САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Факультет Безопасности Информационных Технологий

ОТЧЁТ

по специальной задаче

Выполнил:

Студент группы N3350

Фам Суан Кань

Проверил: Якуба Н. В.

Санкт-Петербург

2020

1. Задача

Реализовать модель системы связи:

- Модель канала – двоичный симметричный канал (ДСК)
- Используемый код – код Рида-Соломона
- Алгоритм кодирования – систематический
- Алгоритм декодирования – алгоритм Берлекэмпа-Месси

2. Краткое описание реализованных алгоритмов

Рассматривались коды Рида-Соломона над полем Галуа $GF(2^m)$

Кодирование:

Кодирование состоит у множении информационного полинома на порождающий многочлен $g(x)$.

$$g(x) = \left(x - \alpha^b\right)\left(x - \alpha^{b+1}\right) \dots (x - \alpha^{b+2t-2})$$

где $b -$ первый последовательный корень,

$t -$ максимальное количество ошибок, которые можно исправить

Умножение исходного слова S длины k на порождающий многочлен при систематическом кодировании можно выполнить следующим образом:

- К исходному слову приписываются $2t$ нулей, получается полином $T = Sx^{2t}$
- Этот полином делится на порождающий полином G, находится остаток R, $Sx^{2t} = QG + R$, где $Q -$ частное
- Этот остаток и будет корректирующим кодом Рида — Соломона, он приписывается к исходному блоку символов. Полученное кодовое слово $C = Sx^{2t} + R$.

Декодирование:

- Вычислить синдромы

  $$S_j = r\left(\alpha^j\right), j = b, b+1, \dots b + 2t - 2$$

  где $r(x) -$ полученный многочлен из канала

  Если все синдромы равны нулевой, то нет ошибок
- Построить многочлен локаторов ошибок с помощью алгоритма Берлекампа-Масси

  Многочлен локаторов ошибок:

  $$\Lambda(x) = \prod_{k=1}^{\nu}(1 - X_k x) = 1 + \Lambda_1 x^1 + \Lambda_2 x^2 + \dots + \Lambda_\nu x^\nu$$

  $\nu -$ количество ошибок

  Корнем многочлена локаторов ошибок является X_k^{-1}

  Если алгоритм Питерсона-Горенстейна-Цирлера вычисляет многочлен локаторов ошибок методом решения системы линейнных алгебрайческих уравнений, то алгоритм Берлэкампа-Месси сводит задачу построения многочлена локаторов ошибок к задаче построения филтра:

  В каждой интерации:
  - Невязка: $\Delta_r = S_r - \widehat{S_r} = \sum_{j=0}^{r-1} \Lambda_j^{(r-1)} S_{r-j}$
  - Если $\Delta_r = 0$, итерация выполнена успешно

    $\Lambda^{(r)}(x) = \Lambda^{(r-1)}(x)$
  - Если $\Delta_r \neq 0$, надо изменить $\Lambda^{(r)}(x)$, чтобы $\Delta_r = 0$

    $\Lambda^{(r)}(x) = \Lambda^{(r-1)}(x) + \frac{\Delta r}{\Delta m} x^{r-m} \Lambda^{(m-1)}$

    $m -$ предыдущая итерации, что $\Delta_m = 0$

- Найти корни многочлена локаторов ошибок, определяющие позиции ошибок, с помощью алгоритма Ченя
- Определить значения ошибок по формуле Форни

$$Y_k = X^{1-b}.\frac{\Omega(X_k^{-1})}{\prod_{j=1,j\neq k}(1 - X_k^{-1}.X_j)}$$

где $\Omega(x) = S(x).\Lambda(x)\ mod\ x^{2t}$

- Исправиfть ошибки

3. Тестирование реализации

Создать таблицу, в которой вычисленны вероятности ошибки на кодовое слово, когда количество ошибок при передаче равно t (теоретическое максимальное количество, которое можно исправить) и равно $t + 1$

- Размер символа $m = 4, 5, \dots 10$ бит
- Скорость кода $R \approx \frac{1}{2}$, например если $m = 6$, то построим $RS(63,31)$
- Генерировать 1000 случайных кодовых слов
- Генерировать количество ошибок при передаче (в канале): $t_0 = \frac{d-1}{2}$, $t_1 = \frac{d-1}{2} + 1$, где d – минимальное расстояние кода
- Вычислить вероятности ошибки на кодовое слово (FER)

Таблица 1. Полученные вероятности ошибки на кодовое слово

Размер символа m	Код	FER (количество ошибок t_0)	FER (количество ошибок t_1)
$m = 4$	RS(15, 7)	0	1
$m = 5$	RS(31,15)	0	1
$m = 6$	RS(63,31)	0	1
$m = 7$	RS(127,63)	0	1
$m = 8$	RS(255,127)	0	1
$m = 9$	RS(511,255)	0	1
$m = 10$	RS(1023,511)	0	1

4. Численные результаты

Для оценки FER в каждой точке было произведено 1000 тестов.

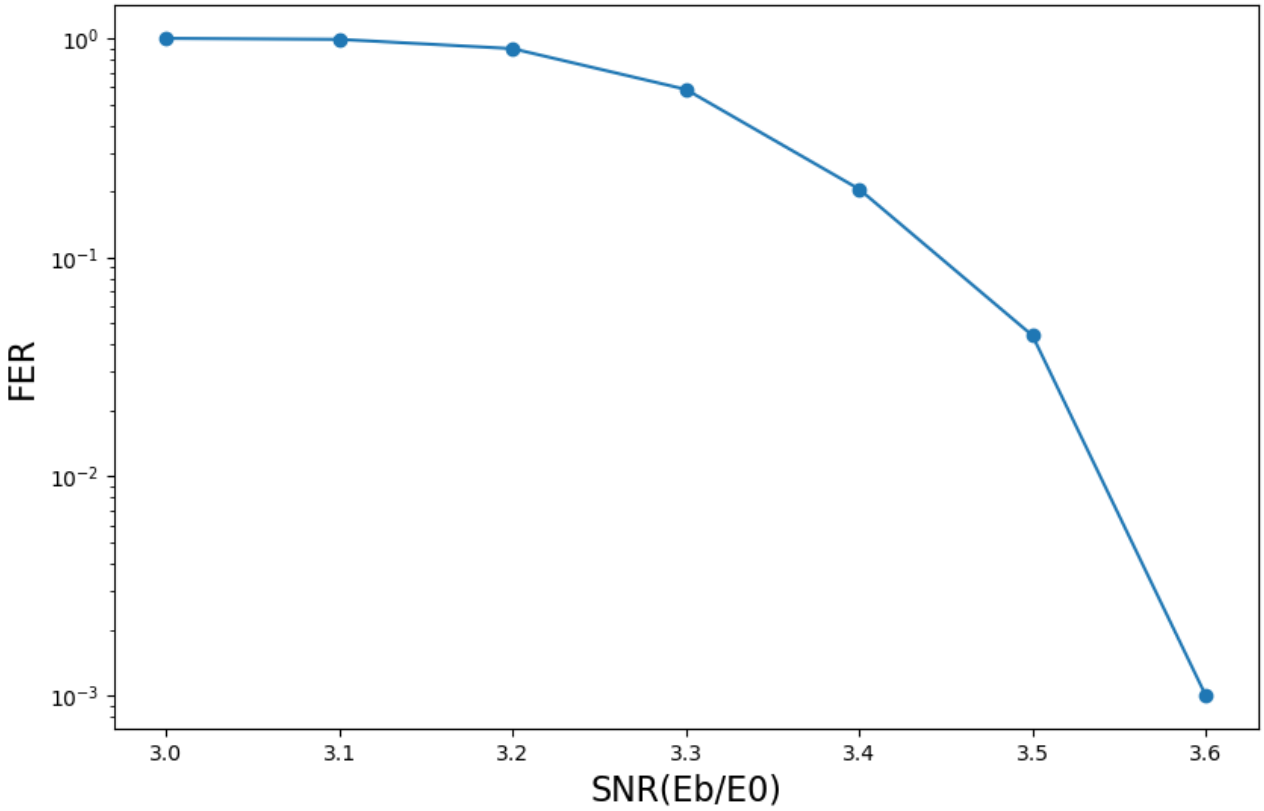

График зависимости вероятности ошибки на кодовое слово от отношения сигнал-шум для кода (1023, 681) для канала с АБГШ и двоичной амплитудно-импульсной модуляцией

5. Вывод

Известно, что максимальное количество ошибок, которые можно исправить в коде Рида-Соломона, равно $t = \frac{d-1}{2}$, где $d -$ минимальное расстояние кода. Из таблицы 1 можно видеть, что если количество ошибок, которое передано в кодовом слове, равно t, то все полученные кодовые слова будут успешно продекодированны. Если количество ошибок больше чем t (например в таблице $t + 1$), то декодирование будет неуспешным.

⇨ *Результаты тестирования в таблице 1 совпадают с теорией.*

При значении отношения сигнал-шум $\frac{E_b}{E_0} = 3.8$дБ, стандартное отклонение шума $\sigma = \sqrt{\frac{N_0}{2RE_b}} \approx 0.444$. С $\sigma \approx 0.444$ вероятность инвертирования бита (ошибки на бит) равна $P_b \approx 0.012$. Вероятность ошибки на символ $P_s = 10P_b \approx 0.12$. Количество ошибок, которое переданно в кодовом слове, близко 122 ошибок и не будет больше чем 171 ($171 = \frac{1023-681}{2}$ – максимальное возможное исправленное количество ошибок). При этом декодирование удается. Вероятность ошибки на кодовое слово будет равно нулевой. Аналогично, в точке $\frac{E_b}{E_0} = 3$дБ, количество ошибок близко 235 ошибок намного больше чем 171, потому что декодирование не удается.

⇨ *Экспериментанльные результаты подходятся к аналитическам результатам*