**МИНОБРНАУКИ РОССИИ**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»  
(БГТУ им. В.Г.Шухова)**

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Лабораторная работа №5  
дисциплина: Теория Информации  
тема: «**Помехоустойчивое кодирование. Код Хемминга**»

Выполнил: ст. группы ВТ-22  
Воскобойников И. С.

Выполнение: \_\_\_\_\_\_\_\_\_\_

Защита: \_\_\_\_\_\_\_\_\_\_

Белгород 2020

**Цель работы:** научиться строить порождающую и проверочную матрицу для кода Хемминга. Научиться строить код Хемминга по матрице. Научиться вычислять синдром.

**Выполнение**

**Задание №1**

Построить систематический код Хемминга для m=4. Вычислить n и k. Вычислить размеры порождающей и проверочной матрицы. Построить проверочную матрицу. Получить проверочную подматрицу порождающей матрицы. Сформировать порождающую матрицу.

m = 4 – исходное число проверочных битов

m = 4; n = 15; k = 11;

1 Проверочная матрица

H m\*n = H 4\*15 =

2 Порождающая матрица

P = P’ =

С k \* n = С 11 \* 15 =

**Задание №2**

Взять произвольное ненулевое двоичное информационное слово i длиной 11. Получить кодовое слово c, полученное перемножением информационного слова и порождающей матрицы.

Произвольное i = 11110001111 С = i \* G

11110001111 \* = 111111100001111

**Задание №3**

Внести в кодовое слово c произвольную ошибку (инвертировать любой бит слова). Вычислить синдром. Локализовать ошибку и исправить её. Получить информационное слово. Убедиться в идентичности полученного информационного и изначального слов.

Инвертируем 5 бит, тогда = 111101100001111= y

\* HT = (0, 1, 0, 1) => Ошибка в 5 бите

111101100001111 \* = 0101   
Видим ошибку в 5 бите, инвертируем его

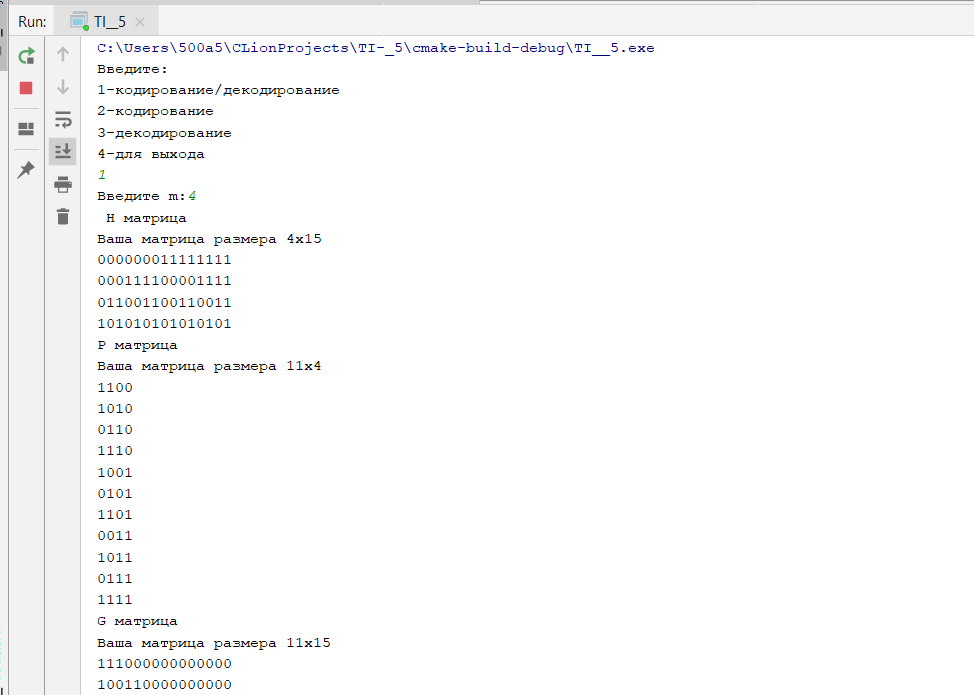
111101100001111

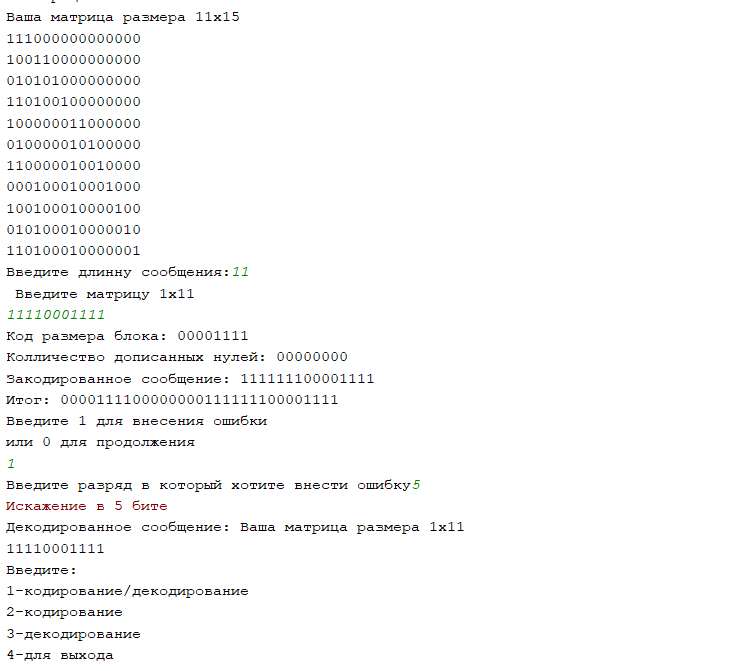
Снова умножим на HT, получим 0000 => верно

4. Создать подпрограмму для реализации алгоритма помехоустойчивого кодирования по Хеммингу для m=4. На вход подпрограммы передаётся информационное слово. Подпрограмма возвращает кодовое слово.

5. Создать подпрограмму для декодирования кодового слова с учётом возможной ошибки. На вход подпрограммы передаётся кодовое слово. Подпрограмма вычисляет синдром, и при наличии ошибки исправляет её. Далее подпрограмма выделяет информационные биты и возвращает информационное слово.

6.Создать программу, демонстрирующую работу подпрограмм. Программа позволяет пользователю ввести информационное слово. Далее вызывается первая подпрограмма, и слово кодируется, затем заносится или не заносится случайная ошибка. Далее программа вызывает вторую подпрограмму и декодирует кодовое слово, исправляя ошибку. Результат каждого этапа выводится на экран.





Ответы:

1. Определение блокового кодирования. Определение двоичного (п,к)-кода.

**Блоковое кодирование** — в информатике тип канального кодирования. Он увеличивает избыточность сообщения так, чтобы в приёмнике можно было расшифровать его с минимальной (теоретически нулевой) погрешностью, при условии, что скорость передачи информации (количество передаваемой информации в битах в секунду) не превысила бы канальную производительность. **Двоичный код** — это способ представления данных в виде кода, в котором каждый разряд принимает одно из двух возможных значений, обычно обозначаемых цифрами 0 и 1

2. Расстояние по Хэммингу.

**Расстояние Хэмминга** — число позиций, в которых соответствующие символы двух слов одинаковой длины различны. В более общем случае расстояние Хэмминга применяется для строк одинаковой длины любых *q*-ичных алфавитов и служит метрикой различия (функцией, определяющей расстояние в метрическом пространстве) объектов одинаковой размерности.

3. Корректирующая способность кода. Линейные блочные коды. Вес Хэмминга и проверочная матрица; их роль в кодировании и декодировании. Систематический код.

**Корректирующая способность -** характеристика t {\displaystyle t} кодаC {\displaystyle C}, описывающая возможность исправить ошибки в кодовых словах. Определяется как целое число, меньшее половины от минимального расстояния d min {\displaystyle d\_{\min }} между кодовыми словами минус один в принятой метрике кода.

**Линейные блочные** коды позволяют представить информационные и ко-довые слова в виде двоичных векторов, что позволяет описать процессы ко-дирования и декодирования с помощью аппарата линейной алгебры, с учетом того, что компонентами вводимых векторов и матриц являются символы«0» и «1». Операции над двоичными компонентами производятся при этом поправилам арифметики по модулю 2.

Кол-во единиц в синдроме кода Хэмминга называют его **«весом».**

**Правила формирования проверочной матрицы:**

1. Транспонируем дописанную подматрицу производящей матрицы;
2. Дописываем к транспонированной подматрицы единичной матрицы

Произведение некоторого кодового слова G*i'*, т.е. с ошибкой, на транспонированную **проверочную матрицу** называется синдромом и обозначается Si: **G*i'*·*H(n, k)T= Si*.**

**Систематический** **код**–**код**, содержащий в себе кроме информационных контрольные разряды.

4. Примитивный код Хэмминга. Его параметры. Проверочная и порождающая матрицы. Корректирующая способность кода Хэмминга.

**Код Хэмминга** – биочный систематический код, то есть состоящий из информационных и корректирующих символов, расположенных по строго определенной системе, имеющих одинаковую длину и всегда занимающих строго определенные места в кодовых комбинациях.

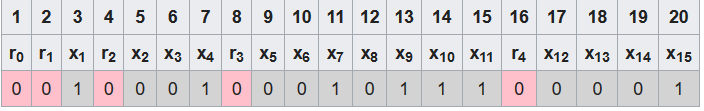
**Параметры помехоустойчивого кодирования:**

* 1. Первый параметр, **скорость кода R** характеризует долю информационных («полезных») данных в сообщении и определяется выражением: ***R=k/n=k/m+k***
  2. Второй параметр, **кратность обнаруживаемых ошибок** – количество ошибочных символов, которые код может обнаружить.
  3. Третий параметр, **кратность исправляемых ошибок** – количество ошибочных символов, которые код может исправить (обозначается буквой t).

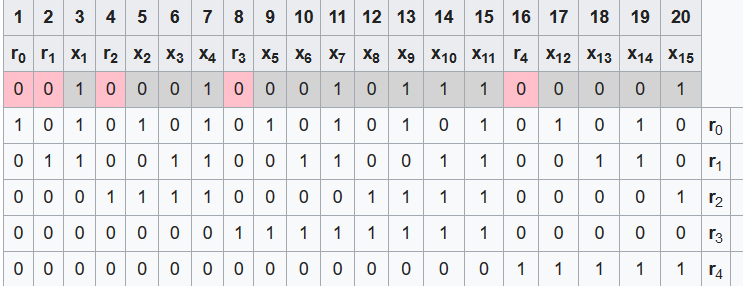
Понятие **корректирующей способности кода** связывают с возможностью обнаружения и исправления ошибки. Количественно корректирующая способность кода определяется вероятностью обнаружения или исправления ошибки.

**Проверочная матрица** в систематическом виде строится на основе матрицы G(n,k), а именно: H(n, k) = |R\*(k,r), I(k)|  
 I(k) - единичная матрица  
 R\*(k,r) - матрица в транспонированном виде из G(n,k)

5. Процесс кодирования и декодирования по Хэммингу.

Предположим, что нужно сгенерировать код Хэмминга для некоторого информационного кодового слова. В качестве примера возьмём 15-битовое кодовое слово **x**1…**x**15, хотя алгоритм пригоден для кодовых слов любой длины. В приведённой ниже таблице в первой строке даны номера позиций в кодовом слове, во второй — условное обозначение битов, в третьей — значения битов.  Вставим в информационное слово контрольные биты **r**0…**r**4 таким образом, чтобы номера их позиций представляли собой целые степени двойки: 1, 2, 4, 8, 16… Получим 20-разрядное слово с 15 информационными и 5 контрольными битами. Первоначально контрольные биты устанавливаем равными нулю. На рисунке контрольные биты выделены розовым цветом.  В общем случае количество контрольных бит в кодовом слове равно двоичному логарифму числа, на единицу большего, чем количество бит кодового слова (включая контрольные биты); логарифм округляется в большую сторону. Например, информационное слово длиной 1 бит требует двух контрольных разрядов, 2-, 3- или 4-битовое информационное слово — трёх, 5…11-битовое — четырёх, 12…26-битовое — пяти и т. д.

Добавим к таблице 5 строк (по количеству контрольных битов), в которые поместим матрицу преобразования. Каждая строка будет соответствовать одному контрольному биту (нулевой контрольный бит — верхняя строка, четвёртый — нижняя), каждый столбец — одному биту кодируемого слова. В каждом столбце матрицы преобразования поместим двоичный номер этого столбца, причём порядок следования битов будет обратный — младший бит расположим в верхней строке, старший — в нижней. Например, в третьем столбце матрицы будут стоять числа 11000, что соответствует двоичной записи числа три: 00011.

 В правой части таблицы мы оставили пустым один столбец, в который поместим результаты вычислений контрольных битов. Вычисление контрольных битов производим следующим образом. Берём одну из строк матрицы преобразования (например, r0) и находим её скалярное произведение с кодовым словом, то есть перемножаем соответствующие биты обеих строк и находим сумму произведений. Если сумма получилась больше единицы, находим остаток от его деления на 2. Иными словами, мы подсчитываем сколько раз в кодовом слове и соответствующей строке матрицы в одинаковых позициях стоят единицы и берём это число по модулю 2.

Если описывать этот процесс в терминах матричной алгебры, то операция представляет собой перемножение матрицы преобразования на матрицу-столбец кодового слова, в результате чего получается матрица-столбец контрольных разрядов, которые нужно взять по модулю 2.

Например, для строки r0:

r0 = (1·0+0·0+1·1+0·0+1·0+0·0+1·1+0·0+1·0+0·0+1·1+0·0+1·1+0·1+1·1+0·0+1·0+0·0+1·0+0·1) mod 2 = 5 mod 2 = 1.

Полученные контрольные биты вставляем в кодовое слово вместо стоявших там ранее нулей. По аналогии находим проверочные биты в остальных строках. Кодирование по Хэммингу завершено. Полученное кодовое слово — 11110010001011110001.

Алгоритм декодирования по Хэммингу абсолютно идентичен алгоритму кодирования. Матрица преобразования соответствующей размерности умножается на матрицу-столбец кодового слова и каждый элемент полученной матрицы-столбца берётся по модулю 2. Полученная матрица-столбец получила название «матрица синдромов». Легко проверить, что кодовое слово, сформированное в соответствии с алгоритмом, описанным в предыдущем разделе, всегда даёт нулевую матрицу синдромов.

Матрица синдромов становится ненулевой, если в результате ошибки (например, при передаче слова по линии связи с шумами) один из битов исходного слова изменил своё значение. Предположим для примера, что в кодовом слове, полученном в предыдущем разделе, шестой бит изменил своё значение с нуля на единицу (на рисунке обозначено красным цветом). Тогда получим следующую матрицу синдромов.

6. Синдромное декодирование. Локализация ошибок в коде Хэмминга

Слово "синдром" означает обычно совокупность признаков, характерных для того или иного явления. Такой же примерно смысл имеет понятие "синдром" и в теории кодирования. Синдром вектора, содержащего, быть может, ошибки, дает возможность распознать наиболее вероятный характер этих ошибок.