardos, as variáveis em $\mathrm{vbl}([v])$ foram reamostradas nos passos $q(w)$ com $w \in S(P, v)$. Como elas também foram amostradas uma vez cada no passo inicial (linha 2), a afirmação segue. Isso termina a prova. □

Falta agora relacionar as árvores-testemunha com as condições do LLL.

4.1.4. *O processo de Galton-Watson e a prova do Teorema 122.* Fixe um evento $A \in \mathcal{A}$ e considere o seguinte processo para gerar uma árvore-testemunha $\tau \in \mathcal{T}_A$. No primeira iteração, construímos uma árvore com apenas um vértíce raíz isolado rotulado com A. Nas iterações subsequentes, consideramos cada vértice produzido na iteração anterior independentemente e, também independentemente, para cada evento $B \in \Gamma^+([v])$ adicionamos a v um vértice filho u tal que $[u] = B$ com probabilidade $x(B)$, e não adicionamos com probabilidade $1 - x(B)$. O processo continua até que uma iteração não produza nenhum vértice (existe, é claro, a possibilidade de que isso nunca aconteça e o processo continue indefinidamente).

Para melhorar a apresentação, defina

$$x'(B) := x(B) \prod_{C \in \Gamma(B)} (1 - x(C)).$$

Note que as hipóteses do LLL são equivalentes a

$$\mathbb{P}[B] \leq x'(B) \quad \text{para todo } B \in \mathcal{A}.$$

Apresentamos agora a probabilidade que o processo acima produza uma árvore $\tau \in \mathcal{T}_A$ fixa.

Lema 127. *Seja $\tau \in \mathcal{T}_A$. A probabilidade p_τ de que o processo acima produza a árvore-testemunha τ é*

$$p_\tau = \frac{1 - x(A)}{x(A)} \prod_{v \in V(\tau)} x'([v]).$$

Demonstração. Para cada $v \in V(\tau)$, defina

$$W_v := \{B \in \Gamma^+([v]) : \nexists\, u \in V(\tau) \text{ filho de } v \text{ tal que } [u] = B\}.$$

Seja $s \in V(\tau)$ a raíz da árvore enraizada de τ. Note que $[s] = A$. Temos que

$$p_\tau = \prod_{C \in W_s} (1 - x(C)) \prod_{v \in V(\tau) \setminus \{s\}} \left(x([v]) \prod_{B \in W_v} (1 - x(B)) \right).$$

Podemos reescrever essa expressão da seguinte forma:

$$p_\tau = \prod_{C \in \Gamma^+(A)} (1 - x(C)) \prod_{v \in V(\tau) \setminus \{s\}} \left(\frac{x([v])}{1 - x([v])} \prod_{B \in \Gamma^+([v])} (1 - x(B)) \right).$$

Podemos colocar o produtório de fora para dentro com um fator de correção, obtendo:

$$\begin{aligned} p_\tau &= \frac{1 - x(A)}{x(A)} \prod_{v \in V(\tau)} \left(\frac{x([v])}{1 - x([v])} \prod_{B \in \Gamma^+([v])} (1 - x(B)) \right) \\ &= \frac{1 - x(A)}{x(A)} \prod_{v \in V(\tau)} \left(x([v]) \prod_{B \in \Gamma([v])} (1 - x(B)) \right) \\ &= \frac{1 - x(A)}{x(A)} \prod_{v \in V(\tau)} x'([v]). \end{aligned}$$

□

Temos agora todos os elementos necessários para completar a prova do Teorema 122.

Prova do Teorema 122. Fixemos $A \in \mathcal{A}$. Usando a equação (12), as hipótestes do Teorema 122 e os lemas 126 e 127, obtemos que

$$\begin{aligned} \mathbb{E}[N_A] &= \sum_{\tau \in \mathcal{T}_A} \mathbb{P}[\tau \text{ ocorre em } C] \leq \sum_{\tau \in \mathcal{T}_A} \prod_{v \in V(\tau)} \mathbb{P}[[v]] \leq \sum_{\tau \in \mathcal{T}_A} \prod_{v \in V(\tau)} x'([v]) \\ &= \frac{x(A)}{1 - x(A)} \sum_{\tau \in \mathcal{T}_A} p_\tau \leq \frac{x(A)}{1 - x(A)}, \end{aligned}$$

como queríamos demonstrar. □

§5. Complexidade de circuitos

5.1. **Aula 13 de junho de 2018: Cotas inferiores para complexidade monótona.** [21]

Circuitos Booleanos são um modelo *não-uniforme* de computação muito estudado em complexidade computacional. Diferentemente do modelo *uniforme* da máquina de Turing, um circuito permite que um algoritmo diferente seja usado para cada tamanho de entrada. Além disso, todo algoritmo polinomial pode ser implementado por uma sequência de circuitos Booleanos de tamanho polinomial. Deste modo, provar uma cota inferior superpolinomial para o tamanho de um menor circuito que computa um problema de decisão em **NP** é suficiente para provar que $\mathbf{P} \neq \mathbf{NP}$.

Definição 128. *Para todo $n \in \mathbb{N}$, um* circuito Booleano *com n entradas e uma saída é um grafo dirigido acíclico com n fontes e um sorvedouro. Todos os vértices que não são fonte são chamados* portas *e são rotulados com um dentre $\{\wedge, \vee, \neg\}$. Os vértices rotulados com $\vee$ ou $\wedge$ tem* fan-in *(isto é, grau de entrada) igual a 2 e os vértices rotulados com $\neg$ tem fan-in 1. Quando todas as portas tem* fan-out *(isto é, grau de saída) no máximo 1, o circuito é chamado* fórmula. *O* tamanho *de um circuito C, denotado por $|C|$, é o número de vértices que ele contém. Se C é um circuito Booleano e $x \in \{0,1\}^n$ é uma entrada, então a* saída *de C em x, denotada por $C(x)$, é definida da maneira natural. Para uma função $f : \{0,1\}^n \to \{0,1\}$, dizemos que C* computa *f se, para todo $x \in \{0,1\}^n$, temos que $f(x) = C(x)$.*

Dado $x \in \{0,1\}^n$, denotaremos o número de bits de valor 1 em x por $|x|_1$. Equivalentemente, $|x|_1 = \sum_i x_i$.

Uma motivação para estudar circuitos Booleanos é a esperança de que, tratando-se de um modelo *finito*, técnicas combinatórias possam ser bem-sucedidas em provar cotas inferiores. Infelizmente, até o momento nenhuma cota inferior superlinear é conhecida para circuitos gerais. A melhor cota inferior geral conhecida é $5n - o(n)$ [5]. Por outro lado, obteve-se até hoje considerável sucesso em provar cotas inferiores para classes restritas de circuitos, como *circuitos monótonos*.

Definição 129. Circuitos monótonos *são circuitos sem portas $\neg$. Dados $x, y \in \{0,1\}^n$, escrevemos $x \leq y$ se $x_i \leq y_i$ para todo $i \in [n]$. Dizemos que uma função Booleana $f : \{0,1\}^n \to \{0,1\}$ é* monótona *se $f(x) \leq f(y)$ sempre que $x \leq y$.*

[21] Notas produzidas por Bruno Pasqualotto Cavalar e REVISOR?.

Observamos que a função computada por um circuito mónotono é sempre monótona, e que toda função monótona é computável por algum circuito monótono.

Denote por $\text{CLIQUE}_{k,n} : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ a função que, dada uma matriz de adjacência de um grafo G de n vértices, vale 1 se, e somente se, G contém um k-clique. A primeira cota inferior superpolinomial para circuitos monótonos foi obtida por Razborov [8] para a função $\text{CLIQUE}_{k,n}$, e posteriormente melhorada por Andreev [2] e Alon e Boppana [1].

Teorema 130 ([1, 2, 8])**.** *Existe uma constante $\varepsilon > 0$ tal que, para todo $k \leq n^{1/4}$, não existe um circuito monótono de tamanho menor que $n^{\varepsilon\sqrt{k}}$ que computa* $\text{CLIQUE}_{k,n}$.

Iremos provar o Teorema para o caso $k = 3$. Mais precisamente, vamos provar o seguinte. Seja $T := T_m := \text{CLIQUE}_{3,m}$.

Teorema 131. *A complexidade monótona de T é $\Omega(m^3/\ln^4 m)$.*

Para uma função booleana f, seja $A(f) := \{x \in \{0,1\}^n : f(x) = 1\}$. Claramente, $A(f \vee g) = A(f) \cup A(g)$ e $A(f \wedge g) = A(f) \cap A(g)$ Seja C um circuito monótono de tamanho s que computa uma função booleana $f = f(x_1, \ldots, x_n)$. É possível descrever C com um *straight-line program*, isto é, uma sequência de funções $x_1, x_2, \ldots, x_n, f_1, \ldots, f_s$, onde $f = f_s$ e todo f_i $(1 \leq i \leq s)$ é um **OR** ou um **AND** de duas funções anteriores na sequência. Deste modo, aplicando A obtemos a seguinte sequência $A(C)$ de subconjuntos de $\{0,1\}^n$: $A_{-n} = A(x_n), \ldots, A_{-1} = A(x_1), A_1 = A(f_1), \ldots, A_s = A(f_s) = A(f)$, onde todo A_i $(1 \leq i \leq s)$ é uma união ou intersecção de dois conjuntos anteriores na sequência. Iremos substituir a sequência $A(C)$ por uma sequência *aproximadora* $M(C) : M_{-n} = A_{-n}, \ldots, M_{-1} = A_{-1}, M_1, \ldots, M_s$, definida substituindo as operações de união e intersecção por operações "aproximadas" $\sqcup$ e $\sqcap$. Essas operações serão definidas adiante, de modo a assegurar que

$$M \sqcup L \supseteq M \cup L \quad \text{e} \quad M \sqcap L \subseteq M \cap L. \tag{13}$$

Portanto, se para algum $j \in [s]$ vale que $A_j = A_\ell \cup A_k$ para $\ell, k < j$, então $M_j = M_\ell \sqcup M_k$; analogamente, se vale que $A_j = A_\ell \cap A_k$, então $M_j = M_\ell \sqcap M_k$. Quando $M_j = M_\ell \sqcup M_k$, definimos $\delta^j_\sqcup = M_j \smallsetminus (M_\ell \cup M_k)$ e $\delta^j_\sqcap = \varnothing$; analogamente, quando $M_j = M_\ell \sqcap M_k$, definimos $\delta^j_\sqcap = (M_\ell \cap M_k) \smallsetminus M_j$ e $\delta^j_\sqcup = \varnothing$.

Lema 132. *Para todo M_i, vale que*

$$A_i \smallsetminus \bigcup_{j \leq i} \delta^j_\sqcap \subseteq M_i \subseteq A_i \cup \bigcup_{j \leq i} \delta^j_\sqcup. \tag{14}$$

Demonstração. Faremos a prova por indução em i. Quando $i < 0$, $M_i = A_i$ e o resultado vale. Suponha então que o resultado vale para todo $j < i$. Iremos provar que o resultado vale para i. Se $A_i = A_\ell \sqcup A_k$, então, pela hipótese de indução, vale que

$$M_i = M_\ell \cup M_k \cup \delta^j_\sqcup \subseteq A_\ell \cup A_k \cup \bigcup_{j\le i} \delta^j_\sqcup = A_i \cup \bigcup_{j\le i} \delta^j_\sqcup$$

e

$$M_i = M_\ell \sqcup M_k \supseteq M_\ell \cup M_k \supseteq \left(A_\ell \setminus \bigcup_{j\le \ell} \delta^j_\sqcap\right) \cup \left(A_k \setminus \bigcup_{j\le k} \delta^j_\sqcap\right) \supseteq A_i \setminus \bigcup_{j\le i} \delta^j_\sqcap.$$

Isso completa a prova no caso $A_i = A_\ell \sqcup A_k$, Quando $A_i = A_\ell \sqcap A_k$, a prova é análoga. □

O Lema 132 é válido para qualquer escolha das operações $\sqcup$ e $\sqcap$ que satisfaça (13). Iremos definir essas operações da seguinte maneira. Seja $r := 36 \ln^2 m$. Para todo conjunto R de no máximo r arestas sobre $V = [m]$, denote por $\lceil R \rceil$ o conjunto de todos os grafos sobre V que contém pelo menos uma aresta de R. Observe que $\lceil \varnothing \rceil = \varnothing$. Denotamos por $\lceil * \rceil$ o conjunto de todos os grafos sobre V. Observe que $M_{-i} = \lceil R \rceil$, onde R é o conjunto unitário que contém a aresta representada por x_i. Para dois conjuntos R_1 e R_2 de no máximo r arestas cada, definimos $\lceil R_1 \rceil \sqcap \lceil R_2 \rceil = \lceil R_1 \cap R_2 \rceil$, $\lceil R_1 \rceil \sqcap \lceil * \rceil = \lceil R_1 \rceil$ e $\lceil * \rceil \sqcap \lceil * \rceil = \lceil * \rceil$. Analogamente, se $|R_1 \cup R_2| \le r$, definimos $\lceil R_1 \rceil \sqcup \lceil R_2 \rceil = \lceil R_1 \cup R_2 \rceil$, ao passo que, quando $|R_1 \cup R_2| > r$, definimos $\lceil R_1 \rceil \sqcup \lceil R_2 \rceil = \lceil * \rceil$. Por fim, definimos $\lceil R_1 \rceil \sqcup \lceil * \rceil = \lceil * \rceil \sqcup \lceil * \rceil = \lceil * \rceil$. Estão assim definidas as operações $\sqcup$ e $\sqcap$ na sequência $M(C)$.

5.2. **Aula 18 de junho de 2018: Complexidade monótona e circuitos de profundidade limitada.** [22]

Demonstração do Teorema 131. Consideramos C circuito com $s \le \binom{m}{3}/(2r^2)$ portas, onde $r = 36(\log_2 m)^2$. Note que $A(T) = \{\text{família de grafos sobre V que contêm triângulo}\}$. Ademais, tomamos $\alpha_s : \{0,1\}^{\binom{V}{2}} \to \{0,1\}$ tal que $\alpha_s^{-1}(1) = M_s$, isto é, α_s aproxima $f_s = T$.

Vamos mostrar que existem muitos F, F grafo sobre V, tais que $T(F) = 1$ mas sua aproximação $\alpha_s(F) = 0$, ou tais que $T(F) = 0$ mas sua aproximação $\alpha_s(F) = 1$. Pelo Lema 132, para cobrir tais diferenças s terá que ser grande pois os $\delta^i_\sqcup, \delta^i_\sqcap$ são pequenos.

Caso 1: $M_s = \lceil R \rceil$ para algum R com $|R| \le r$. Neste caso, sorteamos F como sendo $\binom{X}{3}$ onde $X \subseteq V$, $|X| = 3$, é escolhido uniformemente ao acaso. Claramente, $T(F) = 1$. Ademais,

$$\mathbb{P}(F \in M_s) = \mathbb{P}(F \cap R \neq \varnothing) \le \frac{r(m-2)}{\binom{m}{3}} = o(1).$$

[22] Notas produzidas por Rodrigo Enju e André Nakazawa.

Logo, existe m_0 tal que se $m \geq m_0$, então $\mathbb{P}(F \in M_s) < 1/2$.

Afirmação 133. *Para cada j, com $1 \leq j \leq s$, temos que*

$$\mathbb{P}(F \in \delta^j_{\sqcap}) \leq r^2 \binom{m}{3}^{-1}$$

Demonstração. (Afirmação 133) Se $\delta^j_{\sqcap} = \varnothing$, a afirmação claramente vale. Então suponha que $\delta^j_{\sqcap} \neq \varnothing$. Neste caso, existem $R_a, R_b \subseteq \binom{V}{2}$ tais que $|R_a|, |R_b| \leq r$ e $M_a = \lceil R_a \rceil, M_b = \lceil R_b \rceil$. Logo $\delta^j_{\sqcap} = (M_a \cap M_b) \setminus (M_a \sqcap M_b) = (\lceil R_a \rceil \cap \lceil R_b \rceil) \setminus (\lceil R_a \rceil \sqcap \lceil R_b \rceil)$. Então $\mathbb{P}(F \in \delta^j_{\sqcap}) = \mathbb{P}(F \in (\lceil R_a \rceil \cap \lceil R_b \rceil) \setminus (\lceil R_a \rceil \sqcap \lceil R_b \rceil)) \leq r^2 \binom{m}{3}^{-1}$. □

Como $s \leq \binom{m}{3}/2r^2$, temos que $\mathbb{P}(\bigcup_{j \leq s} \delta^j_{\sqcap}) \leq 1/2$. Assim, temos que $\mathbb{P}((A(T) \setminus \bigcup_{j \leq s} \delta^j_{\sqcap}) \setminus M_j) > 0$. Contradição, pois como a probabilidade é positiva, ainda temos erros que não são cobertos.

Caso 2: $M_s = \lceil * \rceil$. Escolhemos F aleatoriamente como segue: sorteamos $X \subseteq V$ uniformemente ao acaso e tomamos $F = X \times (V \setminus X)$. Claramente, $T(F) = 0$ pois F é bipartido mas $\alpha_s(F) = 1$ dado que $M_s = \lceil * \rceil \Rightarrow \alpha_s \equiv 1$.

Afirmação 134. *Para cada j, com $1 \leq j \leq s$, temos que*

$$\mathbb{P}(F \in \delta^j_{\sqcup}) \leq 2^{-\sqrt{r}/2}.$$

Demonstração. (Afirmação 134) Claramente, podemos supor $\delta^j_{\sqcup} \neq \varnothing$. Logo, segue que existem $R_a, R_b \subseteq \binom{V}{2}$ tais que $|R_a|, |R_b| \leq r$ com $|R_a \cup R_b| > r$ e $M_a = \lceil R_a \rceil, M_b = \lceil R_b \rceil$. Considere $\mathcal{H} = (V, R_a \cup R_b)$. Pelo Teorema de Vizing, sabemos que $\chi'(\mathcal{H}) \leq \Delta(\mathcal{H}) + 1$. Seja $\nu(\mathcal{H}) =$ tamanho máximo de um emparelhamento de $\mathcal{H}$. Então $r < |R_a \cup R_b| \leq (\Delta(\mathcal{H}) + 1)\nu(\mathcal{H})$, donde segue que $\mathcal{H}$ contém uma estrela $K^{1,d}$ com $d \geq \sqrt{2}/2$ ou um conjunto de $d \geq \sqrt{2}/2$ arestas independentes. □

Sejam $e_1, \cdots, e_k$, $k \geq \sqrt{r}/2$, as arestas nesse $K^{1,d}$ ou nesse emparelhamento com pelo menos $\sqrt{r}/2$ arestas.

Se $F \in \delta^j_{\sqcap}$, então $F \notin \lceil R_a \rceil \cup \lceil R_b \rceil$ e assim $F \cap R_a \neq \varnothing$ e $F \cap R_b \neq \varnothing$ e portanto, cada e_i, $1 \leq i \leq k$, está contido em X ou em $V \setminus X$. Isto ocorre com probabilidade $(1/2)^k \leq (1/2)^{\sqrt{r}/2}$ Assim, temos que

$$\mathbb{P}(\bigcup_{j \leq s} \delta^j_{\sqcap}) \leq s 2^{-\sqrt{r}/2} \leq \binom{m}{3} \frac{1}{2r^2} 2^{-6 \log_2 m/2} = o(1).$$

Contradição. □

5.2.1. *Circuitos de profundidade limitada.* Seja C um circuito. Definimos a profundidade de C como o comprimento máximo de um caminho de uma variável até a saída.

Exemplo 135. A função booleana $\oplus_n : \{0,1\}^n \to \{0,1\}$ que conta a paridade do # de bits 1, definida como $f((x_i)_{i=1}^n) = (\sum_{i=1}^n x_i) \mod 2$, admite circuito com $O(n)$ portas e profundidade $O(\log n)$.

Observação 136. Circuitos com profundidade limitada para $\oplus_n$ exigem # superpolinomial de portas.

5.3. Aula 20 de Junho de 2018: Circuitos de profundidade limitada (continuação). [23]

5.3.1. *Circuitos de Profundidade Limitada.* Seja C um circuito. Definimos sua profundidade prof C como sendo o comprimento de um maior caminho entre uma de suas variáveis e uma de suas saídas.

É possível classificar funções booleanas pelo tamanho ou profundidade dos circuitos que as computam. NC^i é a classe das funções que podem ser computadas por algum circuito de profundidade $O(\log^i n)$ com número polinomial de portas, todas com exatamente duas entradas. AC^i, por sua vez, é a classe definida de maneira análoga, na qual as portas possuem fan-in ilimitado. Sabe-se que $AC^0 \subseteq NC^1 \subseteq AC^1$.

Nesta seção, vamos considerar a função paridade de números binários de n bits, que denotaremos por $\oplus_n$. Essa função é definida por

$$\oplus_n : \{0,1\}^n \to \{0,1\}$$
$$(x_i)_1^n \mapsto (\sum_i x_i) \mod 2.$$

Usando cópias do gadget ilustrado na figura 6, que implementa a função $\oplus_2$, podemos construir um circuito com $O(n)$ portas e profundidade $O(\log n)$ para $\oplus_n$. Em outras palavras, temos que $\oplus_n \in AC^1$.

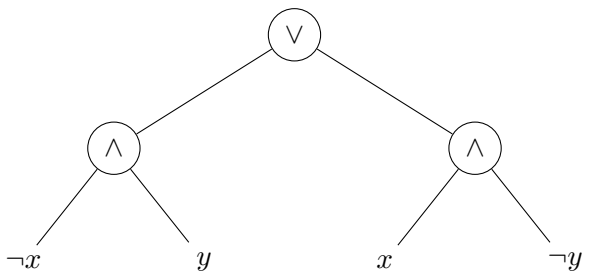

FIGURA 6. Circuito que implementa $\oplus_2$

[23] Notas produzidas por Felix Liu e Ângelo Lovatto

Mostraremos adiante que se C é um circuito para $\oplus_n$ com número polinomial de portas, então $prof(C) = \Omega\left(\frac{\log n}{\log \log n}\right)$. Ou seja, $\oplus_n \in NC^1$. Dito isso, é de se perguntar se $\oplus_n$ não está também em AC^0. Nesta seção, vamos mostrar que não: é impossível construir um circuito para $\oplus_n$ com número polinomial de portas e profundidade limitada i.e. $\oplus_n \notin AC^0$.

Definição 137 (t-CNF e s-DNF)**.** *Um t-CNF é um circuito na forma normal conjuntiva, com a restrição de que cada cláusula tem no máximo t literais.*

Analogamente, um s-DNF é um circuito na forma normal disjuntiva, com a restrição de que cada cláusula tem no máximo s literais.

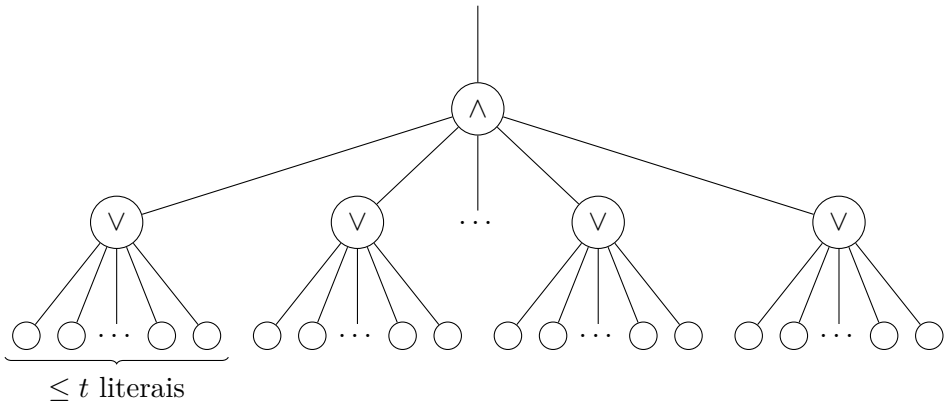

FIGURA 7. t-CNF

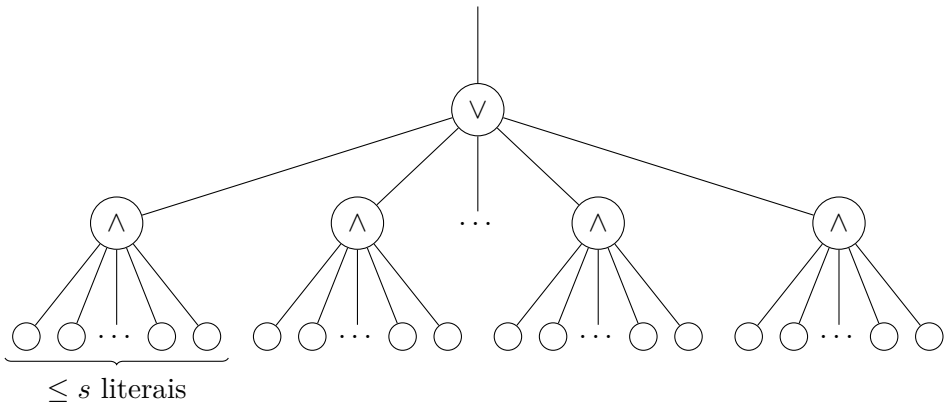

FIGURA 8. s-DNF

Definição 138. *Seja f uma fórmula booleana $f : \{0,1\}^{[n]} \to \{0,1\}$ e $\varrho : [n] \to \{0,1,*\}$.*

Definimos o suporte de ϱ como sendo $supp(\varrho) = \varrho^{-1}(\{0,1\})$.

A função f restrita a ϱ, $f|_\varrho$: $\{0,1\}^{\varrho^{-1}(*)} \to \{0,1\}$, é dada por

$$f|_\varrho(y) = f(x), \text{ com } x_i = \begin{cases} \varrho_i \text{ se } i \in supp(\varrho) \\ y_i \text{ se } i \in \varrho^{-1}(*) \end{cases}$$

Informalmente, fixamos através de ϱ os valores de alguns literais de f, resultando em uma função $f|_\varrho$ que depende dos demais literais. Neste contexto, dizemos que ϱ é uma restrição.

Exemplo 139. Seja $f = (x_1 \wedge x_2) \vee x_3$ e $\varrho(1) = 0, \varrho(2) = \varrho(3) = *$. Então $f|_\varrho = (0 \wedge x_2) \vee x_3$. Observe que $f|_\varrho \equiv x_3$, mas ainda é definida como uma função sobre x_2 e x_3.

Definição 140. *Dado $0 < p < 1$, uma p-restrição aleatória é uma restrição ϱ em que para cada posição i, independentemente, temos*

$$\mathbb{P}(\varrho(i) = *) = p; \text{ e}$$

$$\mathbb{P}(\varrho(i) = 0) = \mathbb{P}(\varrho(i) = 1) = (1-p)/2.$$

Definição 141 (Minterm e Maxterm)**.** *Dada $f(x_1, \ldots, x_n)$ uma função binária, uma restrição ϱ é um minterm de f se $f|_\varrho \equiv 1$ e $supp(\varrho)$ é minimal. Se ϱ é tal que $f|_\varrho \equiv 0$ e $supp(\varrho)$ é minimal, dizemos que ϱ é um maxterm de f.*

Fato 142. *Se f é tal que todo minterm μ tem $|supp(\mu)| \leq s$, então f é s-DNF.*

Fato 143. *Se f é tal que todo maxterm μ tem $|supp(\mu)| \leq t$, então f é t-CNF.*

Para verificar ambos os fatos, basta observar que podemos tomar os minterms como cláusulas para um s-DNF, e os maxterms como cláusulas para um t-CNF.

Lema 144 (Switching Lemma)**.** *Seja $G : \{0,1\}^n \to \{0,1\}$ uma $t-CNF$ e ϱ uma p-restrição aleatória. Então*

$$\mathbb{P}(G|_\varrho \text{ não é } (s-1)\text{-}DNF) \leq \mathbb{P}(G|_\varrho \text{ tem minterm } \geq s) \leq (5pt)^s$$

Observação 145. O Switching Lemma admite uma versão dual, na qual temos $t-$DNF em vez de $t-$CNF e $(s-1)-$CNF em vez de $(s-1)-$DNF e maxterm em vez de minterm.

Demonstração. Dada uma t-DNF de G, podemos aplicar os teoremas de De Morgan para obter uma t-CNF de $\neg G$ em que possamos usar o Switching Lemma. Fixe um ϱ arbitrário. Então aplicando De Morgan podemos constatar que $\neg G|_\varrho$ é $(s-1)$-DNF se e só se $G|_\varrho$ é $(s-1)$-DNF. Além disso, não é difícil ver que $\neg G|_\varrho$ tem minterm $\geq s$ se e só se $G|_\varrho$ tem maxterm $\geq s$. □

Definição 146 (Circuito alternante)**.** *Um circuito alternante C é tal que*

- *Seus literais estão todos no nível 1;*
- *A porta de sua única saída está no nível $d+1$;*
- *Toda porta só tem saídas do nível anterior como entradas;*
- *As portas de um mesmo nível são todas do mesmo operador ($\wedge$ ou $\vee$); e*
- *O operador de cada nível é distinto dos níveis imediatamente adjacentes ($\wedge$ e $\vee$ se alternam a cada nível).*

Definição 147. *Um $C(s, s', d, t)$-circuito é um circuito alternante em que*

- *O total de portas do circuito é no máximo s;*
- *O total de portas do nível 3 ao $d+1$ é no máximo s';*
- *A profundidade do circuito é no máximo d; e*
- *O fan-in das portas do nível 2 é no máximo t.*

Denotaremos por $C_f(s, s', d, t)$, onde $f \in \{\wedge, \vee\}$, $C(s, s', d, t)$-circuitos cujas portas do nível 2 são do tipo f.

Exemplo 148. Podemos obter um $C_\wedge(1 + 2^{n-1}, 1, 2, n)$-circuito para $\oplus_n$ da seguinte maneira: Para cada $\varepsilon \in \{0,1\}^n$ ímpar possível, criamos uma cláusula conjuntiva com n literais, os quais equivalem a $x_i \oplus \varepsilon_i \oplus 1$. Efetivamente, esse circuito limita-se a computar se a entrada é igual a algum dos ε ímpares possíveis e, portanto, é um circuito para $\oplus_n$.

Seja G uma das portas de um $C(s, s', d, t)$-circuito C. Vamos nos referir por "circuito de G" ao circuito formado por G e os literais na entrada de G, se G está no nível 2; ou ao circuito formado por G e pelos circuitos das portas na entrada de G, se G está acima do nível 2.

Dado um $C(s, s', d, t)$-circuito com $d > 2$, podemos sortear uma p-restrição aleatória e aplicar o Switching Lemma aos circuitos das portas do nível 3, para que seu operador seja o mesmo que o do nível 4. Então, podemos remover as portas do nível 3 e ligar as entradas do nível 4 às saídas adequadas do nível 2, obtendo um circuito de profundidade menor. Podemos então repetir esse procedimento até obter um $C_\wedge(\infty, 1, 2, t)$-circuito (se necessário, acrescente um nível $d+2$ e aplique o lema mais uma vez). No pior caso, aplicamos essa redução $d-1$ vezes no total. Tomando $p = \frac{1}{10t}$, podemos mostrar que com alta probabilidade o circuito obtido computa uma restrição da função original. Com esse raciocínio em mente, provamos o seguinte teorema.

Teorema 149. *Seja $f : \{0,1\}^n \to \{0,1\}$ uma função booleana que tem um $C(\infty, s', d, t)$-circuito. Suponha que $(s'+1)/2^t \leq 1/2$ e $n(\frac{1}{10t})^{d-1} \geq 12$. Então f tem minterm de tamanho $\leq n - \frac{n}{2}(\frac{1}{10t})^{d-1} + t$.*

Demonstração. Tome $p = \frac{1}{10t}$ e $s = t$ no Switching Lemma. Cada aplicação do Switching Lemma falha em gerar uma restrição do circuito original com probabilidade no máximo $(5pt)^s \leq \frac{1}{2^t}$. Como aplicamos o Switching Lemma no máximo $s'+1$ vezes (uma vez para cada porta acima do nível 2, e talvez uma a mais) e $(s'+1)/2^t \leq 1/2$, temos que as aplicações foram todas bem sucedidas com probabilidade maior que $1/2$. Obtemos então um $C_\wedge(\infty, 1, 2, t)$-circuito que é uma t-DNF de uma função $g = f|_\varrho$, para um certo ϱ. Pelo Switching Lemma, com alta probabilidade tal g tem minterm $\leq t$.

Seja X o número de variáveis cujos valores não foram fixados no processo para se obter g. Como em cada um dos $d-1$ níveis sorteamos uma p-restrição aleatória distinta, isso significa que $X \sim Bi(n, p^{d-1})$. Assim, temos que

$$\mathbb{P}(X \leq \varepsilon np^{d-1}) \leq e^{-\frac{1}{3}\varepsilon^2 np^{d-1}}.$$

Tomando $\varepsilon = 1/2$, como $p = \frac{1}{10t}$ e supomos que $n(\frac{1}{10t})^{d-1} \geq 12$, temos que $-\frac{1}{3}\varepsilon^2 np^{d-1} \leq -1$. Dessa forma, é verdade que

$$\mathbb{P}(X \leq \frac{n}{2}(\frac{1}{10t})^{d-1}) \leq e^{-1} < \frac{1}{2}.$$

Assim, com probabilidade maior que $1/2$, g é uma função sobre $X \geq \frac{n}{2}(\frac{1}{10t})^{d-1}$ variáveis. Logo, f tem minterm $\leq n - \frac{n}{2}(\frac{1}{10t})^{d-1} + t$, como queríamos. □

Corolário 150. *Suponha $2 \leq d \leq (\log n)/\log 20$. Não existe $C(\infty, 2^{n^{\frac{1}{d}}/10-2}, d, \frac{1}{10}n^{\frac{1}{d}})$ para $\oplus_n$.*

Parte 4. BIBLIOGRAFIA

Referências

[1] N. Alon and R. B. Boppana, *The monotone circuit complexity of Boolean functions*, Combinatorica **7** (1987), no. 1, 1–22. MR905147 ↑5.1, 130

[2] A. E. Andreev, *A method for obtaining lower bounds on the complexity of individual monotone functions*, Dokl. Akad. Nauk SSSR **282** (1985), no. 5, 1033–1037. MR796937 ↑5.1, 130

[3] P. Erdős, *On a combinatorial problem. ii*, Acta Mathematica Academiae Scientiarum Hungarica **15** (1964Sep), no. 3, 445–447. ↑3

[4] P. Erdős and L. Lovász, *Problems and results on 3-chromatic hypergraphs and some related questions*, Infinite and finite sets **10** (197401). ↑3

[5] K. Iwama and H. Morizumi, *An explicit lower bound of* $5n - o(n)$ *for boolean circuits*, Proceedings of the 27th international symposium on mathematical foundations of computer science, 2002, pp. 353–364. ↑5.1

[6] R. A. Moser and G. Tardos, *A constructive proof of the general Lovász local lemma*, J. ACM **57** (2010), no. 2, Art. 11, 15. MR2606086 ↑122

[7] J. Radhakrishnan and A. Srinivasan, *Improved bounds and algorithms for hypergraph 2-coloring*, Random Structures & Algorithms **16** (2000), no. 1, 4–32. ↑3

[8] A. A. Razborov, *Lower bounds on the monotone complexity of some Boolean functions*, Dokl. Akad. Nauk SSSR **281** (1985), no. 4, 798–801. MR785629 ↑5.1, 130

[9] P. R. J. Östergård, *On the minimum size of* 4*-uniform hypergraphs without property B*, Discrete Applied Mathematics **163** (2014), 199–204. Optimal Discrete Structures and Algorithms ODSA 2010. ↑3

Instituto de Matemática e Estatística, Universidade de São Paulo, Rua do Matão 1010, 05508–090 São Paulo, SP