Министерство высшего образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
Санкт-Петербургский государственный университет аэрокосмического приборостроения

КАФЕДРА № 52

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

ассистент		А. А. Бурков
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

ИСПОЛЬЗОВАНИЕ ЦИКЛИЧЕСКИХ КОДОВ ДЛЯ ОБНАРУЖЕНИЯ ОШИБОК В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

по курсу: Сети и системы передачи информации

РАБОТУ ВЫПОЛНИЛА

СТУДЕНТ ГР. №	5711		Е.С. Шамакова
		подпись, дата	инициалы, фамилия

Санкт-Петербург 2020

Цель работы
Исследование типового алгоритма формирования контрольной суммы с использованием циклических кодов, использование численного расчета и имитационного моделирования для оценки вероятности того, что декодер не обнаружит ошибки.
Задача
• Разработать программу, с помощью которой путем имитационного моделирования оценивается вероятность ошибки декодирования при передаче данных по двоично-симметричному каналу. Исходными данными для работы программы являются: порождающий многочлен $g(x)$, длина кодируемой последовательности l (может быть как больше, так и меньше k) и точность ε, с которой программа оценивает вероятность ошибки декодирования. С помощью программы исследовать зависимость вероятности ошибки декодирования от значения вероятности появления ошибки в канале при различных значениях l.
• Исследовать как изменится зависимость оценки ошибки декодирования $\widehat{Pe}$ от вероятности ошибки в канале p при смене модели канала как показано на *рис. 7*. Обосновать полученный результат.

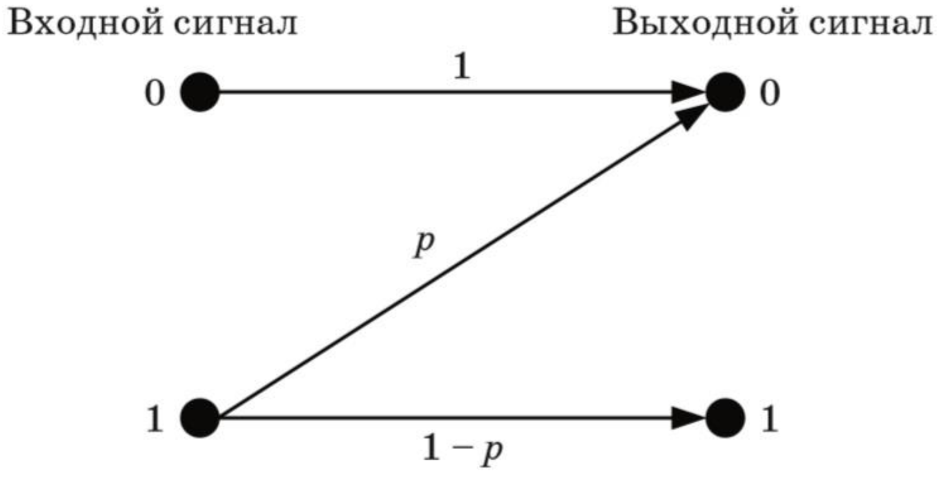

Рис. 7. Измененная модель канала

1. **Описание моделируемой системы**
   На вход кодера поступает некоторое информационное сообщение $\overline{m}$, состоящее из нулей и единиц. Кодер по некоторому алгоритму вычисляет контрольную сумму, дописывает ее к передаваемому сообщению и таким образом формирует закодированное сообщение $\bar{a}$ так же состоящее из 0 и 1.
   В канале могут произойти ошибки, в результате которых некоторые биты сообщения инвертируются $\overline{b}$ (0 становиться 1 или 1 становиться 0). Вектор ошибок $\bar{e}$ показывает на каких позициях произошла ошибка, при этом канал может быть описан как операция XOR передаваемого сообщения и вектора ошибок ($\bar{a} \oplus \bar{e}$). Декодер по некоторому алгоритму проверяет контрольную сумму в принятом сообщении и принимает одно из следующих решений (синдром):

$$E = \begin{cases} 1, \text{если была ошибка;} \\ 0, \text{если не было ошибок.} \end{cases}$$

На рис. 1 изображена структурная схема рассматриваемой в лабораторной работе системы передачи данных.

Рисунок 1 – Структурная схема системы передачи данных.

$\overline{m}$ – информационное сообщение, К – блок кодера, $\overline{a}$ – закодированное сообщение, $\overline{e}$ – вектор ошибок, $\overline{b}$ – сообщение на выходе канала, Д – блок декодера, E –принятое решение, $\overline{m'}$ – сообщение на выходе декодера.

2. **Описание проводимого исследования и рассматриваемого алгоритма**

Пусть задан порождающий многочлен $g(x)$, длина кодируемой последовательности k. Необходимо оценить вероятность ошибки декодирования $\widehat{Pe}$ с заданной точностью ε при использовании имитационного моделирования.

Алгоритм действия:

1. Формируется множество кодовых сообщений по алгоритму:
   • Генерируются всевозможные сообщения $\overline{m}$ длиной l;
   • Для каждого вектора $\overline{m}$ формируется многочлен $m(x)$. Степень многочлена $m(x)$ при этом меньше или равна l −1;
   • Вычисляется многочлен $c(x) = (m(x) * x^r) \; mod \; g(x)$, где r – степень многочлена $g(x)$. Степень многочлена $c(x)$ при этом меньше или равна r −1;
   • Вычисляется многочлен $a(x) = \; m(x) * x^r + c(x)$;
   • На основе многочлена $a(x)$ формируется вектор $\overline{a}$, длина которого n бит, где $n = k + r$.
2. Из множество кодовых сообщений выбирается вектор $\overline{a}$ случайным образом.
3. Генерируется случайный вектор ошибок $\overline{e}$, где для каждой позиции случайно выбирается событие:
   • произошла ошибка с вероятностью p (бит вектора ошибок = 1);
   • ошибки не было с вероятностью 1− p (бит вектора ошибок = 0).
4. Вектор ошибки складывается с результатом кодирования (операция XOR) для получения выхода канала $\overline{b}$.
5. Вычисляется синдром: $s(x) \; = \; b(x) \; mod \; g(x)$:
   • если s(x) = 0, то E = 0;
   • если s(x) ≠ 0, то E = 1.

6. Определяется, были ошибки или нет:
   • Ошибка была, если $\bar{e} \neq 0$ и E = 0;
   • Ошибки не было, если $\bar{e} \neq 0$ и E = 1.

   Данная процедура со 2 шага повторяется N раз. Если в результате моделирования Ne раз произошли ошибки декодирования, то вероятность ошибки декодирования вычисляется по следующей формуле:

$$\widehat{P_e} = \frac{N_e}{N}$$

   Тогда ε = $|Pe - \widehat{Pe}|$, где Pe – теоретическая вероятность декодирования.

   Для определения примерного количества необходимых итераций моделирования N при заранее заданной требуемой точности полученных результатов ε используется формула:

$$N = \frac{9}{4\varepsilon^2}$$

   Следует отметить, что данный подход для определения числа экспериментов N можно использовать только когда известно, что эксперименты, проводимые при имитационном моделировании, независимы друг от друга. В рамках данной лабораторной работы рассматривается канал без памяти, следовательно, эксперименты независимы друг от друга.

   Вычисление ошибки декодирования производится для информационных сообщений разной длины, а также для различной вероятности ошибки в двоичном канале.

   Для следующей задачи изменилась генерация вектора ошибки $\bar{e}$:
   - В случае если в передаваемой последовательности i-тый бит ноль, тогда он передаётся без ошибки, т.е. $\bar{e}_i$ = 0;
   - В случае если в передаваемой последовательности i-тый бит единица, тогда с вероятностью p $\bar{e}_i$ = 1 (произошла ошибка), и с вероятностью 1-p $\bar{e}_i$ = 0 (бит передан верно).

3. **Описание моделирующей программы в виде псевдокода**

   Задание 1.

```
Задать порождающий многочлен g, вероятности ошибки в двоично-
симметричном канале p, допустимую разницу теоретичеой и
полученной вероятности ошибки ε. Вычислить количество
необходимых экспериментов N с учетом ε.
for от минимальной до максимальной длины информационного слова
   count = 0;
   Ne = 0;
   Построить кодовую книгу;
   while count < N
         Выбрать случайным образом слово a из кодовой книги;
         Сформировать вектор ошибки с учетом p;
         Получить вектор b = a xor e;
```

```
            Вычислить синдром E;
            if E=0 и ē≠ 0
                  Ne=Ne+1;
            Nt=Nt+1;
      Вычислить вероятность ошибки декодирования: Pe=Ne/Nt;
Построить график вероятности ошибки декодирования от длины
информационного слова.
```

Задание 2.

```
Задать порождающий многочлен g, сформировать множество кодовых
сообщений, допустимую разницу теоретической и полученной
вероятности ошибки ε. Вычислить количество необходимых
экспериментов N с учетом ε.
   for от минимальной (0) до максимальной (1) вероятности ошибки в
   канале
      count = 0;
      Ne = 0;
      while count < N
            Выбрать случайным образом слово a из кодовой книги;
            Сформировать вектор ошибки:
            if a[i] = 0
                  e[i]=0;
            if a[i] =1
                  с вероятностью p e[i]=1;
                  с вероятностью 1-p e[i]=0;
            Получить вектор b = a xor e;
            Вычислить синдром E;
            if E=0 и ē≠ 0
                  Ne=Ne+1;
            Nt=Nt+1;
      Вычислить вероятность ошибки декодирования: Pe=Ne/Nt;
Построить график вероятности ошибки декодирования от вероятности
ошибки в канале.
```

4. **Результаты проводимых исследований и зависимости**

Результаты проводимых исследований представлены для: $g(x) = x3 + x + 1, d = 3,\ k = 4,\ \varepsilon = 0{,}005$.

В результате выполнения исследования были получены графики зависимость вероятности ошибки декодирования от длины информационного сообщения *l* при различных вероятностях ошибки в двоично-симметричном канале *p*.

При вероятностях ошибки p=1 (Рисунок 2), вектор ошибки будет состоять из всех единиц, таким образом при k=4 вектор ошибки принадлежит множеству кодовых слов, и декодер всегда будет ошибаться (утверждение №2). При увеличении или уменьшении длины информационного сообщения *l*, изменяется кодовая книга и в ней отсутствует данный вектор ошибки, поэтому при различных $l\ \neq k$ кодер ошибаться не будет.

В случае, когда p=0 (Рисунок 4), вектор ошибки состоит из нулей, передаваемая информация передается без ошибок, декодер не ошибается при всех возможных *l*.

При p=0,7 (Рисунок 3), вероятность ошибки декодера максимальна при l=k, это обусловлено тем, что вероятность появления единичного вектора ошибки велика, а значит велика и вероятность ошибки декодера.
При p=0,3 (Рисунок 5), если число ошибок не превысит d-1, то декодер всегда обнаружит ошибку (по утверждению №3). Пока $l < k$ вероятность того, что вес вектора ошибки будет больше или равен d мала, при $l > k$, минимальное расстояние кода d уменьшается, следовательно декодер чаще ошибается (график с увеличением p возрастает).

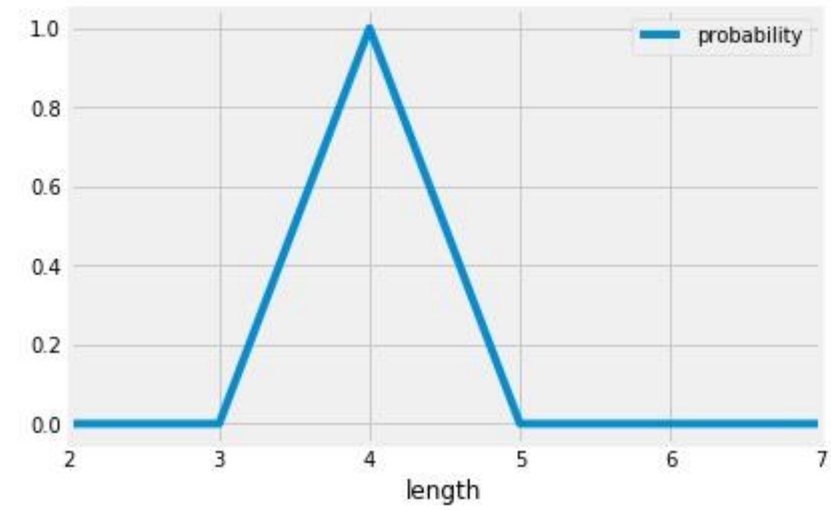

Рисунок 2 – Зависимость вероятности ошибки декодирования от длины информационного слова, при p=1.

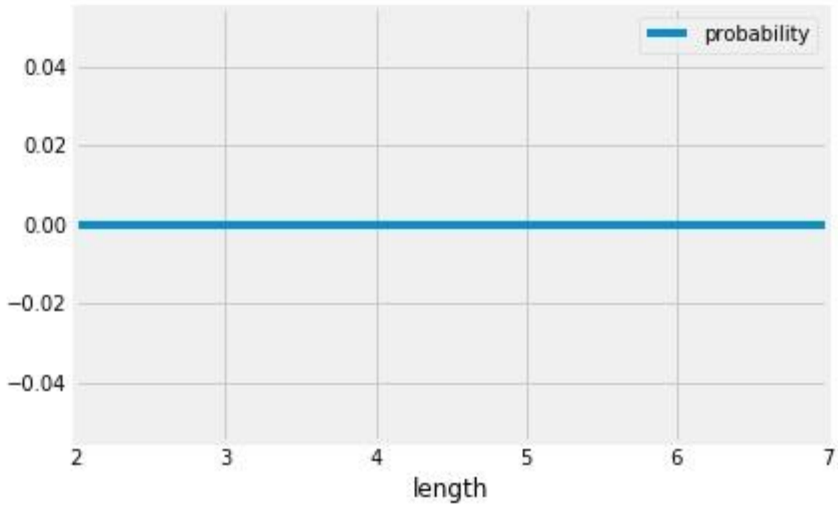

Рисунок 3 – Зависимость вероятности ошибки декодирования от длины информационного слова, при p=0.

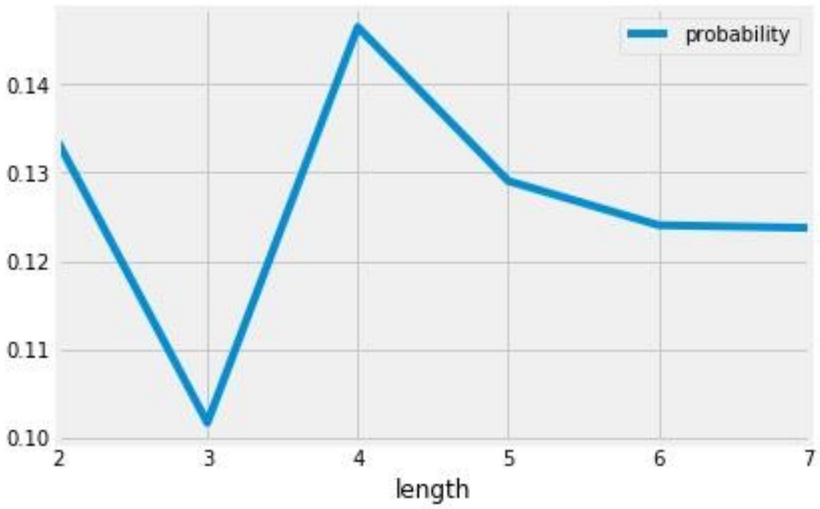

Рисунок 4 – Зависимость вероятности ошибки декодирования от длины информационного слова, при p=0,7.

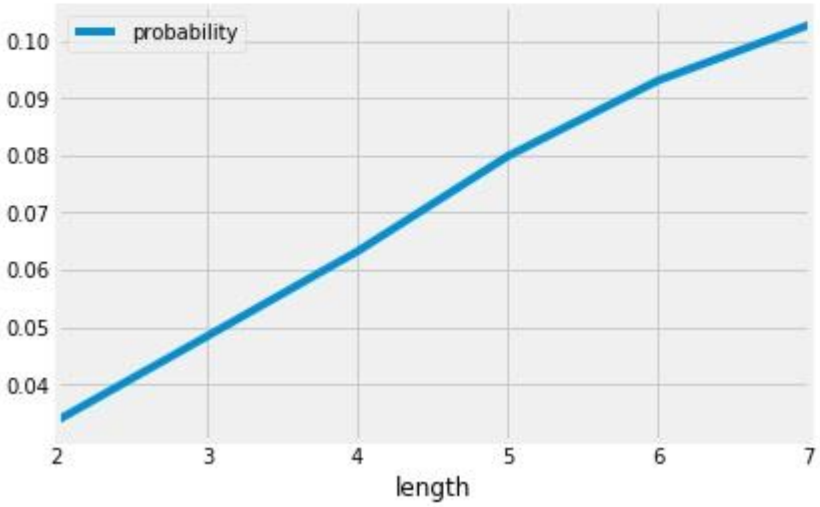

Рисунок 5 – Зависимость вероятности ошибки декодирования от длины информационного слова, при p=0,3.

Также была получена зависимость оценки ошибки декодирования от вероятности ошибки в двоично-симметричном канале при модели канала, представленного на рисунке 7. Графики построены для двух многочленов: $g(x) = x^3 + x + 1$ и $g(x) = x^4 + x + 1$. По графику, приведённому на рисунке 6 можно заметить, что с увеличением вероятности ошибки в канале вероятность ошибки в декодере также возрастает. При это для многочлена 3 степени график лежит выше, это объясняется тем, что чем меньше степень, тем соответственно меньше длина кодового сообщения и количество единиц в составе сообщения больше, следовательно, в связи с тем, что в данной модели канала ошибки происходят только при приёме 1, вероятность ошибки с увеличением степени уменьшается. Данное утверждение было проверено на $g(x) = x^5 + x^2 + 1$ и $g(x) = x^8 + x^4 + x^3 + x^2 + 1$ (рисунок 7)

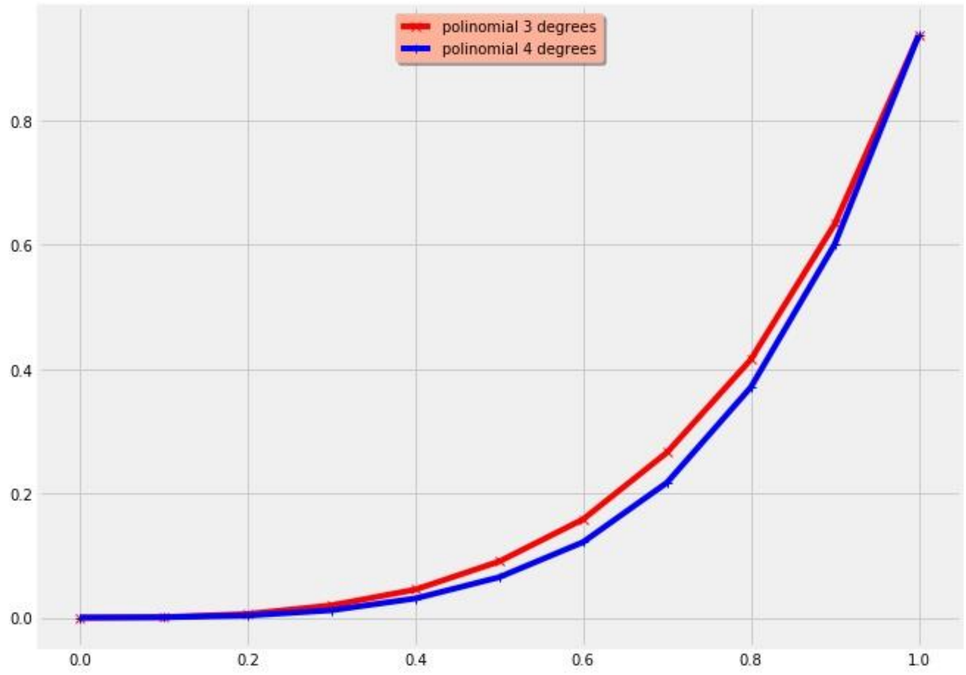

Рисунок 6 – Зависимость вероятности ошибки декодирования от вероятности ошибки в канале для 2 многочленов.

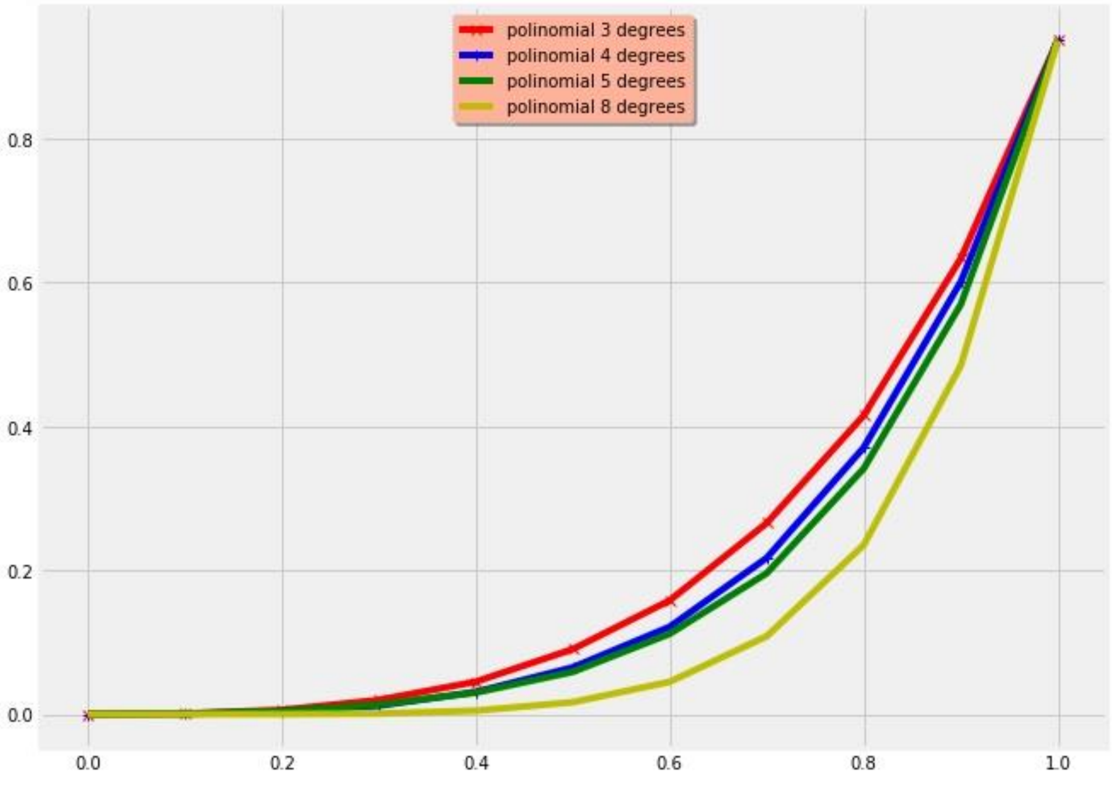

Рисунок 7 – Зависимость вероятности ошибки декодирования от вероятности ошибки в канале для 4 многочленов.