Дискретная математика и математическая логика

Швецова Анна, Ермилов Антон

16 декабря 2016 г.

Содержание

1. Введение в математическую логику **1**

1.1 Пропозициональная логика исчисления высказываний 1

1.2 Предикатная логика 1

1.3 Невыразимость предикатов: метод автоморфизмов 1

2. Дискретная теория вероятностей **2**

2.1 Введение в дискретную теорию вероятностей 2

2.2 Теорема Эрдеша-Ко-Радо 3

2.3 Случайная величина и её математическое ожидание 4

2.4 3-КНФ. Неравенство Маркова. 5

2.5 Энтропия случайной величины 5

1. Введение в математическую логику

1.1. Пропозициональная логика исчисления высказываний

1.2. Предикатная логика

1.3. Невыразимость предикатов: метод автоморфизмов

2. Дискретная теория вероятностей

2.1. Введение в дискретную теорию вероятностей

***Определение* 2.1.1.** Ω — конечное множество, пространство элементарных событий.

Пример. $\{1, 2, 3, 4, 5, 6\}$ — значения, которые могут выпасть на кубике.

***Определение* 2.1.2.** Событие — подмножество Ω.

***Определение* 2.1.3.** Вероятностная мера — $\Pr : 2^\Omega \to [0, 1]$.
Пусть $A \subseteq \Omega$ — некоторое событие. Тогда вероятность события A — $\Pr(A)$.

Свойства.

1) $\Pr(\Omega) = 1$

2) $A \cap B = \varnothing \implies \Pr(A \cup B) = \Pr(A) + \Pr(B)$

***Определение* 2.1.4.** $(\Omega, \Pr)$ — вероятностное пространство.

Свойства вероятностного пространства.

1) $\Pr(\varnothing) = 0$

2) $A \subseteq B \implies \Pr(A) \leqslant \Pr(B)$

3) $\Pr(A_1 \cup A_2 \cup ... \cup A_n) \leqslant \Pr(A_1) + \Pr(A_2) + ... + \Pr(A_n)$

4) Формула включения-исключения:

$\Pr(\bigcup_i A_i) = \sum_i \Pr(A_i) - \sum_{i<j} \Pr(A_i \cap A_j) + \sum_{i<j<k} \Pr(A_i \cap A_j \cap A_k) - ...$

5) $\Omega = \{\omega_1, \omega_2, ..., \omega_n\}$

$p_i = \Pr(\{\omega_i\})$ — вероятность события ω_i

$\Pr(A) = \sum_{\omega_i \in A} p_i$

Доказательство.

1) $\Pr(\varnothing) + \Pr(\Omega) = 1$

2) $B = A \cup (B \setminus A),\ A \cap (B \setminus A) = \varnothing \implies \Pr(B) = \Pr(A) + \Pr(B \setminus A) \geqslant \Pr(A)$

3) По индукции:

$\Pr(A \cup B) \leqslant \Pr(A) + \Pr(B)$, поскольку $\Pr(A \cup B) = \Pr(A) + \Pr(B \setminus A) \leqslant \Pr(A) + \Pr(B)$ □

Пример.

В школе учится n детей, все они ходят на кружки. В каждом кружке учится ровно d человек, всего в школе кружков $k \leqslant 2^{d-1}$, $d \geqslant 2$. Можно ли выдать некоторым детям по айфону так, чтобы в любом кружке были дети как с айфонами, так и без?

Решение:

Опишем наше вероятностное пространство.

Ω — всевозможные способы раздать айфоны детям. Каждое событие — бинарная строка из n нулей и единиц (в i-ой позиции стоит 1, если мы выдаём айфон i-ому ребёнку, и 0 иначе), $|\,\Omega\,| = 2^n$. Вероятность каждого события равна $\frac{1}{2^n}$.

Положим событие A_i — i-ый кружок нарушает описанное правило.

Тогда $\Pr(A_i) = \frac{1}{2^n} \cdot (2^{n-d} + 2^{n-d}) = \frac{2^{n-d+1}}{2^n} = 2^{1-d}$ (то есть считаем, что в кружке или у всех детей есть айфоны, или у всех детей они отсутствуют).

$\Pr(\exists$ *кружок, нарушающий правило*$) = Pr(A_1 \cup A_2 \cup ... \cup A_k)$

$\Pr(A_1 \cup A_2 \cup ... \cup A_k) \leqslant \Pr(A_1) + \Pr(A_2) + ... + \Pr(A_k) \leqslant 2^{1-d} \cdot 2^{d-1} = 1.$

Наихудший случай — когда кружков ровно 2^{d-1}. Однако заметим, что и в таком случае не будет достигаться равенство, поскольку для любых двух кружок существует ненулевая вероятность того, что оба будут нарушать правило.

Таким образом, $\Pr($*все кружки хорошие*$) > 0$. Следовательно, можно так распределить айфоны, что все кружки будут удовлетворять правилу.

2.2. Теорема Эрдеша-Ко-Радо

Теорема 2.2.1.

$S = \{0, 1, ..., n-1\}$

$\mathcal{F} \subseteq 2^S$

Пусть выполняются следующие условия:

1) $\forall\, A \in \mathcal{F} \quad |\, A \,| = k,\ k \leqslant \frac{n}{2}$

2) $\forall\, A, B \in \mathcal{F} \quad A \cap B \neq \varnothing$

Тогда $|\, \mathcal{F} \,| \leqslant \binom{n-1}{k-1}$.

Доказательство.

1) Докажем небольшую лемму.

Рассмотрим все множества $A_s = \{s, s+1, ..., s+k-1\}$ (считаем, что суммирование производится по модулю n). Тогда утверждается, что в $\mathcal{F}$ войдёт не более k множеств такого вида.

Положим, что для некоторого $s \in S : A_s \in \mathcal{F}$.

Помимо A_s, в $\mathcal{F}$ могут входить только некоторые множества из A_{s-k+1}, ..., A_{s-1}, A_{s+1}, ..., A_{s+k-1} (таким образом мы требуем, чтобы эти множества пересекались с A_s).

Разобьём описанные множества по парам следующим образом:

(A_{s-k+1}, A_{s+1}), (A_{s-k+2}, A_{s+2}), ..., (A_{s-1}, A_{s+k-1})

Заметим, что внутри каждой пары множества не пересекаются. Следовательно, из каждой пары мы можем выбрать не более одного представителя. Поскольку всего пар $k-1$, то мы можем выбрать не более k таких множеств.

2) Заметим, что описанную лемму можно обобщить для случая перестановок:

Пусть $\sigma : S \to S$ — биекция.

$A_s^\sigma = \{\sigma(s), \sigma(s+1), ..., \sigma(s+k-1)\}$

Тогда $\forall\, \sigma$ $\mathcal{F}$ содержит $\leqslant k$ множеств A_s^σ.

3) Пусть σ — случайная биекция, i — случайный элемент S.

Положим вероятностное пространство $\Omega = \{(\sigma, i) : \sigma \in S_n,\ i \in S\}$, $|\, \Omega \,| = n! \cdot n$.

Рассмотрим множество $\mathcal{U} = \{(\sigma, i) : A_i^\sigma \in \mathcal{F}\}$.

Заметим, что, с одной стороны, $\Pr(\mathcal{U}) \leqslant \frac{1}{n! \cdot n} \cdot (k \cdot n!) = \frac{k}{n}$ (суммируем по всем перестановкам). С другой стороны, $\Pr(\mathcal{U}) = \frac{|\mathcal{F}|}{\binom{n}{k}}$. Следовательно, $\frac{|\mathcal{F}|}{\binom{n}{k}} \leqslant \frac{k}{n} \implies |\, \mathcal{F} \,| \leqslant \frac{k}{n} \cdot \binom{n}{k} = \binom{n-1}{k-1}$.

□

2.3. Случайная величина и её математическое ожидание

***Определение* 2.3.1.**

$(\Omega,\ \Pr)$ — конечное вероятностное пространство.

Случайной величиной называется функция $X : \Omega \to \mathbb{R}$, сопоставляющая каждому событию некоторое числовое значение.

$[X \in A] = \{\omega \in \Omega : X(\omega) \in A\}$, где $A \subseteq \mathbb{R}$.

Пример.

$\Omega = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$ — значения, которые могут выпасть на игральном кубике.

$X(1) = 1^2,\ X(2) = 2^2,\ ...,\ X(6) = 6^2$

$[X \in \{1,\ 2,\ ...,\ 10\}] = \{1,\ 2,\ 3\}$

***Определение* 2.3.2.**

$(\Omega, \Pr)$ — конечное вероятностное пространство.

$X : \Omega \to \mathbb{R}$ — случайная величина.

$\mathbb{E}[X]$ — математическое ожидание.

$\mathbb{E}[X] = \sum\limits_{\omega\in\Omega} \Pr(\omega) \cdot X(\omega)$

Свойства.

1) Линейность.

$X, Y : \Omega \to \mathbb{R},\ \alpha, \beta \in \mathbb{R}$

Тогда $\mathbb{E}[\alpha X + \beta Y] = \alpha\mathbb{E}[X] + \beta\mathbb{E}[Y]$

2) Принцип усреднения.

$X : \Omega \to \mathbb{R}$

Тогда $\Pr(X \geqslant \mathbb{E}[X]) > 0$ и $\Pr(X \leqslant \mathbb{E}[X]) > 0$

Доказательство.

1) Распишем по определению:

$\mathbb{E}[\alpha X+\beta Y] = \sum\limits_{\omega\in\Omega} \Pr(\omega)\cdot\big(\alpha X(\omega)+\beta Y(\omega)\big) = \alpha \sum\limits_{\omega\in\Omega} \Pr(\omega)X(\omega)+\beta \sum\limits_{\omega\in\Omega} \Pr(\omega)Y(\omega) = \alpha\mathbb{E}[X]+\beta\mathbb{E}[Y]$

2) От противного.

Пусть $\forall\,\omega \in \Omega : \Pr(\omega) > 0 \quad X(\omega) < \mathbb{E}[X]$

$\mathbb{E}[X] = \sum\limits_{\omega\in\Omega} \Pr(\omega)X(\omega) < \sum\limits_{\omega\in\Omega} \Pr(w)\mathbb{E}[X] = \mathbb{E}[X] \sum\limits_{\omega\in\Omega} \Pr(\omega) = \mathbb{E}[X] \implies$ противоречие $\square$

***Определение* 2.3.3.** Турнир — орграф, между любыми двумя вершинами которого ровно 1 ребро.

Теорема 2.3.1.

$\forall\, n\ \exists$ турнир на n вершинах, в котором хотя бы $\frac{n!}{2^{n-1}}$ вершин.

Доказательство.

Ω — множество всех турниров на n вершинах, $|\,\Omega\,| = 2^{\frac{n(n-1)}{2}}$.

$X(\omega)$ — число гамильтоновых путей в ω.

Пусть σ — перестановка вершин.

Скажем, что $X_\sigma(\omega) = \begin{cases} 1 & \text{, если } \sigma \text{ задаёт гамильтонов путь в } \omega \\ 0 & \text{, иначе} \end{cases}$

Таким образом, $X(\omega) = \sum\limits_{\sigma \in S_n} X_\sigma(\omega)$.

$\mathbb{E}[X] = \sum\limits_{\sigma \in S_n} \mathbb{E}[X_\sigma] = \sum\limits_{\sigma \in S_n} (\Pr[X_\sigma = 1] \cdot 1 + \Pr[X_\sigma = 0] \cdot 0) = \sum\limits_{\sigma \in S_n} \Pr[X_\sigma = 1]$

Заметим, что σ задаёт гамильтонов путь, если существуют рёбра $\sigma(1) \to \sigma(2) \to ... \to \sigma(n)$. Направления остальных рёбер нас не интересуют.

Таким образом, $\Pr[X_\sigma = 1] = \frac{2^{\frac{n(n-1)}{2} - (n-1)}}{2^{\frac{n(n-1)}{2}}} = \frac{1}{2^{n-1}}$.

Отсюда получаем, что $\mathbb{E}[X] = \sum\limits_{\sigma \in S_n} \Pr[X_\sigma = 1] = \frac{n!}{2^{n-1}}$.

А по принципу усреднения существует такой турнир, что количество гамильтоновых путей в нём по крайней мере $\frac{n!}{2^{n-1}}$. □

2.4. 3-КНФ. Неравенство Маркова.

Теорема 2.4.1.

φ — формула в 3-КНФ, m — число дизъюнктов в φ.

Тогда $\exists$ набор переменных, который выполняет $\geqslant \frac{7}{8}m$ дизъюнктов.

Доказательство.

TODO □

Теорема 2.4.2. (**Неравенство Маркова**)

TODO

2.5. Энтропия случайной величины

***Определение* 2.5.1.** Энтропия.
(Ω, Pr) – конечное вероятностное пространство
$X : \Omega \to \mathbb{R}^k$ – случайная величина
$X(\Omega) = \{a_1, a_2, \ldots, a_n\}$
$p_i = Pr[x = a_i]$
Тогда энтропия случайной величины выражается следующим образом:

$$H[X] = \sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i}$$

Анонс-пояснение: энтропия – это количество информации, которую несёт в себе случайная величина.

Пример 1. Пусть $X \in \{1, 0\}^n$ – случайная величина, $\forall S \in \{0, 1\}^n \ Pr[x = S] = 2^{-n}$. Тогда:

$$H[X] = \sum_{S \in \{0,1\}^n} \frac{1}{2^n} \log_2 2^n = n$$

Теорема 2.5.1 (Неравенство Йенсена)**.** Пусть $f : (a, b) \to \mathbb{R}$ – выпуклая. То есть:

$$\forall x, y \in (a, b), \alpha \in [0, 1]$$

$$f(\alpha x + (1-\alpha)y) \leqslant \alpha f(x) + (1-\alpha)f(y)$$

Тогда $\forall x_1, x_2, \ldots, x_n \in (a,b)$, $\forall \lambda_1, \lambda_2, \ldots, \lambda_n \in [0,1], \sum_{i=1}^n \lambda_i = 1$

$$f(\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n) \leqslant \lambda_1 f(x_1) + \lambda_2 f(x_2) + \ldots + \lambda_n x_n$$

Замечание. $\log_2 x$ – вогнутая функция (иначе говоря, $-log_2 x$ – выпуклая)

Лемма. $x_1, x_2, \ldots, x_n, x_i > 0, \sum_{i=1}^n x_i = 1;\ y_1, y_2, \ldots, y_n, y_i > 0, \sum_{i=1}^n y_i \leqslant 1$
Тогда:

$$\sum_{i=1}^n x_i \log_2 \frac{1}{x_i} \leqslant \sum_{i=1}^n x_i \log_2 \frac{1}{y_i}$$

Доказательство.

$$\sum_{i=1}^n x_i \log_2 \frac{1}{x_i} - \sum_{i=1}^n x_i \log_2 \frac{1}{y_i} = \sum_{i=1}^n x_i \log_2 \frac{x_i}{y_i} \underset{\text{Неравенство Йенсена}}{\leqslant} \log_2 \sum_{i=1}^n y_i \leqslant 0$$

□

Замечание. $(X,Y) : \Omega \to (X(\Omega), Y(\Omega))$
$X : \Omega \to \mathbb{R}^k$
$Y : \Omega \to \mathbb{R}^l$
$(X,Y) : \Omega \to \mathbb{R}^{k+l}$

Теорема 2.5.2. $H[X,Y] \leqslant H[X] + H[Y]$, причём, равенство достигается тогда и только тогда, когда X и Y независимы

Доказательство. Пусть X принимает значения $\{a_1, a_2, \ldots, a_n\}$, а Y – $\{b_1, b_2, \ldots, b_m\}$ и $p_{a_i} = Pr[x = a_i], q_{b_i} = Pr[y = b_i]$. А также $\rho_{a_i,b_j} = Pr[x = a_i, y = b_j]$, тогда:

$$H[X,Y] = \sum_{i=1}^n \sum_{j=1}^m \rho_{a_i,b_j} \log_2 \frac{1}{\rho_{a_i,b_j}}$$

$$H[X] + H[Y] = \sum_{i=1}^n p_{a_i} \log_2 \frac{1}{p_{a_i}} + \sum_{j=1}^n q_{b_j} \log_2 \frac{1}{q_{b_j}}$$

Заметим, что $p_{a_i} = \sum_{j=1}^m \rho_{a_i,b_j}$ и $q_{b_j} = \sum_{i=1}^n \rho_{a_i,b_j}$. Действительно, вероятность того, что произойдет какое-то конкретное событие из X – сумма вероятностей того, что произойдет такое фиксированное событие и при этом любое событие из Y. И наоборот. Тогда:

$$H[X] + H[Y] = \sum_{i=1}^n \sum_{j=1}^m \rho_{a_i,b_j} \log_2 \frac{1}{p_{a_i}} + \sum_{i=1}^n \sum_{j=1}^m \rho_{a_i,b_j} \log_2 \frac{1}{q_{b_j}} = \sum_{i=1}^n \sum_{j=1}^m \rho_{a_i,b_j} \log_2 \frac{1}{p_{a_i} q_{b_j}}$$

Осталось проверить, что $\sum_{i=1}^n \sum_{j=1}^m p_{a_i} q_{b_j} = 1$. Поменяем порядок суммирования: $\sum_{i=1}^n p_{a_i} \sum_{j=1}^m q_{b_j} = \sum_{i=1}^n p_{a_i} = 1$. Значит, можно использовать неравенство Йенсена, по которому:

$$H[X,Y] = \sum_{i=1}^n \sum_{j=1}^m \rho_{a_i,b_j} \log_2 \frac{1}{\rho_{a_i,b_j}} \leqslant \sum_{i=1}^n \sum_{j=1}^m \rho_{a_i,b_j} \log_2 \frac{1}{p_{a_i} q_{b_j}} = H[X] + H[Y]$$

□

Замечание.
Если X и Y при этом были независимы, то $Pr[x = a_i, y = b_j] = Pr[x = a_i]Pr[y = b_j] \Rightarrow \rho_{a_i,b_j} = p_{a_i}q_{b_j}$ и неравенство обращается в равенство.

Следствие Полуаддитивность энтропии. Пусть $X_1, X_2, \ldots, X_n$ – случайные величины. Тогда $H[X_1, X_2, \ldots, X_n] \leqslant H[X_1] + H[X_2] + \ldots + H[X_n]$

Доказательство. Упражнение. Подсказка: доказазывается по индукции. □

Утверждение 2.5.3.

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{pn} = \sum_{0 \leqslant i \leqslant \lfloor pn \rfloor} \binom{n}{i} \leqslant 2^{n*h(p)}$$

Где $h(p) = p\log_2 \frac{1}{p} + (1-p)\log_2 \frac{1}{1-p}$ – бинарная энтропия
$h(p) \uparrow, p \in [0, \frac{1}{2}]$ и $h(p) \downarrow, p \in [\frac{1}{2}, 1]$

Доказательство. Докажем, что если есть некоторое множество $\mathcal{F} \subseteq \{0,1\}^n : \forall s \in \mathcal{F}$ в $s \leqslant pn$ единиц, то $|\mathcal{F}| = \sum_{0 \leqslant i \leqslant pn} \binom{n}{i}$
Пусть X – случайная величина, равномерная на $|\mathcal{F}|$. Тогда $H[X] = \sum_{s \in \mathcal{F}} \frac{1}{|\mathcal{F}|} \log_2 |\mathcal{F}| = \log_2 |\mathcal{F}|$
Что же это была за величина? $X = x_1 + x_2 + \ldots + x_n$, где $x_i = 1$, если i-й бит s равен 1. Тогда:
$H[X] = H[x_1 + x_2 + \ldots + x_n] \leqslant H[X_1] + H[X_2] + \ldots + H[X_n] =$
TODO () □

Неравенство Крафта и сопутствующее: TODO ()