O LEMA LOCAL DE LOVÁSZ

BRUNO PASQUALOTTO CAVALAR

1. O Lema Local de Lovász (LLL)

Seja $\mathcal{A}$ uma coleção finita de eventos não triviais num mesmo espaço de probabilidade. Se os eventos de $\mathcal{A}$ forem mutuamente independentes, então vale que

$$\mathbb{P}\left[\bigcap_{A\in\mathcal{A}} \overline{A}\right] = \prod_{A\in\mathcal{A}} \mathbb{P}[\overline{A}] > 0.$$

É natural supor que algo similar acontece quando os eventos são "limitadamente dependentes". A seguinte definição ajuda a formalizar esse conceito.

Definição 1. Um digrafo $D = (\mathcal{A}, E)$ é dito um **digrafo de dependência** para $\mathcal{A}$ se cada evento $A \in \mathcal{A}$ é mutuamente independente dos eventos em $\mathcal{A} \setminus (\Gamma(A) \cup \{A\})$, onde

$$\Gamma(A) := \{B \in \mathcal{A} : (A, B) \in E\}.$$

O Lema Local de Lovász é uma ferramenta poderosa que nos permite evitar todos os eventos de $\mathcal{A}$, contanto que as probabilidades dos eventos não sejam muito grandes e o grafo de dependência não tenha muitas arestas.

Lema 2 (Lema Local de Lovász [2])**.** *Seja $\mathcal{A}$ uma coleção finita de eventos e $D = (\mathcal{A}, E)$ um digrafo de dependência para $\mathcal{A}$. Se existe uma função $x : \mathcal{A} \to [0, 1)$ tal que*

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

então

$$\mathbb{P}\left[\bigcap_{A\in\mathcal{A}} \overline{A}\right] = \prod_{A\in\mathcal{A}} (1 - x(A)) > 0.$$

Demonstração. Observe que de (1) temos que

$$\mathbb{P}[A] \le x(A) \prod_{B\in\Gamma(A)} (1 - x(B)) \le x(A) < 1.$$

Logo, temos que $\mathbb{P}[\overline{A}] > 0$.

Provamos agora que, para todo $A \in \mathcal{A}$ e $S \subseteq \mathcal{A}$ tal que $A \notin S$, vale que

$$\mathbb{P}\left[\bigcap_{B\in S} \overline{B}\right] > 0 \quad \text{e} \quad \mathbb{P}\left[A \,\middle|\, \bigcap_{B\in S} \overline{B}\right] \le x(A). \tag{2}$$

Faremos essa prova por indução em $|S|$.

O resultado é imediato quando $|S| = 0$, pois, como provamos acima, $\mathbb{P}[A] \le x(A)$. Suponha agora que $|S| > 0$ e que (2) vale para todo conjunto de tamanho menor que S. Fixe $E \in S$.

Data: 7 de março de 2019, 9:47pm

Pela hipótese de indução, temos que

$$\mathbb{P}\left[\bigcap_{B\in S}\overline{B}\right] = \mathbb{P}\left[\overline{E}\cap\bigcap_{B\in S\setminus\{E\}}\overline{B}\right] = \mathbb{P}\left[\overline{E}\,\middle|\,\bigcap_{B\in S\setminus\{E\}}\overline{B}\right]\mathbb{P}\left[\bigcap_{B\in S\setminus\{E\}}\overline{B}\right]$$
$$\geq (1-x(E))\mathbb{P}\left[\bigcap_{B\in S\setminus\{E\}}\overline{B}\right] > 0.$$

Definamos agora $S_1 := S\cap\Gamma(A)$ e $S_2 := S\setminus S_1$. Observe que

$$\mathbb{P}\left[A\,\middle|\,\bigcap_{B\in S}\overline{B}\right] = \frac{\mathbb{P}\left[A\cap\bigcap_{B\in S_1}\overline{B}\,\middle|\,\bigcap_{C\in S_2}\overline{C}\right]}{\mathbb{P}\left[\bigcap_{B\in S_1}\overline{B}\,\middle|\,\bigcap_{C\in S_2}\overline{C}\right]}. \tag{3}$$

Como A é mutuamente independente dos eventos em S_2, podemos limitar o numerador do seguinte modo:

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

Suponhamos agora que $S_1 = \{B_1,\dots,B_l\}$. Pela hipótese de indução, temos que

$$\mathbb{P}\left[\bigcap_{B\in S_1}\overline{B}\,\middle|\,\bigcap_{C\in S_2}\overline{C}\right] = \mathbb{P}\left[\overline{B_1}\,\middle|\,\bigcap_{C\in S_2}\overline{C}\right]\mathbb{P}\left[\overline{B_2}\,\middle|\,B_1\cap\bigcap_{C\in S_2}\overline{C}\right]\dots\mathbb{P}\left[\overline{B_l}\,\middle|\,B_1\cap\dots\cap B_{l-1}\cap\bigcap_{C\in S_2}\overline{C}\right]$$
$$\geq \prod_{i=1}^{l}(1-x(B_i)) = \prod_{B\in S_1}(1-x(B)) \geq \prod_{B\in\Gamma(B)}(1-x(B)).$$

Portanto de (3) segue que $\mathbb{P}\left[A\,\middle|\,\bigcap_{B\in S}\overline{B}\right] \leq x(A)$. Isso termina a prova de (2).

Escrevamos agora $\mathcal{A} = \{A_1,\dots,A_m\}$. Usando (2) repeditas vezes, podemos concluir que

$$\mathbb{P}\left[\bigcap_{A\in\mathcal{A}}\overline{A}\right] = \mathbb{P}\left[\bigcap_{i=1}^{m}\overline{A_i}\right] = \mathbb{P}\left[\overline{A_1}\right]\mathbb{P}\left[\overline{A_2}\,\middle|\,\overline{A_1}\right]\dots\mathbb{P}\left[\overline{A_m}\,\middle|\,\overline{A_1}\cap\dots\cap\overline{A_{m-1}}\right]$$
$$\geq \prod_{i=1}^{m}(1-x(\overline{A_i})) = \prod_{A\in\mathcal{A}}(1-x(\overline{A})),$$

como queríamos demonstrar. ■

O seguinte fato é muito útil em várias situações para definir um digrafo de dependência e aplicar o LLL. Ele nos permite definir para todo $A\in\mathcal{A}$ um conjunto $\Gamma(A)$ tal que A é mutuamentemente independente dos eventos em $\mathcal{A}\setminus(\Gamma(A)\cup\{A\})$.

Fato 3 (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*

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

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*.* ■

1.1. **Versões alternativas do LLL.** Em muitas aplicações, a versão geral do LLL (Lema 2) é pouco prática. Apresentamos aqui algumas versões do LLL que são mais aplicáveis em vários contextos.

Lema 4 (Lema Local de Lovász Simétrico)**.** *Seja $\mathcal{A}$ uma coleção finita de eventos e $D = (\mathcal{A}, E)$ um digrafo de dependência para $\mathcal{A}$. Suponha que existem $p \in [0,1]$ e $d \in \mathbb{Z}$ um inteiro positivo tais que para todo $A \in \mathcal{A}$ vale*

$$\mathbb{P}[A] \leq p \quad e \quad |\Gamma(A)| \leq d.$$

Se $ep(d+1) \leq 1$, então

$$\mathbb{P}\left[\bigcap_{A \in \mathcal{A}} \overline{A}\right] > 0.$$

Demonstração. Primeiramente, note que se $d = 0$ então os eventos são mutuamente independentes e o resultado segue trivialmente. Suponhamos então que $d > 0$.

Defina a função $x : \mathcal{A} \to [0,1)$ dada por $x(A) = 1/d$ para todo $A \in \mathcal{A}$. Fixemos $A \in \mathcal{A}$. Usando que $1 + x \leq e^x$ para todo $x \in \mathbb{R}$, obtemos:

$$x(A) \prod_{B \in \Gamma(A)} (1 - x(B)) = \frac{1}{d} \prod_{B \in \Gamma(A)} \left(1 - \frac{1}{d}\right) \geq \frac{1}{d}\left(1 - \frac{1}{d}\right)^d \geq \frac{1}{d} e^{-1} \geq p \geq \mathbb{P}[A].$$

Portanto, a condição (1) do Lema 2 é satisfeita. O resultado segue. ■

Lema 5 (Lema Local de Lovász Assimétrico)**.** *Seja $\mathcal{A}$ uma coleção finita de eventos e $D = (\mathcal{A}, E)$ um digrafo de dependência para $\mathcal{A}$. Suponha que para todo $A \in \mathcal{A}$ vale que*

$$\mathbb{P}[A] \leq \frac{1}{4} \quad e \quad \sum_{B \in \Gamma(A)} \mathbb{P}[B] \leq \frac{1}{4}.$$

Então

$$\mathbb{P}\left[\bigcap_{A \in \mathcal{A}} \overline{A}\right] > 0.$$

Demonstração. Defina a função $x : \mathcal{A} \to [0,1)$ dada por $x(A) = 2\mathbb{P}[A]$ para todo $A \in \mathcal{A}$. Note que $x(A) = 2\mathbb{P}[A] \leq 1/2$ para todo $A \in \mathcal{A}$. Fixemos agora $A \in \mathcal{A}$. Usando que $1 - x \geq 2^{-2x}$ para todo $x \in [0, \frac{1}{2}]$, obtemos:

$$\begin{aligned} x(A) \prod_{B \in \Gamma(A)} (1 - x(B)) &\geq x(A) \prod_{B \in \Gamma(A)} 2^{-2x(B)} \\ &= x(A) 2^{-2\sum_{B \in \Gamma(A)} x(B)} \\ &= 2\mathbb{P}[A] 2^{-4\sum_{B \in \Gamma(A)} \mathbb{P}[B]} \\ &\geq 2\mathbb{P}[A] 2^{-1} \\ &= \mathbb{P}[A]. \end{aligned}$$

Portanto, a condição (1) do Lema 2 é satisfeita. O resultado segue. ■

Prosseguimos agora a apresentar algumas aplicações combinatórias do LLL.

1.2. **Colorações frugais.** Uma coloração própria de um grafo G é dita β-frugal se cada cor aparece no máximo β vezes na vizinhança de cada vértice. Defina $F(G)$ como o menor número para o qual existe uma coloração β-frugal de G com $F(G)$ cores. Alon provou que existe uma constante c tal que para todo Δ existe um grafo G com grau máximo Δ que satisfaz $F(G) > c\Delta^{1+1/\beta}$. O seguinte teorema mostra que esse resultado é assintoticamente ótimo.

Teorema 6 (Hind, Molloy e Reed [3])**.** *Se G tem grau máximo $\Delta \geq \beta^\beta$, então G tem uma coloração β-frugal usando no máximo $16\Delta^{1+1/\beta}$ cores.*

Demonstração. Para $\beta = 1$, o resultado é equivalente a encontrar uma coloração própria de G^2, isto é, o grafo obtido de G adicionando arestas entre vértices com distância igual a 2. Como esse grafo tem grau máximo Δ^2, ele tem uma coloração com $\Delta^2 + 1 \leq 16\Delta^2 = 16\Delta^{1+1/\beta}$ cores.

Suponha então que $\beta \geq 2$. Defina $C = 16\Delta^{1+1/\beta}$. Para cada vértice de G atribuímos aleatoriamente uma cor entre $\{1, \ldots, C\}$ com probabilidade uniforme. Para cada aresta uv de G definimos o evento A_{uv} de que os vértices u e v recebam a mesma cor. Chamamos tais eventos de eventos do Tipo A. Além disso, para cada conjunto $\{u_1, \ldots, u_{\beta+1}\}$ de $\beta+1$ vértices todos na vizinhança de um mesmo vértice, definimos o evento $B_{u_1,\ldots,u_{\beta+1}}$ de que cada u_i receba a mesma cor. Chamamos tais eventos de eventos do Tipo B. Claramente, se evitamos todos os eventos do Tipo A e do Tipo B, então a nossa coloração aleatória é β-frugal.

Note que a probabilidade de cada evento do Tipo A é $1/C$, e a probabilidade de cada evento do Tipo B é $1/C^\beta$. Claramente, temos $\mathbb{P}[A] \leq 1/4 \ \forall A \in \mathcal{A}$. Além disso, pelo Princípio da Independência Mútua (Fato 3), cada evento é mutuamente independente de todos os eventos com os quais não compartilha nenhum vértice. Como cada evento (Tipo A ou Tipo B) compartilha vértices com no máximo $(\beta+1)\Delta$ eventos do Tipo A e $(\beta+1)\Delta\binom{\Delta}{\beta}$ eventos do Tipo B, existe um digrafo D de dependência para $\mathcal{A}$ no qual cada evento é vizinho dessa quantidade de eventos. Neste digrafo, para qualquer $A \in \mathcal{A}$ fixado temos que

$$\begin{aligned}
\sum_{B \in \Gamma_D(A)} \mathbb{P}[B] &\leq (\beta+1)\Delta\frac{1}{C} + (\beta+1)\Delta\binom{\Delta}{\beta}\frac{1}{C^\beta} \\
&\leq (\beta+1)\Delta\frac{1}{C} + (\beta+1)\frac{\Delta^{\beta+1}}{\beta!\,C^\beta} \\
&= (\beta+1)\frac{1}{16\Delta^{1/\beta}} + (\beta+1)\frac{1}{\beta!\,16^\beta} \\
&= \frac{\beta}{16\Delta^{1/\beta}} + \frac{1}{16\Delta^{1/\beta}} + \frac{\beta}{\beta!\,16^\beta} + \frac{1}{\beta!\,16^\beta} \\
&\leq 4\frac{1}{16} = \frac{1}{4}.
\end{aligned}$$

O resultado agora segue diretamente do lema local de Lovász assimétrico (Lema 5). ∎

1.3. **Um resultado sobre comprimentos de circuitos.** Apresentamos agora um resultado de Alon e Linial sobre ciclos de tamanho 0 modulo k, que foi provado usando o lema local de Lovász simétrico (Lema 4).

Teorema 7 (Alon e Linial [1])**.** *Seja $D = (V, E)$ um grafo dirigido com grau de saída minimo pelo menos δ e grau de saída máximo no máximo Δ. Então, para todo $k \in \mathbb{N}$ tal que*

$$k \leq \frac{\delta}{1 + \log(1 + \delta\Delta)}, \tag{4}$$

D contém um circuito de comprimento divisível por k.

Demonstração. Podemos supor sem perda de generalidade que todo grau de saída é exatamente δ.

Seja $\chi : V \to \{0, 1, \ldots, k-1\}$ uma coloração aleatória dos vértices de D escolhida uniformemente ao acaso. Denote $N(v) := \{w \in V : (v, w) \in E\}$. Para todo $v \in V$, seja A_v o evento de que nenhum vértice $w \in N(v)$ satisfaz $\chi(w) = \chi(v) + 1 \pmod{k}$. Note que $\mathbb{P}(A_v) = (1 - \frac{1}{k})^\delta$.

Afirmamos agora que, para todo $v \in V$, A_v é independente de todos os eventos A_w com $w \in I(v)$, onde

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

Para provar a afirmação, primeiramente note que para todo $J \subseteq I(v)$ vale que:

$$\mathbb{P}\left[A_v \cap \bigcap_{w \in J} A_w\right] = \sum_{c=0}^{k-1} \mathbb{P}\left[A_v \cap \bigcap_{w \in J} A_w \,\middle|\, \chi(v) = c\right] \mathbb{P}\left[\chi(v) = c\right].$$

Observe ainda que no espaço condicionado $\{\chi(v) = c\}$ o conjunto de vértices cuja escolha de cores determina A_v é disjunto do conjunto de vértices cuja escolha de cores determina $\bigcap_{w \in J} A_w$. Portanto, pelo Princípio de Independência Mútua (Fato 3) podemos concluir que

$$\mathbb{P}\left[A_v \cap \bigcap_{w \in J} A_w \,\middle|\, \chi(v) = c\right] = \mathbb{P}\left[A_v \,|\, \chi(v) = c\right] \mathbb{P}\left[\bigcap_{w \in J} A_w \,\middle|\, \chi(v) = c\right].$$

Observando que $\mathbb{P}\left[A_v \,|\, \chi(v) = c\right] = \mathbb{P}[A_v]$ obtemos que:

$$\begin{aligned}
\mathbb{P}\left[A_v \cap \bigcap_{w \in J} A_w\right] &= \sum_{c=0}^{k-1} \mathbb{P}\left[A_v \cap \bigcap_{w \in J} A_w \,\middle|\, \chi(v) = c\right] \mathbb{P}\left[\chi(v) = c\right] \\
&= \sum_{c=0}^{k-1} \mathbb{P}\left[A_v \,|\, \chi(v) = c\right] \mathbb{P}\left[\bigcap_{w \in J} A_w \,\middle|\, \chi(v) = c\right] \mathbb{P}\left[\chi(v) = c\right] \\
&= \mathbb{P}[A_v] \sum_{c=0}^{k-1} \mathbb{P}\left[\bigcap_{w \in J} A_w \,\middle|\, \chi(v) = c\right] \mathbb{P}\left[\chi(v) = c\right] \\
&= \mathbb{P}[A_v] \mathbb{P}\left[\bigcap_{w \in J} A_w\right],
\end{aligned}$$

o que prova a afirmação.

Portanto, o digrafo D com conjunto de vértices $\mathcal{A} := \{A_v : v \in V\}$ e tal que a vizinhança de um evento A_v é dada por $\Gamma(A_v) = \{A_w : w \in V \setminus \{v\}, w \notin I(v)\}$ é um digrafo de dependencia para $\mathcal{A}$. Note agora que nesse digrafo $|\Gamma(A_v)| \leq \delta + \delta(\Delta - 1) = \delta\Delta$. Além disso, obtemos de (4) que

$$e^{1-\delta/k}(1 + \delta\Delta) \leq 1.$$

Portanto, usando que $1 + x \leq e^x \; \forall x \in \mathbb{R}$ e fazendo $p := (1 - \frac{1}{k})^\delta$ e $d := \delta\Delta$, obtemos

$$ep(d+1) = e\left(1 - \frac{1}{k}\right)^\delta (\delta\Delta + 1) \leq e^{1-\delta/k}(\delta\Delta + 1) \leq 1.$$

Deste modo, pelo lema local de Lovász simétrico (Lema 4) segue que existe uma coloração dos vértices de D satisfazendo que, para todo $v \in V$, existe $w \in N(v)$ tal que $\chi(w) = \chi(v) + 1 \pmod{k}$.

Fixe agora um vértice $v_0 \in V$, e gere uma sequência de vértices $v_0 v_1 \dots$ tal que $(v_i, v_{i+1}) \in E$ e $\chi(v_{i+1}) = \chi(v_i) + 1 \pmod{k}$. Seja j o menor índice tal que existe índice $l < j$ com $v_l = v_j$. O circuito dirigido $v_l v_{l+1} \dots v_j$ é como queremos. ∎

2. Uma versão algoritmica do LLL

A prova original de Lovász é não construtiva, e garante apenas uma probabilidade exponencialmente pequena. Além disso, o espaço de probabilidade que consideramos é tipicamente exponencial, de modo que uma busca exaustiva não é eficiente. Ainda assim, em um celebrado artigo [4], Moser e Tardos mostraram como construir eficientemente tais objetos cuja existência é garantida pelo LLL.

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

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

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 3), temos que A é mutuamente independente de 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     $v_P \leftarrow$ 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   escolha um evento violado $A \in \mathcal{A}$ de acordo com alguma regra qualquer fixada;
5   **para todo** $P \in \mathrm{vbl}(A)$ **faça**
6         $v_P \leftarrow$ 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 8 (Moser e Tardos [4])**.** *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 $\sum_{A\in\mathcal{A}} \frac{x(A)}{1-x(A)}$.

Iremos provar o Teorema 8 nas próximas seções.

2.1. **Alguns conceitos importantes.** Antes de provarmos o Teorema 8, precisaremos definir alguns conceitos.

Definição 9. 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 10. 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 11. *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 $\mathrm{vbl}([u]) \cap \mathrm{vbl}([v]) = \emptyset$.*
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 $\mathrm{vbl}([u]) \cap \mathrm{vbl}([v]) \neq \emptyset$, 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 $\mathrm{vbl}([u]) \cap \mathrm{vbl}([v]) = \emptyset$, 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 11, 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,

$$\mathbb{E}[N_A] = \sum_{\tau \in \mathcal{T}_A} \mathbb{P}[\tau \text{ ocorre em } C]. \tag{5}$$

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 12. *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 $\left(P^{(0)}, P^{(1)}, P^{(2)}, \ldots\right)$ 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 11 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 $P \in \text{vbl}([v])$ também está atribuído o valor $P^{(|S(P,v)|)}$. Note que, na τ-verificação, depois de as variáveis em $\text{vbl}([v])$ serem reamostradas, a tabela dá exatamente esse valor para cada $P \in \text{vbl}([v])$. 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

$$S(P,v) = \{w \in V(\tau) : q(w) < q(v), P \in \text{vbl}([w])\}.$$

Portanto, antes do passo de reamostragem $q(v)$ do algoritmo de Moser-Tardos, as variáveis em $\text{vbl}([v])$ 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.

2.2. **O processo de Galton-Watson e a prova do Teorema 8.** 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 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 13. *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:

$$
\begin{aligned}
p_\tau &= \frac{1-x(A)}{x(A)} \prod_{v\in V(\tau)} \left(\frac{x([v])}{1-x([v])} \prod_{B\in\Gamma^+([v])} (1-x(B)) \right) \\
&= \frac{1-x(A)}{x(A)} \prod_{v\in V(\tau)} \left(x([v]) \prod_{B\in\Gamma([v])} (1-x(B)) \right) \\
&= \frac{1-x(A)}{x(A)} \prod_{v\in V(\tau)} x'([v]). \qquad \blacksquare
\end{aligned}
$$

Temos agora todos os elementos necessários para completar a prova do Teorema 8.

Prova do Teorema 8. Fixemos $A \in \mathcal{A}$. Usando a equação (5), as hipótestes do Teorema 8 e os lemas 12 e 13, obtemos que

$$
\begin{aligned}
\mathbb{E}[N_A] &= \sum_{\tau\in\mathcal{T}_A} \mathbb{P}[\tau \text{ ocorre em } C] \le \sum_{\tau\in\mathcal{T}_A} \prod_{v\in V(\tau)} \mathbb{P}[[v]] \le \sum_{\tau\in\mathcal{T}_A} \prod_{v\in V(\tau)} x'([v]) \\
&= \frac{x(A)}{1-x(A)} \sum_{\tau\in\mathcal{T}_A} p_\tau \le \frac{x(A)}{1-x(A)},
\end{aligned}
$$

como queríamos demonstrar. $\blacksquare$

Referências

[1] Noga Alon and Nati Linial. Cycles of length 0 modulo k in directed graphs. *J. Combin. Theory Ser. B*, 47(1):114–119, 1989. [Cited on page 4]

[2] Paul Erdős and László Lovász. Problems and results on 3-chromatic hypergraphs and some related questions. In *Infinite and finite sets (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday), Vol. II*, pages 609–627. Colloq. Math. Soc. János Bolyai, Vol. 10. North-Holland, Amsterdam, 1975. [Cited on page 1]

[3] Hugh Hind, Michael Molloy, and Bruce Reed. Colouring a graph frugally. *Combinatorica*, 17(4):469–482, 1997. [Cited on page 4]

[4] Robin A. Moser and Gábor Tardos. A constructive proof of the general Lovász local lemma. *J. ACM*, 57(2):Art. 11, 15, 2010. [Cited on page 6]

Instituto de Matemática e Estatística, Universidade de São Paulo, Rua do Matão 1010, 05508–090 São Paulo, SP

Endereços eletrônicos: bruno.cavalar@usp.br