**Задание 7 (на 29.10.14)**

**CC38.** а) Покажите, что для любой конечной (или перечислимой) сигнатуры множество тавтологий в этой сигнатуре перечислимо. б) Покажите, что если в сигнатуре есть достаточное количество функциональных и предикатных символов арности 1 и 2, то множество тавтологий в этой сигнатуре неразрешимо.

**CC39.** Пусть ZPP — это класс языков, которые принимаются вероятностной машиной Тьюринга без ошибки, математическое ожидание времени работы которых полиномиально. а) Докажите, что $L \in \mathrm{ZPP}$ 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) Докажите, что $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$.

**CC40.** Докажите NP-полноту следующей задачи: даны два графа $G_1$ и $G_2$. Проверить, изоморфен ли $G_1$ подграфу $G_2$.

**CC41.** Докажите, что $\mathrm{NSpace}[n^2] \subsetneq \mathrm{NSpace}[n^3]$;

**CC42.** 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 $O(n^3)$.

**CC43.** 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 $\mathrm{BPL} \subseteq \mathrm{P}$.

---

**CC25.** Покажите, что существует такое б) двустороннее ассоциативное исчисление, для которого вопрос о выводимости строки $x$ из строки $y$ является алгоритмически неразрешимым.

**CC27.** Покажите, что язык простых чисел содержится в классе а) co-NP; б) а) Докажите, 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 $a^{n-1} = 1 \bmod n$ и $a^{\frac{n-1}{q}} \neq 1 \bmod n$. в) Докажите, что язык простых чисел лежит в NP.

**CC37.** Докажите, что если $\mathrm{NP} \subseteq \mathrm{BPP}$, то $\mathrm{NP} = \mathrm{RP}$.