МФТИ, бакалавриат ФИВТ. Весна 2014.
«Введение в теорию информации».
к.ф.-м.н. А.Е. Ромащенко.

1. **Комбинаторный подход к понятию информации**.

   1.1. Определение количества информации в конечном объекте (информация по Хартли).

   1.2. Задачи оптимального поиска (поиск фальшивой монеты, сортировка). Доказательство нижних оценок с помощью информации Хартли. Доказательство нижних оценок методом «враждебного оппонента» (adversary argument).

2. **Вероятностный подход к понятию информации**.

   2.1. Энтропия Шеннона: определение и основные свойства.

   2.2. Применение энтропии в задачах комбинаторного поиска («жадные» энтропийные алгоритмы).

   2.3. Информационные неравенства. Энтропийный профиль многомерного распределения вероятностей, множество энтропийных векторов. Описание множества всех энтропийных векторов для пар и троек случайных величин.

   2.4. Теорема Шеннона о кодировании для канала без шума.

   2.5. Напоминание: префиксные коды, неравенство Крафта, код Хаффмана

   2.6. Классические методы кодирования без потерь: код Шеннона–Фано, арифметический код.

   2.7. Теорема о блоковом кодирования для канала без шума (прямая теорема, слабое и сильное обращение).

   2.8. Теорема Вульфа–Слепяна о декодировании с помощником.

   2.9. Задача о совершенном разделении секрета. Пороговые структуры доступа, схема Шамира. Идеальное разделение секрета; структуры доступа, не допускающие идеального разделения секрета.

3. **Каналы с шумом**.

   3.1. Дискретная модель канала с шумом. Оценки Хэмминга и Гилберта (напоминание из курса теории кодирования).

   3.2. Вероятностная модель канала с шумом.

   3.3. Определение пропускной способности дискретного канала без памяти. Вычисление пропускной способности простейших каналов.

   3.4. Теорема Шеннона о кодировании для канала с шумом; доказательство теоремы для двоичного симметричного канала.

4. **Алгоритмический подход к понятию информации**.

   4.1. Колмогоровская сложность слова; относительная колмогоровская сложность. Простейшие свойства колмогоровской сложности.

   4.2. Теорема Колмогорова–Левина о симметрии взаимной информации. Определение взаимной информации и линейные неравенства для колмогоровской сложности.

   4.3. Метод несжимаемых слов. Применения: сложность распознавания языка палиндромов на одноленточных машинах; теорема об иерархии для конечных автоматов с k читающими головками.

   4.4. Существование $(\log n)$-сжимаего префикса у любой бесконечной двоичной последовательности.

   4.5. Префиксная сложность. Случайность по Мартин-Лёфу. Применение: вывод закона больших чисел в форме Харди–Литлвуда.

   4.6. Принцип кратчайшего описания (MDL) и простейшие примеры его применения.

5. **Коммуникационная сложность**.

   5.1. Детерминированные и вероятностные коммуникационные протоколы для двух участников. Определение коммуникационной сложности для функций двух аргументов.

   5.2. Нижняя оценка детерминированной коммуникационной сложности предиката равенства (метод одноцветных комбинаторных прямоугольников).

   5.3. Вероятностные коммуникационные протоколы для вычисления предиката равенства в модели с раздельными источниками случайности.

   5.4. Экспоненциальный разрыв между вероятностной и детерминированной коммуникационной сложностью: $\mathrm{RCC}_\varepsilon(f) = \Omega(\log \mathrm{CC}(f))$ для любого предиката f.

Список литературы

[1] T.M. Cover, J.A. Thomas. Elements of information Theory, 2006.

[2] R.W. Yeung. A First Course in Information Theory, 2002.

[3] Н.К. Верещагин, Е.В. Щепин. Информация, кодирование, предсказание, 2012.

[4] И. Чисар, Я. Кернер. Теория информации, 1985.

[5] Г.А. Кабатянский. Математика разделения секрета, *Математическое просвещение*, т. 2, No 3, стр. 115–126, 1998.

[6] M. Li, and P. Vitanyi. An Introduction to Kolmogorov Complexity and Its Applications, 2008.

[7] В.А. Успенский, Н.К. Верещагин, А. Шень. Введение в колмогоровскую сложность, 2012.

[8] А.М. Яглом, И.М. Яглом. Вероятность и информация, 1973.

[9] Ф.Дж.А. Мак-Вильямс, Н.Дж.А. Слоэн. Теория кодов, исправляющих ошибки, 1979.

[10] Румянцев, Ромащенко, Шень. Заметки о теории кодирования, 2011. `http://www.mccme.ru/~anromash/courses/coding-theory.ps`

[11] E. Nisan, N. Kushilevitz. Communication complexity, 1997.

[12] Р. Галлагер. Теория информации и надежная связь, 1974.