**мех-мат МГУ, весна 2010.**

**Краткий конспект лекций курса *Теория кодирования и сложность вычислений* (А. Ромащенко, весна 2010).**

# 1 Лекция 1, 26 февраля.

Определения кода, исправляющего ошибки. Кодовое расстояние, скорость (коэффициент полезного действия) кода. Оценка Хэмминга. Оценка Гилберта. Формула Стрилинга и асимптотика оценок Хэмминга и Гилберта [RRS, главы 1–2], [Sid, главы 2.0.2,2.0.9].

Линейные коды: порождающая и проверочная матрицы, кодовое расстояние равно минимальному весу ненулевого кодового слова, оценка Варшамова–Гилберта. [RRS, глава 4],[Sid, главы 1.1.2,2.0.8]. .

# 2 Лекция 2, 5 марта.

Существование линейного кода, удовлетворяющего оценке Варшамова–Гилберта [RRS, глава 4].

Оценка расстояния линейного кода для случайно выбранной проверочной матрицей.

NP-трудность общей задачи декодирования линейного кода [RRS, глава 29].

# 3 Лекция 3, 12 марта.

Граница Синглетона [RRS, глава 6]. Код Рида–Соломона, его кодовое расстояние [RRS, глава 7], [McWS, глава 10.2], [Sid, главы 5.0.3–5.0.4]. Эффективный алгоритм декодирования кода Рида–Соломона [RRS, глава 8].

Конкатенация кодов [RRS, глава 9]. Построение асимптотически хорошего кода с помощью конкатенации кода Рида–Соломона и оптимального кода для блоков битов логарифмической длины [RRS, глава 11], [McWS, глава 10.11].

# 4 Лекция 4, 19 марта.

Декодирование конкатенициии кодов (для случая, когда внешним является код Рида–Соломона) с исправлением $d_1e_2$ ошибок [RRS, глава 10].

Код Форни–Возенкрафта. [RRS, глава 12]

Построение кода, у которого расстояние между любыми двумя словами близко к половине кодового расстояния.

## 5 Лекция 5, 26 марта.

NP-трудность задачи вычисления кодового расстояния линейного кода. [VaSTOC, Va97]

## 6 Лекция 6, 2 апреля.

Задача декодирования списком. Построение кода, допускающего декодирование списком полиномиального размера, оценка Элайеса. [RRS, глава 20]

Неявное доказательство возможности декодировать списком код с заданным кодовым расстоянием. [RRS, глава 21]

## 7 Лекция 7, 9 апреля.

Декодирование списком кода Рида–Соломона. [RRS, глава 25]

## 8 Лекция 8, 16 апреля.

Полиномиальный алгоритм декодирование списком конкатенации кода Рида–Соломона и кода Адамара. [RRS, глава 26]

Комбинаторная оценка числа кодовых слов в шаре: Существует абсолютная константа $c$ такая, что при $\delta > c\sqrt{\varepsilon}$ всякий шар радиуса $r = (\frac{1}{2} - \delta)n$ в $\{0,1\}^n$ может содержать не более $O(1/\delta^2)$ кодовых слов из кода с расстоянием $d = (\frac{1}{2} - \varepsilon)n$

Итоговая теорема: существует семейство кодов

$$C_{k,\varepsilon} \ : \ \{0,1\}^k \to \{0,1\}^n,$$

где $n = \mathrm{poly}(k/\varepsilon)$, отображение $C_{k,\varepsilon}$ вычислимо за время полиномиальное от $k$ и $1/\varepsilon$, и для каждого $y \in \{0,1\}^n$ можно за полиномиальное время найти список всех кодовых слов $x_i$, находящихся на расстоянии не более $(\frac{1}{2} - \varepsilon)n$ от $y$; размер такого списка ограничен $O(1/\varepsilon^2)$.

## 9 Лекция 9, 23 апреля.

Псевдо-случайные генераторы Нисана–Вигдерсона. Дерандомизация: доказательство P = BPP в предположении существования трудно-аппроксимируемой функции. [NiWi]

## 10 Лекция 10, 30 апреля (прочитана Н.К.Верещаниным).

Алгоритм Голдрайха–Левина декодирования списком кода Адамара. Существование трудного бита (hard core predicate) в предположении существования необратимной перестановки.

## 11 Лекция 11, 7 мая.

Определение экстрактора. Конструкция экстрактора Тревисана. [Tre01, RaReVa]

## 12 Лекция 12, 14 мая.

Эффективное построение комбинаторных дизайнов и слабых комбинаторных дизайнов. [NiWi, RaReVa]

Определение семейства кодов, допускающих вероятностное декодирование списком за полилогарифмическое время. [SuTreVa]

## 13 Лекция 13, 21 мая.

Существование кодов, допускающих декодирование списком за полилогарифмическое время. Преообразование языка, трудного в худшем случае, в трудно-аппроксимируемый язык. [SuTreVa]

## Список литературы


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

[Sid] В.М. Сидельников. Теория кодирования.

[Gal] Р. Галлагер. Теория информации и надежная связь.

[RRS] А. Ромащенко, А. Румянцев, А. Шень. Заметки по теории кодирования. http://www.mccme.ru/~anromash/courses/coding-theory.ps

[VaSTOC] A. Vardy. Algorithmic Complexity in Coding Theory and the Minimum Distance Problem. STOC 1997.

[Va97] A. Vardy. The Intractability of Computing the Minimum Distance of a Code. IEEE Transactions on Information Theory, vol. 43, no. 6, november 1997, pp. 1757–1766.

[NiWi] N. Nisan, A. Wigderson. Hardness vs. Randomness Journal of Computer Systems and Sciences, vol. 49, no. 2, pp. 149-167, 1994.

[Tre01] L Trevisan. Extractors and Pseudorandom Generators J. of the ACM, 48(4):860-879, 2001.

[RaReVa] R. Raz, O. Reingold, S. Vadhan. Extracting all the Randomness and Reducing the Error in Trevisan's Extractors

[SuTreVa] Madhu Sudan, Luca Trevisan and Salil Vadhan. Pseudorandom Generators Without the XOR Lemma J. of Computer and System Sciences, 62(2):236-266, 2001