Листок 7

Центральной моделью эффективных рандомизированных вычислений является полиномиальная вероятностная машина Тьюринга (ПВМТ). Мы будем считать, что случайные биты не генерируются самой машиной, а подаются на вход на отдельной ленте. Поскольку машина полиномиальна, длину случайной строки можно считать фиксированной. При фиксации длины строки “вероятность” ответа – есть просто доля случайных строк, на которых машина выдаёт нужный ответ.

Пусть дан язык L. Пусть существует ПВМТ $M(x,r)$, работающая за время $p(|x|)$, которая на паре (слово, случайная строка) выдаёт какой-то ответ. Заметим отдельно, что для конкретной строки r ответ на входе x детерминирован – вся случайность работы состоит в случайности строки r на входе машины.

Для каждого $x \in \{0,1\}^*$ можно определить два множества строк $Y_x = \{r \in \{0,1\}^m \mid M(x,r) = 1\}$ и $N_x = \{r \in \{0,1\}^m \mid M(x,r) = 0\}$. Здесь $m = p(|x|)$ и очевидно $Y_x \cup N_x = \{0,1\}^m$.

Для каждого $x \in L$ вероятность правильного ответа есть $\frac{|Y_x|}{2^m}$, вероятность ошибки есть $1 - \frac{|Y_x|}{2^m} = \frac{|N_x|}{2^m}$. Для каждого $x \notin L$ вероятность правильного ответа есть $\frac{|N_x|}{2^m}$, вероятность ошибки есть $1 - \frac{|N_x|}{2^m} = \frac{|Y_x|}{2^m}$. Пусть для всех $x \in L$ одновременно и для всех $x \notin L$ одновременно вероятности правильных и неправильных ответов ограничены каким-то промежутком (отличным от тривиального $[0,1]$). Это позволяет определить вероятность успеха и ошибки “в худшем случае” и тем самым ввести вероятностные классы. Класс $\mathcal{BPP}$ определяется следующим образом.

$\mathcal{BPP}$	$M(x)=1$	$M(x)=0$
$x \in L$	$\geqslant 2/3$	$\leqslant 1/3$
$x \notin L$	$\leqslant 1/3$	$\geqslant 2/3$

Читается таблица следующим образом: язык L принадлежит классу $\mathcal{BPP}$ тогда и только тогда, когда существует ПВМТ M такая что

– если $x \in L$, то доля строк r, на которых $M(x,r) = 1$, составляет не менее $2/3$ (а значит, вероятность ошибки $\leqslant 1/3$),

– если $x \notin L$, то доля строк r, на которых $M(x,r) = 0$, составляет не менее $2/3$ (а значит, вероятность ошибки $\leqslant 1/3$).

Аналогично определяются прочие вероятностные классы

$\mathcal{RP}$	$M(x)=1$	$M(x)=0$
$x \in L$	$\geqslant 1/2$	$\leqslant 1/2$
$x \notin L$	0	1

co$\mathcal{RP}$	$M(x)=1$	$M(x)=0$
$x \in L$	1	0
$x \notin L$	$\leqslant 1/2$	$\geqslant 1/2$

$\mathcal{PP}$	$M(x)=1$	$M(x)=0$
$x \in L$	$> 1/2$	$< 1/2$
$x \notin L$	$< 1/2$	$> 1/2$

Схема, применённая выше, работает и для детерминированных классов:

$\mathcal{NP}$	$M(x)=1$	$M(x)=0$
$x \in L$	> 0	< 1
$x \notin L$	0	1

co$\mathcal{NP}$	$M(x)=1$	$M(x)=0$
$x \in L$	1	0
$x \notin L$	< 1	> 0

$\mathcal{P}$	$M(x)=1$	$M(x)=0$
$x \in L$	1	0
$x \notin L$	0	1

Задача 7.1: амплификация

Пусть мы запускаем $\mathcal{PP}$ или $\mathcal{BPP}$ алгоритм t раз. $X_i = 1$, если ответ алгоритма на запуске i правильный и 0 в противном случае.

Предположим, после t запусков мы принимаем решение о принадлежности слова языку на основании “мнения большинства”. На основе оценки Чернова докажите, что класс $\mathcal{BPP}$ “эффективен”, а класс $\mathcal{PP}$ “не эффективен”, т.е. что для получения малой вероятности ошибки (пусть полиномиально малой или экспоненциально малой) в первом случае требуется полиномиальное число запусков алгоритма, а во втором полиномиального числа запусков может не хватить. (Полиномиальное число – как и время работы алгоритма – считается от длины входа).

Задача 7.2

Назовём классом $\mathcal{BPP}_{(\varepsilon_1,\varepsilon_2)}$ класс языков, распознаваемых ПВМТ M, причём

$x \in L \Rightarrow \mathbb{P}(M(x) = 1) \geqslant 1 - \varepsilon_1$,

$x \notin L \Rightarrow \mathbb{P}(M(x) = 0) \geqslant 1 - \varepsilon_2$.

Напомним, что $\mathcal{BPP} = \mathcal{BPP}_{(1/3,1/3)}$ по определению.

Доказать, что для любых $\varepsilon_1, \varepsilon_2 < 1/2$ выполняется $\mathcal{BPP} = \mathcal{BPP}_{(\varepsilon_1,\varepsilon_2)}$

Задача 7.3

Назовём классом $\mathcal{BPP}_p$ класс языков, распознаваемых ПВМТ M, причём существует положительный полином $p(n)$ и

$x \in L \Rightarrow \mathbb{P}(M(x) = 1) \geqslant \frac{1}{2} + \frac{1}{p(|x|)}$,

$x \notin L \Rightarrow \mathbb{P}(M(x) = 0) \geqslant \frac{1}{2} + \frac{1}{p(|x|)}$.

Доказать, что $\mathcal{BPP} = \mathcal{BPP}_p$

Задача 7.4

Доказать, что

a) $\mathcal{RP} \subset \mathcal{NP}$, $\mathrm{co}\,\mathcal{RP} \subset \mathrm{co}\,\mathcal{NP}$

b) $\mathcal{RP} \subset \mathcal{BPP}$, $\mathrm{co}\,\mathcal{RP} \subset \mathcal{BPP}$

c) $\mathcal{BPP} \subset \mathcal{PP}$, $\mathcal{NP} \subset \mathcal{PP}$

Задача 7.5

Назовём классом $\mathcal{PP}_{\text{more equal}}$ класс языков, распознаваемых ПВМТ M, причём

$x \in L \Rightarrow \mathbb{P}(M(x) = 1) > 1/2$,

$x \notin L \Rightarrow \mathbb{P}(M(x) = 0) \geqslant 1/2$.

Докажите, что $\mathcal{PP}_{\text{more equal}} = \mathcal{PP}$.

Задача 7.6

Назовём классом $\mathcal{PP}_{\text{even more equal}}$ класс языков, распознаваемых ПВМТ M, причём

$x \in L \Rightarrow \mathbb{P}(M(x) = 1) \geqslant 1/2$,

$x \notin L \Rightarrow \mathbb{P}(M(x) = 0) \geqslant 1/2$.

Докажите, что $\mathcal{PP}_{\text{even more equal}} = 2^{\Sigma^*}$.

Задача 7.7

Доказать, что классы $\mathcal{RP}$, co$\mathcal{RP}$, $\mathcal{BPP}$ замкнуты относительно объединения, пересечения и полиномиальной сводимости.

Задача 7.8: лемма Шварца-Зиппеля

Пусть $p \in F[x_1, x_2, \dots, x_n]$ – ненулевой полином от n переменных степени $d \geqslant 0$ над полем F. Пусть S конечное подмножество F и пусть элементы $r_1, r_2, \dots, r_n$ были выбраны из S равномерно и независимо друг от друга.

Тогда
$$\mathbb{P}[p(r_1, r_2, \dots, r_n) = 0] \leqslant \frac{d}{|S|}$$

Решить с помощью леммы задачу PIT (polynomial identity testing). Дан полином p, верно ли, что после раскрытия всех скобок и приведения его к сумме мономов все коэффициенты перед мономами будут равны нулю? В данном случае "решить" – это "предъявить эффективный вероятностный алгоритм".

Задача 7.9

Определим задачу EZE (evaluate to zero everywhere). Дан полином p от n переменных степени $d \geqslant 0$ над полем F, верно ли, что при любом выборе элементов $r_1, r_2, \dots, r_n$ из поля F, значение $p(r_1, r_2, \dots, r_n) = 0$?

Доказать, что EZE $\in$ co$\mathcal{NP}$-hard.

Следует ли из вышесказанного, что co$\mathcal{RP}$ = co$\mathcal{NP}$?

Задача 7.10

Пусть $\mathcal{ZPP} = \mathcal{RP} \cap \text{co}\mathcal{RP}$. Доказать, что следующие утверждения эквивалентны:

1) $L \in \mathcal{ZPP}$;

2) существует вероятностная машина Тьюринга, выдающая на слове x правильный ответ с вероятностью единица, при этом не *худшее* время работы у неё полиномиально, а **ожидаемое** время работы полиномиально;

3) существует ПВМТ, которая на слове x с вероятностью 1/2 отвечает верно (правильно определяется принадлежность или непринадлежность слова языку), а с вероятностью 1/2 отвечает "ответ неясен".

Задача 7.11

Класс $\mathcal{BPL}$ состоит из языков, распознаваемых логарифмическими по памяти (случайная строка не включается в используемую память) вероятностными МТ, при этом вероятности ошибок те же, что у $\mathcal{BPP}$. Докажите, что $\mathcal{BPL} \subset \mathcal{P}$

Задача 7.12

MAXCUT – это задача (не язык) следующего вида: дан граф G, нужно найти разбиение вершин графа на два множества так, чтобы число рёбер, у которых концы лежат в разнах множествах, максимально.

1) Доказать, что MAXCUT является $\mathcal{NP}$-трудной.

2) Придумать простой вероятностный алгоритм решения MAXCUT.

3) Дерандомизировать алгоритм, используя метод условных матожиданий.

Задача 7.13

MAXSAT – это задача (не язык) следующего вида: дана булева формула в виде КНФ, нужно найти набор переменных, на котором выполняется наибольшее возможное число дизъюнктов.

1) Доказать, что MAXSAT является $\mathcal{NP}$-трудной.

2) Придумать простой вероятностный алгоритм решения MAXSAT.

3) Дерандомизировать алгоритм, используя метод условных матожиданий.