

Практика 8

OV59. (Код Адамара) Рассмотрим код $C : \{0, 1\}^n \rightarrow \{0, 1\}^{2^n}$, который задается следующим образом:
 $C(x)_r = \sum_{i=1}^n x_i r_i$. Чему равно кодовое расстояние?

OV60. Алиса задумывает целое число от 1 до n . Боб должен отгадать это число, задавая Алисе вопросы, требующие ответы да или нет. Алиса может солгать в одном из ответов. Стратегия Боба называется адаптивной, если очередной задаваемый вопрос может зависеть от ответов, данных Алисой на предыдущих шагах. Стратегия называется неадаптивной, если Боб сразу предъявляет список всех своих вопросов, не дожидаясь первых ответов Алисы.

- (а) Какое минимальное число вопросов должен задать Боб, чтобы гарантированно узнать задуманное Алисой число для $n = 200$ (для адаптивной стратегии)?
- (б) Какое минимальное число неадаптивных вопросов должен задать Боб для $n = 150$.
- (в) Какое минимальное число адаптивных вопросов должен задать Боб для $n = 150$.

OV61. Добавим к кодовым словам кода Хемминга бит проверки четности: значение добавленного бита выбирается так, чтобы число единиц в каждом кодовом слове было бы чётно. Понятно, что число кодовых слов при этом не меняется, а их длина увеличивается на 1. Как при этом изменяется кодовое расстояние?

def. Код $C : \{0, 1\}^k \rightarrow \{0, 1\}^n$ называется *систематическим*, если существуют такие числа j_1, \dots, j_k , что для любого $(x_1, \dots, x_k) \in \{0, 1\}^k$ в кодовом слове $(y_1, \dots, y_n) = C(x_1, \dots, x_k)$ биты y_{j_1}, \dots, y_{j_k} равны соответствующим битам исходного слова. Другими словами, все «информационные биты» непосредственно входят в кодовое слово.

OV62. Докажите, что всякий линейный код $C : \{0, 1\}^k \rightarrow \{0, 1\}^n$ можно переделать в систематический линейный код $C' : \{0, 1\}^k \rightarrow \{0, 1\}^n$, сохранив прежнее множество кодовых слов (и проверочную матрицу).

Remark. Пусть для каждого символа алфавита c_i задана вероятность p_i .

OV63. Докажите, что для любого однозначно декодируемого кода выполняется

$$\sum_{i=1}^n p_i |c_i| \geq \sum_{i=1}^n p_i \log \frac{1}{p_i}.$$

def. Будем называть кодирование *сбалансированным*, если для некоторой константы c и для всех i выполняется $|c_i| \leq -\log p_i + c$.

OV64. Докажите, что кодирование Хаффмана не является сбалансированным.