

Задание 9 (на 15.04).

СС 49. Покажите, что:

- (а) задача вычисления числа полных паросочетаний в двудольном графе сводится к вычислению перманента;
- (б) четность числа полных паросочетаний в двудольном графе можно узнать за полиномиальное время;
- (в) если граф представляет собой шахматную доску с выбитыми клетками (вершины — клетки, ребра соединяют соседние клетки), то существует полиномиальный алгоритм, который считает число полных паросочетаний (подсказка: иногда вес ребра удобно взять комплексным).

СС 50. (повторяем лекцию, $\mathbf{IP} = \mathbf{PSPACE}$ пользоваться нельзя) Докажите, что:

- (а) $\mathbf{AMA} \subseteq \mathbf{PSPACE}$;
- (б) $\mathbf{AMA} \subseteq \mathbf{PSPACE}$ с приватными случайными битами.

СС 51. Существует вариант класса \mathbf{MA} с односторонней ошибкой. $L \in \mathbf{MA}_1$, если существует такая полиномиальная вероятностная машина V и полином p , что если $x \in L$, то найдется такая строка $y \in \{0, 1\}^{p(n)}$, что $\Pr[V(x, y) = 1] = 1$, а если $x \notin L$, то для любой строки $y \in \{0, 1\}^{p(n)}$ выполняется $\Pr[V(x, y) = 1] < \frac{1}{3}$. Покажите, что $\mathbf{MA} = \mathbf{MA}_1$.

СС 52. Покажите, что $\mathbf{MA} \subseteq \Sigma_2^P$.

СС 10. Докажите, что:

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

СС 26. (подсказка: $\mathbf{NEXP}^{\mathbf{NP}} \text{ vs. } \mathbf{NEXP}$) Докажите, что если $\mathbf{P} = \mathbf{NP}$, то существует язык из \mathbf{EXP} , схемная сложность которого не меньше $\frac{2^n}{10n}$.

СС 33. Докажите, что задача $\mathbf{CircuitEval}$ \mathbf{P} -полная.

СС 37. (подсказка: представьте формулу, как дерево и найдите “среднюю” вершину) Покажите, что язык можно разрешить булевой формулой размера s тогда и только тогда, когда этот язык можно разрешить булевой схемой глубина $O(\log(s))$.

СС 43. (подсказка: понизьте ошибку) Докажите, что $\mathbf{MA} \subseteq \mathbf{AM}$.

СС 44. Покажите, что:

- (а) если $\mathbf{VPTIME}(f(n)) = \mathbf{VPTIME}(g(n))$, то $\mathbf{VPTIME}(f(h(n))) = \mathbf{VPTIME}(g(h(n)))$, где f, g, h — конструктивные по времени, $f(n), g(n) \geq \log n$, $h(n) \geq n$ — возрастающая функция;
- (б) $\mathbf{DTime}(f(n)) \subseteq \mathbf{VPTIME}(f(n)) \subseteq \mathbf{DTime}(2^{O(f(n))})$;
- (в) $\mathbf{BPP} \subseteq \mathbf{VPTIME}(n^{\log n}) \subsetneq \mathbf{VPTIME}(2^n)$.

СС 45. Определим язык

$$\mathbf{QNR} = \{(y, m) \mid y \text{ не является квадратичным вычетом по модулю } m\}.$$

Докажите, что $\mathbf{QNR} \in \mathbf{IP}$.

СС 46. \mathbf{BPL}_H — это класс языков, для которых существует вероятностная машина Тьюринга M , которая использует логарифмическую память, останавливается с

вероятностью 1, и для всех x выполняется, что $\Pr[M(x) = L(x)] \geq \frac{2}{3}$. Покажите, что $\mathbf{BPL}_H \subseteq \mathbf{P}$.

СС 47. Докажите, что $\mathbf{BPP} = \mathbf{BPP}^{\mathbf{BPP}}$.

СС 48. Докажите, что $\mathbf{BPP}/\mathbf{poly} \subseteq \mathbf{P}/\mathbf{poly}$ ($\mathbf{BPP}/\mathbf{poly}$ — класс языков, которые разрешаются вероятностными (есть специальные гейты, куда подаются случайные биты) схемами полиномиального размера).