Коды Рида-Маллера

Всероссийская студенческая конференция ”Студенческая научная весна“

студент	СГН3-64Б	Сковпень Т.Н.
научный руководитель	ст. преп. каф. ФН-1	Труфанов Н.Н.

Кафедра ФН-1 “Высшая математика”
МГТУ им. Н.Э. Баумана

15 апреля 2025

Постановка задачи

В работе рассматривается модель Шеннона (рис. 1) передачи данных по зашумлённому каналу.

Необходимо обеспечить качественную передачу аудиоданных в рамках рассматриваемой модели с помощью реализации кодов Рида–Маллера, позволяющих обнаружать и исправлять возникающие ошибки.

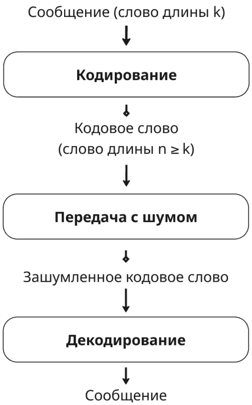


Рис. 1. Общая схема модели Шеннона

Модель передачи данных

Исходные аудиоданные представляются в форме двоичной последовательности.

При этом в рамках рассматриваемой модели каждый символ указанной последовательности с вероятностью p независимо может изменить своё значение.

Общая вероятностная схема приведена на рисунке 2.

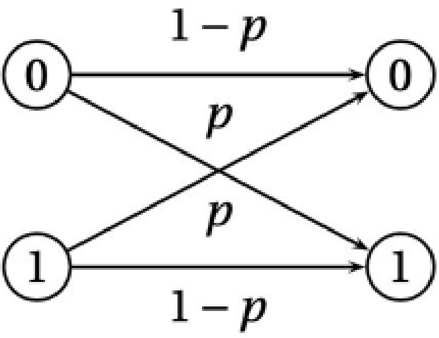


Рис. 2. Вероятностная схема

Линейные коды

Линейный код

Линейным кодом $\mathcal{C}$ с параметрами $(n,\ k)$ называют линейное подпространство n-мерного булева пространства V_n, где n – длина кода, k – размерность кода.

Порождающая матрица

Порождающей матрицей кода $\mathcal{C}$ называется матрица $G_{k\times n}$, составленная по строкам из базисных векторов $\mathrm{g}_1, \mathrm{g}_2, \ldots, \mathrm{g}_k \in V_n$.

Проверочная матрица

Проверочной матрицей H кода $\mathcal{C}$ называется матрица размерности $(n-k)\times n$, такая что

$$H \odot \mathrm{c}^T = 0, \quad \forall \mathrm{c} \in \mathcal{C}, \tag{1}$$

где $\odot$ – матричное произведение по модулю 2.

Минимальное расстояние

Расстояние Хэмминга

Для векторов $\mathrm{u} = (u_1, \ldots, u_n)$ и $\mathrm{v} = (v_1, \ldots, v_n)$ определено **расстояние Хэмминга** как

$$d(\mathrm{u}, \mathrm{v}) = \#\{i \mid u_i \neq v_i\}. \tag{2}$$

Код $\mathcal{C}$ исправляет t ошибок тогда и только тогда, когда:

1. Сферы радиуса t вокруг кодовых слов не пересекаются.
2. $d(\mathcal{C}) = \min d(c, c')$.

Связь минимального расстояния и корректирующей способности кода определятся как

$$d(\mathcal{C}) \geq 2t + 1, \tag{3}$$

где t – максимальное количество ошибок, которое код гарантированно может исправить.

Коды Рида-Маллера

Коды Рида-Маллера

Для произвольных натуральных m и r, $0 \leq r \leq m$, **кодом Рида–Маллера** $\mathrm{RM}(r, m)$ порядка r и длины $n = 2^m$ называется множество всех строк Ω_f тех булевых функций $f \in F_m$, степень нелинейности $\deg f$ которых не превосходит r, т.е.

$$\mathrm{RM}(r, m) = \{\Omega_f \mid f \in F_m,\ \deg f \leq r\}. \tag{4}$$

$$f(v_1, \ldots, v_m) = a_0 \oplus a_1 v_1 \oplus a_2 v_2 \oplus a_{12} v_1 v_2 \oplus \ldots \oplus a_{1\ldots m} v_1 \ldots v_m. \tag{5}$$

- Порядок кода $r \leq m$ – максимальная степень монома.
- Размерность $k = \sum_{i=0}^{r} \binom{m}{i}$.
- Минимальное расстояние $d = 2^{m-r}$.
- Допустимое число ошибок $t = 2^{m-r-1} - 1$.

Порождающая матрица

Рассмотрим построение порождающей матрицы для $\mathrm{RM}(2,3)$.

- Формирование мономов при $r = 2$.

Степень	Мономы
0	1
1	$v_1,\ v_2,\ v_3$
2	$v_1 v_2,\ v_1 v_3,\ v_2 v_3$

- Каждый моном вычисляется на всех 8 векторах $\mathrm{v} \in \{0,1\}^3$.

Порождающая матрица имеет вид

$$G_2(3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Проверочная матрица

Для кода $\mathrm{RM}(r, m)$ проверочная матрица совпадает с порождающей матрицей дуального кода

$$H = G(RM(m - r - 1, m)). \tag{6}$$

С помощью проверочной матрицы вычисляется синдром

$$\mathrm{s} = H \odot \mathrm{c}^T. \tag{7}$$

Если $\mathrm{s} \neq 0$, то это свидетельствует о наличии ошибок в принятом слове, что позволяет проводить их обнаружение.

Пример обнаружения ошибки

Рассмотрим сообщение

$$x = \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}.$$

Так как $r = 1$ и $m = 3$, порождающая матрица примет вид

$$G_1(3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Получаем кодовое слово

$$y = x \odot G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

При передаче был искажен бит y_3

$$y' = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Для обнаружения ошибки построим проверочную матрицу

$$H = G(RM(m - r - 1, 3)).$$

$$H = G(RM(1, 3)).$$

Вычисляем синдром

$$s = y' \odot H^T = 1.$$

Полученное значение синдрома $s = 1$ указывает на наличие ошибки в переданном кодовом слове.

Декодирование

Так как последовательность информационных символов сообщения x кодируется в кодовое слово как

$$\mathrm{y} = \mathrm{x} \odot G = x_0 \oplus x_1 v_1 \oplus x_2 v_2 \oplus x_3 v_3 \oplus x_{12} v_1 v_2 \oplus x_{13} v_1 v_3 \oplus x_{23} v_2 v_3. \tag{8}$$

Нашей задачей декодирования является восстановление коэффициентов x_i исходного сообщения x.
Восстановление коэффициентов начинаем с мономов наивысшей степени r, затем последовательно переходим к младшим степеням.

Декодирование

1. Формируем проверочные уравнения. Для этого фиксируем значения двух переменных, не входящих в моном. Например, для x_1 фиксируются x_2 и x_3.

$$\begin{aligned}
y_0 \oplus y_4 &= x_1, \quad (x_2 = 0,\, x_3 = 0),\\
y_1 \oplus y_5 &= x_1, \quad (x_2 = 0, x_3 = 1),\\
y_2 \oplus y_6 &= x_1, \quad (x_1 = 0, x_3 = 0),\\
y_3 \oplus y_7 &= x_1, \quad (x_2 = 1, x_3 = 1).
\end{aligned}$$

2. Применяем метод мажоритарного голосования. Из полученных уравнений получаем значения для $x_1 : 0, 0, 0, 1$. Большинство значений 0, значит итоговое значение $x_1 = 0$, аналогично $x_2 = 1$, $x_3 = 0$.
3. Вычитаем вклад восстановленных коэффициентов из вектора y' и получаем новый вектор

$$y^{(0)} = y' \oplus \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} \odot G_1(3) = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

4. Повторяем алгоритм рекурсивно и получаем $x_0 = 1$. Таким образом, получаем

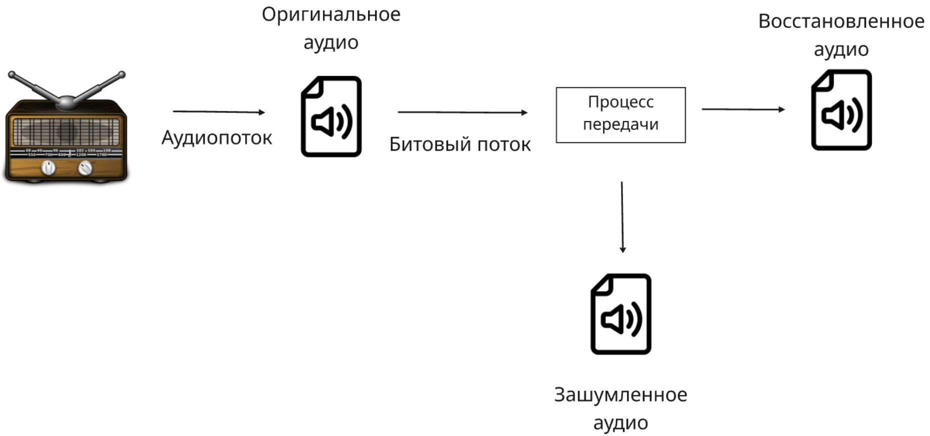
$$x = \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}.$$

Экспериментальная часть

Для проведения эксперимента использовался следующий план действий:

1. Отправка запроса к заданному URL, который транслирует аудиоданные.
2. Считывание данных блоками до тех пор, пока длина полученного аудиосегмента не достигнет целевого значения (в миллисекундах).
3. Сохранение оригинального аудио.
4. Преобразование аудио в битовый поток.
5. Разбиение битового потока на блоки фиксированной длины k.
6. Кодирование и симуляция передачи.
7. Восстановление и сохранение исправленного аудиосигнала.

Экспериментальная часть



Результаты

- Реализована модель передачи данных по зашумлённому каналу.
- Проведена симуляция передачи с искусственным внесением ошибок в битовый поток.
- Применён декодер, восстанавливающий исходные данные на основе избыточности кодов.

Проведенный эксперимент продемонстрировал, что применение кодов Рида-Маллера позволяет обеспечить надежность передачи данных в условиях воздействия помех.

Литература

Логачёв О. А., Сальников А. А.,
Ященко В. В.
Булевы функции в теории кодирования и криптологии.
М.: МЦНМО, 2004

Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.
Теория кодов, исправляющих ошибки
М.: Связь, 1979

И. В. Агафонова
Коды Рида–Маллера: примеры исправления ошибок
URL: https://dha.spb.ru/PDF/ReedMullerExamples.pdf (дата обращения: 14.04.2025), 2012

Спасибо за внимание!