z	z^0	z^1	z^2	z^3	z^4	z^5	z^6
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1
3	1	3	2	6	4	5	1
4	1	4	2	1	4	2	1
5	**1**	**5**	**4**	**6**	**2**	**3**	**1**
6	1	6	1	6	1	6	1

Исследование кодов Рида-Соломона

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНОЙ РАБОТЕ ПО СИСТЕМАМ СВЯЗИ

НОВИКОВ А.В., УТЕГЕНОВ Д.Д.

ТУСУР
2018

Оглавление

Введение

Основная идея помехоустойчивого кодирования кодом Рида-Соломона заключается в умножении информационного слова, представленного в виде полинома $a(x)$, на порождающий полином $g(x)$, известный в передатчике и приемнике, в результате чего получается кодовое слово $s(x)$, представленное в виде полинома. Декодирование осуществляется с точностью до наоборот: если при делении кодового слова $v(x)=s(x)+e(x)$ на полином $g(x)$ декодер получает ненулевой остаток (синдром), то он может рапортовать наверх об ошибке. Соответственно, если кодовое слово $v(x)$ разделилось нацело, то либо ошибки нет, либо она не обнаруживаемая.

Коды Рида-Соломона обладают хорошими корректирующими свойствами, для них разработаны относительно простые и конструктивные методы кодирования [1]. Коды Рида-Соломона не являются двоичными. Это надо понимать в том смысле, что символами кодовых слов являются не двоичные знаки, а элементы множества чисел, состоящего более чем из двух знаков. Коды Рида-Соломона также относятся к классу *циклических кодов*.

Программный макет предназначен для изучения кодов Рида-Соломона студентами. Он поможет изучить процесс кодирования и декодирования в плане обнаружения и исправления ошибок. Дополнительно в макет планируется ввести блок статистических испытаний в канале с независимыми символьными ошибками, а также блок подсчета ошибочных кодовых слов, слов с обнаруженными ошибками и слов с исправленными ошибками, наподобие того, как это сделано в [2] для двоичных циклических кодов.

Отчет по работе должен состоять из следующих пунктов:

- Титульный лист;

- Ход работы;
- Ответы на вопросы;
- Выводы.

Сведения из теории

Коды Рида-Соломона (РС) – недвоичные циклические коды, позволяющие исправлять ошибки в блоках данных. Элементами кодового вектора являются не биты, а группы битов (блоки). Очень распространены коды РС, работающие с байтами. Коды РС являются частным случаем так называемых БЧХ-кодов [1].

В настоящее время коды РС широко используются в системах цифрового телевизионного вещания, в системах сотовой связи, в твердотельных накопителях, при контроле данных на компакт-дисках, в системах беспроводной (Wi-Fi) связи.

Достоинства кодов Рида-Соломона:

- Имеют наибольшее возможное кодовое расстояние;
- Исправляют пакеты битовых ошибок.

Примеры несистематического кодирования и декодирования

Рассмотрим для примера код РС над полем GF(p=5) с параметром α=3. Зададимся кодовым расстоянием d=3, тогда требуемое число проверочных символов $r=d-1=3-1=2$, а потому порождающий полином кода РС будет иметь вид

$$g(x)=(x-\alpha)(x-\alpha^2).$$

Для понимания правил сложения и умножения степеней "альфа", следует вместо "альфы" про себя иметь ввиду выбранное выше число и заполнить таблицу сложения и умножения по модулю p=5.

Таблица 1 Таблица сложения элементов поля GF(5)

+	1	α	α^2	α^3
1	α^3	α^2	0	α
α	α^2	1	α^3	0
α^2	0	α^3	α	1
α^3	α	0	1	α^2

Нулевой элемент поля в таблице не указан, потому что операция сложения с нулем тривиальна. Как понять, например, то, что $1+\alpha^2=0$? Просто: подставляем вместо альфы число 3 и получаем 10, что по модулю 5 дает 0. А почему $1+\alpha^3=\alpha$? Подставляем и получаем

$1+3^3=1+27=1+2=3=\alpha$ (ведь $27=5\cdot5+2$, то есть $27 \equiv 2 \bmod 5$). Ну, и чтобы докончить, рассмотрим равенство $\alpha+\alpha^2=\alpha^3$. Подставляем $3+9=12 \equiv 2 \bmod 5$, а $2=\alpha^3$.

Вообще, удобно заранее выписать степени альфа по модулю 5:

$\alpha^0=1$, $\alpha^1=3$, $\alpha^2=9=4$, $\alpha^3=\alpha^2\cdot\alpha=4\cdot3=12=2$, $\alpha^4=2\cdot3=6=1$, то есть $\alpha^4=\alpha^0=1$.

Длина кода $n=p-1=4$. Код РС, напомним, является циклическим, а потому порождающий полином должен делить полином x^n-1. Доказано, что если $n=p-1$, где p является простым числом, то корнями уравнения x^n-1 будут все степени некоторого числа альфа, α^i, где альфа такое, что все его степени дают разные значения. В нашем случае эти степени дают набор чисел {1, 3, 4, 2} – все они разные (по модулю 5). Другими словами

$$x^4-1=(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3).$$

Для порождающего полинома мы выбрали второй и третий сомножители. Для кодов РС важно, чтобы в порождающий полином входили множители <u>с подряд идущими степенями</u> альфа, то есть нельзя брать произведение, например, "альфа в первой" и "альфа в третьей", при этом максимум можно взять $n-1$ множителей.

По аналогии с таблицей сложения составим таблицу умножения элементов поля GF(5).

Таблица 2 Таблица умножения элементов поля GF(5)

*	1	α	α^2	α^3
1	1	α	α^2	α^3
α	α	α^2	α^3	1
α^2	α^2	α^3	1	α
α^3	α^3	1	α	α^2

Почему, например, $\alpha^2\cdot\alpha^2=1$? Подставляем $4\cdot4=16=1$.

Раскроем порождающий полином

$$g(x)=(x-\alpha)(x-\alpha^2)=x^2-x(\alpha+\alpha^2)+\alpha^3=x^2+x\alpha+\alpha^3.$$

Заметим, что из таблицы сложения следует факт $(-\alpha^3)=\alpha$.

Порождающая матрица кода РС (как циклического кода)

$$G=\begin{pmatrix} \alpha^3 & \alpha & 1 & 0 \\ 0 & \alpha^3 & \alpha & 1 \end{pmatrix}.$$

Путем эквивалентных преобразований эту матрицу можно привести к систематической форме

$$G_{\text{сист}}=\begin{pmatrix} 1 & 0 & \alpha^3 & \alpha \\ 0 & 1 & \alpha^2 & \alpha \end{pmatrix},$$

что позволяет просто определить проверочную матрицу

$$H_{\text{сист}}=\begin{pmatrix} -\alpha^3 & -\alpha^2 & 1 & 0 \\ -\alpha & -\alpha & 0 & 1 \end{pmatrix}=\begin{pmatrix} \alpha & 1 & 1 & 0 \\ \alpha^3 & \alpha^3 & 0 & 1 \end{pmatrix}.$$

Коды РС таковы, что имеют максимально возможное кодовое расстояние $d=r+1$. Доказано, что порождающие матрицы таких кодов (коды РС лежат на границе Синглтона), записанные в систематической форме, имеют такую правую часть, что все определители, составленные из этой правой части, отличны от нуля. В нашем случае эта правая часть является матрицей

$$Q = \begin{pmatrix} \alpha^3 & \alpha \\ \alpha^2 & \alpha \end{pmatrix}.$$

В частности, определителями являются элементы этой матрицы (видно, что они отличны от нуля). Также определителем является определитель матрицы Q, который равен

$$\alpha^4 - \alpha^3 = 1 + \alpha = \alpha^2 \neq 0.$$

В качестве несистематического способа кодирования рассмотрим способ, взятый из циклических кодов:

$$s(x) = a(x)g(x).$$

Задаем вектор информационных символов длиной $k=n-r=4-2=2$

$$a = (\alpha^3, \alpha),$$

чему соответствует полином

$$a(x) = \alpha^3 + x\alpha.$$

Перемножая полиномы, получим

$$s(x) = a(x)g(x) = (\alpha^3 + x\alpha)(x^2 + x\alpha + \alpha^3) = \alpha^2 + x\alpha^3 + x^2 + x^3\alpha,$$

или в векторном виде

$$s = \alpha^3(\alpha^3, \alpha, 1,0) + \alpha(0, \alpha^3, \alpha, 1) = (\alpha^2, \alpha^3, 1, \alpha).$$

Умножению $g(x)$ на x соответствует циклический сдвиг вектора g на один символ вправо.

Декодирование несистематического кода можно выполнить путем деления полинома $s(x)$ на порождающий $g(x)$. Это соответствует варианту, когда ошибок нет. Это не особенно интересно (хотя и важно, так как в системах связи ошибки, все-таки, редки). Введем ошибку в третьем символе

$$v = s + e = (\alpha^2, \alpha^3, 1, \alpha) + (0,0, \alpha, 0) = (\alpha^2, \alpha^3, \alpha^2, \alpha).$$

Найдем частное $b(x)$ и остаток $res(x)$ от деления $v(x)$ на $g(x)$

$$v(x) = b(x)g(x) + res(x) = (\alpha x)g(x) + (x + \alpha^2).$$

(при этом говорят, что $res(x) = v(x) \bmod g(x)$)

Остаток не равен нулю, значит ошибка есть. Если принять остаток за синдром и заранее вычислить таблицу остатков для всех однократных ошибок

$$res(x) = v(x) \bmod g(x) = e(x) \bmod g(x) = \alpha^i x^j \bmod g(x),$$

(при этом $s(x) = 0 \bmod g(x)$)

то получившийся остаток можно отыскать в этой таблице и применить коррекцию:

$$a(x) = b(x) + corr(x),$$

$$corr(x) = \frac{res(x) - e(x)}{g(x)}.$$

Такая коррекция применима к любым циклическим кодам при несистематическом способе кодирования

$$s(x) = a(x)g(x).$$

Найдем синдром-остаток для произвольной однократной ошибки в третьем символе

$$e(x) = \alpha^i x^2.$$

Приравнивая порождающий полином к нулю, получим равенство

$$x^2 = \alpha^3 x + \alpha,$$

что означает то, что остаток от деления x^2 на $g(x)$ равен $\alpha^3 x + \alpha$. Осталось перечислить все i=1, 2, 3. Находим, что при умножении на α получаем искомый остаток

$$\alpha x^2 = x + \alpha^2.$$

Значит корректор будет таким:

$$corr(x) = \frac{x + \alpha^2 - \alpha x^2}{g(x)} = \frac{x + \alpha^2 + \alpha^3 x^2}{x^2 + x\alpha + \alpha^3} = \alpha^3,$$

а восстановленный информационный полином

$$a(x) = b(x) + corr(x) = \alpha x + \alpha^3.$$

Ошибка исправлена.

Отметим, что для кодов РС существуют специальные способы кодирования и декодирования. В данной работе они не изучаются. В частности, показано, что кодирование кодом РС эквивалентно преобразованию Фурье (в конечных полях, естественно) информационного вектора, дополненного нулями до длины кода n.

Описание лабораторного макета

Лабораторный макет представляет из себя приложение ReedSolomon на написанное на языке C++ с использованием библиотеки Qt (рис. 1).

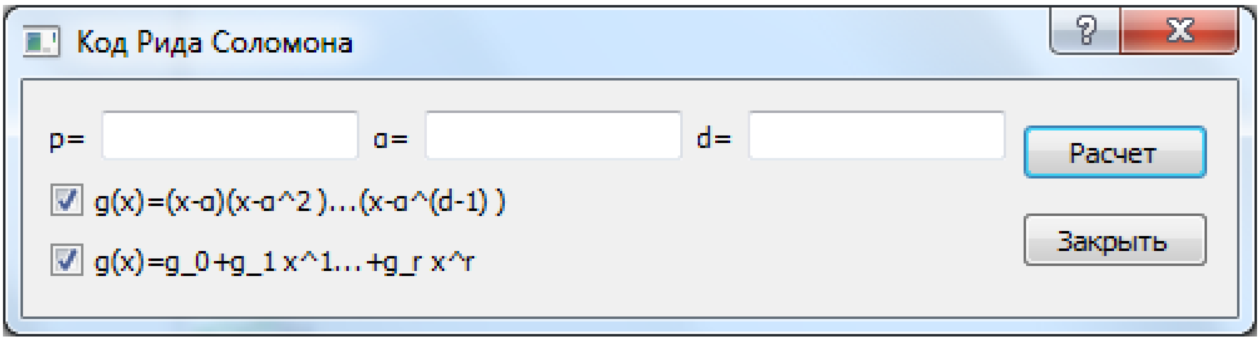


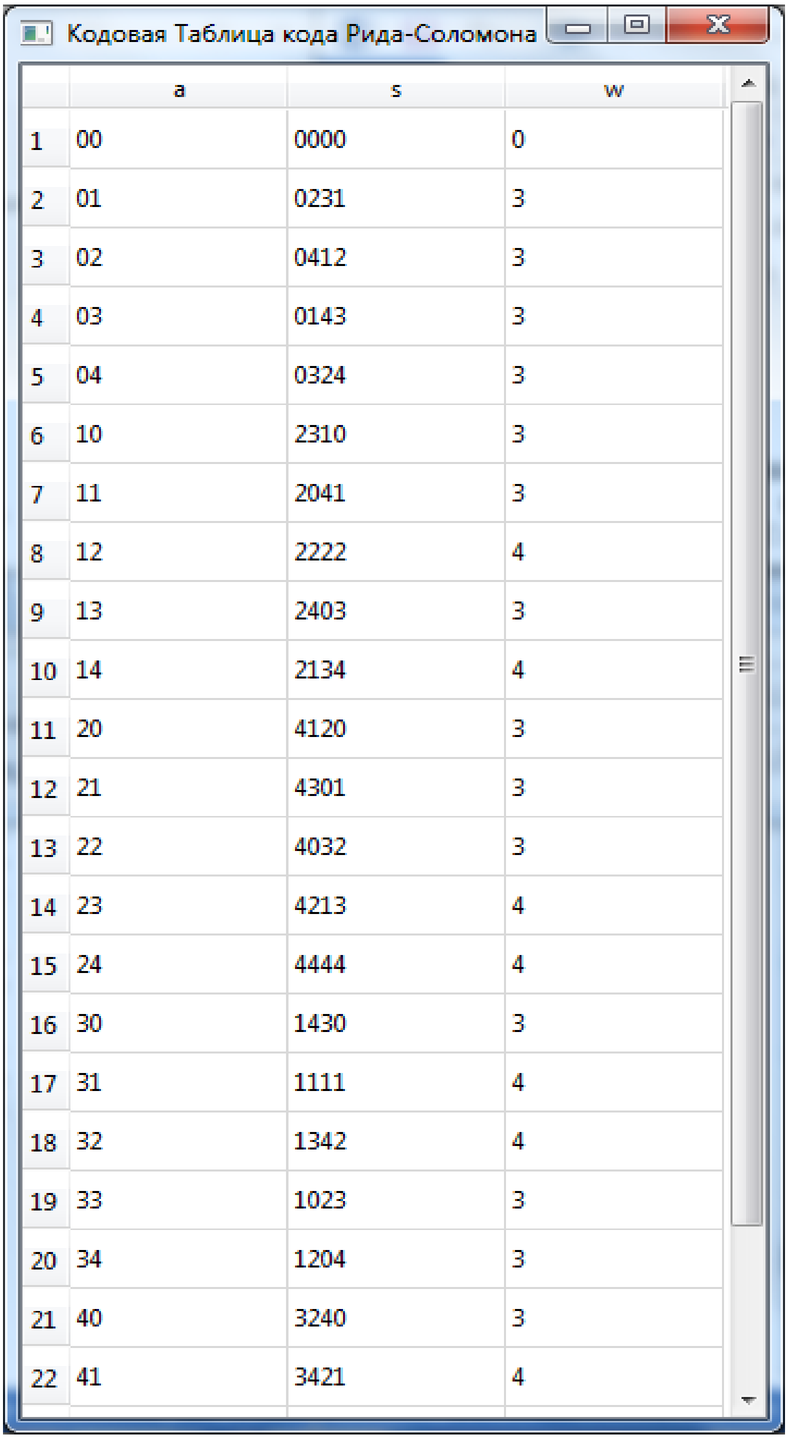
Рисунок 1 Программный макет для изучения кода РС

Программный макет (рис. 1) реализован в виде Qt-приложения[1] с графическим интерфейсом. Входными параметрами макета являются: простое число p=2, 3, 5, 7, 11…, определяющее код Рида-Соломона над полем GF(p), вспомогательное число a из поля GF(p), кодовое расстояние d.

Программный макет после ввода входных параметров генерирует коэффициенты порождающего полинома $g(x)$, а также кодовую таблицу кода РС (рис. 2).

Первая строка в таблице на рис. 2 пустая — она соответствует нулевому кодовому слову с нулевым весом w. В столбце a перечислены все входные слова, в столбце s перечислены соответствующие разрешенные кодовые слова, а в столбце w указан вес разрешенного кодового слова s.

1 Сайт qt.io



Кодовая Таблица кода Рида-Соломона

	a	s	w
1	00	0000	0
2	01	0231	3
3	02	0412	3
4	03	0143	3
5	04	0324	3
6	10	2310	3
7	11	2041	3
8	12	2222	4
9	13	2403	3
10	14	2134	4
11	20	4120	3
12	21	4301	3
13	22	4032	3
14	23	4213	4
15	24	4444	4
16	30	1430	3
17	31	1111	4
18	32	1342	4
19	33	1023	3
20	34	1204	3
21	40	3240	3
22	41	3421	4

Рис. 2. Пример таблицы с результатами кодирования кодом РС

С помощью программного макета был задан код РС с кодовым расстоянием d = 3, что подтверждается кодовой таблицей (рис. 2), в которой минимальный вес *w*, отличный от нуля, равен 3, то есть кодовому расстоянию кода. Заметим, что так как код РС является циклическим, то любые циклические сдвиги любых разрешенных кодовых слов *s* дают разрешенное слово. Допустим, сдвиг 4032 вправо на один символ дает слово 2403, которое есть в таблице (13 и 9 строки).

Таблица остатков (синдромов) для однократных ошибок

	e(n)	c(r)
1	1000	10
2	0100	01
3	0010	32
4	0001	12
5	2000	20
6	0200	02
7	0020	14
8	0002	24
9	3000	30
10	0300	03
11	0030	41
12	0003	31
13	4000	40
14	0400	04
15	0040	23
16	0004	43

Рисунок 3 Таблица остатков (синдромов) для однократных ошибок

Заметим, что остатки для всех однократных ошибок разные (и отличные от нуля), поэтому данный код РС исправляет все однократные ошибки.

Рассмотренная выше однократная ошибка в третьем символе

$$\alpha x^2 = x + \alpha^2$$

соответствует строке 11 на рис.3 (вспомним, что $\alpha^2 = 4$), а разрешенное кодовое слово соответствует строке 14 на рис.2.

Задание на работу

1. Задать $\alpha = 2$. Построить таблицы сложения и умножения в поле GF(5).
2. Определить порождающий полином кода РС с кодовым расстоянием d=3.
3. Определить порождающую матрицу кода РС как циклического кода. Найти матрицу в систематической форме. Определить проверочную матрицу в систематической форме.

4. Вручную выписать кодовую таблицу и таблицу синдромов (остатков). Проверить таблицы с помощью программы. Убедиться, что веса кодовых слов не менее d=3.
5. Выбрать случайное информационное слово. Ввести случайную однократную ошибку. Определить полином $v(x)$. Декодировать получившееся слово. Ввести случайную двукратную ошибку и декодировать получившееся слово, предполагая ошибку однократной. Убедиться, что двукратную ошибку данный код не исправляет, но обнаруживает.
6. Задать в программе $\alpha = 4$ и убедиться в том, что код получается некорректным (не Рида-Соломона). Объяснить в чем его некорректность.

Вопросы

1. Что означает тот факт, что коды РС лежат на границе Синглтона?
2. Являются ли коды РС циклическими?
3. Как определить операции сложения и умножения элементов конечного поля GF(p)?
4. Каково строение порождающего полинома кодов РС?

Литература

1. Сагалович, Ю. Л. Введение в алгебраические коды. [Электронный ресурс] … http://iitp.ru/upload/content/790/algebcodes.pdf
2. Новиков, А. В. Сборник компьютерных лабораторных работ по системам связи: Методические указания к лабораторным работам [Электронный ресурс] / Новиков А. В. — Томск: ТУСУР, 2018. — 151 с. — Режим доступа: https://edu.tusur.ru/publications/7149.