

МФТИ, бакалавриат ФИВТ. Весна 2011.
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 (поиск фальшивой монеты за минимальное число взвешиваний; задача об оптимальной сортировке).

2. Вероятностный подход к понятию информации.

Энтропия Шеннона: определение и основные свойства. Информационные неравенства.

Оценки для комбинаторных задач оптимального поиска с помощью энтропии Шеннона.

Неравенство Крафта. Использование стохастических закономерностей для сжатия данных: код Шеннона–Фано, код Хаффмана, арифметический код.

Теоремы Шеннона об оптимальном кодировании для каналов без шума.

Теорема об оптимальном блочном кодировании для последовательности независимых одинаково распределенных случайных величин.

Задача об совершенном разделении секрета: метод Шамира разделения секрета для пороговой структуре доступа; пример структуры доступа, не допускающей идеального разделения секрета.

3. Алгоритмический подход к понятию информации.

Определение Колмогоровской сложности слов, простейшие свойства.

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

Комбинаторные применения колмогоровской сложности: задача о копировании слова на одноленточной машине Тьюринга; задача о конечном автомате с k головками.

Префиксная колмогоровская сложность. Эффективно нулевые множества, случайность по Мартин–Лёфу.

Закон повторного логарифма для случайных по Мартин–Лёфу последовательностей.

4. Коды, исправляющие ошибки.

Комбинаторные модели канала с шумом. Границы Хэмминга и Гилберта.

Линейные коды, граница Варшавова–Гилберта. Коды Хэмминга.

Коды Рида–Соломона. Полиномиальный алгоритм декодирования кода Рида–Соломона. Каскадные коды; конструкция асимптотически хорошего кодов с эффективной процедурой декодирования.

5. Коммуникационная сложность.

Детерминированные коммуникационные протоколы, коммуникационная сложности. Примеры верхних и нижних оценок для детерминированной коммуникационной сложности.

Вероятностная коммуникационная модель. Вероятностный протокол Яо для вычисления предиката равенства. Экспоненциальный разрыв между вероятностной и детерминированной коммуникационной сложностью.

Литература

1. Р. Галлагер. Теория информации и надежная связь, 1974.
2. Т.М. Cover, J.A. Thomas. Elements of information Theory, 2006.
3. И. Чисар, Я. Кернер. Теория информации, 1985.
4. R.W. Yeung. A First Course in Information Theory, 2002.
5. M. Li, P. Vitanyi. Kolmogorov complexity and applications, 2008.
6. Ф.Дж.А. Мак-Вильямс, Н.Дж.А. Слоэн. Теория кодов, исправляющих ошибки, 1979.
7. E. Nisan, N. Kushilevitz. Communication complexity, 1997.
8. В.А. Успенский, Н.К. Верещагин, А. Шень. Колмогоровская сложность (черновик книги):
<ftp://ftp.mscme.ru/users/shen/kolmbook.pdf>