Листок 13. Вероятностные вычисления.

Определение 1 *Пусть A — класс языков. Класс $\mathbf{NP}^{A[k]}$ — класс языков, для которых существует полиномиальный недетерминированный алгоритм, который может обращаться к оракулу из класса A не более k раз.*

ML 73. Рассмотрим задачу Max-3-SAT, в которой ко формуле в 3-КНФ необходимо найти максимальное число клозов, которые можно одновременно удовлетворить. Придумайте полиномиальный вероятностный алгоритм, который по 3-КНФ формуле "в среднем" (мат. ожидание) выдает $\frac{7}{8}$ приближение задачи Max-3-SAT.

ML 74. Придумайте "в среднем" (мат. ожидание) полиномиальный вероятностный алгоритм, который по 3-КНФ формуле выдает $\frac{7}{8}$ приближение задачи Max-3-SAT.

ML 75. Докажите, что если $\mathbf{NP} \subseteq \mathbf{BPP}$, то $\mathbf{NP} = \mathbf{RP}$.

ML 76. Пусть **ZPP** — это класс языков, которые принимаются вероятностной машиной Тьюринга без ошибки, математическое ожидание времени работы которых полиномиально. Докажите, что:

(а) $L \in \mathbf{ZPP}$ тогда и только тогда, когда существует полиномиальная по времени вероятностная машина Тьюринга M, которая выдает $\{0, 1, ?\}$, что для всех $x \in \{0,1\}^*$ с вероятностью 1, $M(x) \in \{L(x), ?\}$ и $\Pr[M(x) = ?] \leq \frac{1}{2}$;

(б) $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$.

ML 77. **BPL** — это класс языков, для которых существует вероятностная машина Тьюринга M, которая использует логарифмическую память, останавливается при всех последовательностях случайных битов и для всех x выполняется, что $\Pr[M(x) = L(x)] \geq \frac{2}{3}$. Покажите, что $\mathbf{BPL} \subseteq \mathbf{P}$.

ML 78. Пусть $\mathbf{NP} \subseteq \mathbf{DTime}[n^{\log(n)}]$, докажите, что $\mathbf{PH} \subseteq \bigcup_k \mathbf{DTime}[n^{\log^k(n)}]$ (подсказка: вспомните задачу $\mathbf{P} = \mathbf{NP} \Rightarrow \mathbf{EXP} = \mathbf{NEXP}$).

ML 23.

Задача Поста состоит в следующем: есть доминошки n видов $\left[\frac{s_1}{t_1}\right], \left[\frac{s_n}{t_n}\right]$, s_i и t_i — конечные строки, есть неограниченный запас доминошек каждого вида, доминошки переворачивать нельзя. Требуется определить, можно ли составить несколько доминошек так, чтобы в верхней и нижней их половине читалась одна и та же строка, такие последова-

тельности доминошек будем называть согласованными. Докажите, что задача Поста алгоритмически неразрешима.

ML 33. Теперь секвенцией будем называть $\Gamma \vdash \Delta$, где Γ и Δ — это списки предикатных формул.

Добавим в секвенциальное счисление четыре новых правила которые соответствуют кванторам (см. табличку).

В правилах $(\forall\vdash)$ и $(\vdash\exists)$, $A(t/x)$ обозначает, что в формуле A переменная x заменяется на терм t, при этом для каждого вхождения переменной x никакие переменные терма t не должны попасть в область действия кванторов по одноименным переменным (в формуле A). Например для формулы $\forall y\ P(x,y)$ вместо x нельзя подставить $f(y)$.

А в других двух правилах $A(y/x)$ означает, что в формуле A мы заменили все вхождения x на переменную y, при этом переменная y должна быть свежей то есть не входить ни в A, ни в другие формулы из секвенции.

Докажите корректность секвенциального исчисления (покажите, что если секвенция $\Gamma \vdash \Delta$ выводима, то в любой интерпретации либо хотя бы одна формула из Γ ложна, либо хотя бы одна формула из Δ истинна).

ML 40. Пусть T — замкнутая формула в некоторой сигнатуре, и пусть существует интерпретация со сколь угодно большим носителем, в которой данная формула истинна. Докажите, что существует интерпретация с бесконечным носителем, в которой данная формула истинна.

ML 50. Будет ли теория $\mathrm{Th}((\mathbb{N},<,=))$ конечно аксиоматизируемой.

ML 58. Докажите, что:

(а) что число n простое тогда и только тогда, когда для каждого простого делителя q числа $n-1$ существует $a \in \{2,3,\ldots,n-1\}$ при котором $a^{n-1} \equiv 1 \pmod n$, а $a^{\frac{n-1}{q}} \not\equiv 1 \pmod n$;

ML 60. Докажите, что существует язык, для которого любой алгоритм, работающий время $O(n^2)$ решает его правильно на менее, чем на половине входов какой-то длины, но этот язык распознается алгоритмом, работающим время $O(n^3)$.

ML 61. Докажите, что:

(б) $\mathbf{NSpace}[n^3] \not\subseteq \mathbf{NSpace}[n^2]$.

ML 72. Докажите, что язык

$$L = \{(\phi, 1^k) \mid \text{функция, заданная формулой } \phi, \text{ не может быть посчитана формулой размера } k\}$$

лежит в $\mathbf{PH}$.