Математические основы Computer Science
Часть 2: Вероятностный метод. Лекция 5.

Дмитрий Ицыксон

ПОМИ РАН

1 ноября 2009

Содержание лекции

1. Конечное вероятностное пространство.
2. Основная идея вероятностного метода.
3. Числа Рамсея
4. Монотонная схема для функции голосования.
5. Теорема Эрдеша-Ко-Радо.

Литература

1. Н. Алон, Дж. Спенсер. Вероятностный метод.
2. Н.К. Верещагин, А. Шень. Языки и исчисления
3. М. Айгнер, Г. Циглер. Доказательства из Книги.

Конечное вероятностное пространство

Определение. Конечным вероятностным пространством называется пара (Ω, p), где

- Ω — конечное множество, пространство элементарных событий;
- $p : 2^{\Omega} \to [0, 1]$ — вероятностная мера:
  1. $p(\Omega) = 1$
  2. Если $A, B \subseteq \Omega$ и $A \cap B = \emptyset$, то $p(A \cup B) = p(A) + p(B)$.

- $p(\emptyset) = 0$;
- $A \subseteq B$, тогда $p(B) = p(A) + p(B \setminus A) \implies p(A) \leq p(B)$;
- $\Omega = \{1, 2, \ldots, n\}$. $p_1, p_2, \ldots, p_n \geq 0$, $\sum_{i=1}^{n} p_i = 1$, $p(i) = p_i$. $p(A) = \sum_{i \in A} p_i$.

Простейшие свойства вероятности

- $p(\emptyset) = 0,\ p(\Omega) = 1;$
- $p(A_1 \cup A_2 \cup \cdots \cup A_n) \leq \sum_{i=1}^{n} p(A_i);$
- (формула включений-исключений) $p(A_1 \cup A_2 \cup \cdots \cup A_n) = \sum_{i=1}^{n} p(A_i) - \sum_{i<j} p(A_i A_j) + \cdots + (-1)^n p(A_1 A_2 \ldots A_n)$
- $p(A_1 \cup A_2 \cup \cdots \cup A_n) \geq \sum_{i=1}^{n} p(A_i) - \sum_{i<j} p(A_i A_j)$

Пример про галстуки

- Пример. В школе есть несколько кружков, в каждом кружке ровно d человек, всего кружков не более 2^{d-1}. Тогда можно некоторым детям выдать галстуки так, чтобы в каждом кружке были дети как с галстуками, так и без них.

  Доказательство.
  - Каждому ребенку выдадим галстук с вероятностью $\frac{1}{2}$.
  - A_i — все дети в i-м кружке либо в галстуках, либо без галстуков.
  - $\Pr[A_i] = \frac{1}{2^{d-1}}$.
  - $\Pr[\cup_i A_i] < \sum \Pr[A_i] \leq 2^{d-1} \frac{1}{2^{d-1}} = 1$
  - Значит, вероятность того, что во всех кружках есть как люди с галстуками, так и без галстуков, положительна.

Числа Рамсея

- Среди любых 6 человек найдется либо 3 человека, попарно знакомых друг с другом, либо 3 человека попарно не знакомых друг с другом.
- В полном графе ребра покрашены в 2 цвета: черный и белый. Обязательно ли найдется белый n-вершинный подграф или черный k-вершинный подграф?
- $R(m, n)$ — наименьшее число, что в графе с таким количеством вершин найдется либо m-вершинный белый подграф, либо n-вершинный черный подграф.
- $R(3, 3) = 6,\ R(2, k) = k$
- $R(m, n) = R(n, m)$
- $R(m, n) \leq R(m-1, n) + R(m, n-1)$
- $R(m, n) \leq C_{m+n-2}^{n-1}$
- $R(m, n) \leq R(m-1, n) + R(m, n-1) \leq C_{m+n-3}^{n-1} + C_{m+n-3}^{n-2} = C_{m+n-2}^{n-1}$

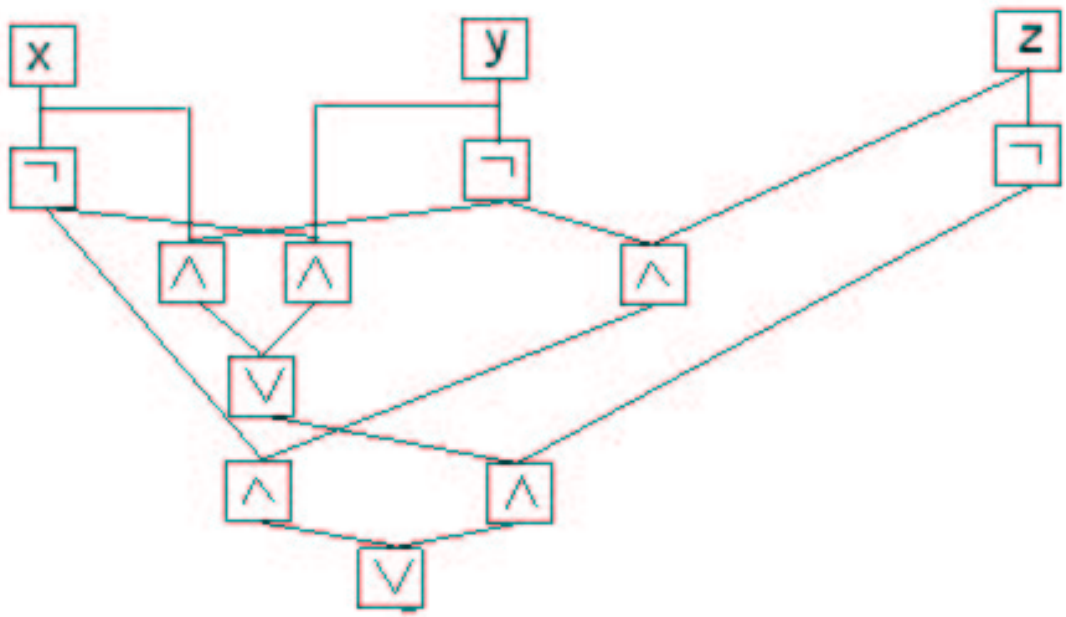
Оценки на число $R(k,k)$

- $R(k,k) \leq C_{2k-2}^{k-1} \leq 2^{2k-2}$
- Теорема. При $k \geq 2$ выполняется $R(k,k) \geq 2^{\frac{k}{2}}$
- $R(2,2) = 2, R(3,3) = 6$, далее $k \geq 4$
- Пусть $N < 2^{\frac{k}{2}}$.
- Красим каждое ребро случайным образом в один из 2-х цветов.
- Все раскраски равновероятны: $p_i = 2^{-C_N^2}$
- A — множество из k вершин.
- A_w: все вершины A соединены белыми ребрами, $p(A_w) = 2^{-C_k^2}$.
- $p_w = p(\cup_{|A|=k} A_w) \leq \sum_{|A|=k} p(A_w) = C_N^k 2^{-C_k^2}$
- $p_w \leq C_N^k 2^{-C_k^2} \leq \frac{N^k}{2^{k-1}} 2^{-C_k^2} < 2^{\frac{k^2}{2} - C_k^2 - k + 1} = 2^{-\frac{k}{2}+1} \leq \frac{1}{2}$

Булевы схемы

Булева схема - это

- Ориентированный граф без циклов
- Ровно одна вершина, из которой не выходит ребер (выход)
- n вершин в которые не входят ребра
- Все остальные вершины помечены логическими связками $\vee, \wedge, \neg$. (арность связки должна равняться числу исходящих ребер)



Монотонные булевы функции и схемы

- $x, y \in \{0,1\}^n$, $x \leq y \iff \forall i, x_i \leq y_i$
- $f : \{0,1\}^n \to \{0,1\}$ монотонная, если $\forall x \leq y, f(x) \leq f(y)$.
- f — монотонная, если при замене 0 на 1, значение f не уменьшается.
- Монотонная схема: все связки $\wedge$ и $\vee$.
- Монотонная схема вычисляет монотонную функцию.
- Любую монотонную функцию (отличную от константы) можно вычислить с помощью монотонных схем.

Монотонная схема для функции голосования

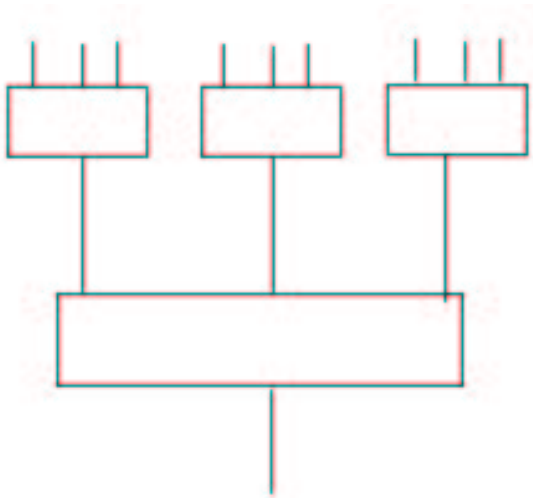
- $Maj(x_1, x_2, \cdots x_{2k+1}) = \begin{cases} 1, x_1 + x_2 + \cdots + x_{2k+1} > k \\ 0, \text{иначе} \end{cases}$
- Монотонная схема функции голосования:

$$\bigvee_{|I|=k+1} \bigwedge_{i \in I} x_i$$

- Размер: $C_n^{\lceil n/2 \rceil}$ — экспоненциальный.
- Теорема. Существует монотонная схема для функции голосования, размера $O(n^c)$ и глубины $O(\log n)$.

Вероятностная конструкция

- $Maj_3(a, b, c) = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c)$
- Составим ℓ уровней блоков из Maj_3
- Глубина ℓ, входов 3^ℓ
- Независимо случайным образом выберем переменную, которая попадет на вход.
- Проверим, что получившаяся схема с положительной вероятностью вычисляет функцию голосования.
- Если глубина $\ell = c \log n$, то размер $O(3^{c \log n}) = O(n^{c'})$



Оценка вероятности

- Выберем набор значений переменных. И покажем, что схема дает правильный ответ с вероятностью $1 - \varepsilon$.
- Тогда с вероятностью $1 - 2^n\varepsilon$ схема дает правильный ответ на всех входах.
- Пусть доля единиц на входе равняется p.
- Если на вход Maj_3 единица приходит с вероятностью p, то вероятность единицы на выходе равняется $\varphi(p) = 3p^2(1-p) + p^3 = 3p^2 - 2p^3$.
- Вероятность единицы на следующем уровне $\varphi(\varphi(p))$.
- $\varphi^{(l)}(p)$.

Анализ

- $\varphi(x) = 3x^2 - 2x^3$, $\varphi(0) = 0, \varphi(\frac{1}{2}) = \frac{1}{2}, \varphi(1) = 1$
- $\varphi'(x) = 6x - 6x^2 = 6(1-x)x > 0$
- $\varphi'(x) > \frac{18}{16}$ при $\frac{1}{2} < x < \frac{3}{4}$
- Пусть $p > \frac{1}{2}$, тогда $p > \frac{1}{2} + \frac{1}{2n}$.
- При $\frac{1}{2} < x < \frac{3}{4}$ выполняется
  $\varphi(x) - \frac{1}{2} = \varphi(x) - \varphi(\frac{1}{2}) = \varphi'(\xi)(x - \frac{1}{2}) > \frac{18}{16}(x - \frac{1}{2})$
- $\varphi^{(m)}(p) > \frac{3}{4}$ для некоторого $m = O(\log n)$.
- При $x \geq \frac{3}{4}$ выполняется
  $1 - \varphi(x) = (1-x)^2(2x+1) < \frac{3}{4}(1-x)$
- Значит $\varphi^{(m)}(p) > 1 - 2^{-n}$ для некоторого $m = O(\log n)$.
- Аналогично, если $p < \frac{1}{2} - \frac{1}{2n}$, то $\varphi^{(m)}(p) < 2^{-n}$ для некоторого $m = O(\log n)$.

Теорема Эрдеша-Ко-Радо

- $S = \{0, 1, 2, \ldots, n-1\}$, $\mathcal{F} \subseteq 2^S$
- $\forall A \in \mathcal{F}$, $|A| = k$, $k \leq \frac{n}{2}$
- $\forall A, B \in \mathcal{F}$, $A \cap B \neq \emptyset$
- Теорема. $|\mathcal{F}| \leq C_{n-1}^{k-1}$.
- Равенство достигается, когда $\mathcal{F}$ состоит из всех k-элементных множеств, имеющих общий элемент.
- Лемма. $A_s = \{s, s+1, \ldots, s+k-1\}$, $0 \leq s \leq n-1$. Тогда $\mathcal{F}$ содержит не более k множеств A_s.
  Доказательство.
  - Пусть $A_s \in \mathcal{F}$.
  - С A_s могут пересекаться только $A_{s-k+1}, A_{s-k+2}, \ldots A_{s+k-1}$.
  - Разобем на пары: A_{s-i}, A_{s+k-i}, $1 \leq i \leq k-1$.
  - Всего $k-1$ пара.
  - Из каждой пары максимум одно множество в $\mathcal{F}$.
- Порядок элементов может быть любой.

Теорема Эрдеша-Ко-Радо

- Лемма. $A_s = \{s, s+1, \ldots, s+k-1\}$, $0 \le s \le n-1$. Тогда $\mathcal{F}$ содержит не более k множеств A_s.
- Теорема. $|\mathcal{F}| \le C_{n-1}^{k-1}$.
  Доказательство.
  - Выберем σ — случайную перестановку множества S и случайное $i \in S$.
  - $A = \{\sigma(i), \sigma(i+1), \ldots, \sigma(i+k-1)\}$
  - $\Pr[A \in \mathcal{F}] \le \frac{k}{n}$
  - Все k-элементные множества с равной вероятностью могут быть множествами A.
  - $\frac{k}{n} \ge \Pr[A \in \mathcal{F}] = \frac{|\mathcal{F}|}{C_n^k}$
  - $|\mathcal{F}| \le \frac{k}{n} C_n^k = \frac{k}{n} \cdot \frac{n!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-k)!} = C_{n-1}^{k-1}$.