Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

А. И. МИТЮХИН

ДЕКОДИРОВАНИЕ КОДОВ МЕТОДОМ МАКСИМАЛЬНОГО ПРАВДОПОДОБИЯ

МЕТОДИЧЕСКОЕ ПОСОБИЕ

к лабораторной работе

Минск БГУИР 2020

УДК [621.39+004.932](076)
ББК 32.811я73+32.973.26-018.2я73
М67

Митюхин, А. И.
М67 Декодирование кодов методом максимального правдоподобия: метод. пособие к лаб. работе / А. И. Митюхин. – Минск : БГУИР, 2020 с. : ил.
ISBN 978-585-543-190-0.

Представлено одно из направлений теории информации – помехоустойчивое кодирование с целью защиты информации от ошибок. Рассмотрен вычислительный алгоритм декодирования по максимуму правдоподобия кода, корректирующего ошибки. В лабораторной работе изучается метод декодирования низкоскоростных кодов на основе принципа максимального правдоподобия. Вычислительный алгоритм изложен на основе практического использования математического аппарата.

УДК [621.391+004.932](076)
ББК32.811я73+32.973.26-018.2я73

ISBN 978-985-543-190-0

ЦЕЛЬ РАБОТЫ

Изучение алгоритма декодирования помехоустойчивых кодов на основе применения метода максимального правдоподобия.

1. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Одной из основных задач теории информации является разработка информационных методов обработки и передачи сигналов, обеспечивающих прием, хранение и перераспределение информации в канале с шумом с максимально возможной надежностью (точностью) при минимальных энергетических затратах.

Очевидно, если для передачи выбраны два кодовых слова, например, $c_1 = (110)$ и $c_2 = (111)$, которые мало отличаются друг от друга, то из-за воздействия шума одно слово может принято за другое. Потребуются значительные затраты энергии, чтобы гарантировать различие этих слов на фоне шумов.

К. Шеннон показал, что при любом фиксированном количестве энергии сигнала существует такой метод преобразования (кодирования) информации и ее передачи, при котором информация может приниматься практически без ошибок. При этом происходит ограничение скорости передачи информации, а скорость не должна превышать пропускную способность канала.

1.1. Основная теорема кодирования для канала с шумом (вторая теорема Шеннона)

Теорема 1.1. Пусть C – пропускная способность дискретного канала без памяти, источник характеризуется энтропией H. Если $H < C$, тогда для любого $\varepsilon > 0$ существует метод кодирования информации $[n, k, d]$-двоичным кодом, вероятность ошибки P_f декодирования которого $< \varepsilon$.

1.2. Вектор ошибок

Пусть двоичный симметричный канал (ДСК) характеризуется вероятностью ошибки p на символ. Введем вектор ошибки $\boldsymbol{e} = (e_0 \dots e_j \dots e_{n-1})$, где $e_i \in \{0, 1\}$. Элемент $e_i = 1$ появляется с вероятностью p и $e_i = 0$ с вероятностью $(1 - p)$. Найдем вероятность возникновения следующих конфигураций векторов ошибок $\boldsymbol{e}$ для слова длиной $n = 5$:

– $\text{prob}\{\boldsymbol{e} = (00000)\} = (1-p)^5$ – есть вероятность правильного приема кодового слова длиной 5;

– $\text{prob}\{\boldsymbol{e} = (10000)\} = p(1-p)^4$ вероятность возникновения однократной ошибки при приеме слова длиной 5.

– $\text{prob}\{\boldsymbol{e} = (10010)\} = p^2(1-p)^3$ вероятность возникновения двукратной ошибки при приеме слова длиной 5.

В общем случае, вероятность возникновения вектора ошибок $\boldsymbol{e}$ веса i запишется в виде

$$\text{prob}\{\boldsymbol{e}_{wt(i)}\} = p^i(1-p)^{n-1}. \quad (1.1)$$

Вероятность правильного приема кодового слова длиной n равна

$$\text{prob}\{\boldsymbol{e}_{wt(0)}\} = (1-p)^n.$$

Пример 1.1. Пусть $p = 0{,}2$; $n = 5$. Вычислим некоторые возможные вероятности возникновения векторов ошибок.

1. Вероятность того, что не произошло ни одной ошибки на длине кодового слова, равна

$$\text{prob}\{\boldsymbol{e}_{wt(0)} = (00000)\} = (1-0{,}2)^5 \cong 0{,}32.$$

2. Вероятность того, что на длине кодового слова имеется ошибка единичного веса, равна

$$\text{prob}\{\boldsymbol{e}_{wt(1)} = (10000)\} = p^1(1-p)^4 = 0{,}2(1-0{,}2)^4 \cong 0{,}081.$$

3. Вероятность того, что произошли две ошибки на длине кодового слова, равна

$$\text{prob}\{\boldsymbol{e}_{wt(2)} = (10010)\} = p^2(1-p)^3 = 0{,}2^2(1-0{,}2)^3 \cong 0{,}01.$$

Из приведенного примера следуют очевидные выводы.

1. Вектор ошибок единичного веса более вероятен, чем вектор ошибок веса два и т.д.;

2. Ошибки малого веса необходимо обнаруживать и исправлять в первую очередь.

1.3. Декодирование

Пусть код состоит из множества $\{\boldsymbol{x}\}$ кодовых слов $\boldsymbol{x} = (x_0\, x_1 \ldots x_{n-1}),\ x_i \in \{0, 1\}$. Предположим, что по ДСК с шумом передается или хранится в памяти двоичный вектор $\boldsymbol{x} = (x_0\, x_1 \ldots x_{n-1})$, а принимается, или считывается из памяти вектор

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e} = (y_0\, y_1 \ldots y_{n-1}), y_i \in \{0, 1\}. .$$

Тогда вектор ошибок

$$\boldsymbol{e} = \boldsymbol{y} - \boldsymbol{x} = (e_0\, e_1 \ldots e_{n-1}), e_i \in \{0, 1\}.$$

Форма (структура) вектора ошибок указывает местоположение ошибок. Количество единиц (или по другом вес) на длине вектора ошибок $\boldsymbol{e}$ определяет число ошибок t.

Декодер, анализируя (наблюдая) вектор $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$, должен решить, какой вектор $\boldsymbol{x} \in \{\boldsymbol{x}\}$ передавался. Декодирование сводится к нахождению наиболее вероятного вектора ошибок $\boldsymbol{e}$ для принятого вектора $\boldsymbol{y}$. Если передаваемые кодовые слова имеют равные вероятности, такая стратегия декодирования является оптимальной. В этом случае декодер работает с минимально возможной ошибкой декодирования P_f, а стратегия называется декодированием по максимуму правдоподобия.

Рассматриваемый алгоритм эквивалентен декодированию в ближайшее кодовое слово. Практическая реализация этого алгоритма выполняется путем сравнения входа $\boldsymbol{y}$ со всеми словами множества $\{\boldsymbol{x}\}$ и принятия решения о ближайшем слове. Так как вектор ошибок меньшего веса более вероятен, то входной вектор $\boldsymbol{y}$ декодируется в вектор $\boldsymbol{x}$ из множества $\{\boldsymbol{x}\}$, который менее всего отличается от $\boldsymbol{y}$. Говорят, вектор $\boldsymbol{y}$ декодируется в ближайший вектор $\boldsymbol{x}$ в смысле расстояния.

1.3.1. Расстояние

Степень различия векторов, удаленности векторов характеризуется понятием, определяемым как расстояние в n -мерном пространстве. Каждое кодовое слово $\boldsymbol{x} = (x_0\, x_1 \ldots x_{n-1})$ представляется некоторой точкой в n -мерном пространстве. Точка задается координатами $x_0,\ x_1, \ldots x_{n-1}$. Расстояние между двумя точками в n -мерном пространстве определяется на основе применения теоремы Пифагора. Например, расстояние d_E (Евклида) на евклидовой плоскости между точкой с координатами $x = (4, 6)$ и любой точкой с координатами (x_i, x_j) равно

$$d_E = \sqrt{(x_i - 4)^2 + (x_j - 6)^2}.$$

Пример 1.2. Вычислить расстояние Евклида между точками (кодовыми словами) $x_1 = (1\ 1\ 1\ 0{,}5)$ и $x_2 = (0{,}5\ 0{,}5\ 0{,}5\ 0{,}5)$.

Решение. $d_E = \sqrt{(1 - 0{,}5)^2 + (1 - 0{,}5)^2 + (1 - 0{,}5)^2 + (0{,}5 - 0{,}5)^2} =$

$$= \sqrt{0{,}75} \cong 0{,}866.$$

Чем больше d_E, тем дальше удалены точки (слова) друг от друга в n -мерном пространстве. Для надежной различимости кодовых слов они должны быть разделены некоторым минимальным расстоянием.

Важнейшей характеристикой множества кодовых слов является минимальная энергетическая затрата на их передачу. Физически значению (числу) x_i

слова $\boldsymbol{x} = (x_0\ x_1\ \dots x_{n-1})$ соответствует некоторый уровень напряжения в канале передачи. Из определения энергии (энергия прямо пропорциональна квадрату напряжения, деленному на сопротивление электрической цепи) суммарная энергия необходимая для передачи слова $\boldsymbol{x} = (x_0\ x_1\ \dots x_{n-1})$ определяется как

$$E = \sum_{i=0}^{n-1} |\ x_i|^2. \qquad (1.2)$$

Например, слово $x_2 = (1\ 1\ 1\ 0{,}5)$ характеризуется энергией

$$E = \sum_{i=0}^{4} |\ x_i|^2 = 3{,}25.$$

Замечание. Формула (1.2) определяет квадрат расстояния ${d_E}^2$ от точки представляющей слово $\boldsymbol{x} = (x_0\ x_1\ \dots x_{n-1})$ в n-мерном пространстве до точки $\boldsymbol{x} = (0\ 0\ \dots 0)$ представляющей начало координат.

Квадрат расстояния ${d_E}^2$ от точки $x_2 = (1\ 1\ 1\ 0{,}5)$ до начала координат равен

$${d_E}^2 = E = 3{,}25.$$

Выводы

1. Решение задачи повышения надежности информационной системы требует, чтобы кодовые слова были удалены на некоторое минимальное расстояние.
2. Решение задачи минимизации энергетических затрат требует размещения точек (слов) как можно ближе к началу системы координат n -мерного пространства.
3. Желательно, чтобы все кодовые слова обладали одинаковой энергией.

1.4. Избыточность

Увеличение надежности передачи информации по каналу с шумом требует введения информационной избыточности в сообщение.

Пусть выходом блокового источника X^k являются последовательности (блоки) из k одиночных статистически независимых символов алфавита $X = \{x_1, x_2, \dots, x_m\}$ источника X. На выходе блокового источника можно сформировать m^k символов. Например, для $X = \{0, 1\}$, $k = 2$ множество символов источника с 2-кратным расширением источника X есть

$$X^2 = \{c_1, c_2, c_3, c_4\},$$

где $c_1 = (00), c_2 = (01), c_3 = (10), c_4 = (11)$ образуют информационное множество, состоящее из $m^k = 2^2 = 4$-х символов блокового источника. Кодер источника последовательно выдает информационные слова фиксированной длины.

Пример 1.3. Пусть для передачи сообщения "$DANK$" используется следующий алфавит $\{A, K, N, D\}$. Этому алфавиту сообщения соответствуют двоичные слова блокового источника X^2:

$$A \to (00);$$
$$K \to (01);$$
$$N \to (10);$$
$$D \to (11).$$

Кодер помехоустойчивого кода (кодер канала) заменяет каждое информационное слово кодовым словом, длина которого может значительно превышать исходную. Таким образом, в передаваемую информацию вводится избыточность. Например, символам блокового источника можно поставить в соответствие слова помехоустойчивого (избыточного) кода $\{\boldsymbol{c}\} = \{\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3, \boldsymbol{c}_4\}$:

$$A \to (00) \to (0000) = \boldsymbol{c}_1,$$
$$K \to (01) \to (0101) = \boldsymbol{c}_2,$$
$$N \to (10) \to (1011) = \boldsymbol{c}_3,$$
$$D \to (11) \to (1101) = \boldsymbol{c}_4.$$

Как видно, кодовые символы A и N имеют различия в одной позиции, а кодовые слова $\boldsymbol{c}_1$ и $\boldsymbol{c}_3$ в трех позициях.

1.5. Параметры помехоустойчивых кодов

Определение 1.1. Код – это множество дискретных последовательностей, разрешенное для передачи сообщений.

Коды характеризуются следующими параметрами.

1. Размерность q кодового алфавита – число различных элементов алфавита, выбранное для построения кода.

В качестве кодового алфавита могут использоваться символы двоичного $\{0,1\}$ или бинарного алфавита $\{1, -1\}$. Например, слово $x = (x_1 x_2 \dots x_7) = (-1 - 1 - 111 - 11)$ представлено символами бинарного алфавита источника, $q = 2$.

Определение 1.2. Длина *n* кода (значность) – число символов кодового слова. Последовательности символов называются кодовыми словами или кодовыми векторами.

Параметр *n* определяет следующие особенности кодов. Коды бывают:

– равномерные (блоковые), *n* = const;

– неравномерные, *n* = var;

– бесконечные, *n* = ∞.

Определение 1.3. Размерность *k* кода – число информационных элементов

(позиций) кодового слова.

Определение 1.4. Мощность $M = q^k$ кода – это число различных кодовых последовательностей (комбинаций), разрешенных для кодирования.

Различают $M_{\max} = q^n$ максимальное число кодовых слов при заданных q и n. Например, для q = 3, n = 6 имеем $M_{\max} = q^n = 729$ слов. Код, у которого используются все комбинации, т. е. его мощность $M_{\max}$, называется полным (безизбыточным). Для него $k = n$.

Если код определяется числом $M < M_{\max}$, то код называется избыточным.

Пример 1.4. Код с параметрами: q = 2, n = 5, $M = 4$ является избыточным. Кодовые слова записаны в виде матрицы

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Определение 1.5. Число проверочных (избыточных) $r = (n - k)$ позиций кодового слова.

Пусть n = 7, q = 2, k = 4. Тогда на длине слова из семи символов три избыточных.

Определение 1.6. Скорость $R = \frac{k}{n}$ передачи кода.

Для приведенного выше примера $R = \frac{4}{7}$.

Определение 1.7. Кратность ошибки t. Параметр t указывает, что все конфигурации из t или менее ошибок в любом кодовом слове могут быть исправлены и (или) обнаружены.

Определение 1.8. Расстояние Хэмминга d_x между двумя векторами (степень удаленности любых кодовых последовательностей друг от друга). Если $\boldsymbol{x} = (x_0\, x_1 \ldots x_{n-1})$ и $\boldsymbol{y} = (y_0\, y_1 \ldots y_{n-1})$ кодовые векторы, то расстояние Хэмминга равно числу позиций, в которых они различаются.

Расстояние Хэмминга может обозначаться и как dist (x, y). Например,

$$\text{dist}\,((a\ b\ b\ c\ b), (c\ b\ c\ a\ a) = 4,$$

Замечание. С позиции теории кодирования d_x показывает, сколько символов в слове надо исказить, чтобы перевести одно кодовое слово в другое.

Определение 1.9. Наименьшее значение расстояния Хэмминга для всех пар кодовых последовательностей кода G называют кодовым расстоянием d (минимальное расстояние кода),

$$d = \min\{\text{dist}(x, y)\}, \text{ где } x \in G,\ y \in G,\ x \neq y.$$

Кодовое расстояние d характеризует корректирующею способность кода

$$t = f(d).$$

Определение 1.10. Код значностью n, размерностью k и расстоянием d называется $[n, k, d]$- кодом.

Пример 1.5. Можно построить следующий код:

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Данный код можно использовать для кодирования 2-х битовых двоичных чисел, используя следующее (произвольное) соответствие:

0 0 ↔ 0 0 0 0 0;
1 0 ↔ 1 0 1 1 0;
0 1 ↔ 0 1 0 1 0;
1 1 ↔ 1 1 1 0 0.

Найдем кодовое расстояние этого кода:

dist((1 0 1 0), (0 1 1 1)) = 3;
dist((1 0 1 0), (1 1 0 1)) = 3;
dist((0 1 1 1), (1 1 0 1)) = 2.

Следовательно, для этого кода $d = \min\{\text{dist}(x, y)\} = 2$.

Определение 1.11. Вес Хэмминга вектора $\boldsymbol{x} = (x_0\ x_1 \ldots x_{n-1})$ равен числу ненулевых позиций вектора x; обозначается wt($\boldsymbol{x}$).

Например, wt(1 2 3 0 4 3 0) = 5. Используя определение веса Хэмминга,

получим очевидное выражение

$$\mathrm{dist}(x, y) = \mathrm{wt}(x - y). \qquad (1.3)$$

Пример 1.6. $\boldsymbol{x}$ = (1 2 0 2)$^{\mathrm{T}}$, $\boldsymbol{y}$ = (2 0 1 2)$^{\mathrm{T}}$.

$$\mathrm{dist}(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{wt}(\begin{bmatrix}1\\2\\0\\2\end{bmatrix} - \begin{bmatrix}2\\0\\1\\2\end{bmatrix}) = \mathrm{wt}\begin{bmatrix}2\\2\\2\\0\end{bmatrix} = 3.$$

Из выражения (1.3) следует, что минимальное расстояние Хэмминга равно

$$d = \min\{\mathrm{dist}(\boldsymbol{x}, \boldsymbol{y})\} = \min\{\mathrm{wt}(\boldsymbol{x} - \boldsymbol{y}), \text{ где } \boldsymbol{x} \in \boldsymbol{G},\ \boldsymbol{y} \in \boldsymbol{G},\ \boldsymbol{x} \neq \boldsymbol{y}.$$

Теорема 1.2. Минимальное расстояние линейного кода равно минимальному весу ненулевых кодовых слов.

Замечание. Для нахождения минимального расстояния линейного кода не обязательно сравнивать все возможные пары кодовых слов. Если $\boldsymbol{x} \in \boldsymbol{G},\ \boldsymbol{y} \in \boldsymbol{G}$ то $\boldsymbol{x} - \boldsymbol{y} = \boldsymbol{u} \in \boldsymbol{G}$ также является кодовым словом кода $\boldsymbol{G}$. Такой код является аддитивной группой (определена операция сложения) и, следовательно,

$$d = \min\{\mathrm{dist}(\boldsymbol{x}, \boldsymbol{y})\} = \mathrm{minwt}(\boldsymbol{u}),$$

где $\boldsymbol{u} \in \boldsymbol{G},\ \boldsymbol{u} \neq 0$.

Теорема 1.3. Код, имеющий минимальное расстояние d может исправлять t ошибок:

$$t = \left\lceil \frac{d-1}{2} \right\rceil,$$

где $\lceil l \rceil$ обозначает наибольшее целое число, меньшее или равное l.

1.6. Способы задания линейных кодов

Линейные коды задаются с помощью:

– порождающей матрицы $\boldsymbol{G}$ размерностью $k \times n$;
– проверочной матрицы $\boldsymbol{H}$ размерностью $r \times n$.

Матрицы связаны основным уравнением кодирования

$$\boldsymbol{G} \times \boldsymbol{H}^T = 0. \qquad (1.4)$$

Из (1.4) следует, что для всякой матрицы $\boldsymbol{G}$ существует матрица $\boldsymbol{H}$, удовлетворяющая этому равенству. И наоборот, заданной матрице $\boldsymbol{H}$ будет соответствовать только одна матрица $\boldsymbol{G}$. В качестве строк матрицы $\boldsymbol{G}$ выбираются линейно-независимые слова длиной n, отстоящие друг от друга на заданное кодовое расстояние d.

Поскольку линейно независимые векторы могут быть выбраны произвольным образом, очевидно, можно построить множество матриц $\boldsymbol{G}$ с одним и тем же кодовым расстоянием d.

1.7. Каноническая форма порождающей матрицы

Порождающая матрица кода в канонической форме записывается как

$$\boldsymbol{G} = [\boldsymbol{I}_k|\boldsymbol{G}^*] \tag{1.5}$$

где $\boldsymbol{I}_k$ – единичная подматрица размером $k \times k$, а $\boldsymbol{G}^*$ – подматрица размером $k \times (n - k$.

С учётом формы матрицы (1.5) уравнение кодирования представим, как

$$\boldsymbol{G}\boldsymbol{H}^T = [\boldsymbol{I}_k|\boldsymbol{G}^*]\left[\frac{-\boldsymbol{G}^*}{\boldsymbol{I}_r}\right] = -\boldsymbol{G}^* + \boldsymbol{G}^* = 0.$$

Отсюда определяем проверочную матрицу $\boldsymbol{H}$ в канонической форме:

$$\boldsymbol{H} = [-\boldsymbol{G}^{*T}|\boldsymbol{I}_r], \tag{1.6}$$

где $\boldsymbol{I}_r$ – единичная матрица размером $r \times r$.

В поле $GF(2)$ $-\boldsymbol{G}^{*T} = \boldsymbol{G}^{*T}$, поэтому

$$\boldsymbol{H} = [\boldsymbol{G}^{*T}|\boldsymbol{I}_r].$$

Матрицы (1.5) и (1.7) соответствуют систематическому линейному коду. Если известна проверочная матрица систематического кода

$$\boldsymbol{H} = [\boldsymbol{H}^*|\boldsymbol{I}_r], \tag{1.7}$$

то матрица $\boldsymbol{G}$ записывается в виде

$$\boldsymbol{G} = [\boldsymbol{I}_k|\boldsymbol{H}^{*T}].$$

1.8. МЕТОДЫ ДЕКОДИРОВАНИЯ ЛИНЕЙНЫХ КОДОВ

Известны и применяются четыре основных метода декодирования.

1. Декодирование по синдрому.
2. Декодирование на основе принципа максимального правдоподобия.
3. Спектральное декодирование.
4. Мажоритарное декодирование, или декодирование по большинству проверок.

Первый и четвертый методы применяются для коррекции независимых, модульных и пакетных ошибок кратностью t равной 1 – 4 . Второй и четвертый методы декодирования используются, как правило, в радиоэлектронных системах, работающих при низких отношениях сигнал/помеха на входе декодера, сложной помеховой обстановке.

В лабораторной работе изучается метод декодирования низкоскоростных кодов на основе принципа максимального правдоподобия.

1.9. Декодирование низкоскоростных кодов на основе принципа максимального правдоподобия

Определение 1.12. Декодирование кода на основе вычисления вектора ошибки $\boldsymbol{E}$ с наименьшим весом называется декодированием на основе принципа максимального правдоподобия, или декодированием в ближайшее кодовое слово.

1.9.1. Низкоскоростные коды

Низкоскоростными являются коды, у которых $k \ll r$ и скорость передачи кода $R = k/n \ll 1$. Как правило, кодовое расстояние низкоскоростных кодов приближается к значению $d = \frac{n}{2}$. Следовательно, такие коды могут корректировать $t = \left\lceil \frac{d-1}{2} \right\rceil = \left\lceil \frac{\frac{n}{2}-1}{2} \right\rceil \cong \frac{n}{4}$ ошибок. Свойства низкоскоростных кодов позволяют использовать их в качестве основы для формирования так называемых сложных сигналов для систем связи, радиолокации, радиолокации, для обеспечения синхронизации, структурной и криптографической защиты информации. Практический интерес представляют различные семейства низкоскоростных кодов (кодовых последовательностей), их корреляционные свойства, мощность кодов, сложность кодовой структуры и вычислительная сложность обработки.

Свойства кодовых последовательностей. *Корреляционные свойства*.

Наиболее важными для низкоскоростных кодов являются их периодические и апериодические корреляционные свойства. Корреляционная функция – это показатель сходства или общих свойств двух последовательностей. Функция корреляции описывает последовательное изменение отклика линейной системы

на входное воздействие в виде кодового слова. Отклик формируется при изменении временного положения последовательности.

Нормированная периодическая взаимная корреляционная функция $r(\tau)$ последовательностей $x = (x_0 x_1 \dots x_{n-1})$ и $h = (h_0 h_1 \dots h_{n-1})$ записывается как

$$r_\tau = \frac{1}{n}\sum_{k=0}^{n-1} x_k h_{\tau+k},\ \tau = 0, 1, \dots, n-1. \qquad (1.8)$$

где $\big((\tau + k)\big) = (\tau + k) \bmod n$.

Эта функция периодична, т. е. $r_\tau = r_{((\tau+n))}$. Если временного рассогласования нет, $\tau = 0$. Значение $r_\tau = 0$ указывает на нулевую корреляцию. Это означает, что последовательности независимы. Если корреляция последовательностей в выражено слабо, то

$$|r_{xh}(\tau)| \ll 1, \text{ при любых } \tau.$$

1.9.2. Матричное представление корреляции

Пусть длина последовательности $n = 3$. По формуле (1.8) получаем следующие значения коэффициентов корреляции:

$$r(0) = \frac{1}{3}(x(0)h(0) + x(1)h(1) + x(2)h(2));$$
$$r(1) = \frac{1}{3}(x(0)h(1) + x(1)h(2) + x(2)h(0));$$
$$r(2) = \frac{1}{3}\big(x(0)h(2) + x(1)h(0) + x(2)h(1)\big).$$

Полученные выражения могут быть представлены в матричной форме

$$\boldsymbol{r} = \frac{1}{n}\boldsymbol{h}\boldsymbol{x}^T,$$
$$\begin{bmatrix} r(0) \\ r(1) \\ r(2) \end{bmatrix} = \frac{1}{3}\begin{bmatrix} h(0) & h(1) & h(2) \\ h(1) & h(2) & h(0) \\ h(2) & h(0) & h(1) \end{bmatrix}\begin{bmatrix} x(0) \\ x(1) \\ x(2) \end{bmatrix}. \qquad (1.9)$$

Из примера следует, что вычисление взаимной корреляции двух n-периодических последовательностей сводится к циклическому сдвигу одной последовательности относительно другой и усреднения их произведения за период n.

Если последовательности x и h идентичны, то выражение (1.8) будет определять автокорреляционную функцию

$$r_\tau = \frac{1}{n}\sum_{k=0}^{n-1} x_k x_{\tau+k},\ \tau = 0, 1, \dots, n-1. \qquad (1.10)$$

Пример 1.7. Вычислить взаимную корреляционную функцию последовательностей $x = (-1, -1, -1, 1)$ и $h = (1, -1, -1, -1)$.

Решение

$$\begin{bmatrix} r(0) \\ r(1) \\ r(2) \\ r(3) \end{bmatrix} = \begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \end{bmatrix} \begin{bmatrix} -1 \\ -1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 4 \\ 0 \\ 0 \end{bmatrix}.$$

На рис. 1.1 показан график ненормированной взаимной корреляционной функции.

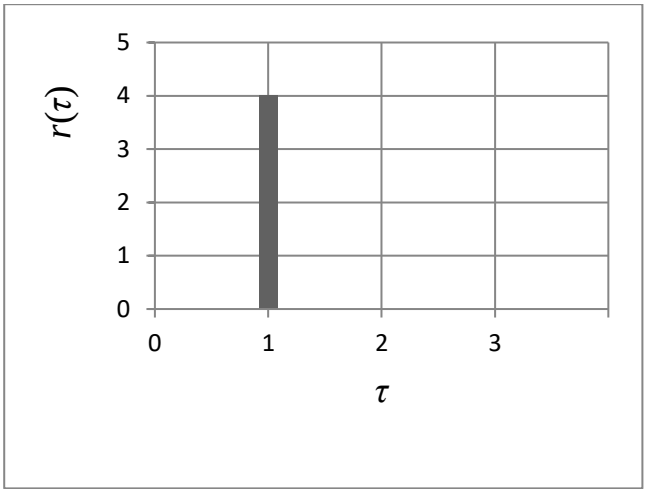

Рис. 1.1. Графическое представление взаимной корреляционной функции

Пример 1.8. Вычислить автокорреляционную функцию псевдошумовой последовательности $x = (0\ 0\ 1\ 0\ 111)$.

Решение. При переходе к бинарной записи последовательности x, которая получается путем замены 0 на 1 и 1 на –1, автокорреляционная функция равна

$$\begin{bmatrix} r(0) \\ r(1) \\ r(2) \\ r(3) \\ r(4) \\ r(5) \\ r(6) \end{bmatrix} = \frac{1}{7} \begin{bmatrix} 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & -1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \\ -1 \\ -1 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 \\ -1/7 \\ -1/7 \\ -1/7 \\ -1/7 \\ -1/7 \\ -1/7 \end{bmatrix}.$$

На рис. 1.3 показан график автокорреляционной функции псевдошумовой последовательности.

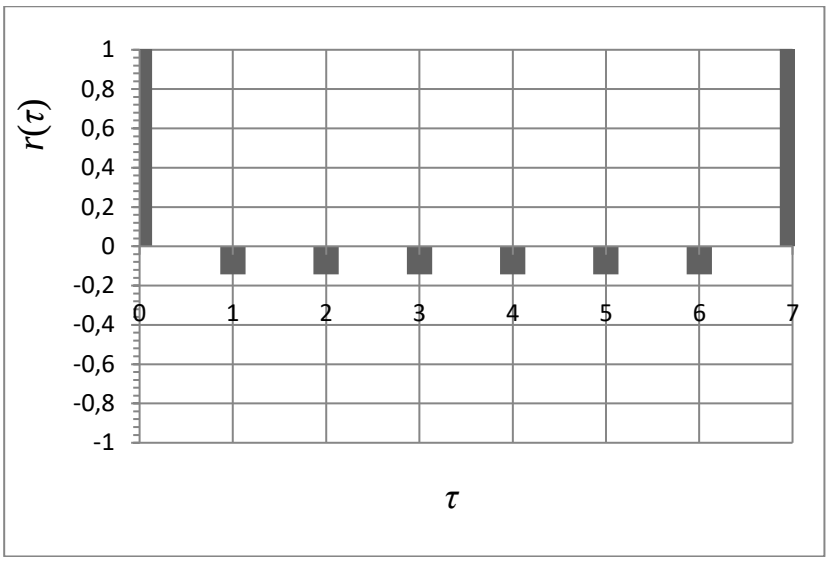

Рис.1.3. Автокорреляционная функция последовательности $x = (1\ 1 -\ 1 - 1 - 1 - 1)$.

1.9.3. Корреляционный метод декодирования кодов

Низкоскоростные коды в основном используются при низком отношении сигнал/шум на входе декодера системы. Декодирование таких кодов целесообразно реализовывать на основе принципа максимального правдоподобия (минимума расстояния Хэмминга). В этом случае достигается минимальная ошибка декодирования, повышается достоверность передачи-приема (обработки) информации. Декодирование на основе принципа максимального правдоподобия эквивалентно корреляционному методу. Тогда декодирование сводится к вычислению корреляции принимаемой последовательности со всеми кодовыми словами кода.

Пусть имеется псевдослучайная последовательность $X = (x_0 x_1 \dots x_{n-1})$, задающая помехоустойчивый $[n, k, d]$-код. Циклические сдвиги последовательности X определяют разрешенное пространство кодовых слов кода, записанное в виде матрицы $\boldsymbol{A}$ размером $(2^k - 1) \times n$, где $M = (2^k - 1)$ – мощность кода, $k \geq 3$. Строки матрицы $\boldsymbol{A}$ образуют множество $\{X\} = (X_1, \dots, X_M)$ слов кода.

В канале без шумов, декодирование заключается в вычислении вектора

$$\boldsymbol{Y} = \frac{1}{\boldsymbol{n}} \boldsymbol{A}\boldsymbol{X} = (y_0 y_1 \dots y_{n-1})^T, \boldsymbol{X} \in \boldsymbol{A} \qquad (1.11)$$

и определении номера l координаты y_l, для которой выполняется условие

$$y_l = \max_i y_i.$$

Пример 1.9. Пусть имеется источник на множестве символов алфавита $\{A, B, C, D, E, F, I\}$. Этому множеству ставится в соответствие ансамбль

$\{X\} = (X_1 \dots, X_M)$ кодовых слов, заданных матрицей $\boldsymbol{A}$. В качестве задающего код выбрана псевдослучайная последовательность $X = (x_0 x_1 \dots x_6)$ m-кода

$$X = (1\ 1 - 1\ 1 - 1 - 1 - 1).$$

$$\boldsymbol{A} = \begin{bmatrix} 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 \end{bmatrix}. \qquad (1.13)$$

Матрица $\boldsymbol{A}$ определяет помехоустойчивый код с параметрами: $n = 7, k = 3, d = 4$. Символ A кодируется словом $X_1 = (1\ 1 - 1\ 1 - 1 - 1 - 1)$, символ B – соответственно словом $X_2 = (1 - 1\ \ 1 - 1 - 1 - 1\ 1)$ и т. д.

Предположим, на вход декодера поступила последовательность

$$X = (-1 - 1\ 1\ 1 - 11 - 1).$$

Вычисляя по формуле (1.12), получим вектор

$$\boldsymbol{Y} = \left({}^{-1}/_{7}, {}^{-1}/_{7}, {}^{-1}/_{7}, {}^{-1}/_{7}, {}^{-1}/_{7}, 1, {}^{-1}/_{7}\right)^{T}.$$

Максимальное значение имеет компонента $y_5 = 1$, поэтому по каналу передавался символ F. На рис. 1.4. показан график функции $r(\tau) = y(\tau), \tau = 0, 1, \dots, n - 1$.

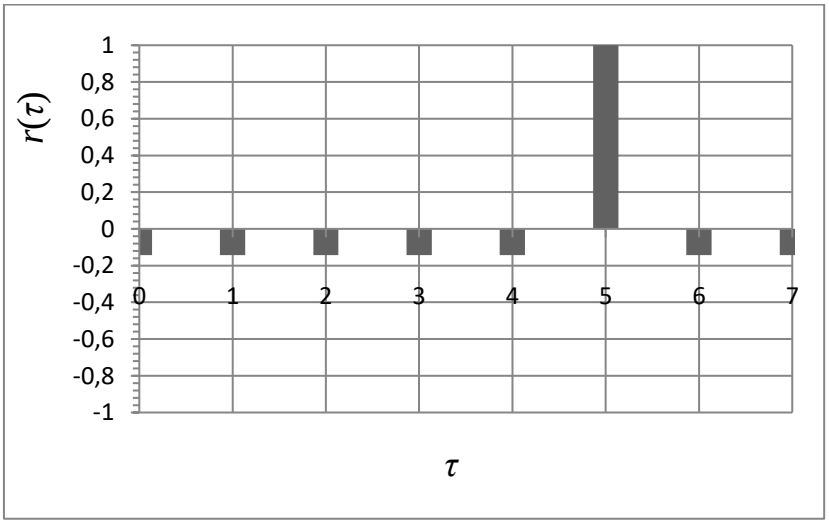

Рис.1.4. Корреляционная функция последовательности $x = (-1 - 1\ 11 - 1\ 1 - 1)$.

Предположим, что подлежит передаче по каналу с шумами некоторый вектор $\boldsymbol{X} \in \boldsymbol{A}$. Из-за возможного воздействия шумов, на выходе канала наблюдается (принимается) вектор вида

$$\boldsymbol{Z} = (\boldsymbol{X} + \boldsymbol{E})\mathrm{mod}2 = (z_0 z \dots z_{n-1}),$$

где $\boldsymbol{E}$= $(e_0\ e_1 \dots e_{n-1}), e_i \in \{1, -1\}$ – вектор ошибок, определяемый как

$$\boldsymbol{E} = (\boldsymbol{Z} - \boldsymbol{X})\mathrm{mod}2.$$

Если ошибок не произошло, то все $e_i = 0$. Вектор ошибок указывает место ошибки на длине вектора $\boldsymbol{X}$. Количество единиц на длине вектора ошибок $\boldsymbol{E}$ определяет число ошибок t.

Декодер, анализируя вектор $\boldsymbol{Z} = \boldsymbol{X} + \boldsymbol{E}$, должен решить, какой вектор $\boldsymbol{X}$ из множества $\{\boldsymbol{X}\}$ передавался. Вектор $\boldsymbol{Z}$ декодируется в ближайший вектор $\boldsymbol{X}$ на множестве $\{\boldsymbol{X}\}$ в смысле расстояния Хэмминга. Практическая реализация этого алгоритма декодирования выполняется путем сравнения входа Z со всеми словами множества $\{X\}$ и принятия решения о ближайшем слове.

Пример 1.11. Пусть имеется источник и код, задаваемый матрицей $\boldsymbol{A}$ (см. пример 1.10). На вход декодера поступил вектор $\boldsymbol{Z} = (1\ 1\ 1 - 1\ 1 - 1 - 1)$. Определить принимаемый символ источника.

Решение. Выполняя корреляционное декодирование по формуле

$$\boldsymbol{Y} = \boldsymbol{A}\boldsymbol{Z}^T = (y_0 y_1 \dots y_{n-1})^T,$$

получим вектор

$$\boldsymbol{Y} = (1, 1, -3, 1, -3, -3, 5)^T.$$

Максимальное значение имеет координата $y_6 = 5$, рис. 1.5. По каналу передавалось кодовое слово $X_6 = (-1\ 1\ 1 - 1\ 1 - 1 - 1)$. Этому слову соответствует символ I.

Вектор ошибки $\boldsymbol{E}$ соответствует следующей последовательности с наименьшим весом (единичным) весом:

$$\boldsymbol{E} = (\boldsymbol{Z} - \boldsymbol{X})\mathrm{mod}2 = (1\ 1\ 1 - 1\ 1 - 1 - 1) - (-1\ 1\ 1 - 1\ 1 - 1 - 1) =$$
$$= (-1\ 1\ 1\ 1\ 1\ 1\ 1) \rightarrow (1\ 0\ 0\ 0\ 0\ 0\ 0).$$

Как видно, ошибка произошла в первом чипе слова X_6. Найденный вектор $\boldsymbol{E}$ является наиболее вероятным для принятого вектора $\boldsymbol{Z}$. Расстояние Хэмминга между векторами $\boldsymbol{Z}$ и $\boldsymbol{X_6}$ равно $d_x = 1$. Это расстояние является минимальным на пространстве кодовых векторов кода (матрицы $\boldsymbol{A}$).

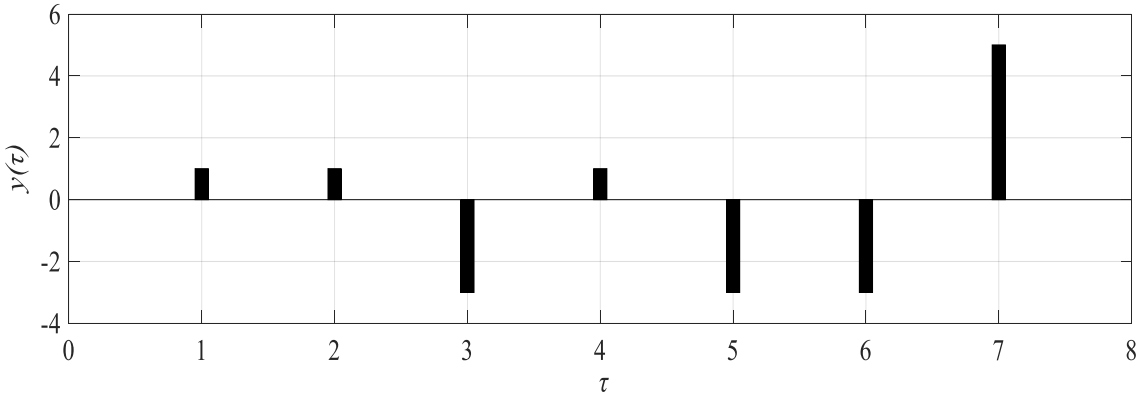

Рис. 1.5. Корреляционная функция
последовательности $Z = (1\ 1\ 1 - 1\ 1 - 1 - 1)$

2. Предварительное задание
(выполняется при подготовке к лабораторной работе)

2.1. Изучить теоретические принципы построения помехоустойчивых кодов.

2.2. Записать порождающую и проверочную матрицы $[6, 3, 3]$-кода.

2.3. Записать параметры кода, построенного в п. 2.2.

3. Порядок выполнения лабораторной работы

Лабораторная работа может выполняется с использованием ПК, с применением программирования в системе MATLAB. Лабораторная работа предусматривает выполнение экспериментальных исследований. В отчете представляются промежуточные расчеты, необходимое графическое описание, подтверждающие достоверность полученных экспериментальных результатов.

Исходные данные. Имеется источник на множестве символов алфавита $\{1, -1\}$. Этому множеству ставится в соответствие низкоскоростной $[15, 4, 8]$-код $\{X\} = \{X_1, \dots, X_{15}\}$. Код задается псевдослучайной последовательностью $X = (x_0 x_1 \dots x_{14})$ m-кода.

3.1. Построить множество ненулевых кодовых слов $[15, 4, 8]$-кода в виде матрицы $\boldsymbol{A}$ циклически сдвинутых псевдослучайных последовательностей. Порождающая код псевдослучайная последовательность имеет форму

$$X = (x_0 x_1 \dots x_{14}) = (-1 - 1 - 1 - 1\ 1 - 1\ 1 - 1 - 1\ 1\ 1 - 1\ 1\ 1\ 1).$$

3.2. Декодировать произвольно выбранное кодовое слово кода (п. 3.1) с использованием корреляционного алгоритма.

3.3. Декодировать входные кодированные сообщения (векторы) $\boldsymbol{Z}$:

$$\boldsymbol{Z}_1 = (-1\ -1\ -1\ -1\ 1\ 1\ 1\ -1\ -1\ 1\ 1\ -1\ 1\ 1\ 1),$$
$$\boldsymbol{Z}_2 = (1\ -1\ -1\ 1\ -1\ -1\ -1\ 1\ 1\ -1\ 1\ -1\ -1\ 1\ 1\ 1\ -1),$$
$$\boldsymbol{Z}_3 = (1\ 1\ 1\ -1\ 1\ 1\ -1\ -1\ -1\ 1\ 1\ -1\ 1\ -1\ -1\ -1\ -1),$$
$$\boldsymbol{Z}_4 = (1\ 1\ -1\ 1\ -1\ -1\ -1\ -1\ 1\ 1\ -1\ 1\ 1\ 1\ -1\ 1\ ).$$

Наряду с расчетными данными представить графические пояснения результатов декодирования.

3.4. Используя результаты п. 3.3, найти векторы ошибок $\boldsymbol{E}$ и определить местоположение ошибок в кодированных сообщениях.

4. СОДЕРЖАНИЕ ОТЧЕТА

3.1. Результаты выполнения предварительного задания.

3.2. Расчеты и графики лабораторного задания. Результаты экспериментальных исследований.

3.3. Анализ результатов и выводы.

5. Контрольные вопросы

1. Поясните физическую сущность помехоустойчивых кода, обнаруживающего и исправляющего t ошибок.

2. Поясните сущность параметров кодов, корректирующих ошибки.

3. В чем состоит различие понятий расстояние Хэмминга и кодовое расстояние кода.

4. Сколько ошибок может исправить и обнаружить код?

5. Поясните сущность основной теоремы кодировании для канала с шумом (вторая теорема Шеннона).

6. Поясните метод декодирования помехоустойчивых кодов на основе принципа максимального правдоподобия.

7. Почему стратегия декодирование помехоустойчивых кодов по минимуму расстояния Хэмминга является оптимальной.

8. Поясните понятие энергетических затрат на их передачу кода.

6. Список использования источников

1. Кудряшов, Б. Д. Основы теории кодирования : учеб. пособие / Б. Д. Кудряшов. – СПб. : БХВ-Петербург, 2016.

2. Кудряшов, Б. Д. Теория информации : учебник для вузов / Б. Д. Кудряшов. – СПб. : Питер, 2018.

3. Митюхин А. И. Прикладная теория информация. Минск, 2018.

4. Митюхин А. И. Элементы алгебры для теории кодирования. Akademikerverlag GmbH, Saarbrücken, Germany, 2013.

5. Ипатов В. Широкополосные системы и кодовое разделение каналов. Принципы и приложения. М., 2007

6. Теория прикладного кодирования : учеб. пособие. В 2 т. / В. К. Конопелько [и др.]. – Минск : БГУИР, 2004.

7. Ватолин, Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М. : Диалог-МИФИ, 2002.

8. Луенбергер, Д. Дж. Информатика / Д. Дж. Луенбергер. – М. : Техносфера, 2008.

9. Митюхин, А. И. Элементы алгебраических структур теории кодирования : учеб. пособие / А. И. Митюхин, Пачинин В. И. – Минск : БГУИР, 2012.

10. Вернер, М. Основы кодирования : учебник для вузов / М. Вернер. – М. : Техносфера, 2004.

11. Андерсон, Дж. А. Дискретная математика и комбинаторика / Дж. А. Андерсон; пер. с англ. – М. : Вильямс, 2004.

12. Лидл, Р. Конечные поля. В 2 т. / Р. Лидл, Г. Нидеррайдер. – М. : Мир, 1988.

13. Хаггарти, Р. Дискретная математика для программистов / Р. Хаггарти.– М. : Техносфера, 2005.

Учебное издание

Митюхин Анатолий Иванович

МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор
Корректор
Компьютерная верстка

Подписано в печать Формат 60×84 1/16 Бумага офсетная.
Гарнитура «Таймс» Отпечатано на ризографе Усл. печ. л.
Уч.-изд. л. Тираж 75 экз. Заказ 150

Издатель и полиграфическое исполнение: учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».
ЛИ № от ЛП № от
220013, Минск, П. Бровки, 6