Применение энтропии Шеннона в комбинаторных задачах

Андрей Ромащенко, LIRMM & ИППИ

06.04.2019 ВШЭ

Outline

Outline

Основные определения (1)

Как измерить неопределенность / количество информации в случайном объекте (в распределении вероятностей)?

Основные определения (1)

Как измерить неопределенность / количество информации в случайном объекте (в распределении вероятностей)?

Клод Шеннон определил энтропию

$$\mathrm{H}(\alpha) := \sum p_i \log \frac{1}{p_i}$$

для распределения с вероятностями $(p_1, \ldots, p_k)$

Основные определения (1)

Как измерить неопределенность / количество информации в случайном объекте (в распределении вероятностей)?

Клод Шеннон определил энтропию

$$\mathrm{H}(\alpha) := \sum p_i \log \frac{1}{p_i}$$

для распределения с вероятностями $(p_1, \ldots, p_k)$

комбинаторный смысл: в алфавите с k буквами число слов длины n с частотами букв $p_1, \ldots, p_k$ равно

$$2^{(\sum p_i \log \frac{1}{p_i})n + o(n)}$$

Основные определения (1)

Как измерить неопределенность / количество информации в случайном объекте (в распределении вероятностей)?

Клод Шеннон определил энтропию

$$\mathrm{H}(\alpha) := \sum p_i \log \frac{1}{p_i}$$

для распределения с вероятностями $(p_1, \ldots, p_k)$

комбинаторный смысл: в алфавите с k буквами число слов длины n с частотами букв $p_1, \ldots, p_k$ равно

$$2^{(\sum p_i \log \frac{1}{p_i})n + o(n)}$$

простейшее применение: доля двойчных слов длины n, в которых $< 30\%$ нулей и $> 70\%$ единиц, оценивается

$$< 2^{(\frac{1}{3}\log 3 + \frac{2}{3}\log \frac{3}{2} - 1)n + o(n)}$$

Основные определения (2)

Как измерить неопределенность / количество информации в *частично известном* случайном объекте?

Основные определения (2)

Как измерить неопределенность / количество информации в *частично известном* случайном объекте?

Клод Шеннон: энтропия условного распределения

$$\mathrm{H}(\alpha \,|\, \beta) := \sum \mathrm{prob}[\beta = B_i] \cdot \mathrm{H}(\alpha \,|\, \beta = B_i)$$

Основные определения (3)

Как измерить полезность / количество информации
в *одном объекте* **для описания** *другого* **объекта?**

Основные определения (3)

Как измерить полезность / количество информации в *одном объекте* для описания *другого* объекта?

Клод Шеннон:

$$\mathrm{I}(\alpha : \beta) := \mathrm{H}(\beta) - \mathrm{H}(\beta \,|\, \alpha)$$

Основные определения (4)

Как измерить полезность / количество информации в *одном объекте* для описания *другого* объекта?

Клод Шеннон:

$$\mathrm{I}(\alpha : \beta \,|\, \gamma) := \mathrm{H}(\beta \,|\, \gamma) - \mathrm{H}(\beta \,|\, \alpha, \gamma)$$

Outline

Основные свойства энтропии

Основные свойства энтропии

Определение $\mathrm{H}(a) := \sum_{i=1}^{k} p_i \log \frac{1}{p_i}$

Основные свойства энтропии

Определение $\mathrm{H}(a) := \sum_{i=1}^{k} p_i \log \frac{1}{p_i}$

- $0 \leq \mathrm{H}(a) \leq \log k$ (неравенство Йенсена + вогнутость логарифма)

Основные свойства энтропии

Определение $\mathrm{H}(a) := \sum_{i=1}^{k} p_i \log \frac{1}{p_i}$

- $0 \le \mathrm{H}(a) \le \log k$ (неравенство Йенсена + вогнутость логарифма)
- $\mathrm{H}(a, b) = \mathrm{H}(a) + \mathrm{H}(b \mid a)$ (тривиально)

Основные свойства энтропии

Определение $\mathrm{H}(a) := \sum_{i=1}^{k} p_i \log \frac{1}{p_i}$

- $0 \le \mathrm{H}(a) \le \log k$ (неравенство Йенсена + вогнутость логарифма)
- $\mathrm{H}(a,b) = \mathrm{H}(a) + \mathrm{H}(b \mid a)$ (тривиально)
  $\le \mathrm{H}(a) + \mathrm{H}(b)$ (неравенство Йенсена)

Базовые неравенства для энтропии

- монотонность: $\mathrm{H}(a) \leq \mathrm{H}(a, b)$

Базовые неравенства для энтропии

- монотонность: $\mathrm{H}(a) \le \mathrm{H}(a,b)$ (a.k.a. $\mathrm{H}(b \mid a) \ge 0$)

Базовые неравенства для энтропии

- монотонность: $\mathrm{H}(a) \le \mathrm{H}(a,b)$ (a.k.a. $\mathrm{H}(b \mid a) \ge 0$)
- субаддитивность: $\mathrm{H}(a,b) \le \mathrm{H}(a) + \mathrm{H}(b)$

Базовые неравенства для энтропии

- монотонность: $\mathrm{H}(a) \le \mathrm{H}(a,b)$ (a.k.a. $\mathrm{H}(b \mid a) \ge 0$)
- субаддитивность: $\mathrm{H}(a,b) \le \mathrm{H}(a) + \mathrm{H}(b)$ (a.k.a. $\mathrm{I}(a:b) \ge 0$)

Базовые неравенства для энтропии

- монотонность: $\mathrm{H}(a) \le \mathrm{H}(a,b)$ (a.k.a. $\mathrm{H}(b \mid a) \ge 0$)
- субаддитивность: $\mathrm{H}(a,b) \le \mathrm{H}(a) + \mathrm{H}(b)$ (a.k.a. $\mathrm{I}(a:b) \ge 0$)
- субмодулярность: $\mathrm{H}(a,b,c) + \mathrm{H}(a) \le \mathrm{H}(a,b) + \mathrm{H}(a,c)$

Базовые неравенства для энтропии

- монотонность: $\mathrm{H}(a) \le \mathrm{H}(a,b)$ (a.k.a. $\mathrm{H}(b \mid a) \ge 0$)
- субаддитивность: $\mathrm{H}(a,b) \le \mathrm{H}(a) + \mathrm{H}(b)$ (a.k.a. $\mathrm{I}(a:b) \ge 0$)
- субмодулярность: $\mathrm{H}(a,b,c) + \mathrm{H}(a) \le \mathrm{H}(a,b) + \mathrm{H}(a,c)$
  (a.k.a. $\mathrm{I}(b:c \mid a) \ge 0$)

Базовые неравенства для энтропии

- монотонность: $\mathrm{H}(a) \le \mathrm{H}(a,b)$ (a.k.a. $\mathrm{H}(b \mid a) \ge 0$)
- субаддитивность: $\mathrm{H}(a,b) \le \mathrm{H}(a) + \mathrm{H}(b)$ (a.k.a. $\mathrm{I}(a:b) \ge 0$)
- субмодулярность: $\mathrm{H}(a,b,c) + \mathrm{H}(a) \le \mathrm{H}(a,b) + \mathrm{H}(a,c)$ (a.k.a. $\mathrm{I}(b:c \mid a) \ge 0$)

плюс подстановки

Базовые неравенства для энтропии

- монотонность: $\mathrm{H}(a) \le \mathrm{H}(a,b)$ (a.k.a. $\mathrm{H}(b \mid a) \ge 0$)
- субаддитивность: $\mathrm{H}(a,b) \le \mathrm{H}(a) + \mathrm{H}(b)$ (a.k.a. $\mathrm{I}(a:b) \ge 0$)
- субмодулярность: $\mathrm{H}(a,b,c) + \mathrm{H}(a) \le \mathrm{H}(a,b) + \mathrm{H}(a,c)$ (a.k.a. $\mathrm{I}(b:c \mid a) \ge 0$)

плюс подстановки
e.g., $\mathrm{H}(a_1,a_2) \le \mathrm{H}(a_1,a_2,b)$

Базовые неравенства для энтропии

- монотонность: $\mathrm{H}(a) \le \mathrm{H}(a,b)$ (a.k.a. $\mathrm{H}(b \mid a) \ge 0$)
- субаддитивность: $\mathrm{H}(a,b) \le \mathrm{H}(a) + \mathrm{H}(b)$ (a.k.a. $\mathrm{I}(a:b) \ge 0$)
- субмодулярность: $\mathrm{H}(a,b,c) + \mathrm{H}(a) \le \mathrm{H}(a,b) + \mathrm{H}(a,c)$ (a.k.a. $\mathrm{I}(b:c \mid a) \ge 0$)

плюс подстановки
e.g., $\mathrm{H}(a_1,a_2) \le \mathrm{H}(a_1,a_2,b)$

плюс все (положительные) линейные комбинации

Базовые неравенства для энтропии

- монотонность: $\mathrm{H}(a) \le \mathrm{H}(a,b)$ (a.k.a. $\mathrm{H}(b \mid a) \ge 0$)
- субаддитивность: $\mathrm{H}(a,b) \le \mathrm{H}(a) + \mathrm{H}(b)$ (a.k.a. $\mathrm{I}(a:b) \ge 0$)
- субмодулярность: $\mathrm{H}(a,b,c) + \mathrm{H}(a) \le \mathrm{H}(a,b) + \mathrm{H}(a,c)$ (a.k.a. $\mathrm{I}(b:c \mid a) \ge 0$)

плюс подстановки
e.g., $\mathrm{H}(a_1,a_2) \le \mathrm{H}(a_1,a_2,b)$

плюс все (положительные) линейные комбинации
e.g., $2\mathrm{H}(a) + \mathrm{H}(a,b,c) \le 2\mathrm{H}(a,b) + \mathrm{H}(a,c)$

чуть менее стандартные неравенства (1)

- $2\mathrm{H}(a,b,c) \leq \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$

чуть менее стандартные неравенства (1)

- $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$

Магическое доказательство:

чуть менее стандартные неравенства (1)

- $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$

Магическое доказательство:

$$\mathrm{I}(b:c) \ge 0$$

чуть менее стандартные неравенства (1)

- $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$

Магическое доказательство:

$$\mathrm{I}(b:c) \ge 0 \quad \longrightarrow \quad \mathrm{H}(b,c) \le \mathrm{H}(b) + \mathrm{H}(c)$$

чуть менее стандартные неравенства (1)

- $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$

Магическое доказательство:

$$\begin{array}{r} \mathrm{I}(b:c) \ge 0 \\ \mathrm{I}(a:c\,|\,b) \ge 0 \end{array} \quad \longrightarrow \quad \mathrm{H}(b,c) \le \mathrm{H}(b) + \mathrm{H}(c)$$

чуть менее стандартные неравенства (1)

- $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$

Магическое доказательство:

$$\begin{array}{rcrcl} \mathrm{I}(b:c) \ge 0 & \longrightarrow & \mathrm{H}(b,c) & \le & \mathrm{H}(b) + \mathrm{H}(c) \\ \mathrm{I}(a:c \mid b) \ge 0 & \longrightarrow & \mathrm{H}(b) + \mathrm{H}(a,b,c) & \le & \mathrm{H}(a,b) + \mathrm{H}(b,c) \end{array}$$

чуть менее стандартные неравенства (1)

- $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$

Магическое доказательство:

$$\begin{array}{rcrcl} \mathrm{I}(b:c) \ge 0 & \longrightarrow & \mathrm{H}(b,c) & \le & \mathrm{H}(b) + \mathrm{H}(c) \\ \mathrm{I}(a:c\,|\,b) \ge 0 & \longrightarrow & \mathrm{H}(b) + \mathrm{H}(a,b,c) & \le & \mathrm{H}(a,b) + \mathrm{H}(b,c) \\ \mathrm{I}(a:b\,|\,c) \ge 0 & & & & \end{array}$$

чуть менее стандартные неравенства (1)

- $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$

Магическое доказательство:

$$\begin{array}{rcrcl}
\mathrm{I}(b:c) \ge 0 & \longrightarrow & \mathrm{H}(b,c) & \le & \mathrm{H}(b) + \mathrm{H}(c) \\
\mathrm{I}(a:c\,|\,b) \ge 0 & \longrightarrow & \mathrm{H}(b) + \mathrm{H}(a,b,c) & \le & \mathrm{H}(a,b) + \mathrm{H}(b,c) \\
\mathrm{I}(a:b\,|\,c) \ge 0 & \longrightarrow & \mathrm{H}(c) + \mathrm{H}(a,b,c) & \le & \mathrm{H}(a,c) + \mathrm{H}(b,c)
\end{array}$$

чуть менее стандартные неравенства (1)

- $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$

Магическое доказательство:

$$
\begin{array}{rcrcl}
\mathrm{I}(b:c) \ge 0 & \longrightarrow & \mathrm{H}(b,c) & \le & \mathrm{H}(b) + \mathrm{H}(c) \\
\mathrm{I}(a:c\,|\,b) \ge 0 & \longrightarrow & \mathrm{H}(b) + \mathrm{H}(a,b,c) & \le & \mathrm{H}(a,b) + \mathrm{H}(b,c) \\
\mathrm{I}(a:b\,|\,c) \ge 0 & \longrightarrow & \mathrm{H}(c) + \mathrm{H}(a,b,c) & \le & \mathrm{H}(a,c) + \mathrm{H}(b,c) \\
 & & & & \\
\text{суммируем} & \longrightarrow & 2\mathrm{H}(a,b,c) & \le & \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)
\end{array}
$$

чуть менее стандартные неравенства (2)

- $\mathrm{H}(c) \leq \mathrm{H}(c|a) + \mathrm{H}(c|b) + \mathrm{I}(a:b)$

чуть менее стандартные неравенства (2)

- $\mathrm{H}(c) \le \mathrm{H}(c|a) + \mathrm{H}(c|b) + \mathrm{I}(a:b)$

Магическое доказательство:

чуть менее стандартные неравенства (2)

- $\mathrm{H}(c) \le \mathrm{H}(c|a) + \mathrm{H}(c|b) + \mathrm{I}(a:b)$

Магическое доказательство:

$\mathrm{I}(a:b|c) \ge 0$

чуть менее стандартные неравенства (2)

- $\mathrm{H}(c) \le \mathrm{H}(c|a) + \mathrm{H}(c|b) + \mathrm{I}(a:b)$

Магическое доказательство:

$$\mathrm{I}(a:b|c) \ge 0 \quad \longrightarrow \quad \mathrm{H}(a,b,c) + \mathrm{H}(c) \quad \le \quad \mathrm{H}(a,c) + \mathrm{H}(b,c)$$

чуть менее стандартные неравенства (2)

- $\mathrm{H}(c) \le \mathrm{H}(c|a) + \mathrm{H}(c|b) + \mathrm{I}(a:b)$

Магическое доказательство:

$$\begin{array}{l} \mathrm{I}(a:b|c) \ge 0 \\ \mathrm{H}(c|a,b) \ge 0 \end{array} \quad \longrightarrow \quad \mathrm{H}(a,b,c) + \mathrm{H}(c) \quad \le \quad \mathrm{H}(a,c) + \mathrm{H}(b,c)$$

чуть менее стандартные неравенства (2)

- $\mathrm{H}(c) \le \mathrm{H}(c|a) + \mathrm{H}(c|b) + \mathrm{I}(a:b)$

Магическое доказательство:

$$\begin{array}{lcccc} \mathrm{I}(a:b|c) \ge 0 & \longrightarrow & \mathrm{H}(a,b,c) + \mathrm{H}(c) & \le & \mathrm{H}(a,c) + \mathrm{H}(b,c) \\ \mathrm{H}(c|a,b) \ge 0 & \longrightarrow & \mathrm{H}(a,b) & \le & \mathrm{H}(a,b,c) \end{array}$$

чуть менее стандартные неравенства (2)

- $\mathrm{H}(c) \le \mathrm{H}(c|a) + \mathrm{H}(c|b) + \mathrm{I}(a:b)$

Магическое доказательство:

$$
\begin{array}{lcrcl}
\mathrm{I}(a:b|c) \ge 0 & \longrightarrow & \mathrm{H}(a,b,c) + \mathrm{H}(c) & \le & \mathrm{H}(a,c) + \mathrm{H}(b,c) \\
\mathrm{H}(c|a,b) \ge 0 & \longrightarrow & \mathrm{H}(a,b) & \le & \mathrm{H}(a,b,c) \\
\text{суммируем} & \longrightarrow & \mathrm{H}(c) & \le & \mathrm{H}(a,c) + \mathrm{H}(b,c) - \mathrm{H}(a,b) \\
 & & & = & \mathrm{H}(a,c) - \mathrm{H}(a) + \mathrm{H}(b,c) - \mathrm{H}(b) \\
 & & & & + \mathrm{H}(a) + \mathrm{H}(b) - \mathrm{H}(a,b)
\end{array}
$$

Двойственное описание: энтропийный профиль распределения

Что ограничивают информационные неравенства?

Двойственное описание: энтропийный профиль распределения

Что ограничивают информационные неравенства?

энтропийный профиль:

$(a, b) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(a, b) \rangle$

Двойственное описание: энтропийный профиль распределения

Что ограничивают информационные неравенства?

энтропийный профиль:

$(a, b) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(a, b) \rangle$

$(a, b, c) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(c), \mathrm{H}(a, b), \mathrm{H}(a, c), \mathrm{H}(b, c), \mathrm{H}(a, b, c) \rangle$

Двойственное описание: энтропийный профиль распределения

Что ограничивают информационные неравенства?

энтропийный профиль:

$(a, b) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(a, b) \rangle$

$(a, b, c) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(c), \mathrm{H}(a, b), \mathrm{H}(a, c), \mathrm{H}(b, c), \mathrm{H}(a, b, c) \rangle$

[n случайных величин] $\mapsto$ [набор из $2^n - 1$ энтропий]

Двойственное описание: энтропийный профиль распределения

Что ограничивают информационные неравенства?

энтропийный профиль:

$(a, b) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(a, b) \rangle$

$(a, b, c) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(c), \mathrm{H}(a, b), \mathrm{H}(a, c), \mathrm{H}(b, c), \mathrm{H}(a, b, c) \rangle$

[n случайных величин] $\mapsto$ [набор из $2^n - 1$ энтропий]

Информационные неравенства суть ограничения для множества *энтропийных профилей*.

Двойственное описание: энтропийный профиль распределения

энтропийный профиль:

$[n$ случайных величин$] \mapsto$ [набор из $2^n - 1$ энтропий]

- [2 случайные величины] $\mapsto$ [набор из $2^2 - 1 = 3$ энтропий]
  $(a, b) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(a, b) \rangle$
- [3 случайные величины] $\mapsto$ [набор из $2^3 - 1 = 7$ энтропий]
  $(a, b, c) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(c), \mathrm{H}(a, b), \mathrm{H}(a, c), \mathrm{H}(b, c), \mathrm{H}(a, b, c) \rangle$
- . . . . . .

  . . . . . .

Двойственное описание: энтропийный профиль распределения

энтропийный профиль:

$$[n \text{ случайных величин}] \mapsto [\text{набор из } 2^n - 1 \text{ энтропий}]$$

- $[2 \text{ случайные величины}] \mapsto [\text{набор из } 2^2 - 1 = 3 \text{ энтропий}]$
  $(a, b) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(a, b) \rangle$
- $[3 \text{ случайные величины}] \mapsto [\text{набор из } 2^3 - 1 = 7 \text{ энтропий}]$
  $(a, b, c) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(c), \mathrm{H}(a, b), \mathrm{H}(a, c), \mathrm{H}(b, c), \mathrm{H}(a, b, c) \rangle$
- . . . . . .
  . . . . . .

другая система координат:

Двойственное описание: энтропийный профиль распределения

энтропийный профиль:

$$[n \text{ случайных величин}] \mapsto [\text{набор из } 2^n - 1 \text{ энтропий}]$$

- $[2 \text{ случайные величины}] \mapsto [\text{набор из } 2^2 - 1 = 3 \text{ энтропий}]$
  $(a, b) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(a, b) \rangle$
- $[3 \text{ случайные величины}] \mapsto [\text{набор из } 2^3 - 1 = 7 \text{ энтропий}]$
  $(a, b, c) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(c), \mathrm{H}(a, b), \mathrm{H}(a, c), \mathrm{H}(b, c), \mathrm{H}(a, b, c) \rangle$
- . . . . . .
  . . . . . .

другая система координат:

$(a, b) \mapsto \langle \mathrm{H}(a \mid b), \mathrm{H}(b \mid a), \mathrm{I}(a : b) \rangle$

Двойственное описание: энтропийный профиль распределения

энтропийный профиль:

$$[n \text{ случайных величин}] \mapsto [\text{набор из } 2^n - 1 \text{ энтропий}]$$

- $[2 \text{ случайные величины}] \mapsto [\text{набор из } 2^2 - 1 = 3 \text{ энтропий}]$
  $(a, b) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(a, b) \rangle$
- $[3 \text{ случайные величины}] \mapsto [\text{набор из } 2^3 - 1 = 7 \text{ энтропий}]$
  $(a, b, c) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(c), \mathrm{H}(a, b), \mathrm{H}(a, c), \mathrm{H}(b, c), \mathrm{H}(a, b, c) \rangle$
- . . . . . .
  . . . . . .

другая система координат:

$(a, b) \mapsto \langle \mathrm{H}(a \mid b), \mathrm{H}(b \mid a), \mathrm{I}(a : b) \rangle$

$(a, b, c) \mapsto \langle \mathrm{H}(a|b, c), \mathrm{H}(b|a, c), \mathrm{H}(c|a, b), \mathrm{I}(a : b|c), \mathrm{I}(a : c|b), \mathrm{I}(b : c|a) \rangle$

Двойственное описание: энтропийный профиль распределения

энтропийный профиль:

$[n$ случайных величин$] \mapsto$ [набор из $2^n - 1$ энтропий]

- [2 случайные величины] $\mapsto$ [набор из $2^2 - 1 = 3$ энтропий]
  $(a, b) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(a, b) \rangle$
- [3 случайные величины] $\mapsto$ [набор из $2^3 - 1 = 7$ энтропий]
  $(a, b, c) \mapsto \langle \mathrm{H}(a), \mathrm{H}(b), \mathrm{H}(c), \mathrm{H}(a, b), \mathrm{H}(a, c), \mathrm{H}(b, c), \mathrm{H}(a, b, c) \rangle$
- . . . . . .
  . . . . . .

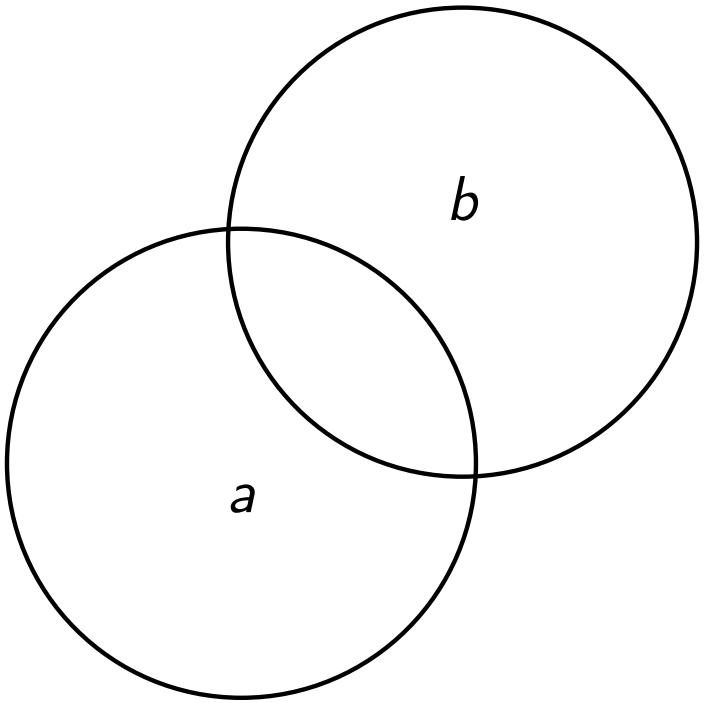
другая система координат:

$(a, b) \mapsto \langle \mathrm{H}(a \mid b), \mathrm{H}(b \mid a), \mathrm{I}(a : b) \rangle$

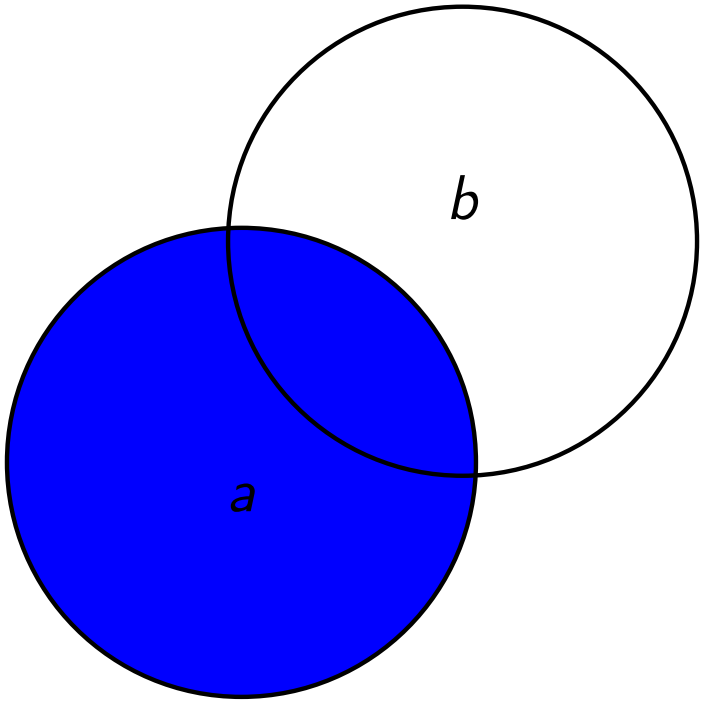
$(a, b, c) \mapsto \langle \mathrm{H}(a|b, c), \mathrm{H}(b|a, c), \mathrm{H}(c|a, b), \mathrm{I}(a : b|c), \mathrm{I}(a : c|b), \mathrm{I}(b : c|a) \rangle$

. . . . . .

Диаграммы Эйлера для энтропийного профиля

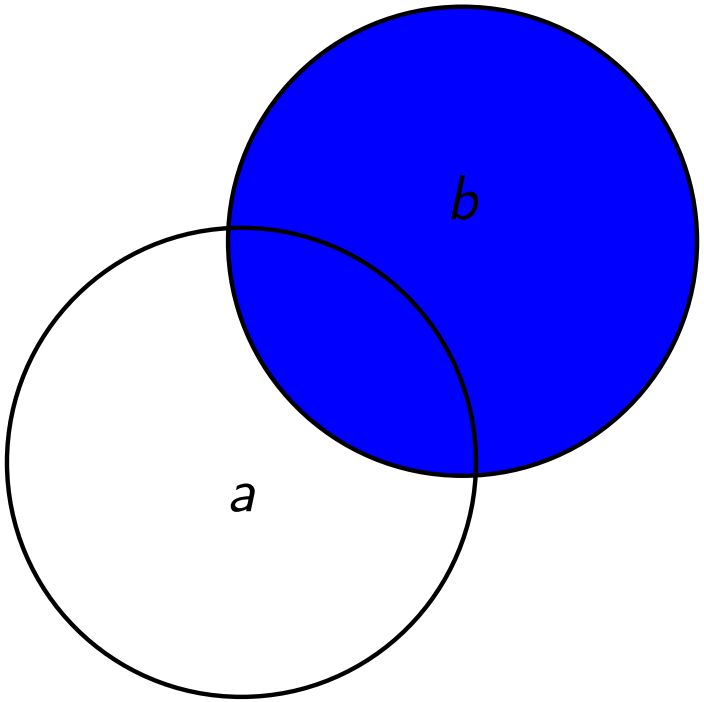


Диаграммы Эйлера для энтропийного профиля



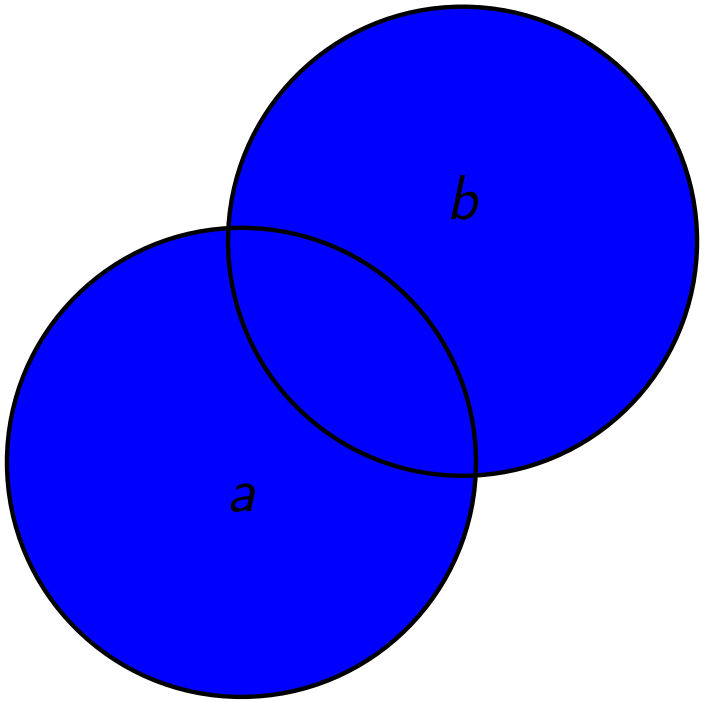
$\mathrm{H}(a)$

Диаграммы Эйлера для энтропийного профиля



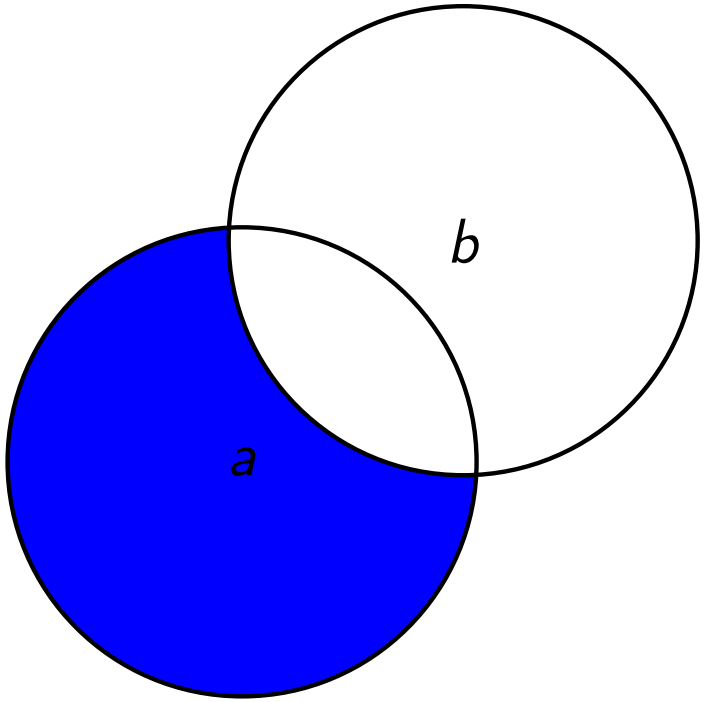
$\mathrm{H}(b)$

Диаграммы Эйлера для энтропийного профиля



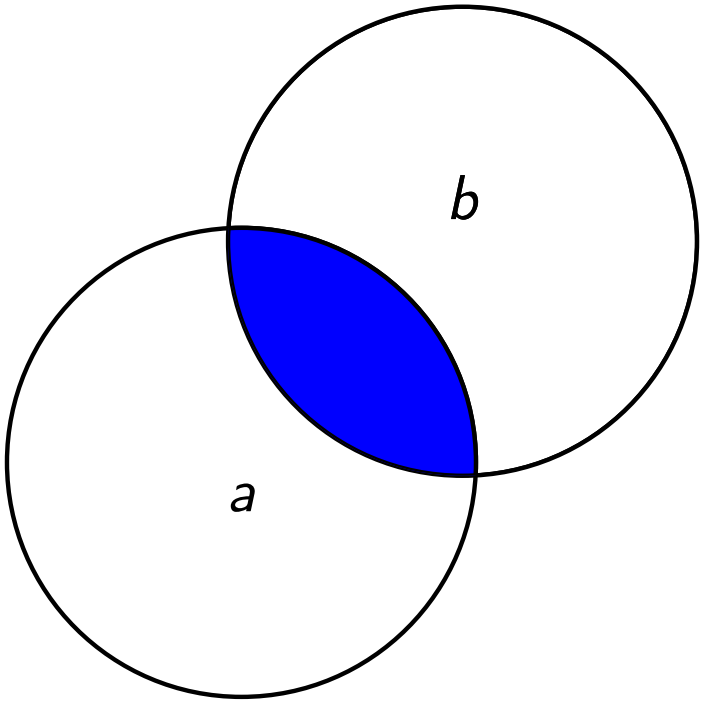
$\mathrm{H}(a, b)$

Диаграммы Эйлера для энтропийного профиля



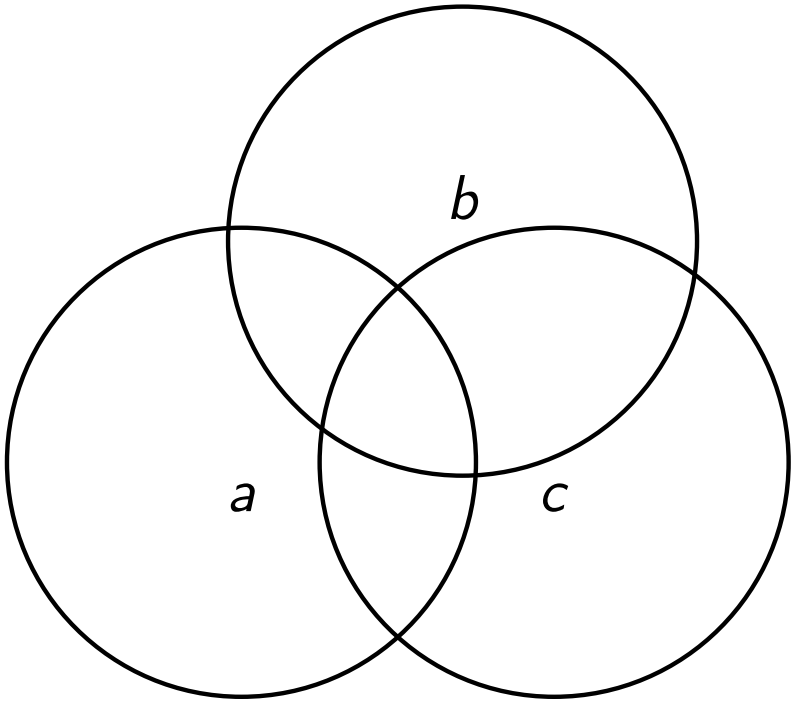
$$\mathrm{H}(a \mid b) = \mathrm{H}(a, b) - \mathrm{H}(b)$$

Диаграммы Эйлера для энтропийного профиля

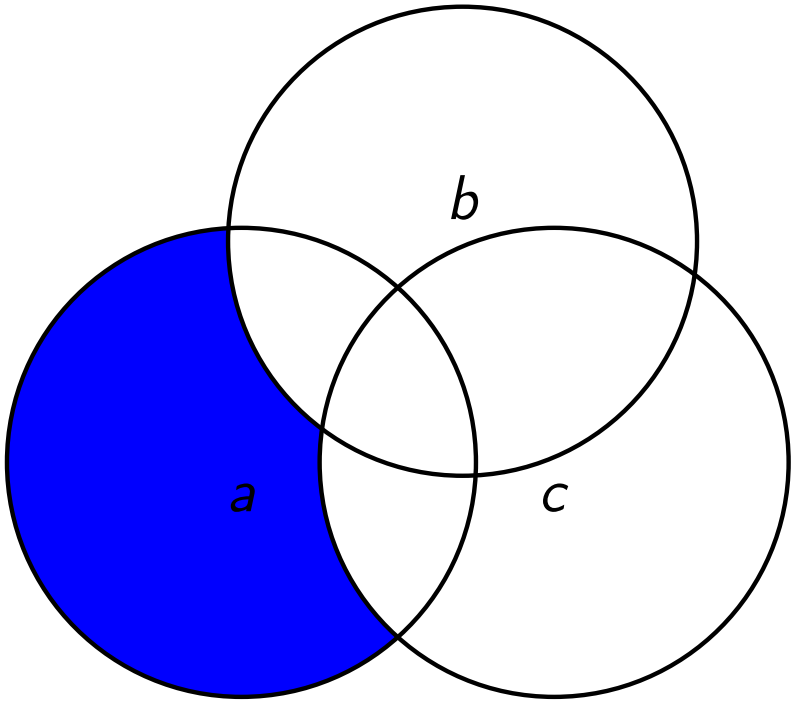


$$\mathrm{I}(a : b) = \mathrm{H}(a) + \mathrm{H}(b) - \mathrm{H}(a, b)$$

Диаграммы Эйлера для энтропийного профиля

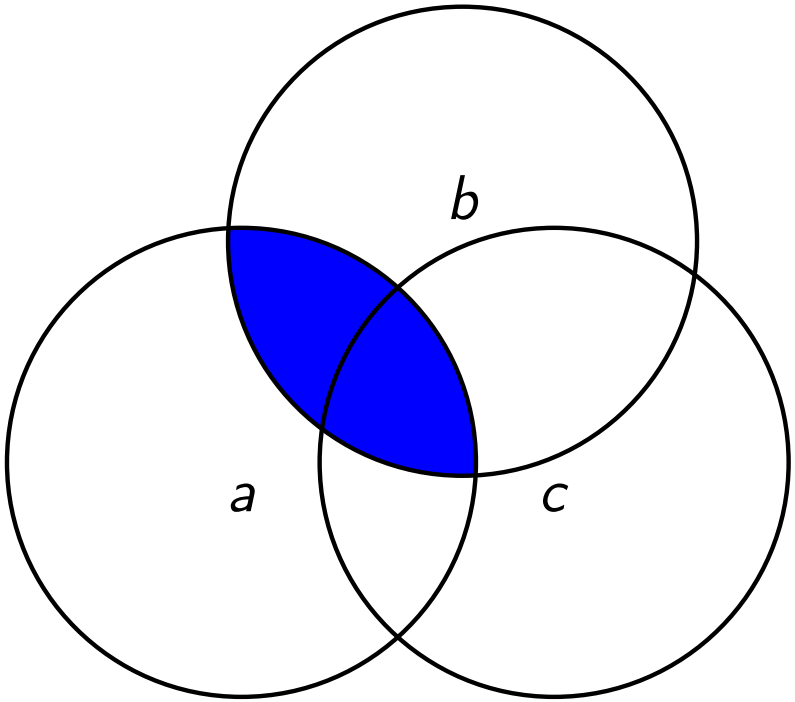


Диаграммы Эйлера для энтропийного профиля



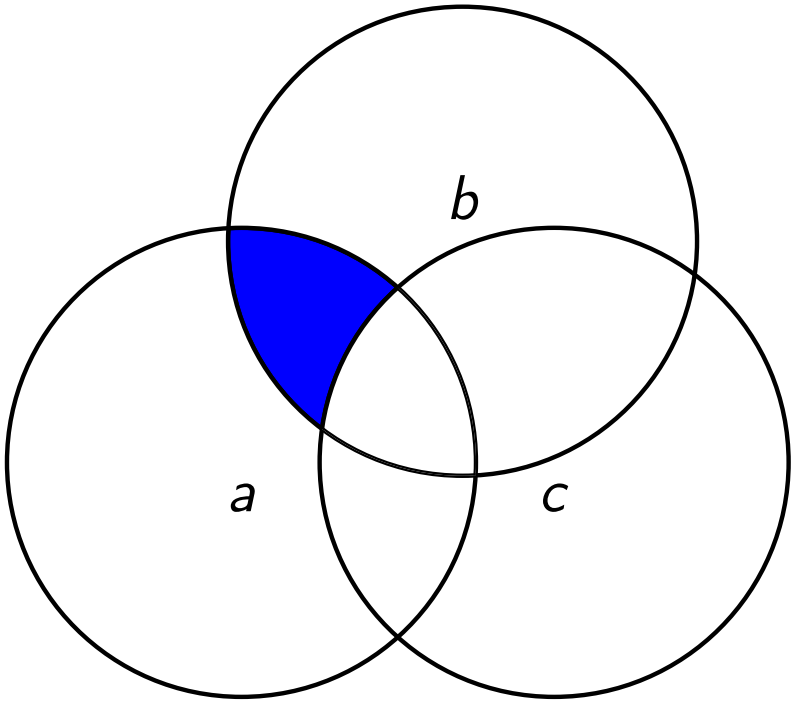
$$\mathrm{H}(a \mid b, c) = \mathrm{H}(a, b, c) - \mathrm{H}(b, c)$$

Диаграммы Эйлера для энтропийного профиля



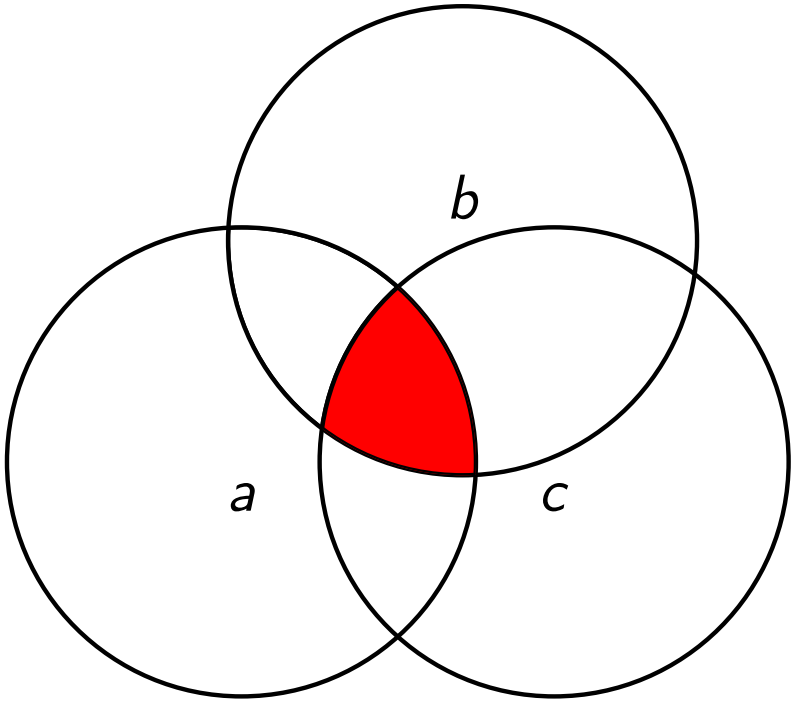
$$\mathrm{I}(a : b) = \mathrm{H}(a) + \mathrm{H}(b) - \mathrm{H}(a, b)$$

Диаграммы Эйлера для энтропийного профиля



$$\mathrm{I}(a : b \,|\, c) = \mathrm{H}(a, c) + \mathrm{H}(b, c) - \mathrm{H}(a, b, c) - \mathrm{H}(c)$$

Диаграммы Эйлера для энтропийного профиля



$$\mathrm{I}(a:b:c) = \mathrm{H}(a) + \mathrm{H}(b) + \mathrm{H}(c) - \mathrm{H}(a,b) - \mathrm{H}(a,c) - \mathrm{H}(b,c) + \mathrm{H}(a,b,c)$$

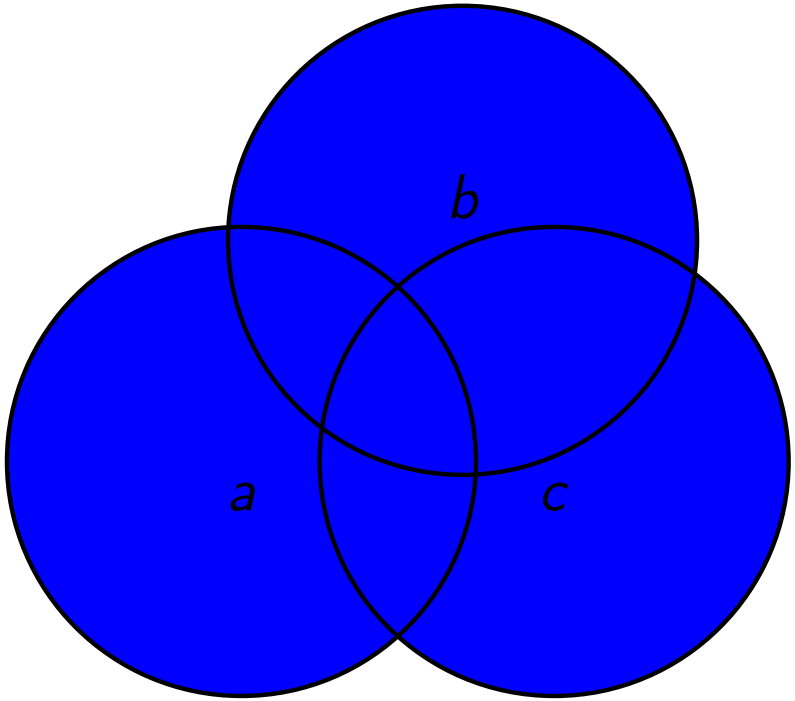
(может быть отрицательной!)

Пример доказательства с помощью диаграммы

Как доказать $2\mathrm{H}(a,b,c) \leq \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?

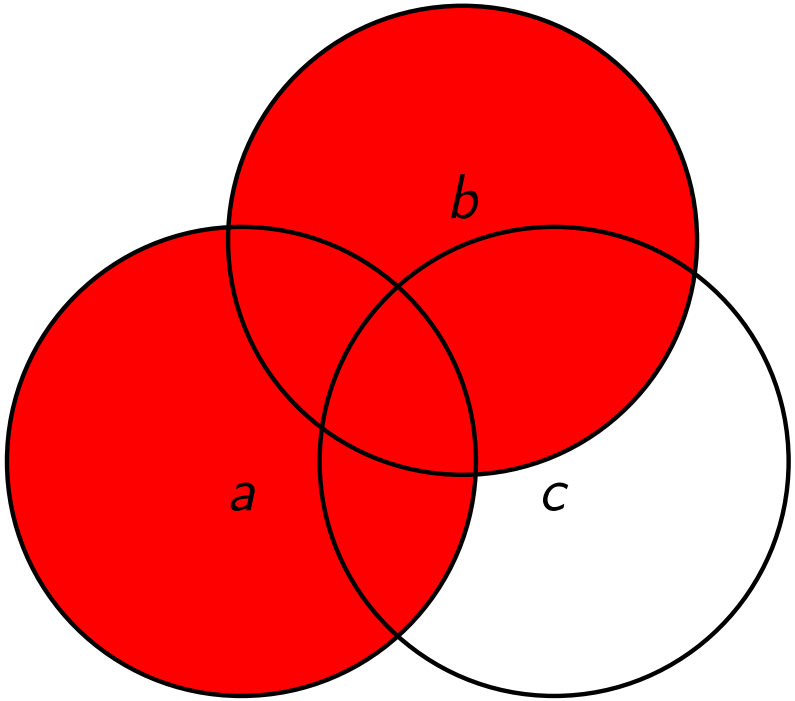
Пример доказательства с помощью диаграммы

Как доказать $2\mathrm{H}(a,b,c) \leq \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



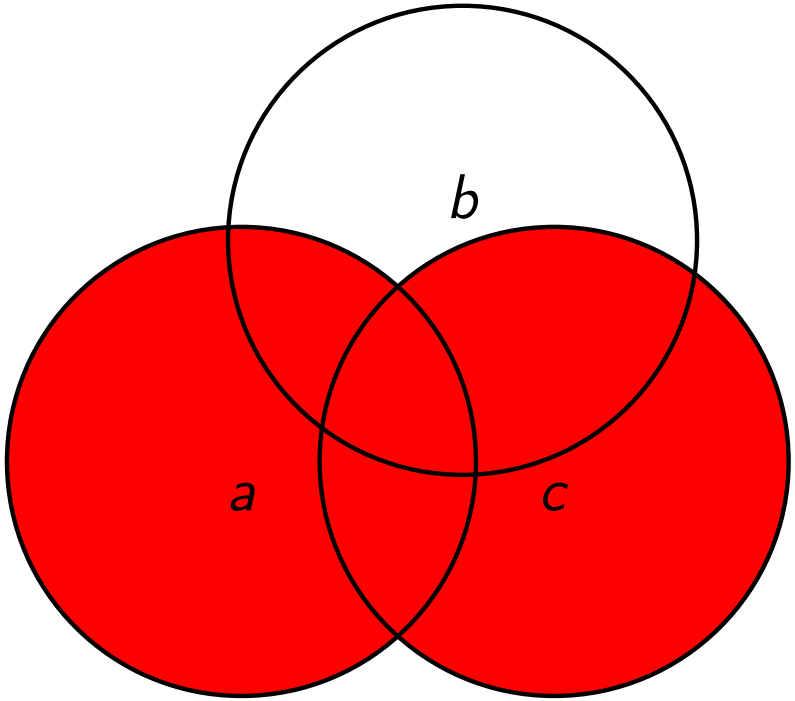
Пример доказательства с помощью диаграммы

Как доказать $2\mathrm{H}(a,b,c) \leq \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



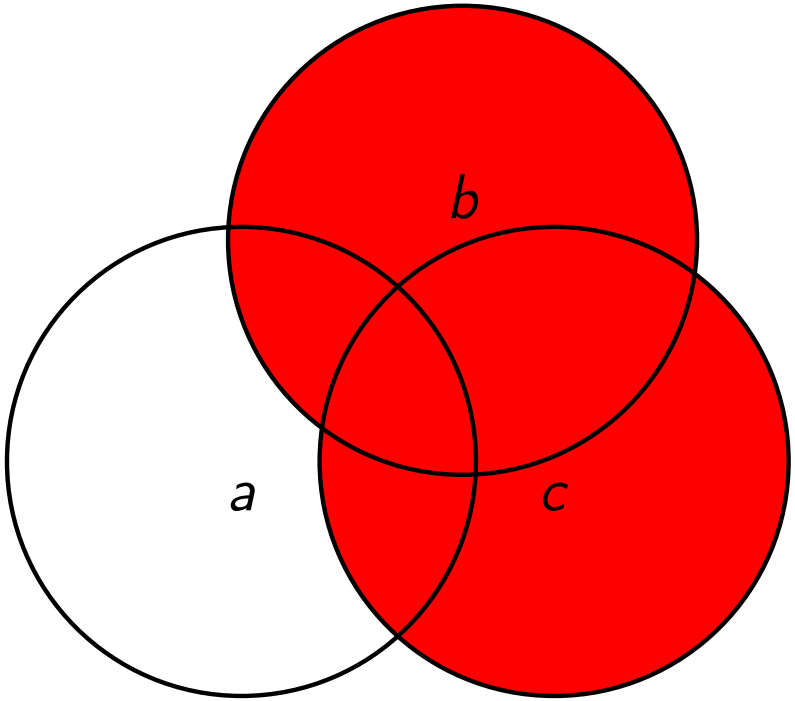
Пример доказательства с помощью диаграммы

Как доказать $2\mathrm{H}(a,b,c) \leq \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



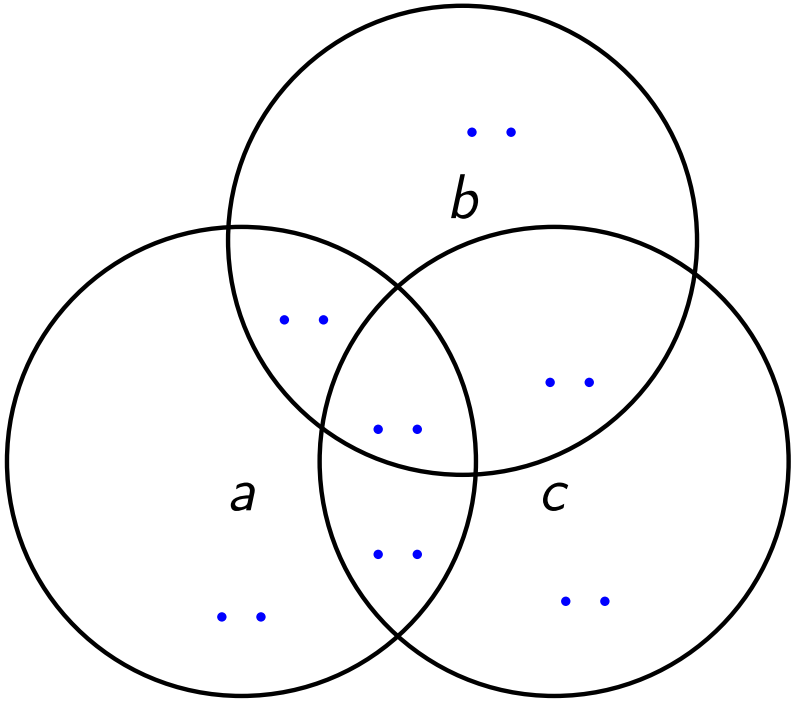
Пример доказательства с помощью диаграммы

Как доказать $2\mathrm{H}(a,b,c) \leq \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



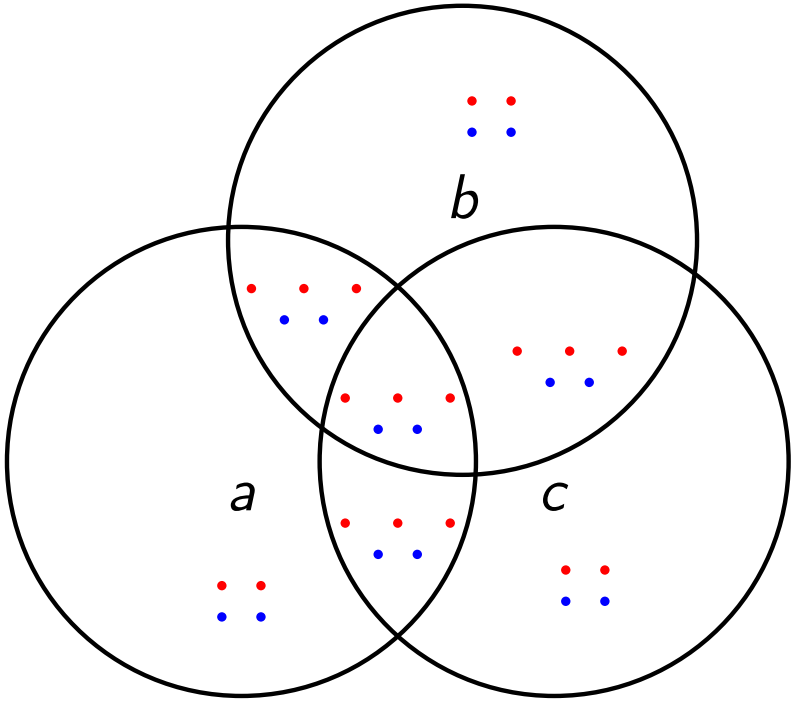
Пример доказательства с помощью диаграммы

Как доказать $2\mathrm{H}(a,b,c) \leq \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



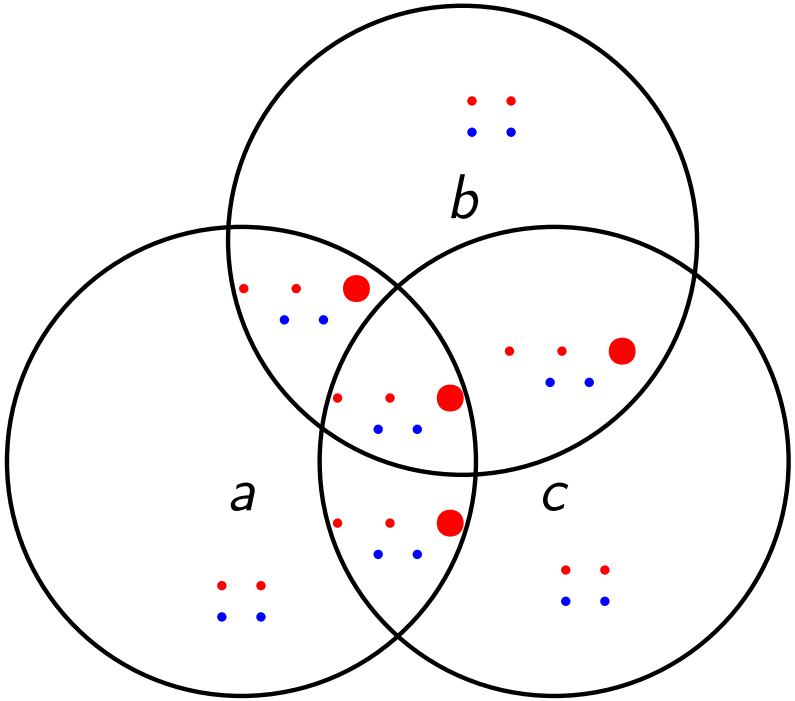
Пример доказательства с помощью диаграммы

Как доказать $2\mathrm{H}(a,b,c) \leq \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



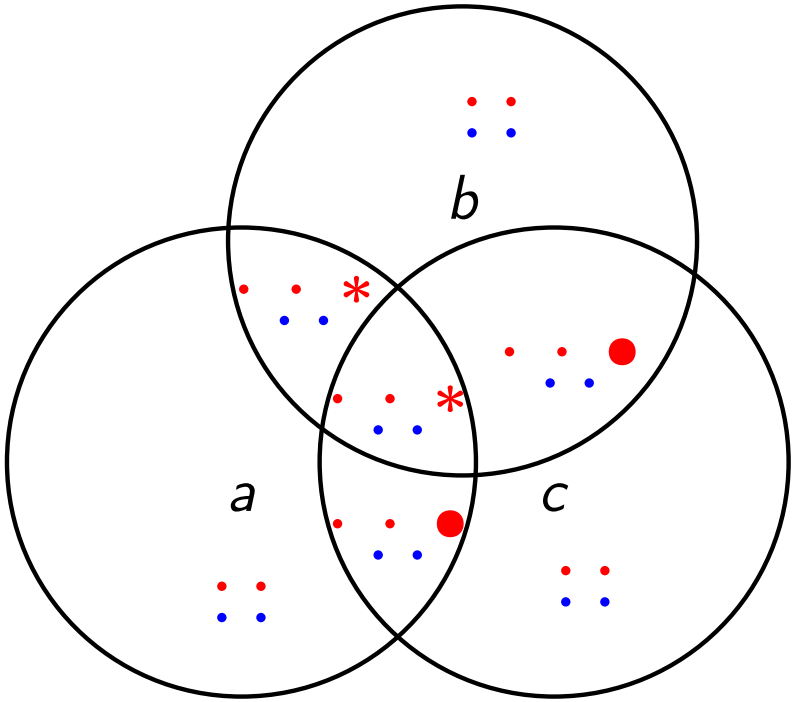
Пример доказательства с помощью диаграммы

Как доказать $2\mathrm{H}(a,b,c) \leq \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



Пример доказательства с помощью диаграммы

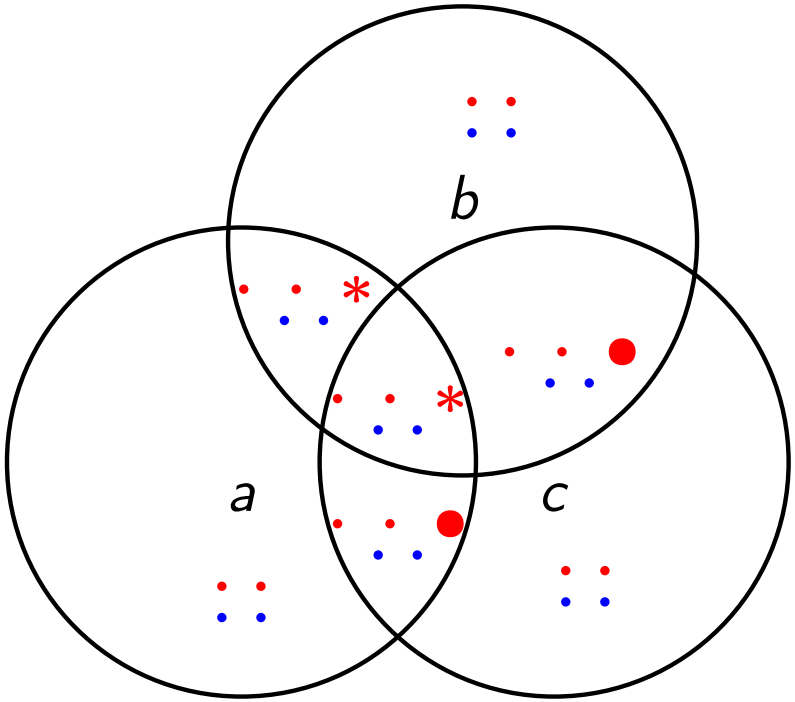
Как доказать $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



[правая часть] $-$ [левая часть] $= \mathrm{I}(a:b) + \mathrm{I}(a:c\,|\,b) + \mathrm{I}(b:c\,|\,a)$

Пример доказательства с помощью диаграммы

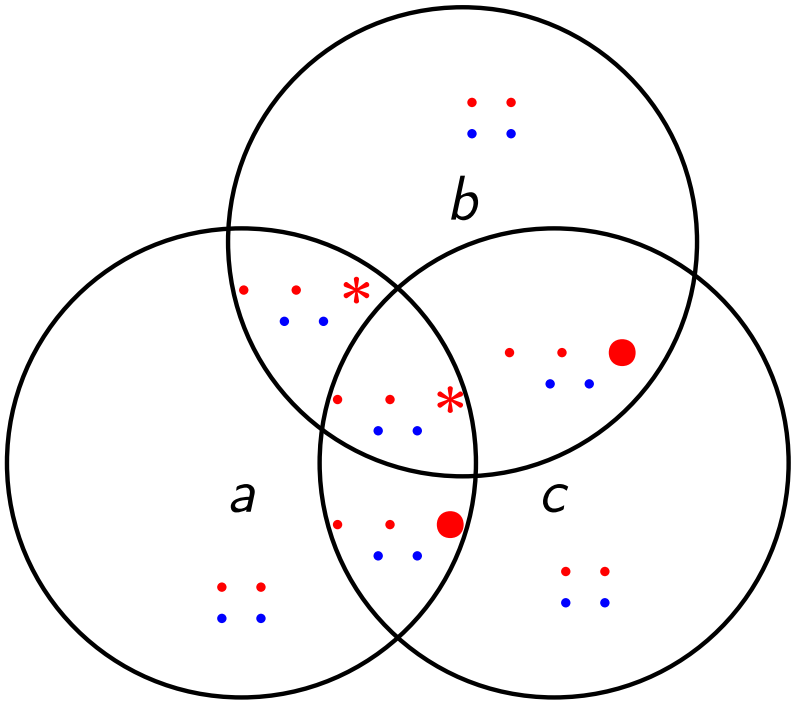
Как доказать $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



[правая часть] $-$ [левая часть] $= \mathrm{I}(a:b) + \mathrm{I}(a:c\,|\,b) + \mathrm{I}(b:c\,|\,a) \ge 0$

Пример доказательства с помощью диаграммы

Как доказать $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



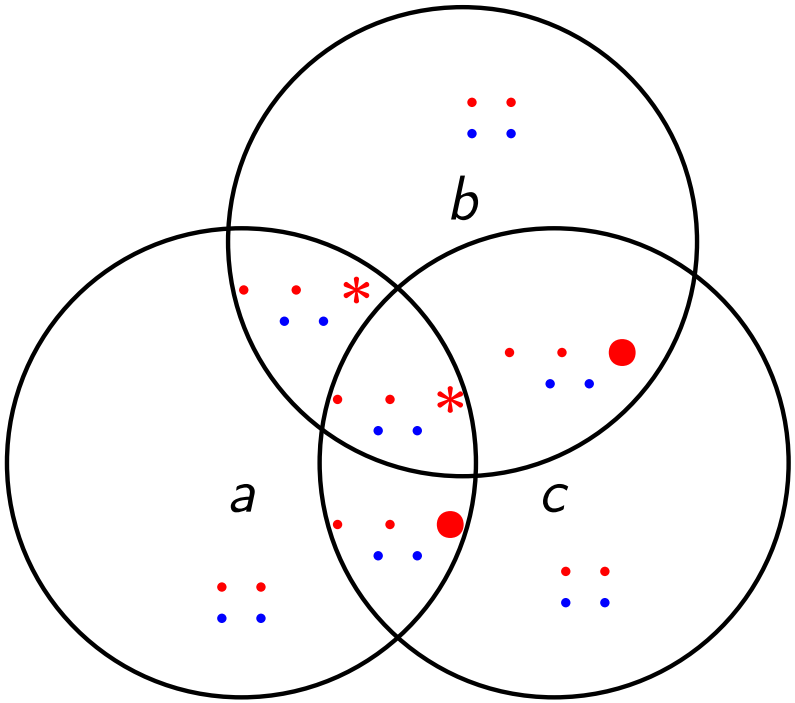
[правая часть] $-$ [левая часть] $= \mathrm{I}(a:b) + \mathrm{I}(a:c\,|\,b) + \mathrm{I}(b:c\,|\,a) \ge 0$

Простое доказательство, простая картинка...

Что делать, если нам нужны неравенства для > 3 переменных?

Пример доказательства с помощью диаграммы

Как доказать $2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(a,c) + \mathrm{H}(b,c)$?



$$[\text{RHS}] - [\text{LHS}] = \mathrm{I}(a:b) + \mathrm{I}(a:c \mid b) + \mathrm{I}(b:c \mid a) \ge 0$$

Outline

Комбинаторное применение 1: теорема Брэгмана (1)

Теорема. Если в двудольном графе $|L| = |R| = n$, то число совершенных паросочетаний не больше

$$\prod_{v \in A} (\deg(v)!)^{1/\deg(v)}.$$

Комбинаторное применение 1: теорема Брэгмана (1)

Теорема. Если в двудольном графе $|L| = |R| = n$, то число совершенных паросочетаний не больше

$$\prod_{v \in A} (\deg(v)!)^{1/\deg(v)}.$$

Наивное рассуждение: Обозначим случайное паросочетание σ.

$$\begin{aligned} \mathrm{H}(\sigma) &= \sum_i \mathrm{H}(\sigma(v_i) \mid \sigma(v_1) \dots \sigma(v_{i-1})) \\ &\leq \sum_i \mathrm{H}(\sigma(v_i)) \end{aligned}$$

Комбинаторное применение 1: теорема Брэгмана (1)

Теорема. Если в двудольном графе $|L| = |R| = n$, то число совершенных паросочетаний не больше

$$\prod_{v \in A} (\deg(v)!)^{1/\deg(v)}.$$

Наивное рассуждение: Обозначим случайное паросочетание σ.

$$\begin{aligned} \mathrm{H}(\sigma) &= \sum_i \mathrm{H}(\sigma(v_i) \mid \sigma(v_1) \dots \sigma(v_{i-1})) \\ &\leq \sum_i \mathrm{H}(\sigma(v_i)) \\ &\leq \sum_i \log \deg(v_i) \end{aligned}$$

Комбинаторное применение 1: теорема Брэгмана (1)

Теорема. Если в двудольном графе $|L| = |R| = n$, то число совершенных паросочетаний не больше

$$\prod_{v \in A} (\deg(v)!)^{1/\deg(v)}.$$

Наивное рассуждение: Обозначим случайное паросочетание σ.

$$\begin{aligned} \mathrm{H}(\sigma) &= \sum_i \mathrm{H}(\sigma(v_i) \mid \sigma(v_1) \dots \sigma(v_{i-1})) \\ &\leq \sum_i \mathrm{H}(\sigma(v_i)) \\ &\leq \sum_i \log \deg(v_i) \\ &\leq \log \prod_i \deg(v_i) \end{aligned}$$

Комбинаторное применение 1: теорема Брэгмана (1)

Теорема. Если в двудольном графе $|L| = |R| = n$, то число совершенных паросочетаний не больше

$$\prod_{v \in A} (\deg(v)!)^{1/\deg(v)}.$$

Наивное рассуждение: Обозначим случайное паросочетание σ.

$$\begin{aligned} \mathrm{H}(\sigma) &= \sum_i \mathrm{H}(\sigma(v_i) \mid \sigma(v_1) \dots \sigma(v_{i-1})) \\ &\leq \sum_i \mathrm{H}(\sigma(v_i)) \\ &\leq \sum_i \log \deg(v_i) \\ &\leq \log \prod_i \deg(v_i) \end{aligned}$$

число совершенных паросочетаний $\leq \prod_i \deg(v_i)$

Комбинаторное применение 1: теорема Брэгмана (2)

Теорема. Если в двудольном графе $|L| = |R| = n$, то число совершенных паросочетаний не больше

$$\prod_{v \in A} (\deg(v)!)^{1/\deg(v)}.$$

Комбинаторное применение 1: теорема Брэгмана (2)

Теорема. Если в двудольном графе $|L| = |R| = n$, то число совершенных паросочетаний не больше

$$\prod_{v \in A} (\deg(v)!)^{1/\deg(v)}.$$

Более точный подсчет: Выберем *случайную нумерацию вершин*

$$\begin{aligned} \mathrm{H}(\sigma) &= E_{\text{numeration}} \sum_i \mathrm{H}(\sigma(v_i) \mid \sigma(v_1) \dots \sigma(v_{i-1})) \\ &\leq \sum_{v \in A} E_{\text{numeration}} \mathrm{H}(\sigma(v) | \sigma(w_j) \text{ for the previous vertices } w_j) \end{aligned}$$

Комбинаторное применение 1: теорема Брэгмана (2)

Теорема. Если в двудольном графе $|L| = |R| = n$, то число совершенных паросочетаний не больше

$$\prod_{v \in A} (\deg(v)!)^{1/\deg(v)}.$$

Более точный подсчет: Выберем *случайную нумерацию вершин*

$$\begin{aligned} \mathrm{H}(\sigma) &= E_{\text{numeration}} \sum_i \mathrm{H}(\sigma(v_i) \mid \sigma(v_1) \dots \sigma(v_{i-1})) \\ &\leq \sum_{v \in A} E_{\text{numeration}} \mathrm{H}(\sigma(v) | \sigma(w_j) \text{ for the previous vertices } w_j) \\ &\leq \sum_{v \in A} \tfrac{1}{\deg(v)} (\log 1 + \log 2 + \ldots + \log \deg(v)) \end{aligned}$$

Комбинаторное применение 1: теорема Брэгмана (2)

Теорема. Если в двудольном графе $|L| = |R| = n$, то число совершенных паросочетаний не больше

$$\prod_{v \in A} (\deg(v)!)^{1/\deg(v)}.$$

Более точный подсчет: Выберем *случайную нумерацию вершин*

$$\begin{aligned}
\mathrm{H}(\sigma) &= E_{\text{numeration}} \sum_i \mathrm{H}(\sigma(v_i) \mid \sigma(v_1) \dots \sigma(v_{i-1})) \\
&\le \sum_{v \in A} E_{\text{numeration}} \mathrm{H}(\sigma(v) | \sigma(w_j) \text{ for the previous vertices } w_j) \\
&\le \sum_{v \in A} \tfrac{1}{\deg(v)} (\log 1 + \log 2 + \ldots + \log \deg(v)) \\
&\le \log \prod_{v \in A} (\deg(v)!)^{1/\deg(v)}
\end{aligned}$$

Комбинаторное применение 1: теорема Брэгмана (2)

Теорема. Если в двудольном графе $|L| = |R| = n$, то число совершенных паросочетаний не больше

$$\prod_{v \in A} (\deg(v)!)^{1/\deg(v)}.$$

Более точный подсчет: Выберем *случайную нумерацию вершин*

$$\begin{aligned} \mathrm{H}(\sigma) &= E_{\text{numeration}} \sum_i \mathrm{H}(\sigma(v_i) \mid \sigma(v_1) \dots \sigma(v_{i-1})) \\ &\le \sum_{v \in A} E_{\text{numeration}} \mathrm{H}(\sigma(v) | \sigma(w_j) \text{ for the previous vertices } w_j) \\ &\le \sum_{v \in A} \tfrac{1}{\deg(v)} (\log 1 + \log 2 + \ldots + \log \deg(v)) \\ &\le \log \prod_{v \in A} (\deg(v)!)^{1/\deg(v)} \end{aligned}$$

число совершенных паросочетаний $\le \prod_{v \in A} (\deg(v)!)^{1/\deg(v)}$

Комбинаторное применение 2: раскраска графа и псевдослучайные перестановки (1)

Тривиальное утверждение:
Пусть все ребра полного графа (клики) G на n вершинах покрыты двудольными графами $G_1, \ldots, G_n$. Тогда $t \geq \log n$.

Комбинаторное применение 2: раскраска графа и псевдослучайные перестановки (1)

Тривиальное утверждение:
Пусть все ребра полного графа (клики) G на n вершинах покрыты двудольными графами $G_1, \ldots, G_n$. Тогда $t \geq \log n$.

Доказательство в терминах энтропии:

Комбинаторное применение 2: раскраска графа и псевдослучайные перестановки (1)

Тривиальное утверждение:
Пусть все ребра полного графа (клики) G на n вершинах покрыты двудольными графами $G_1, \ldots, G_n$. Тогда $t \geq \log n$.

Доказательство в терминах энтропии:

- x: случайная вершина графа G

Комбинаторное применение 2: раскраска графа и псевдослучайные перестановки (1)

Тривиальное утверждение:
Пусть все ребра полного графа (клики) G на n вершинах покрыты двудольными графами $G_1, \ldots, G_n$. Тогда $t \geq \log n$.

Доказательство в терминах энтропии:

- x: случайная вершина графа G
- y_i: цвет вершины в графе G_i

Комбинаторное применение 2: раскраска графа и псевдослучайные перестановки (1)

Тривиальное утверждение:
Пусть все ребра полного графа (клики) G на n вершинах покрыты двудольными графами $G_1, \dots, G_n$. Тогда $t \geq \log n$.

Доказательство в терминах энтропии:

- x: случайная вершина графа G
- y_i: цвет вершины в графе G_i
- $0 = \mathrm{H}(x|y_1 \dots y_n)$

Комбинаторное применение 2: раскраска графа и псевдослучайные перестановки (1)

Тривиальное утверждение:
Пусть все ребра полного графа (клики) G на n вершинах покрыты двудольными графами $G_1, \ldots, G_n$. Тогда $t \geq \log n$.

Доказательство в терминах энтропии:

- x: случайная вершина графа G
- y_i: цвет вершины в графе G_i
- $0 = \mathrm{H}(x|y_1 \ldots y_n) \geq \mathrm{H}(x) - \sum \mathrm{H}(y_i)$

Комбинаторное применение 2: раскраска графа и псевдослучайные перестановки (1)

Тривиальное утверждение:
Пусть все ребра полного графа (клики) G на n вершинах покрыты двудольными графами $G_1, \ldots, G_n$. Тогда $t \geq \log n$.

Доказательство в терминах энтропии:

- x: случайная вершина графа G
- y_i: цвет вершины в графе G_i
- $0 = \mathrm{H}(x|y_1 \ldots y_n) \geq \mathrm{H}(x) - \sum \mathrm{H}(y_i) \geq \log n - t$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \dots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \dots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Доказательство:

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Доказательство:

- x: случайная вершина графа G

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Доказательство:

- x: случайная вершина графа G
- y_i: цвет вершины x, если она не изолирована в G_i;

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Доказательство:

- x: случайная вершина графа G
- y_i: цвет вершины x, если она не изолирована в G_i;
  цвет случайной неизолированной вершины в G_i,
  если x изолирована в G_i

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Доказательство:

- x: случайная вершина графа G
- y_i: цвет вершины x, если она не изолирована в G_i;
  цвет случайной неизолированной вершины в G_i,
  если x изолирована в G_i
- $0 = \mathrm{H}(x|y_1 \ldots y_n)$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Доказательство:

- x: случайная вершина графа G
- y_i: цвет вершины x, если она не изолирована в G_i;
  цвет случайной неизолированной вершины в G_i,
  если x изолирована в G_i
- $0 = \mathrm{H}(x|y_1 \ldots y_n) = \mathrm{H}(xy_1 \ldots y_n) - \sum \mathrm{H}(y_1 \ldots y_n)$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Доказательство:

- x: случайная вершина графа G
- y_i: цвет вершины x, если она не изолирована в G_i;
  цвет случайной неизолированной вершины в G_i,
  если x изолирована в G_i
- $0 = \mathrm{H}(x|y_1 \ldots y_n) = \mathrm{H}(xy_1 \ldots y_n) - \sum \mathrm{H}(y_1 \ldots y_n)$
  $= \mathrm{H}(x) + \mathrm{H}(y_1 \ldots y_n|x) - \sum \mathrm{H}(y_1 \ldots y_n)$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Доказательство:

- x: случайная вершина графа G
- y_i: цвет вершины x, если она не изолирована в G_i;
  цвет случайной неизолированной вершины в G_i,
  если x изолирована в G_i
- $0 = \mathrm{H}(x|y_1 \ldots y_n) = \mathrm{H}(xy_1 \ldots y_n) - \sum \mathrm{H}(y_1 \ldots y_n)$
  $= \mathrm{H}(x) + \mathrm{H}(y_1 \ldots y_n|x) - \sum \mathrm{H}(y_1 \ldots y_n)$
  $\geq \log n + \mathrm{H}(y_1 \ldots y_n|x) - \sum \mathrm{H}(y_i)$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Доказательство:

- x: случайная вершина графа G
- y_i: цвет вершины x, если она не изолирована в G_i;
  цвет случайной неизолированной вершины в G_i,
  если x изолирована в G_i
- $0 = \mathrm{H}(x|y_1 \ldots y_n) = \mathrm{H}(xy_1 \ldots y_n) - \sum \mathrm{H}(y_1 \ldots y_n)$
  $= \mathrm{H}(x) + \mathrm{H}(y_1 \ldots y_n|x) - \sum \mathrm{H}(y_1 \ldots y_n)$
  $\geq \log n + \mathrm{H}(y_1 \ldots y_n|x) - \sum \mathrm{H}(y_i)$
  $= \log n + \sum \mathrm{H}(y_i|x) - \sum \mathrm{H}(y_i)$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (2)

Не столь тривиальное утверждение:

Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Доказательство:

- x: случайная вершина графа G
- y_i: цвет вершины x, если она не изолирована в G_i; цвет случайной неизолированной вершины в G_i, если x изолирована в G_i
- $0 = \mathrm{H}(x|y_1 \ldots y_n) = \mathrm{H}(xy_1 \ldots y_n) - \sum \mathrm{H}(y_1 \ldots y_n)$
  $= \mathrm{H}(x) + \mathrm{H}(y_1 \ldots y_n|x) - \sum \mathrm{H}(y_1 \ldots y_n)$
  $\geq \log n + \mathrm{H}(y_1 \ldots y_n|x) - \sum \mathrm{H}(y_i)$
  $= \log n + \sum \mathrm{H}(y_i|x) - \sum \mathrm{H}(y_i)$
  $= \log n + \sum (1 - \frac{size(G_i)}{n}) \mathrm{H}(y_i) - \sum \mathrm{H}(y_i)$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (3)

Утв. Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (3)

Утв. Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Следствие [Füredi]. Назовем семейство перестановок на $\{1, \ldots, n\}$ 3-*перемешивающим*, если для любых i, j, k найдется такая перестановка π, что $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$. В каждом 3-перемешивающем семействе S содерижится не менее $2 \ln n$ перестановок.

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (3)

Утв. Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Следствие [Füredi]. Назовем семейство перестановок на $\{1, \ldots, n\}$ 3-*перемешивающим*, если для любых i, j, k найдется такая перестановка π, что $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$. В каждом 3-перемешивающем семействе S содерижится не менее $2 \ln n$ перестановок.

Доказательство.

- вершины: множество пар (i, j) т.ч. $i \neq j$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (3)

Утв. Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Следствие [Füredi]. Назовем семейство перестановок на $\{1, \ldots, n\}$ 3-*перемешивающим*, если для любых i, j, k найдется такая перестановка π, что $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$. В каждом 3-перемешивающем семействе S содерижится не менее $2 \ln n$ перестановок.

Доказательство.

- вершины: множество пар (i, j) т.ч. $i \neq j$
- ребра графа G_i: $\langle (i, j), (k, j) \rangle$ т.ч. $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (3)

Утв. Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Следствие [Füredi]. Назовем семейство перестановок на $\{1, \ldots, n\}$ 3-*перемешивающим*, если для любых i, j, k найдется такая перестановка π, что $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$. В каждом 3-перемешивающем семействе S содерижится не менее $2 \ln n$ перестановок.

Доказательство.

- вершины: множество пар (i, j) т.ч. $i \neq j$
- ребра графа G_i: $\langle (i, j), (k, j) \rangle$ т.ч. $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$
- $\cup G_i$ состоит из n клик, каждая на $(n-1)$ вершине

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (3)

Утв. Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Следствие [Füredi]. Назовем семейство перестановок на $\{1, \ldots, n\}$ 3-*перемешивающим*, если для любых i, j, k найдется такая перестановка π, что $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$. В каждом 3-перемешивающем семействе S содерижится не менее $2 \ln n$ перестановок.

Доказательство.

- вершины: множество пар (i, j) т.ч. $i \neq j$
- ребра графа G_i: $\langle (i, j), (k, j) \rangle$ т.ч. $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$
- $\cup G_i$ состоит из n клик, каждая на $(n-1)$ вершине $\to n \times \log(n-1)$

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (3)

Утв. Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Следствие [Füredi]. Назовем семейство перестановок на $\{1, \ldots, n\}$ 3-*перемешивающим*, если для любых i, j, k найдется такая перестановка π, что $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$. В каждом 3-перемешивающем семействе S содерижится не менее $2 \ln n$ перестановок.

Доказательство.

- вершины: множество пар (i, j) т.ч. $i \neq j$
- ребра графа G_i: $\langle (i, j), (k, j) \rangle$ т.ч. $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$
- $\cup G_i$ состоит из n клик, каждая на $(n-1)$ вершине $\to n \times \log(n-1)$
- G_i распадается на $(n-2)$ полных двудольных графа

Комбинаторное применение 2: раскраски графа и псевдослучайные перестановки (3)

Утв. Пусть все ребра полного графа (клики) G на n вершинах покрыты графами $G_1, \ldots, G_n$ и вершины каждого из этих графов раскрашены правильным образом. Обозначим ξ_i цвета неизолированных вершин G_i. Тогда

$$\sum \frac{size(G_i)}{n} \mathrm{H}(\xi_i) \geq \log n.$$

Следствие [Füredi]. Назовем семейство перестановок на $\{1, \ldots, n\}$ 3-*перемешивающим*, если для любых i, j, k найдется такая перестановка π, что $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$. В каждом 3-перемешивающем семействе S содержится не менее $2 \ln n$ перестановок.

Доказательство.

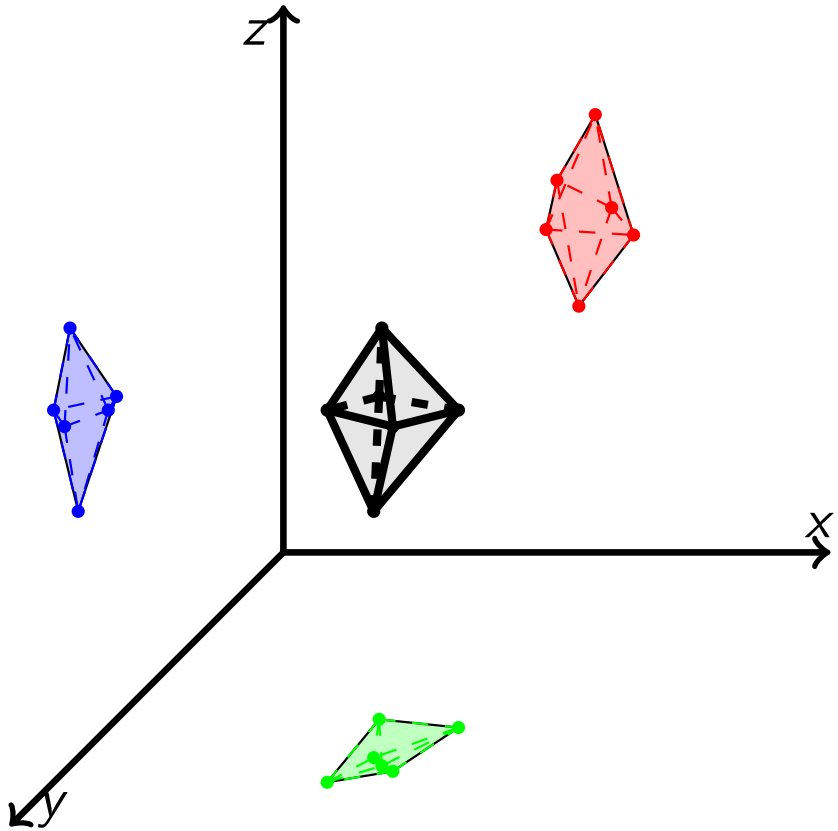
- вершины: множество пар (i, j) т.ч. $i \neq j$
- ребра графа G_i: $\langle (i, j), (k, j) \rangle$ т.ч. $\pi(j)$ лежит между $\pi(i)$ и $\pi(k)$
- $\cup G_i$ состоит из n клик, каждая на $(n-1)$ вершине $\to n \times \log(n-1)$
- G_i распадается на $(n-2)$ полных двудольных графа $\to \sum_{i=1}^{n-2} \mathrm{H}(\frac{i}{n-1}) \leq (n-1) \int_0^1 \mathrm{H}(t)dt = \frac{\log e}{2}(n-1)$

Комбинаторное применение 3: неравенство Ширера и теорема Лумиса–Уитни (1)

$$|A|^2 \le |\pi_{12}(A)| \cdot |\pi_{23}(A)| \cdot |\pi_{13}(A)| \Longleftarrow 2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$$

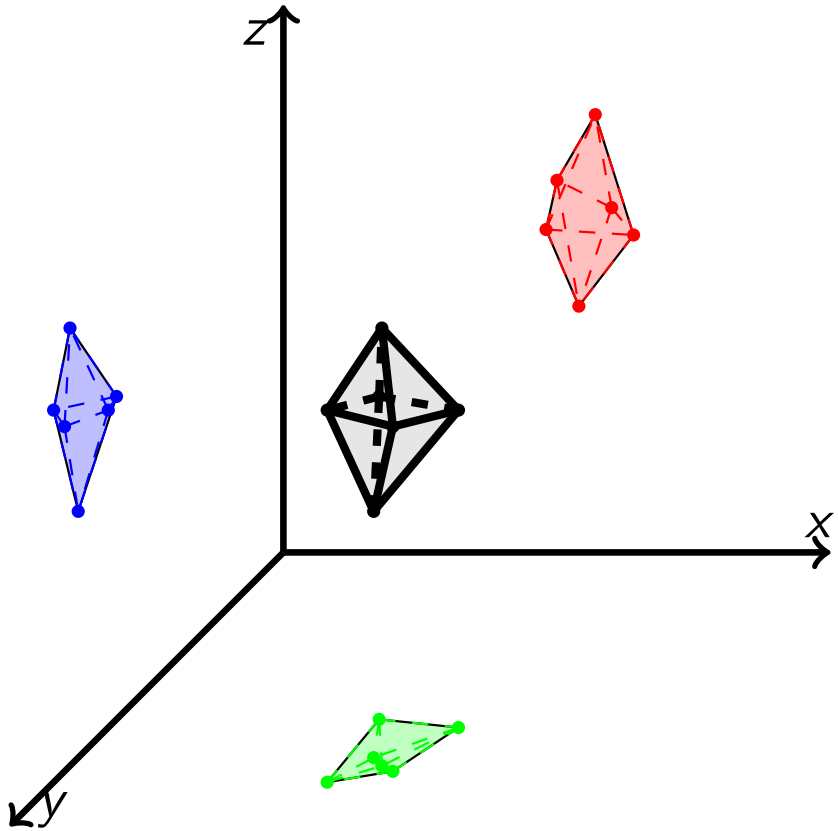
Комбинаторное применение 3: неравенство Ширера и теорема Лумиса–Уитни (1)

$$|A|^2 \le |\pi_{12}(A)| \cdot |\pi_{23}(A)| \cdot |\pi_{13}(A)| \Longleftarrow 2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$$



Комбинаторное применение 3: неравенство Ширера и теорема Лумиса–Уитни (1)

$$|A|^2 \le |\pi_{12}(A)| \cdot |\pi_{23}(A)| \cdot |\pi_{13}(A)| \Longleftarrow 2\mathrm{H}(a,b,c) \le \mathrm{H}(a,b) + \mathrm{H}(b,c) + \mathrm{H}(a,c)$$



$$\mathrm{Volume}(\text{тело})^2 \le \mathrm{Shade}_{xy}(\text{тело}) \cdot \mathrm{Shade}_{xz}(\text{тело}) \cdot \mathrm{Shade}_{yz}(\text{тело})$$

Комбинаторное применение 3: общий вид неравенства Ширера (2)

энтропийные неравенства:

$$3\mathrm{H}(a_1, a_2, a_3, a_4) \leq \mathrm{H}(a_2, a_3, a_4) + \mathrm{H}(a_1, a_3, a_4) + \mathrm{H}(a_1, a_2, a_4) + \mathrm{H}(a_1, a_2, a_3)$$

$$2\mathrm{H}(a_1, a_2, a_3, a_4) \leq \mathrm{H}(a_1, a_2) + \mathrm{H}(a_2, a_3) + \mathrm{H}(a_3, a_4) + \mathrm{H}(a_1, a_4)$$

. . .

Комбинаторное применение 3: общий вид неравенства Ширера (2)

энтропийные неравенства:

$$3\mathrm{H}(a_1, a_2, a_3, a_4) \le \mathrm{H}(a_2, a_3, a_4) + \mathrm{H}(a_1, a_3, a_4) + \mathrm{H}(a_1, a_2, a_4) + \mathrm{H}(a_1, a_2, a_3)$$

$$2\mathrm{H}(a_1, a_2, a_3, a_4) \le \mathrm{H}(a_1, a_2) + \mathrm{H}(a_2, a_3) + \mathrm{H}(a_3, a_4) + \mathrm{H}(a_1, a_4)$$

...

комбинаторные неравенства:

$$|A|^3 \le |\pi_{234}(A)| \cdot |\pi_{134}(A)| \cdot |\pi_{124}(A)| \cdot |\pi_{123}(A)|$$

$$|A|^2 \le |\pi_{12}(A)| \cdot |\pi_{23}(A)| \cdot |\pi_{34}(A)| \cdot |\pi_{14}(A)|$$

...

Комбинаторное применение 3: общий вид неравенства Ширера (2)

энтропийные неравенства:

$3\mathrm{H}(a_1, a_2, a_3, a_4) \le \mathrm{H}(a_2, a_3, a_4) + \mathrm{H}(a_1, a_3, a_4) + \mathrm{H}(a_1, a_2, a_4) + \mathrm{H}(a_1, a_2, a_3)$

$2\mathrm{H}(a_1, a_2, a_3, a_4) \le \mathrm{H}(a_1, a_2) + \mathrm{H}(a_2, a_3) + \mathrm{H}(a_3, a_4) + \mathrm{H}(a_1, a_4)$

...

комбинаторные неравенства:

$|A|^3 \le |\pi_{234}(A)| \cdot |\pi_{134}(A)| \cdot |\pi_{124}(A)| \cdot |\pi_{123}(A)|$

$|A|^2 \le |\pi_{12}(A)| \cdot |\pi_{23}(A)| \cdot |\pi_{34}(A)| \cdot |\pi_{14}(A)|$

...

Общее утверждение: дано семейство подмножеств $\mathcal{S}$ координат $\{1, \dots, n\}$ т.ч. каждая координата покрыта $\ge k$ множествами семейства. Тогда

$$|A|^k \le \prod_{F \in \mathcal{S}} |\pi_F(A)|$$

Комбинаторное применение 3: применение неравенства Ширера

Общее утверждение: дано семейство подмножеств $\mathcal{S}$ координат $\{1, \ldots, n\}$ т.ч. каждая координата покрыта $\geq k$ множествами семейства. Тогда

$$|A|^k \leq \prod_{F \in \mathcal{S}} |\pi_F(A)|$$

Комбинаторное применение 3: применение неравенства Ширера

Общее утверждение: дано семейство подмножеств $\mathcal{S}$ координат $\{1, \ldots, n\}$ т.ч. каждая координата покрыта $\geq k$ множествами семейства. Тогда

$$|A|^k \leq \prod_{F \in \mathcal{S}} |\pi_F(A)|$$

Chung, Frankl, Graham, Shearer: Если семейство $\mathcal{G}$ состоит из графов на n вершинах, т.ч. любые два графа имеют общий *треугольник*, то

$$|\mathcal{G}| \leq 2^{\frac{n(n-1)}{2}-2}.$$

Комбинаторное применение 3: применение неравенства Ширера

Общее утверждение: дано семейство подмножеств $\mathcal{S}$ координат $\{1, \dots, n\}$ т.ч. каждая координата покрыта $\geq k$ множествами семейства. Тогда

$$|A|^k \leq \prod_{F \in \mathcal{S}} |\pi_F(A)|$$

Chung, Frankl, Graham, Shearer: Если семейство $\mathcal{G}$ состоит из графов на n вершинах, т.ч. любые два графа имеют общий *треугольник*, то

$$|\mathcal{G}| \leq 2^{\frac{n(n-1)}{2}-2}.$$

Набросок доказательства:

Комбинаторное применение 3: применение неравенства Ширера

Общее утверждение: дано семейство подмножеств $\mathcal{S}$ координат $\{1, \ldots, n\}$ т.ч. каждая координата покрыта $\geq k$ множествами семейства. Тогда

$$|A|^k \leq \prod_{F \in \mathcal{S}} |\pi_F(A)|$$

Chung, Frankl, Graham, Shearer: Если семейство $\mathcal{G}$ состоит из графов на n вершинах, т.ч. любые два графа имеют общий *треугольник*, то

$$|\mathcal{G}| \leq 2^{\frac{n(n-1)}{2}-2}.$$

Набросок доказательства:

- рассмотрим всевозможные разбиения $\{1, \ldots, n\} = A \cup B$ на два множества по $n/2$ вершин

Комбинаторное применение 3: применение неравенства Ширера

Общее утверждение: дано семейство подмножеств $\mathcal{S}$ координат $\{1, \dots, n\}$ т.ч. каждая координата покрыта $\geq k$ множествами семейства. Тогда

$$|A|^k \leq \prod_{F \in \mathcal{S}} |\pi_F(A)|$$

Chung, Frankl, Graham, Shearer: Если семейство $\mathcal{G}$ состоит из графов на n вершинах, т.ч. любые два графа имеют общий *треугольник*, то

$$|\mathcal{G}| \leq 2^{\frac{n(n-1)}{2}-2}.$$

Набросок доказательства:

- рассмотрим всевозможные разбиения $\{1, \dots, n\} = A \cup B$ на два множества по $n/2$ вершин
- $\pi_{(A,B)}(\mathcal{G}) \geq \frac{1}{2} \cdot 2^{[\text{число ребер, не пересек. границу между } A \text{ и } B]} =: 2^{m-1}$

Комбинаторное применение 3: применение неравенства Ширера

Общее утверждение: дано семейство подмножеств $\mathcal{S}$ координат $\{1, \dots, n\}$ т.ч. каждая координата покрыта $\geq k$ множествами семейства. Тогда

$$|A|^k \leq \prod_{F \in \mathcal{S}} |\pi_F(A)|$$

Chung, Frankl, Graham, Shearer: Если семейство $\mathcal{G}$ состоит из графов на n вершинах, т.ч. любые два графа имеют общий *треугольник*, то

$$|\mathcal{G}| \leq 2^{\frac{n(n-1)}{2}-2}.$$

Набросок доказательства:

- рассмотрим всевозможные разбиения $\{1, \dots, n\} = A \cup B$ на два множества по $n/2$ вершин
- $\pi_{(A,B)}(\mathcal{G}) \geq \frac{1}{2} \cdot 2^{[\text{число ребер, не пересек. границу между } A \text{ и } B]} =: 2^{m-1}$
- Если $k =$ число разбиений (A, B), не разрезающих фикс. ребро, то $k \cdot C_n^2 = m \cdot [\text{число пар } (A, B)]$.

Комбинаторное применение 3: применение неравенства Ширера

Общее утверждение: дано семейство подмножеств $\mathcal{S}$ координат $\{1, \dots, n\}$ т.ч. каждая координата покрыта $\geq k$ множествами семейства. Тогда

$$|A|^k \leq \prod_{F \in \mathcal{S}} |\pi_F(A)|$$

Chung, Frankl, Graham, Shearer: Если семейство $\mathcal{G}$ состоит из графов на n вершинах, т.ч. любые два графа имеют общий *треугольник*, то

$$|\mathcal{G}| \leq 2^{\frac{n(n-1)}{2}-2}.$$

Набросок доказательства:

- рассмотрим всевозможные разбиения $\{1, \dots, n\} = A \cup B$ на два множества по $n/2$ вершин
- $\pi_{(A,B)}(\mathcal{G}) \geq \frac{1}{2} \cdot 2^{[\text{число ребер, не пересек. границу между } A \text{ и } B]} =: 2^{m-1}$
- Если $k =$ число разбиений (A, B), не разрезающих фикс. ребро, то $k \cdot C_n^2 = m \cdot [\text{число пар } (A, B)]$.
- $|\mathcal{G}|^k \leq (2^{m-1})^{[\text{число разбиений } (A, B)]}$

Комбинаторное применение 3: применение неравенства Ширера

Общее утверждение: дано семейство подмножеств $\mathcal{S}$ координат $\{1, \dots, n\}$ т.ч. каждая координата покрыта $\geq k$ множествами семейства. Тогда

$$|A|^k \leq \prod_{F \in \mathcal{S}} |\pi_F(A)|$$

Chung, Frankl, Graham, Shearer: Если семейство $\mathcal{G}$ состоит из графов на n вершинах, т.ч. любые два графа имеют общий *треугольник*, то

$$|\mathcal{G}| \leq 2^{\frac{n(n-1)}{2}-2}.$$

Набросок доказательства:

- рассмотрим всевозможные разбиения $\{1, \dots, n\} = A \cup B$ на два множества по $n/2$ вершин
- $\pi_{(A,B)}(\mathcal{G}) \geq \frac{1}{2} \cdot 2^{[\text{число ребер, не пересек. границу между } A \text{ и } B]} =: 2^{m-1}$
- Если $k =$ число разбиений (A, B), не разрезающих фикс. ребро, то $k \cdot C_n^2 = m \cdot [\text{число пар } (A, B)]$.
- $|\mathcal{G}|^k \leq (2^{m-1})^{[\text{число разбиений } (A,\, B)]} = 2^{(m-1)\cdot \frac{k \cdot C_n^2}{m}}$

Комбинаторное применение 4 [пропушенный слайд]: энтропия графа по Кёрнеру

Задан граф G и распределение P на его вершинах.

Комбинаторное применение 4 [пропушенный слайд]: энтропия графа по Кёрнеру

Задан граф G и распределение P на его вершинах.

Опр. Энтропия Кёрнера $\mathrm{H}(G, P) := \min \mathrm{I}(X : Y)$, где

- X случайная вершина по распределению P
- Y независимое множество вершин, содержащее X.

Комбинаторное применение 4 [пропушенный слайд]: энтропия графа по Кёрнеру

Задан граф G и распределение P на его вершинах.

Опр. Энтропия Кёрнера $\mathrm{H}(G, P) := \min \mathrm{I}(X : Y)$, где

- X случайная вершина по распределению P
- Y независимое множество вершин, содержащее X.

Интуиция: Две вершины «различимы», если они соединены ребром. Сколько информации можно передать, послав вершину графа?

Комбинаторное применение 4 [пропушенный слайд]: энтропия графа по Кёрнеру

Задан граф G и распределение P на его вершинах.

Опр. Энтропия Кёрнера $\mathrm{H}(G, P) := \min \mathrm{I}(X : Y)$, где

- X случайная вершина по распределению P
- Y независимое множество вершин, содержащее X.

Интуиция: Две вершины «различимы», если они соединены ребром. Сколько информации можно передать, послав вершину графа?

Энтропия полного графа: обычная $\mathrm{H}(P)$ (все вершины «различимы»).

Комбинаторное применение 4 [пропушенный слайд]: энтропия графа по Кёрнеру

Задан граф G и распределение P на его вершинах.

Опр. Энтропия Кёрнера $\mathrm{H}(G, P) := \min \mathrm{I}(X : Y)$, где

- X случайная вершина по распределению P
- Y независимое множество вершин, содержащее X.

Интуиция: Две вершины «различимы», если они соединены ребром. Сколько информации можно передать, послав вершину графа?

Энтропия полного графа: обычная $\mathrm{H}(P)$ (все вершины «различимы»).

Объединение графов: Энтропия Кёрнера субаддитивна.

Комбинаторное применение 4 [пропушенный слайд]: энтропия графа по Кёрнеру

Задан граф G и распределение P на его вершинах.

Опр. Энтропия Кёрнера $\mathrm{H}(G, P) := \min \mathrm{I}(X : Y)$, где

- X случайная вершина по распределению P
- Y независимое множество вершин, содержащее X.

Интуиция: Две вершины «различимы», если они соединены ребром. Сколько информации можно передать, послав вершину графа?

Энтропия полного графа: обычная $\mathrm{H}(P)$ (все вершины «различимы»).

Объединение графов: Энтропия Кёрнера субаддитивна.

Стягивание независимого множества: Энтропия графа не уменьшается.

Комбинаторное применение 4 [пропушенный слайд]: энтропия графа по Кёрнеру

Задан граф G и распределение P на его вершинах.

Опр. Энтропия Кёрнера $\mathrm{H}(G, P) := \min \mathrm{I}(X : Y)$, где

- X случайная вершина по распределению P
- Y независимое множество вершин, содержащее X.

Интуиция: Две вершины «различимы», если они соединены ребром. Сколько информации можно передать, послав вершину графа?

Энтропия полного графа: обычная $\mathrm{H}(P)$ (все вершины «различимы»).

Объединение графов: Энтропия Кёрнера субаддитивна.

Стягивание независимого множества: Энтропия графа не уменьшается.

Классическое приложение [Fredman–Komlos]: семейство хэш-функций

$$f_i \ : \ \{1, \dots, n\} \to \{1, \dots, b\},$$

которое совершенно для всех k-множеств, должно иметь размер не меньше

$$\frac{b^{k-1}}{b(b-1)(b-2)\dots(b-k+2)} \cdot \frac{\log n}{\log(b-k+2)} \cdot (1 + o_n(1))$$

Применение 5: secret key commitment (1)

Применение 5: secret key commitment (1)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Утверждение. Число компонент связности $\leq \frac{|A| \cdot |B|}{|E|}$.

Применение 5: secret key commitment (1)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Утверждение. Число компонент связности $\leq \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра.

Применение 5: secret key commitment (1)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Утверждение. Число компонент связности $\leq \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра.

- $\mathrm{H}(x, y) = \log |E|$, $\mathrm{H}(x) = \log |A|$, $\mathrm{H}(y) = \log |B|$

Применение 5: secret key commitment (1)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Утверждение. Число компонент связности $\leq \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра.

- $\mathrm{H}(x, y) = \log |E|$, $\mathrm{H}(x) = \log |A|$, $\mathrm{H}(y) = \log |B|$
- Обозначим z индекс компоненты связности.

Применение 5: secret key commitment (1)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Утверждение. Число компонент связности $\leq \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра.

- $\mathrm{H}(x, y) = \log |E|$, $\mathrm{H}(x) = \log |A|$, $\mathrm{H}(y) = \log |B|$
- Обозначим z индекс компоненты связности.
  $\mathrm{H}(z|x) = \mathrm{H}(x|y) = 0$.

Применение 5: secret key commitment (1)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Утверждение. Число компонент связности $\leq \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра.

- $\mathrm{H}(x, y) = \log |E|$, $\mathrm{H}(x) = \log |A|$, $\mathrm{H}(y) = \log |B|$
- Обозначим z индекс компоненты связности.
  $\mathrm{H}(z|x) = \mathrm{H}(x|y) = 0$.
- применим неравенство $\mathrm{H}(z) \leq \mathrm{H}(z|x) + \mathrm{H}(z|y) + \mathrm{I}(x : y)$.

Применение 5: secret key commitment (2)

Применение 5: secret key commitment (2)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Теорема. G нельзя разбить на непересекающиеся индуцированные подграфы, в каждом из которых число компонент связности $> \frac{|A| \cdot |B|}{|E|}$.

Применение 5: secret key commitment (2)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Теорема. G нельзя разбить на непересекающиеся индуцированные подграфы, в каждом из которых число компонент связности $> \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра и t покрывающий его подграф.

Применение 5: secret key commitment (2)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Теорема. G нельзя разбить на непересекающиеся индуцированные подграфы, в каждом из которых число компонент связности $> \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра и t покрывающий его подграф.

- покажем, что $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$

Применение 5: secret key commitment (2)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Теорема. G нельзя разбить на непересекающиеся индуцированные подграфы, в каждом из которых число компонент связности $> \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра и t покрывающий его подграф.

- покажем, что $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$
- применим неравенство $\mathrm{H}(z|t) \leq \mathrm{H}(z|x) + \mathrm{H}(z|y) + \mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Применение 5: secret key commitment (2)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Теорема. G нельзя разбить на непересекающиеся индуцированные подграфы, в каждом из которых число компонент связности $> \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра и t покрывающий его подграф.

- покажем, что $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$
- применим неравенство $\mathrm{H}(z|t) \leq \mathrm{H}(z|x) + \mathrm{H}(z|y) + \mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Основная лемма. $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Применение 5: secret key commitment (2)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Теорема. G нельзя разбить на непересекающиеся индуцированные подграфы, в каждом из которых число компонент связности $> \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра и t покрывающий его подграф.

- покажем, что $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$
- применим неравенство $\mathrm{H}(z|t) \leq \mathrm{H}(z|x) + \mathrm{H}(z|y) + \mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Основная лемма. $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Доказательство:

Применение 5: secret key commitment (2)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Теорема. G нельзя разбить на непересекающиеся индуцированные подграфы, в каждом из которых число компонент связности $> \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра и t покрывающий его подграф.

- покажем, что $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$
- применим неравенство $\mathrm{H}(z|t) \leq \mathrm{H}(z|x) + \mathrm{H}(z|y) + \mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Основная лемма. $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Доказательство: Строим распределение (t, x', y'), где

- распределение (x', t) совпадает с распределением (x, t)
- распределение (y', t) совпадает с распределением (y, t)
- x' и y' независимы относительно t

Применение 5: secret key commitment (2)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Теорема. G нельзя разбить на непересекающиеся индуцированные подграфы, в каждом из которых число компонент связности $> \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра и t покрывающий его подграф.

- покажем, что $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$
- применим неравенство $\mathrm{H}(z|t) \leq \mathrm{H}(z|x) + \mathrm{H}(z|y) + \mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Основная лемма. $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Доказательство: Строим распределение (t, x', y'), где

- распределение (x', t) совпадает с распределением (x, t)
- распределение (y', t) совпадает с распределением (y, t)
- x' и y' независимы относительно t

Замечаем, что $\mathrm{H}(x', y', t) = \mathrm{H}(t) + \mathrm{H}(x|t) + \mathrm{H}(y|t) \leq \mathrm{H}(x) + \mathrm{H}(y)$

Применение 5: secret key commitment (2)

Дан рёберно транзитивный двудольный граф $G = (A, B, E)$.

Теорема. G нельзя разбить на непересекающиеся индуцированные подграфы, в каждом из которых число компонент связности $> \frac{|A| \cdot |B|}{|E|}$.

Доказательство. Обозначим (x, y) концы случайно выбранного ребра и t покрывающий его подграф.

- покажем, что $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$
- применим неравенство $\mathrm{H}(z|t) \leq \mathrm{H}(z|x) + \mathrm{H}(z|y) + \mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Основная лемма. $\mathrm{I}(x : y|t) \leq \mathrm{I}(x : y)$.

Доказательство: Строим распределение (t, x', y'), где

- распределение (x', t) совпадает с распределением (x, t)
- распределение (y', t) совпадает с распределением (y, t)
- x' и y' независимы относительно t

Замечаем, что $\mathrm{H}(x', y', t) = \mathrm{H}(t) + \mathrm{H}(x|t) + \mathrm{H}(y|t) \leq \mathrm{H}(x) + \mathrm{H}(y)$, что эквивалентно утв. леммы.

Применение 5: secret key commitment (3)

Применение 5: secret key commitment (3)

Задача о нахождении общего секретного ключа.

- выбирается случайное ребро из графа G
- Алисе сообщается вершина x, Бобу сообщается вершина y.
- Обмениваясь сообщениями по открытому каналу связи, Алиса и Боб хотят договориться о «секретном» ключе z.
- Участники протокола могут использовать источники случайных битов.

Применение 5: secret key commitment (3)

Задача о нахождении общего секретного ключа.

- выбирается случайное ребро из графа G
- Алисе сообщается вершина x, Бобу сообщается вершина y.
- Обмениваясь сообщениями по открытому каналу связи, Алиса и Боб хотят договориться о «секретном» ключе z.
- Участники протокола могут использовать источники случайных битов.

Теорема. Максимальный размер секретного ключа, о котором Алиса и Боб могу договориться с вероятностью ошибки ϵ, равен взаимной информации

$$\mathrm{I}(x : y) + O(\log\log \frac{|A||B|}{\epsilon}).$$