30.11.20. Дискр. матем. д/з от семинара 13.

1. $F_{n,2} = \{f \in P_2(n) : \deg f \le 2\}$.

$? \lesssim \max\limits_{f\in F_{n,2}} L(f) \lesssim ?$ Ответ: $\sim \frac{n^2}{4\log n}$

Решение: нижняя оценка: используем т. 11.4 со стр. 198.

$m=1$ – т.к. у нас 1 ф-ция, а не вектор-функция.

$|F_{n,2}| = 2^{C_n^2+C_n^1+C_n^0}$

$\log|F_{n,2}| = C_n^2+C_n^1+C_n^0 \sim \frac{n^2}{2}$

$\log\log|F_{n,2}| = 2\log n$

$\Rightarrow \frac{\log|F_{n,2}|}{\log\log|F_{n,2}|} = \frac{n^2}{4\log n}$

$n+1 \overset{?}{=} \bar{o}\left(\frac{n^2}{4\log n}\right)$ – верно $\Rightarrow$ т. выполнена

$\Rightarrow \max\limits_{f\in F_{n,2}} L(f) \gtrsim \frac{n^2}{4\log n}$

Верхняя оценка: сначала заметим, что основной вклад даёт квадратичная часть, т.е. если $f = \underbrace{f_2}_{\deg=2} \oplus \underbrace{f_1}_{\deg=1} \oplus \underbrace{f_0}_{\deg=0}$,

то $L(f) \geq \frac{n^2}{4\log n}$, а $L(f_1 \oplus f_0) \sim n$.

$\Rightarrow$ рассм. только квадр. часть.

$f_2(x_1\dots x_n) = \sum\limits_{i,j=1}^{n} x_i x_j = x_n(\underbrace{\dots\dots}_{l_1(x_1\dots x_n)}) + x_{n-1}(\underbrace{l_2}_{l_2(x_1\dots x_{n-1})}) + \dots + x_1\cdot(l_n) = \sum\limits_{i=1}^{n} x_i \cdot \sum\limits_{j=1}^{i} \alpha_{ij} x_j$

т.е. для вычисления $f_2(x_1\dots x_n)$ нам нужно вычислить систему линейных ф-ций с матрицей $\begin{pmatrix} \alpha_{11} & & 0 \\ \alpha_{21} & \alpha_{22} & \\ \dots & & \ddots \\ \alpha_{n1} & \alpha_{n2} \dots & \alpha_{nn} \end{pmatrix}$

Она $n \times n$.

По лемме 11.4 на стр. 194 для линейных ф-ций:

$L(f_2) \le \frac{n(n+\log_2 n)}{\log_2 n} \sim \frac{n^2}{\log_2 n}$.

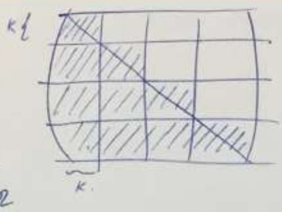
На самом деле, можно получить и $L(f_2) \lesssim \frac{n^2}{2\log_2 n}$,

ведь наша матрица – нижнетреугольная; а лемма 11.4 – для произвольных квадратных матриц.

Итак, разобьём матрицу на квадратики со стороной k.

k – выберем позже.

Тогда $L(\triangle) \le L(\text{мм}) + \underbrace{k}_{\text{строк в полосе}} \cdot \underbrace{\left(1+\dots+\left(\frac{n}{k}-1\right)\right)}_{\text{на суммирование кусков внутри одной полосы}} =$



$= L(\text{мм}) + k \cdot \frac{1}{2}\left(\frac{n}{k}-1\right)\cdot\frac{n}{k} \approx L(\text{мм}) + \frac{k\cdot n^2}{2k^2} = L(\text{мм}) + \frac{n^2}{2k} = \frac{n^2}{2\log k} + \frac{n^2}{2k} \overset{?}{\approx} \frac{n^2}{2\log n}$

$L(\text{мм}) = \underbrace{L(▦)}_{\frac{k^2}{\log k}} \cdot \underbrace{\frac{1}{2}\left(\frac{n}{k}\right)^2}_{\text{кол-во квадратиков}} = \frac{n^2}{2\log k}.$

=> Хотим: $\frac{n^2}{2\log k} + \frac{n^2}{2k} \approx \frac{n^2}{2\log n}.$

Для этого положим $k := \frac{n}{(\log n)^2}$

$\Rightarrow \frac{n^2}{2\log k} \approx \frac{n^2}{2\log n}$,

а $\frac{n^2}{2k} = \frac{n^2 \cdot (\log n)^2}{2n} = \frac{n(\log n)^2}{2} = \bar{o}\left(\frac{n^2}{2\log n}\right)$

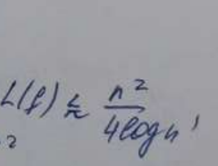
$$\boxed{\text{Ответ: } \frac{n^2}{4\log n} \lesssim \max_{f\in F_{n,2}} L(f) \lesssim \frac{n^2}{2\log n}}$$

(2) Док-ть, что $\frac{n^2}{4\log n} \sim \max_{f\in F_{n,2}} L(f)$

Решение:

Для этого нам нужно док-ть, что $\max_{f\in F_{n,2}} L(f) \lesssim \frac{n^2}{4\log n}$, т.е. в 2 раза уменьшить предыдущую оценку.

Заметим, что лемма 11.4, на которую мы ссылаемся, делит матрицу на ~~кусочки~~ полосы высоты $k = \log n - 2\log\log n$, и для них применяет лемму 11.3, по которой сложность такого куска ~ числу переменных.



При таком порядке

$L(f) = k + 2k + \dots + \frac{n}{k}\cdot k = k\cdot\left(1+2+\dots+\frac{n}{k}\right) = k\cdot\frac{n^2}{2k^2} = \frac{n^2}{2k} \approx \frac{n^2}{2\log n}$, т.к. $k = \log n - 2\log\log n$.

Где можно сэкономить?

Ну в лемме 11.3 max кол-во операций тратится

на вычисление $y_j = \bigoplus_{x_i \in M_j} x_i$, т.е на формирование мн-в M_j,
содержащих т.е переменные, у которых столбцы одинаковы и равны двоичному представлению j.

Заметим, что если какая-то пара переменных $x_1 \oplus x_2$ встречается ≥ 2 раз,
то нам выгодно заранее вычислить (нужна 1-я вычисления) $x_1 \oplus x_2$, а второй раз уже не прибавлять
отдельно $\underbrace{\text{что-то} \oplus x_1 \oplus x_2}_{2 \text{ операции}}$, а прибавить $\underbrace{\text{что-то} \oplus (x_1 \oplus x_2)}_{1 \text{ операция}}$.

~~Т.е~~ Т.е берем все пары, упорядочиваем по убыванию кол-ва раз встречаемости, $\underbrace{\text{вычисляем}}_{\text{последовательно}}$ сумму каждой пары, и одновременно выкидываем эту пару из всех мн-в (т.к тройки переменных хранить уже нет смысла, т.к разных троек $\sim n^3$, а у нас встречается $\sim n^2$ троек, т.е с большой вероятностью в нашей матрице окажется так, что во мн-вах все тройки будут разные, т.е еще сэкономить за счёт предварительного вычисления троек не получится).
При выкидывании некоторые мн-ва могут стать пустыми — но мы их всё равно считаем, т.к min пар $\underbrace{\text{останется}}_{\text{после выкидывания}}$, если во всех мн-вах — одинаковое число переменных. Посчитаем, какое именно.

$k = \log n - 2\log\log n$. (т.к по н-ву Иенсена $\sum_{i=1}^{m} C_{n_i}^{k} \geq m \cdot C^{k}_{\frac{n}{m}}$)

В каждой из $\frac{n}{k}$ полос есть $\leq 2^k = 2^{\log n - 2\log\log n} = \frac{n}{(\log n)^2}$ мн-в M_j

$\Rightarrow$ всего в таблице $\frac{\text{кол-во}}{\text{мн-в}}$ равно $N = \frac{n}{k} \cdot 2^k = \frac{n}{\log n} \cdot \frac{n}{(\log n)^2} = \frac{n^2}{(\log n)^3}$.

После выбрасывания пар min $\underbrace{\text{кол-ва}}_{\text{суммарного}}$ ~~...~~ оставшихся в мн-вах элементов (т.е переменных, которые остались без пары) — будет, если все мн-ва имеют одинаковое кол-во элементов, пусть x.

$\Rightarrow \underbrace{N}_{= \frac{n^2}{(\log n)^3}} \cdot C_x^2 < \underbrace{C_n^2 \approx \frac{n^2}{2}}_{\text{всего возможных разных пар}}$ — т.к процесс выкидывания остановится, когда все оставшиеся пары будут различны, т.к если ~~...~~ пара встречается ≥ 2 раза, то выгодно её считать заранее

$\Rightarrow \frac{n^2}{(\log n)^3} \cdot \frac{x^2}{2} < \frac{n^2}{2}$

$\Rightarrow x^2 < (\log n)^3$

$\Rightarrow x < (\log n)^{3/2}$

⇒ без пары останется $\le \underset{\substack{\text{кол-во}\\ \text{мн-в}}}{N}\cdot\underset{\substack{\text{кол-во}\\ \text{элем в}\\ \text{каждом мн-ве}}}{X} = \frac{n^2}{(\log n)^3}\cdot(\log n)^{3/2} = \frac{n^2}{(\log n)^{3/2}}$

А изначально в объединении мн-в содержались все переменные треугольной матрицы, т.е $\frac{n^2}{2k^2} = \frac{n^2}{2\log n}$.

Но заметим, что $\frac{n^2}{(\log n)^{3/2}} = \bar{o}\left(\frac{n^2}{2\log n}\right)$

т.е осталось без пары (т.е без выигрыша в 2 раза в числе операций) — всего $\bar{o}$ (от изначального кол-ва элементов).

Т.е мы почти всем элементам уменьшили в 2 раза кол-во операций.

⇒ изначальная оценка $\frac{n^2}{2\log n}$ уменьшилась в 2 раза,

и получилась как раз $\frac{n^2}{4\log n}$ чтд.

<u>Зам.</u> покажем, что тройки действительно ~~[illegible]~~ считать заранее — не поможет.

У нас всего $N = \frac{n^2}{(\log n)^3}$ мн-в.

А элементов всего $\frac{n^2}{2k^2} = \frac{n^2}{2\log n}$

⇒ каждое мн-во по $\sim(\log n)^2$ элементов

⇒ троек в каждом мн-ве $\sim(\log n)^6$.

⇒ всего во всех мн-вах $N\cdot(\log n)^6 = \frac{n^2}{(\log n)^3}\cdot(\log n)^6 = n^2\cdot(\log n)^3$ троек ~~[illegible]~~

легко может случиться, что ~~[illegible]~~ все они разные, т.к ~~[illegible]~~ всего различных троек бывает $C_n^3 \sim n^3$,

а $n^2(\log n)^3 = \bar{o}(n^3)$.

(3.) $A = \{f \in P_2(n) : f(x) = f(y), \text{ если } |x| = |y| \pmod{n^3}\}$

$? \le \max\limits_{f\in A} L(f) \le ?$ Ответ: $\frac{n^3}{3\log n}$

<u>Решение:</u> $|x| = \sum_{i=1}^{n} x_i\cdot 2^{n-i}$ — представляет собой двоичную запись какого-то числа до 2^n

т.е у нас по усл. только n^3 ~~[illegible]~~ наборов, на которых ~~[illegible]~~ могут быть разные значения, остальные значения будут повторять эти n^3 значе-

$\Rightarrow |A| = 2^{n^3}$

$\Rightarrow \log_2 |A| = n^3$

$\left.\begin{array}{l}\log\log|A| = 3\log n.\end{array}\right\} \Rightarrow \dfrac{\log|A|}{\log\log|A|} \approx \dfrac{n^3}{3\log n}$

$m = 1$ – т.к. 1 выход у ф-ции

$n+1 = \bar{o}\left(\dfrac{n^3}{3\log n}\right) \xRightarrow{\text{по}}$ теореме 11.4 : $L(f) \geq \dfrac{\log|A|}{\log\log|A|} = \dfrac{n^3}{3\log n}$.

Попробуем сверху оценить:

Закодируем наши n^3 наборов двоичными наборами,

т.е $n^3 \rightsquigarrow 2^s$ – наборов длины s

$\Rightarrow s = \lceil 3\log n \rceil$

Метод Лупанова каждую $f(x_1 \ldots x_n)$ – ю $\leq \dfrac{2^n}{n}$ реализует.
асимпт. оптим. способ

$\Rightarrow$ ф-цию из наборов длины s можно за $\leq \dfrac{2^s}{s} = \dfrac{2^{\overbrace{\lceil 3\log n \rceil}^{= 3\log n + 1}}}{\lceil 3\log n \rceil} \simeq \dfrac{2 \cdot n^3}{3\log n}$.

Но можно и в 2 раза меньше, если использовать частичные ф-ции: нам из 2^s наборов нужны не все, а только n^3 наборов, а на остальных – наша ф-ция не определена.

~~$\Rightarrow$ по теореме~~

$\Rightarrow$ по теореме 11.7 для частично определенных ф-ций:

$L(f) \sim \dfrac{|D|}{\log|D|} = \dfrac{n^3}{3\log n}$.

$\boxed{\text{Ответ: } L(f) \sim \dfrac{n^3}{3\log n}}$

4. $B = \{f(x_1 \ldots x_n; y_1 \ldots y_n);\ f\text{-симм. отн-е } x_i\}$

$? \leq \max\limits_{f \in B} L(f) \leq ?$

ответ $\dfrac{(n+1) \cdot 2^n}{n + \log n}$

Решение: Наборов, на которых разное значение – их $\underbrace{(n+1)}_{\substack{\text{т.к.} \\ \text{зависит} \\ \text{только от} \\ \text{кол-ва единиц}}} \cdot \underbrace{2^n}_{\text{по } y}$

$\Rightarrow |B| = 2^{(n+1) \cdot 2^n}$

$\left.\begin{array}{l}\log|B| = (n+1) \cdot 2^n \\ \log\log|B| \approx n + \log n\end{array}\right\} \Rightarrow \dfrac{\log|B|}{\log\log|B|} = \dfrac{(n+1) \cdot 2^n}{n + \log n}$

переменных – их $2n$
выход – один

$$2n+1 = \bar{o}\left(\frac{(n+1)\cdot 2^n}{n+\log n}\right) \Rightarrow \text{по теореме 11.4: } L(f) \geq \frac{(n+1)\cdot 2^n}{n+\log n}.$$

Теперь оценим сверху:
Загоним $(n+1)\cdot 2^n$ в двоичные наборы длины $s = \lceil \log((n+1)\cdot 2^n) \rceil = n+\log(n+1)+1$

$\Rightarrow$ по теореме Лупанова $L(f) \leq \frac{2^s}{s} = \frac{2^{\lceil \log(n+1)\cdot 2^n \rceil}}{n+\log(n+1)+1} \sim \frac{2(n+1)\cdot 2^n}{n+\log n}.$

Теперь за счёт частичных ф-ций избавимся от двойки:
мы не все 2^s наборов используем, а только $(n+1)\cdot 2^n$ из них
$\Rightarrow$ по теореме 11.7: $L(f) \leq \frac{|D|}{\log |D|} = \frac{(n+1)\cdot 2^n}{n+\log n}.$

$$\boxed{\text{Ответ: } L(f) \sim \frac{(n+1)\cdot 2^n}{n+\log n}}$$

5. Найти $\max\limits_{k=1\ldots n} L(\text{вычисления } x^k) = ?$ Ответ. $L(x^n) \sim \log n$

Решение: Тривиальная оценка: $L(x^n) \leq n-1$ – но это не интересно.
Через быстрое возведение в степень: раскладываем n в двоичную запись, накапливая степени двойки, а потом перемножая
если s – кол-во единиц в двоичном разложении числа,
то $L(x^n) \leq \lfloor \log n \rfloor + s \leq 2\lfloor \log n \rfloor$.
Но вообще-то для $n=15$ схема, вычисляющая x^{15} в соответствии с двоичным разложением – не является минимальной,
т.к. $15 = 0\ldots01111$ $\Rightarrow$ будет $2\cdot 3 = 6$

$z_1 = x\cdot x = x^2$
$z_2 = z_1\cdot z_1 = x^4$
$z_3 = z_2\cdot z_2 = x^8$
$z_4 = z_3\cdot z_2 = x^{12}$
$z_5 = z_4\cdot z_1 = x^{14}$
$z_6 = z_5\cdot x = x^{15}$

но можно за 5:
$z_1 = x\cdot x = x^2$
$z_2 = z_1\cdot z_1 = x^4$
$z_3 = z_2\cdot x = x^5$
$z_4 = z_3\cdot z_3 = x^{10}$
$z_5 = z_4\cdot z_3 = x^{15}$

~~Теорема 1~~ Докажем сначала, что если схема S вычисляет x^n, (Ср4)

то $n \le 2^{L(S)}$ (т.е $L(S) \ge \log n + 1$)

Док-во: Индукция по величине $L(S)$.

$L(S)=0 \Rightarrow S$ вычисляет саму переменную x и $1 \le 2^0$ - верно.

Шаг. В схеме S рассм. последний элемент.

Этот элемент вычисляет x^n, перемножая какие-то степени x^a и x^b,

вычисляемые в свою очередь какими-то схемами сложности $\le L(S)-1$.

$\Rightarrow n = a+b \le 2^{L(S)-1} + 2^{L(S)-1} = 2 \cdot 2^{L(S)-1} = 2^{L(S)}$. ч.т.д.

~~научимся~~

получаем: $\log n \le L(x^n) \le 2\log n$

научимся всё-таки асимптотически за $\log n$ вычислять.

Теорема 2 при $n \to \infty$: $L(x^n) \le \log n + \frac{\log n}{\log\log n}\left(1 + O\left(\frac{\log\log\log n}{\log\log n}\right)\right)$

Док-во: пусть d - натур. параметр, выберем его позже.

представим n в системе счисления по основанию 2^d:

$n = a_0(2^d)^0 + a_1(2^d)^1 + \ldots + a_s \cdot (2^d)^s$; $0 \le a_i \le 2^d - 1$.

$\Rightarrow 2^{sd} < n < 2^{(s+1)d}$

На 1 этапе, используя sd операций умножения,

путём последовательного возведения в квадрат, вычисляем

степени $x^2, x^4, \ldots x^{2^d}, \ldots x^{2^{2d}} \ldots x^{2^{sd}}$

положим $u_0 = x^{2^{0d}}$

$u_1 = x^{2^d}$

$\vdots$

$u_s = x^{2^{sd}}$

Для $k = 1 \ldots 2^d - 1$ положим: $I_k = \{i \mid a_i = k\}$

$x^n = u_0^{a_0} u_1^{a_1} \ldots u_s^{a_s} =$ $\qquad J_k = \{j \mid a_j \ge k\}$.

$$= \left(\prod_{i \in I_{2^d-1}} u_i\right)^{2^d-1} \cdot \left(\prod_{i \in I_{2^d-2}} u_i\right)^{2^d-2} \cdots \left(\prod_{i \in I_1} u_i\right)^1 = \underbrace{\left(\prod_{i \in J_{2^d-1}} u_i\right)\left(\prod_{i \in J_{2^d-2}} u_i\right) \cdots \left(\prod_{i \in J_1} u_i\right)}$$

нужно s операций для вычисления скобок

ещё $2^d - 2$ операций для перемножения скобок.

$\Rightarrow L(x^n) \le sd + s + 2^d - 2 \le \log n + \frac{\log n}{d} + 2^d$.

положим $d = \lfloor \log\log n - 2\log\log\log n \rfloor$.

$$\Rightarrow L(x^n) \le \log n + \frac{\log n}{\log\log n\left(1 - \frac{2\log\log\log n}{\log\log n}\right)} + \frac{\log n}{(\log\log n)^2} =$$

$$= \log n + \frac{\log n}{\log\log n}\left(1 + \frac{2\log\log\log n}{\log\log n} + \frac{2}{\log\log n} + \bar{o}\left(\frac{1}{\log\log n}\right)\right). \text{ чтд}$$

$$\boxed{\underline{\text{Ответ}}:\quad L(x^n) \sim \log n.}$$