МФТИ, бакалавриат ФИВТ. Весна 2013.
Программа курса Введение в теорию информации.
А.Е. Ромащенко.

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

   Определение количества информации в конечном объекте (информация по Хартли). Задачи оптимального поиска; доказательство нижних оценок с помощью инофрмации Хартли.

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

   Энтропия Шеннона: определение и основные свойства. Неравенство Крафта. Теорема Шеннона о кодировании для канала без шума. Код Шеннона–Фано, код Хаффмана, арифметический код.

   Теорема о блоковом кодирования для канала без шума.

   Применение энтропии в задачах комбинаторного поиска.

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

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

3. **Коды, исправляющие ошибки**.

   Комбинаторные модели канала с шумом. Граница Хэмминга и граница Гилберта.

   Линейные коды. Граница Варшамова–Гилберта.

   Коды Хэмминга, коды Рида–Соломона. Граница Синглтона. Алгоритм декодирования кода Рида–Соломона за полиномиальное время.

   Каскадные коды. Эффективная конструкция асимптотически хорошего кода с полиномиальными алгоритмами кодирования и декодирования.

   Вероятностные модели канала с шумом; дискретный канал без памяти. Теорема Шеннона о кодировании для канала с шумом; сильное и слабое обращение.

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

   Колмогоровская сложность слова и относительная колмогоровская сложность. Простейшие свойства колмогоровской сложности.

   Теорема Колмогорова–Левина о симметрии взаимной информации. Линейные неравенства для колмогоровской сложности.

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

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

Принцип кратчайшего описания (MDL) и примеры его применения.

5. **Коммуникационная сложность**.

   Основные модели теории коммуникационной сложности: детерминированные и вероятностные коммуникационные протоколы для двух участников. Определение коммуникационной сложности для функций двух аргументов.

   Метод одноцветных комбинаторных прямоугольников и нижняя оценка детерминированной коммуникационной сложности предиката равенства.

   Вероятностные коммуникационные протоколы для вычисления предиката равенства в моделях с общими и раздельными источниками случайности. Экспоненциальный разрыв между вероятностной и детерминированной коммуникационной сложностью. Теорема о преобразовании коммуникационного протокола с общим источником случайности в протокол с раздельными источниками случайности.

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

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

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

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

Дополнительная литература.

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

[13] В.М. Сидельников. Теория кодирования, 2008.