Задачи к курсу Теория кодирования и сложность вычислений (А.Е. Ромащенко; мехмат МГУ, весна 2010)

Задача 1. Докажите, что всякий линейный код можно сделать систематическим (не меняя множество кодовых слов).

Задача 2. Найти максимальное возможное число кодовых слов в двоичном коде с кодовым расстоянием 60% от длины n кодового слова (таким образом, код позволяет исправляеть 30% ошибок).

Задача 3. Докажите, что для любых целых q, k, для любого $\varepsilon > 0$ для некоторого $n = n(k, q, \varepsilon)$ существует код

$$C \ : \ \{1, \ldots, q\}^k \to \{1, \ldots, q\}^n$$

допускающего декодирование списком размера $\mathrm{poly}(k/\varepsilon)$ с исправлением $(1 - \frac{1}{q} - \varepsilon)n$ ошибок. Другими словами, в окрестности радиуса $(1 - \frac{1}{q} - \varepsilon)n$ любого слова длины n в q-буквенном алфавите найдётся не более $\mathrm{poly}(k/\varepsilon)$ кодовых слов.

Задача 4. Покажите, что в предыдущей задаче нельзя заменить $(1 - \frac{1}{q} - \varepsilon)n$ на $(1 - \frac{1}{q} + \varepsilon)n$.

Задача 5. У Алисы и Боба имеются двоичные слова длины n, которые отличаются друг от друга не более чем в r битах. Алиса хочет переслать Бобу своё слово; при этом Алиса и Боб могут обмениваться сообщениями по двустороннему каналу связи.

Пусть существует линейный код

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

позволяющий исправлять r ошибок. Придумайте коммункационный протокол, поозволяющий Бобу узнать слово Алисы, и требующий обмена не более чем $(n - k)$ битами. Какую оценку для k даёт граница Варшамова–Гилберта?

Задача 6. (продолжение) Пусть существует линейный код

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

допускающий декодирование списком размера $\mathrm{poly}(n)$ с исправлением r ошибок. Придумайте коммункационный протокол, позволяющий Бобу узнать слово Алисы, и требующий обмена не более чем $(n - k) + O(\log n)$ битами. Какую оценку для k даёт граница Хэмминга?

Задача 7. Пусть задано оторажение

$$Ext \ : \ \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

такое, что для некоторого распределения X на $\{0,1\}^d$ и равномерного распределения $\{0,1\}^n$ первый бит значения $Ext(X, U_d)$ равен нулю (с вероятностью один). Докажите, статистическое расстояние между распределением $Ext(X, U_d)$ и равномерным распределением на m битах не меньше $1/2$.

Задача 8. Предположим, что для любых k, n мы умеем строить за полиномиальное время $(k, 1/10)$-экстрактор

$$Ext \ : \ \{0,1\}^n \times \{0,1\}^{O(\log n)} \to \{0,1\}^{k/2}$$

который выделяет из любого распределения на n битах с мин-энтропией k некоторое "почти равномерное" (1/10-близкое к равномерному) распределение на $k/2$ битах.

Пусть имеется датчик случайных чисел, в котором очередной бит принимает значения 0 и 1 с вероятностями не менее $1/4$ и не более $3/4$ (при этом разные биты датчика могут быть зависимы). Покажите, что с помощью такого датчика случайных битов можно за полиномиальное время решать любую задачу из BPP (с ограниченной вероятностью ошибки на любом входе). Какое время работы удаётся получить, если заменить $O(\log n)$ на произвольную функцию $d = d(n)$?

Задача 9. Заменим в экстракторе Тревисана код LDC (допускающий декодирование списком) на тождественное отображение. Оцените параметры полученного экстрактора (как ε связано с мин-энтропией k).

Задача 10. Докажите NP-трудность следующей задачи: заданы (своей двоичной записью) целые числа d, k, m, простое число p, а также набор пар остатков по модулю p: $(x_1, y_1), \ldots, (x_m, y_m)$; требуется узнать, существует ли такой многочлен $p(x)$ степени не выше d, график которого проходит хотя бы через k заданных точек (т.е., $p(x_i) = y_i$ не менее чем для k различных i).

Задача 11. Пусть дан код $C \ : \ \{1, \ldots, q\}^k \to \{1, \ldots, q\}^n$ с параметрами $[n, k, d]_q$. Обозначим $\gamma = \frac{n-d}{n}$. Докажите, что при $\delta > C\sqrt{\gamma}$ (для некоторой абсолютной константы C) в $(1-\delta)n$-окрестности произвольного слова $y \in \{1, \ldots, q\}^n$ может лежать не более $O(1/\delta)$ кодовых слов.

Задача 12. (продолжение) Заменим в предыдущей задаче условие для δ на

$$\delta > \frac{1}{q} + \sqrt{\gamma - \frac{1}{q}}$$

Покажите, что в $(1-\delta)n$-окрестности произвольного слова $y \in \{1, \ldots, q\}^n$ может лежать не более $O(\frac{1}{\delta^2 - (1/q)})$ кодовых слов.

Задача 13. (продолжение) Обозначим $\mathbb{F}_q$ поле из q элементов, и пусть задана некоторая функция $f \ : \ \mathbb{F}_q^m \to \mathbb{F}_q$. Рассмотрим многочлены от m переменных степени d (над полем $\mathbb{F}_q$), которые совпадают с f не менее, чем в δq^m точек. Выведите из двух предыдущих задач, что

(а) если $\delta > C\sqrt{\frac{d}{q}}$ (для некоторой абсолютной константы C), то количество указанных многочленов не превосходит $O(1/\delta)$;

(б) если $\delta > \frac{1}{q} + \sqrt{\frac{d}{q}}$, то количество указанных многочленов не превосходит $O(\frac{1}{\delta^2 - (d/q)})$.

Задача 14. Запишите доказательство теоремы Вигдресона–Импальяццо о преобразовании трудно-вычислимой функции в трудно-аппроксомируемую.