

## Вопросы к экзамену по курсу “Теория сложности вычислений”, АУ 2013

1. Машины Тьюринга. Нижняя оценка для палиндрома на одноленточной машине.
2. Многоленточные машины Тьюринга. Универсальная машина Тьюринга. Эффективное моделирование  $k$ -ленточной машины на 2-ленточной.
3. Недетерминированные машины Тьюринга. Определения класса NP. Примеры.
4. Сведения по Карпу. Понятие полноты. Полнота задачи об ограниченной упаковке. Полнота задачи SAT и 3-SAT.
5. NP-задачи поиска. Сведения по Куку. Сведение задач поиска к задачам распознавания.
6. Оптимальный алгоритм для NP-задач поиска.
7. Теорема Ладнера о не NP-полном языке в классе NP.
8. Классы с оракулами. Существование оракулов  $A, B$ , при которых  $P^A = NP^A$  и  $P^B \neq NP^B$ .
9. Теоремы об иерархии по времени для детерминированных и недетерминированных вычислений.
10. Вычисления с ограничением по памяти. Теорема Савича и следствие о  $NPSPACE = PSPACE$ .
11. Полнота  $TQBF$  в классе PSPACE.
12. Логарифмические по памяти сведения и их свойства. Класс NL, полная задача в нем. Замкнутость классов  $NSpace[s(n)]$  относительно дополнения.
13. Полиномиальная иерархия. Простейшие свойства, полные задачи в  $\Sigma_i^P$  и  $\Pi_i^P$ .
14. Оракульное определение полиномиальной иерархии.
15. Альтернирующие машины Тьюринга и полиномиальная иерархия.
16. Вычисления с ограничением по времени и по памяти. Нижняя оценка для SAT.
17. Булевы схемы. Вычисления с подсказкой. Класс P/poly. Включение  $P \in P/poly$ . Существование функций большой схемной сложности.
18. Теорема Карпа-Липтона.
19. Языки большой схемной сложности в полиномиальной иерархии (теорема Каннана).
20. Равномерные схемы. Классы  $NC^i$ . P-полные задачи. Соотношение между  $NC^1, L, NL$  и  $NC^2$ . Замкнутость NC относительно логарифмических по памяти сведений.
21. Эффективные параллельные схемы для сложения и умножения чисел.
22. Вероятностная машина Тьюринга. Классы BPP и RP. Лемма Шварца-Зипшеля и вероятностный тест равенства двух многочленов.
23. Понижение ошибки в классе BPP,  $BPP \subseteq P/poly$ ,  $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$ .
24. Интерактивные протоколы. Примеры: интерактивный протокол для неизоморфизмов графов,  $IP \subseteq PSPACE$ .
25. Теорема Шамира ( $PSPACE \subseteq IP$ ) и ее следствия.
26. Универсальное семейство попарно независимых хеш-функций. Конструкция.
27. Протокол для нижней оценки на размер множества. Открытые и закрытые случайные биты, игры Мерлина и Артура.  $GNI \in AM$ . Теорема Голдвассера-Сипсера

(без доказательства). Если для GI является NP-полным, то полиномиальная иерархия схлопывается на втором уровне.

**28.** Лемма Вэлианта-Вазирани. И ее  $\oplus$ -версия.

**29.** Операции с числом выполняющих наборов и следствия из них.  $\oplus$ -версия леммы Вэлианта-Вазирани для полиномиальной иерархии.

**30.** Классы  $\#P$  и  $RP$ . Теорема Toda.  $P^{RP} = P^{\#P}$ .

**31.** Теорема Вэлианта о  $\#P$ -полноте 0/1 перманента (без доказательства). Интерактивное доказательство для перманента. Следствие об интерактивном доказательстве для  $P^{RP}$ .

**32.** Включение  $MA \subseteq RP$ . Схемная сложность  $RP$ .

**33.** Приближенные алгоритмы для задачи MAXSAT и минимальном вершинном покрытии. Вероятностно проверяемые доказательства. Формулировка PCP-теоремы. Эквивалентные формулировки. Неаппроксимируемость  $MAX-3-SAT$ .

**34.** Код Уолша-Адамара и его локальное декодирование.

**35.**  $NP \subseteq PCP(poly, 1)$ .

**36.** Тестирование функции на гомоморфизм в абелевых группах.

**37.** Тестирование и восстановление многочленов небольшой степени над полем  $\mathbb{F}_p$ .

**38.**  $MIP = PCP(poly, poly)$ ,  $MIP \subseteq NEXP$ .

**39.**  $NEXP \subseteq MIP$ .

### Требования к экзамену

Экзамен состоит из трех частей:

1. В первой части экзамена требуется ответить на два вопроса из списка вопросов. Для получения оценки хотя бы 4 требуется полностью сформулировать основные результаты из двух вопросов и провести все доказательства, для получения оценки 3 в одном из двух вопросов разрешается не доказывать незначительное верное утверждение, при том, что общий план доказательства верен. Пользоваться во время подготовки можно только официальной собственноручно написанной шпаргалкой (на листе A4 с двух сторон) без ограничения времени, так же можно посмотреть в конспект или книжку, но не более, чем на 15 минут.
2. Во второй части экзамена выдается 6 простых (дурацких) вопросов на знание и понимание. Примеры вопросов: а) сформулируйте определение класса  $IP$ ; б) Почему из того, что  $NP = NEXP$  следует, что полиномиальная иерархия не схлопывается? На оценку  $t$  необходимо ответить на не менее, чем  $t$  вопросов. Пользоваться источниками информации запрещено.
3. Третья часть экзамена только для тех, кто претендует на оценку 5. На оценку 5 необходимо решить задачу. Можно пользоваться конспектом и книжкой, но решать нужно самостоятельно.
4. Итоговая оценка: максимальная оценка, для которой выполнены условия пунктов 1, 2, 3.