Санкт-Петербургский Политехнический Университет Петра Великого
Институт компьютерных наук и технологий
Кафедра компьютерных систем и программных технологий

Телекоммуникационные технологии

Отчет по лабораторной работе №7
Помехоустойчивое кодирование

Работу выполнил:
Болдырев А.В.
Группа: 33501/3
Преподаватель:
Богач Н.В.

Санкт-Петербург
2017

Содержание

1. Цель и задачи

1.1. Цель работы

Изучение методов помехоустойчивого кодирования и сравнения их свойств.

1.2. Постановка задачи

Провести кодирование/декодирование сигнала, полученного с помощью функции randerr кодом Хэмминга 2-мя способами: с помощью встроенных функций encode/decode, а также через создание проверочной и генераторной матриц и вычисление синдрома. Оценить корректирующую способность кода.

Выполнить кодирование/декодирование циклическим кодом, кодом БЧХ, кодом Рида-Соломона. Оценить корректирующую способность кода.

2. Теоретическая информация

2.1. Кодирование

Физическое кодирование — линейное преобразование двоичных данных, осуществляемое для их передачи по физическому каналу (такому как оптическое волокно или витая пара). Физическое кодирование может менять форму, ширину полосы частот и гармонический состав сигнала в целях осуществления синхронизации приёмника и передатчика, устранения постоянной составляющей или уменьшения аппаратных затрат.

Обнаружение ошибок в технике связи — действие, направленное на контроль целостности данных при записи/воспроизведении информации или при её передаче по линиям связи. Исправление ошибок (коррекция ошибок) — процедура восстановления информации после чтения её из устройства хранения или канала связи.

Для обнаружения ошибок используют коды обнаружения ошибок, для исправления — корректирующие коды (коды, исправляющие ошибки, коды с коррекцией ошибок, помехоустойчивые коды).

2.2. Типы помехоустойчивого кодирования

2.2.1. Кодирование Хэмминга

Коды Хемминга — простейшие линейные коды с минимальным расстоянием 3, то есть способные исправить одну ошибку. Код Хемминга может быть представлен в таком виде, что синдром

$$\vec{s} = \vec{r}H^T \tag{1}$$

Это принятый вектор, будет равен номеру позиции, в которой произошла ошибка. Это свойство позволяет сделать декодирование очень простым.

Коды Хэмминга являются самоконтролирующимися кодами, то есть кодами, позволяющими автоматически обнаруживать ошибки при передаче данных. Для их построения достаточно приписать к каждому слову один добавочный (контрольный) двоичный разряд и выбрать цифру этого разряда так, чтобы общее количество единиц в изображении любого числа было, например, нечетным. Одиночная ошибка в каком-либо разряде передаваемого слова (в том числе, может быть, и в контрольном разряде) изменит четность общего количества единиц. Счетчики по модулю 2, подсчитывающие количество единиц, которые содержатся среди двоичных цифр числа, могут давать сигнал о наличии ошибок.

При этом невозможно узнать, в каком именно разряде произошла ошибка, и, следовательно, нет возможности исправить её. Остаются незамеченными также ошибки, возникающие одновременно в двух, четырёх, и т. д. — в четном количестве разрядов. Впрочем, двойные, а тем более четырёхкратные ошибки полагаются маловероятными.

Коды, в которых возможно автоматическое исправление ошибок, называются самокорректирующимися. Для построения самокорректирующегося кода, рассчитанного на исправление одиночных ошибок, одного контрольного разряда недостаточно. Как видно из дальнейшего, количество контрольных разрядов k должно быть выбрано так, чтобы удовлетворялось неравенство

$$2^k \geq k + m + 1 \tag{2}$$

или

$$k \geq \log_2(k + m + 1) \tag{3}$$

где m — количество основных двоичных разрядов кодового слова.

Минимальные значения k при заданных значениях m, найденные в соответствии с этим неравенством, приведены в таблице.

Диапазон m	k_{min}
1	2
2-4	3
5-11	4
12-26	5
27-57	6

Рис. 2.2.1. Значения K_{min} в зависимости от m.

В настоящее время наибольший интерес представляют двоичные блочные корректирующие коды. При использовании таких кодов информация передаётся в виде блоков одинаковой длины и каждый блок кодируется и декодируется независимо друг от друга. Почти во всех блочных кодах символы можно разделить на информационные и проверочные. Таким образом, все комбинации кодов разделяются на разрешенные (для которых соотношение информационных и проверочных символов возможно) и запрещенные.

Построение кодов Хэмминга основано на принципе проверки на четность числа единичных символов: к последовательности добавляется такой элемент, чтобы число единичных символов в получившейся последовательности было четным.

$$r_1 = i_1 \oplus i_2 \oplus ... \oplus i_k \tag{4}$$

где $\oplus$ - операция XOR.

$$S = i_1 \oplus i_2 \oplus ... \oplus i_n \oplus r_1 \tag{5}$$

Тогда если $S = 0$ - ошибки нет, иначе есть однократная ошибка.

Такой код называется $(k + 1, k)$ или $(n, n - 1)$. Первое число — количество элементов последовательности, второе — количество информационных символов.

Для каждого числа проверочных символов $r = 3, 4, 5..$ существует классический код Хэмминга с маркировкой $(n, k) = (2^r - 1, 2^r - 1 - r)$, то есть — $(7, 4), (15, 11), (31, 26)$. При иных значениях k получается так называемый усеченный код, например международный телеграфный код МТК-2, у которого $k = 5$. Для него необходим код Хэмминга $(9, 5)$, который является усеченным от классического $(15, 11)$.

Для примера рассмотрим классический код Хемминга $(7, 4)$. Сгруппируем проверочные символы следующим образом:

$$r_1 = i_1 \oplus i_2 \oplus i_3 r_2 = i_2 \oplus i_3 \oplus i_4 r_3 = i_1 \oplus i_2 \oplus i_4 \tag{6}$$

Получение кодового слова выглядит следующим образом:

$$(i_1\ i_2\ i_3\ i_4) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (i_1\ i_2\ i_3\ i_4\ r_1\ r_2\ r_3) \tag{7}$$

На вход декодера поступает кодовое слово $V = (i_1', i_2', i_3', i_4', r_1', r_2', r_3')$ где штрихом помечены символы, которые могут исказиться в результате помехи. В декодере в режиме исправления ошибок строится последовательность синдромов:

$S_1 = r_1 \oplus i_1 \oplus i_2 \oplus i_3$

$S_2 = r_2 \oplus i_2 \oplus i_3 \oplus i_4$

$S_3 = r_3 \oplus i_1 \oplus i_2 \oplus i_4$

$S = (S_1, S_2, S_3)$ называется синдромом последовательности.

Получение синдрома выглядит следующим образом:

$$(i_1\ i_2\ i_3\ i_4\ r_1\ r_2\ r_3) \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} S_1 & S_2 & S_3 \end{pmatrix} \tag{8}$$

Кодовые слова $(7, 4)$ кода Хэмминга:

i_1	i_2	i_3	i_4	r_1	r_2	r_3
0	0	0	0	0	0	0
0	0	0	1	0	1	1
0	0	1	0	1	1	0
0	0	1	1	1	0	1
0	1	0	0	1	1	1
0	1	0	1	1	0	0
0	1	1	0	0	0	1
0	1	1	1	0	1	0
1	0	0	0	1	0	1
1	0	0	1	1	1	0
1	0	1	0	0	1	1
1	0	1	1	0	0	0
1	1	0	0	0	1	0
1	1	0	1	0	0	1
1	1	1	0	1	0	0
1	1	1	1	1	1	1

Рис. 2.2.2. Кодовые слова $(7, 4)$ кода Хэмминга.

Синдром $(0, 0, 0)$ указывает на то, что в последовательности нет искажений. Каждому ненулевому синдрому соответствует определенная конфигурация ошибок, которая исправляется на этапе декодирования.

Для кода $(7, 4)$ в таблице указаны ненулевые синдромы и соответствующие им конфигурации ошибок (для вида: $i_1 i_2 i_3 i_4 r_1 r_2 r_3$).

Синдром	001	010	011	100	101	110	111
Конфигурация ошибок	0000001	0000010	0001000	0000100	1000000	0010000	0100000
Ошибка в символе	r_3	r_2	i_4	r_1	i_1	i_3	i_2

Рис. 2.2.3. Ненулевые синдромы для различных конфигураций ошибок в сообщении.

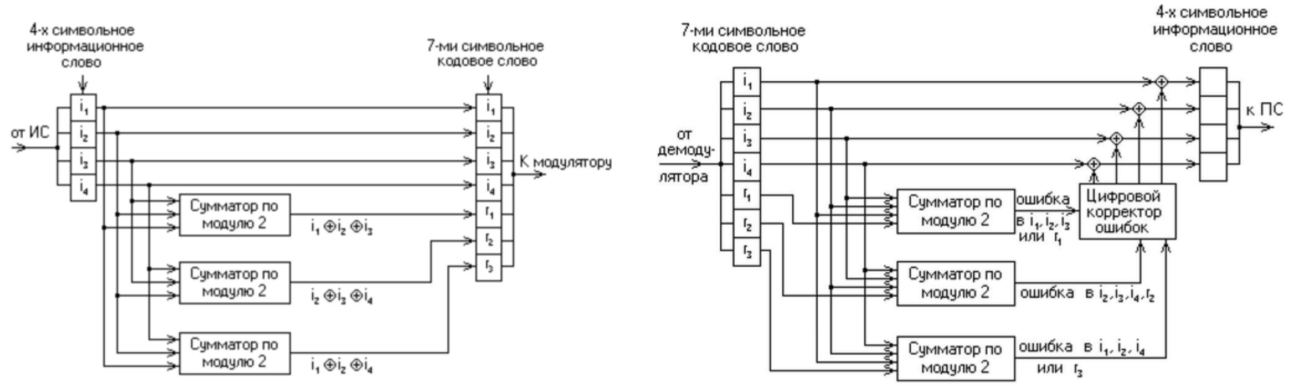

Рис. 2.2.4. Устройство кодера/декодера Хэмминга.

2.2.2. Циклические коды

Циклический код — линейный код, обладающий свойством цикличности, то есть каждая циклическая перестановка кодового слова также является кодовым словом. Используется для преобразования информации для защиты её от ошибок.

2.2.3. Коды Боуза-Чоудхури-Хоквингема (БЧХ)

Коды Боуза — Чоудхури — Хоквингема (БЧХ-коды) — в теории кодирования это широкий класс циклических кодов, применяемых для защиты информации от ошибок. Отличается возможностью построения кода с заранее определёнными корректирующими свойствами, а именно, минимальным кодовым расстоянием. Частным случаем БЧХ-кодов является код Рида — Соломона.

2.2.4. Коды Рида-Соломона

Коды Рида — Соломона (англ. Reed–Solomon codes) — недвоичные циклические коды, позволяющие исправлять ошибки в блоках данных. Элементами кодового вектора являются не биты, а группы битов (блоки). Очень распространены коды Рида — Соломона, работающие с байтами (октетами).

Код Рида — Соломона является частным случаем БЧХ-кода.

В настоящее время широко используется в системах восстановления данных с компакт-дисков, при создании архивов с информацией для восстановления в случае повреждений, в помехоустойчивом кодировании.

3. Ход работы

Реализация различных типов кодирования с помощью MATLAB:

Листинг 1: Код в МатЛаб

```
% n = 15;
%
% params = bchgenpoly(n);
% n = params(1,1);
%
% k = params(1,2);
% m = log2(n+1);
```

```
% msg = randint(100,1,[0,2^k-1]);
%
% codehamming = encode(msg,n,k,'hamming/decimal');
% [parmat,genmat] = hammgen(m);
% codehamming2 = encode(msg,n,k,'linear/decimal',genmat);
% if codehamming==codehamming2
% disp('The ''linear'' method can create Hamming code.')
% end
% codebch = encode(msg,n,k,'bch/decimal');
% codecyclic = encode(msg,n,k,'cyclic/decimal');
%
% decodedhamming = decode(codehamming,n,k,'hamming/decimal');
% decodedbch = decode(codebch,n,k,'bch/decimal');
% decodedcyclic = decode(codecyclic,n,k,'cyclic/decimal');
% if (decodedhamming==msg & decodedbch==msg & decodedcyclic==msg)
% disp('All decoding worked flawlessly in this noiseless world.')
% end


% n = 10;
% k = 5;
% out = randerr(2,5);
% disp(out);
% out_enc = encode(out, n, k, 'hamming');

out = randerr(1,4);
code = encode (out, 7, 4, 'hamming/binary');
dcode = decode (code, 7, 4, 'hamming/binary');
if (dcode == out) disp('Got it!'); end;
```

3.1. Коды Хэмминга

3.2. Циклические коды

3.3. Коды Боуза-Чоудхури-Хоквингема (БЧХ)

3.4. Коды Рида-Соломона

4. Выводы

Кодирование - важный процесс при передаче сигналов по каналам связи. Методы кодирования дополняют методы модуляции для обеспечения улучшения качества передачи, для предотвращения ошибок при передаче, а также защищенности данных от получения злоумышлинниками. Рассмотрены различные методы кодирования - коды Хэмминга, циклические коды, коды Боуза-Чоудхури-Хоквингема, коды Рида-Соломона.