

Вопросы к экзамену по „теории информации“

10 июня 2017 г.

1. **Информация по Хартли.** Мотивация и определение. Информация в проекциях. Игра в 10 вопросов. Цена информации. Упорядочение камней по весу. Поиск фальшивой монетки (разные вариации). Логика знаний.
2. **Энтропия Шеннона.** Мотивация и определение. Свойства энтропии. Энтропия пары. Условная энтропия. Свойства условной энтропии. Взаимная информация. Свойства взаимной информации. Применение энтропии к задаче о поиске фальшивой монетки.
3. **Кодирование.** Однозначно декодируемые коды. Неравенство Крафта-Макмилана. Префиксные коды. Теоремы Шеннона об однозначно декодируемых кодах. Код Шеннона-Фано, код Хаффмана.
4. **Блоковое кодирование с ошибками.** Блоковое кодирование. Арифметическое кодирование. Теоремы Шеннона о блоковом кодировании с ошибками.
5. **Свойства распределений.** Энтропийные профили для одного, двух и трёх распределений. Неравенства о тройке распределений (два).
6. **Криптография.** Теорема Шеннона об энтропии ключа шифрования. Схемы разделения секрета. Пороговая схема Шамира. Энтропия секрета существенного участника. Нижняя оценка $3/2$ на энтропию ключа участника. Теорема Чирмаза.
7. **Коммуникационная сложность.** Верхние оценки на коммуникационную сложность функций. Нижние оценки: метод размера прямоугольников, метод трудного множества и метод ранга матрицы. Сложность EQ и GE .
8. **Связь протоколов и формул.** Теорема Карчмера-Вигдерсона. Внешнее и внутреннее информационное разглашение и их связь. Теорема о связи размера протокола и внешнего информационного разглашения. Теорема Храпченко.
9. **Колмогоровская сложность.** Теорема о существовании оптимального способа описания. Определение колмогоровской сложности. Свойства колмогоровской сложности. Слов большой сложности. Невычислимость колмогоровской сложности. Связь колмогоровской сложности и энтропии.

10. **Условная колмогоровская сложность и сложность пары.** Условная сложность: существование оптимального способа описания, определение и свойства. Сложность пары. Теорема Колмогорова-Левина.
11. **Метод несжимаемых объектов.** Теорема об иерархии языков, распознаваемых конечными автоматами с несколькими головками.
12. **Алгоритмическая случайность.** Случайность по Мартину-Лёфу. Свойства. Теорема о том, что случайные последовательности случайны по Мартину-Лёфу.
13. **Применение колмогоровской сложности.** Перенос информации по ленте. Нижняя оценка на копирование на одноленточной машине Тьюринга. Алгоритм сложения битовых чисел.
14. **Локальная лемма Ловаса.** Локальная лемма Ловаса. Симметричная локальная лемма Ловаса. Применение локальной леммы Ловаса к последовательностям с запрещёнными словами.
15. **Эффективное доказательство леммы Ловаса.** Теорема Мозера-Тардом.