Глава 1. Коды Рида—Соломона

1.1. Построение кода

1.1.1. Выбор поля и канал передачи данных

Код Рида—Соломона — многочлен над некоторым конечным полем $GF(q)$. По-хорошему, выбор поля определяется набором символов, передаваемых по каналу.

Как правило, на практике символом является 8-битный байт (октет), так что код строится над полем $GF(2^8) = GF(256)$ из 256 элементов. Для доски ранее был принят 4-битный байт (тетрада), что требовало бы кода над полем $GF(2^4) = GF(16)$ из 16 элементов.

К сожалению, арифметические действия в полях $GF(2^n)$ при $n > 1$ контринтуитивны (сложение как xor и умножение по таблице степеней примитивного элемента), поэтому на лекции и здесь рассматриваются поля $GF(p) = \mathbb{Z}_p$ из простого количества элементов $p > 2$ (арифметические действия по модулю p).

На данном семинаре было выбрано поле $GF(7) = \mathbb{Z}_7$ из семи элементов: $0, 1, 2, 3, 4, 5, 6$. Это соответствует гипотетическому каналу, который умеет передавать символы $\{0, 1, 2, 3, 4, 5, 6\}$ и только их. Ошибка передачи — это замена одного из символов сообщения на другой символ из набора $\{0, 1, 2, 3, 4, 5, 6\}$.

К вопросу «как это реализовать?»

Канал, передающий сообщения на семисимвольном алфавите, можно эмулировать как каналом, передающим октеты, так и каналом, передающим 32-битные числа (*int* или *unsigned*), так как в обоих случаях алфавит поля $\mathbb{Z}_7$ (множество символов $A_7 = \{0, 1, 2, 3, 4, 5, 6\}$) — часть алфавита канала A:

1. При передаче символа $a \in A_7 \subseteq A$ передаётся символ a. Значения из $A \setminus A_7$ никогда не передаются.
2. При получении символа $a \in A_7 \subseteq A$ он воспринимается как a.
   При получении символа $b \in A \setminus A_7$ (любого, кроме $0, 1, 2, 3, 4, 5, 6$) он воспринимается как один из символов A_7 — например, всегда как 0; или как случайно выбранный от 0 до 6.

1.1.2. Длина кода

Максимально возможная длина кода (общее число информационных и проверочных символов) равна количеству ненулевых элементов (6 для $\mathbb{Z}_7$).

При желании — можно меньше (взять меньше информационных на то же число проверочных; так, для $GF(256)$ максимальная длина 255 нечётна).

Если ниже взять не примитивный β — это технически возможно, но максимальная длина кода будет равна его порядку $< 6 \implies$ не используется.

1.1.3. Примитивный элемент

Для построения кода Рида—Соломона необходим примитивный элемент поля β. На семинаре был выбран $\beta = 3$:

$$\begin{aligned}\beta^0 &= 1\\ \beta^1 &= 3\\ \beta^2 &= 2\\ \beta^3 &= 6\\ \beta^4 &= 4\\ \beta^5 &= 5\\ \beta^6 &= 1\end{aligned}$$

Все шесть (по Малой теореме Ферма, x^{p-1} в любом случае равно 1) степеней разные $\implies$ 3 — действительно примитивный элемент $\mathbb{Z}_7$.

1.1.4. Степень порождающего полинома Рида—Соломона = число проверочных символов κ

В блоке Рида—Соломона с κ проверочных символов может быть исправлено до $\left\lfloor \frac{\kappa}{2} \right\rfloor$ ошибок.

Таким образом, по-хорошему-2, выбор числа проверочных символов определяется зашумлённостью канала. Для выбора κ необходимо:

1. Задаться конкретной общей длиной кода $\mu \leqslant \mu_{\max}$ (для $\mathbb{Z}_7$ $\mu \leqslant 6$).
2. Рассчитать прогнозируемо-максимальное количество ошибок $u_{\max}$ такое, что при передаче блока из μ символов по рассматриваемому каналу:
   - вероятностью $u_{\max} + 1$ ошибки в блоке уже можно пренебречь,
   - а вероятностью $u_{\max}$ ошибок ещё нельзя.

После расчёта принимается $\kappa = 2u_{\max}$.

К вопросу «всегда ли κ чётно?»

На практике — всегда чётно; в некоторых источниках написано сразу «$2u_{\max}$ проверочных символов». Использовать $\kappa = 2u_{\max} + 1$ проверочных символов технически можно, но при этом:

- исправляется только $u_{\max}$ ошибок, как и для $\kappa = 2u_{\max}$;
- повышается сложность расчёта как при кодировании, так и при проверке;
- при той же общей длине блока μ число информационных символов блока $\nu = \mu - \kappa$ меньше, чем для $\kappa = 2u_{\max}$.

Если $\kappa = 2u_{\max} \geqslant \mu$ — по рассматриваемому каналу *невозможно* вести достаточно надёжную (то есть с пренебрежимо малой вероятностью неисправленной и незамеченной ошибки) передачу блоками длины μ при помощи кодов Рида—Соломона (нужны другая μ, другие коды или другой канал).

Так как мы рассматриваем гипотетический канал передачи данных с неизвестным шумом, κ на семинаре выбиралось произвольно. Рассматривались варианты с общей длиной $\mu = 6$:

– $\kappa = 2$ ($\nu = 4$ информационных символа, исправление одной ошибки);
– $\kappa = 4$ ($\nu = 2$ информационных символа, исправление двух ошибок);

выбрано $\kappa = 2$.

1.1.5. Порождающий полином Рида—Соломона

Порождающий полином Рида—Соломона имеет вид:

$$g(x) = (x - \beta)(x - \beta^2) \dots (x - \beta^\kappa), \tag{1.1}$$

что при выбранных $\beta = 3$ и $\kappa = 2$ означает

$$g(x) = (x - 3^1)(x - 3^2) = (x - 3)(x - 2) = x^2 - 5x + 6 = x^2 + 2x + 6. \tag{1.2}$$

1.2. Кодирование

Для порождающего полинома (1.2) с $\kappa = 2$ возможно количество информационных символов ν от 1 до 4 и, соответственно, общая длина от 3 до 6. Далее рассматривается случай $\nu = 4$ информационных символов и, соответственно, общая длина кода $\mu = \kappa + \nu = 2 + 4 = 6$.

Сообщение из ν информационных символов $(a_0, a_1, a_2, ..., a_{\nu-1})$ рассматривается как *информационный полином* степени $\nu - 1$:

$$a(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{\nu-1} x^{\nu-1}. \tag{1.3}$$

Систематический полиномиальный код, в том числе код Рида—Соломона — это полином $C(x)$, который должен:

– делиться на порождающий $g(x)$ — как любой полиномиальный код;
– содержать в явном виде информационные символы $(a_0, a_1, a_2, ..., a_{\nu-1})$ (коэффициенты $a(x)$) — как любой систематический код;

и получается следующим образом:

$$C(x) = a(x) \cdot x^\kappa - r(x), \tag{1.4}$$

где $r(x) = a(x) \cdot x^\kappa \bmod g(x)$.

То есть:
- информационные символы сдвигаются на κ позиций, чтобы освободить место для проверочных ($a(x) \cdot x^\kappa$ содержит $(a_0, a_1, a_2, ..., a_{\nu-1})$ в правильном порядке, но в общем случае не делится на $g(x)$);
- освободившиеся κ позиций заполняются так, чтобы результат делился на $g(x)$:

$$\begin{gathered} C(x) \bmod g(x) = \Big(a(x) \cdot x^\kappa - r(x)\Big) \bmod g(x) = \\ = \Big(a(x) \cdot x^\kappa \bmod g(x)\Big) - \Big(r(x) \bmod g(x)\Big) = r(x) - r(x) = 0, \end{gathered} \tag{1.5}$$

$r(x)$ имеет не более κ коэффициентов: $deg(r) \leqslant deg(g) - 1 = \kappa - 1$.

1.3. Кодирование конкретного сообщения

На семинаре рассматривалось сообщение $(1, 1, 1, 1)$, то есть полином

$$a(x) = x^3 + x^2 + x + 1. \tag{1.6}$$

1.3.1. На семинаре обсчитались при делении

При делении на доске в столбик $a(x) \cdot x^2 = x^5 + x^4 + x^3 + x^2$ на $g(x) = x^2 + 2x + 6$ получили $r(x) = -x - 3$, то есть:

$$C(x) = a(x) \cdot x^2 - r(x) = x^5 + x^4 + x^3 + x^2 + x + 3. \tag{1.7}$$

На семинаре проверяли делением $C(x)$ на $g(x) = x^2 + 2x + 6$ онлайн (над $\mathbb{R}$) — получили в остатке $-7x - 75$, а 75 не кратно 7.

Проверим иначе: делится ли $C(x)$ на $g(x) = (x - 3)(x - 2)$ — рассчитаем в Octave $C(2)$ и $C(3)$ в $\mathbb{R}$.

```
octave:1> x=2
x =  2
octave:2> x^5 + x^4 + x^3 + x^2 + x + 3
ans =  65
octave:4> x=3
x =  3
octave:5> x^5 + x^4 + x^3 + x^2 + x + 3
ans =  366
```

Получили значения $65 = 7 \cdot 9 + 2$ и $366 = 52 \cdot 7 + 2$ — то есть в $\mathbb{Z}_7$ полином (1.7) не имеет корней в точках 2 и 3.

1.3.2. Исправляем ошибку

При повторном делении $a(x) \cdot x^2 = x^5 + x^4 + x^3 + x^2$ на $g(x) = x^2 + 2x + 6$ в столбик, уже после семинара, было получено $r(x) = -x + 6 = -x - 1$, то есть

$$C(x) = a(x) \cdot x^2 - r(x) = x^5 + x^4 + x^3 + x^2 + x + 1. \tag{1.8}$$

В этом случае при делении $C(x)$ на $g(x)$ онлайн $-7x - 77$ в остатке — всё-таки и тут коэффициенты должны быть нулевые или кратные 7!

Значения $C(2)$ и $C(3)$ в $\mathbb{R}$, рассчитанные в Octave:

```
octave:10> x=2
x =  2
octave:11> x^5 + x^4 + x^3 + x^2 + x + 1
ans =  63
octave:12> x=3
x =  3
octave:13> x^5 + x^4 + x^3 + x^2 + x + 1
ans =  364
octave:14> 63/7, 364/7
ans =  9
ans =  52
```

делятся без остатка на 7 в $\mathbb{R}$, то есть нулевые в $\mathbb{Z}_7 \implies C(x)$ делится на $x - 2$ и $x - 3$, то есть и на $g(x)$.

1.4. Проверка и декодирование

Декодирование систематического кода тривиально, так как информационные символы содержатся в нём в явном виде. Но они могут оказаться искажёнными, то есть перед чтением необходимо проверить корректность сообщения.

1.4.1. Проверка корректности

Корректность полученного сообщения $\widetilde{C}(x)$ определяет *синдром* — многочлен степени $\kappa - 1$

$$s(x) = s_0 + s_1 x + ... + s_{\kappa-1} x^{\kappa-1}. \tag{1.9}$$

где

$$s_i = \widetilde{C}(\beta^{i+1}). \tag{1.10}$$

Нулевой синдром соответствует корректному (делящемуся на $g(x)$) сообщению $\widetilde{C}(x)$. Действительно, если $\widetilde{C}(x)$ делится на $g(x)$ ($\widetilde{C}(x) = A(x) \cdot g(x)$), то все коэффициенты s_i нулевые, так как соответствующие β^{i+1} — корни $g(x)$.

Считается, что делящееся на $g(x)$ (с нулевым синдромом) полученное сообщение $\widetilde{C}(x)$ есть неискажённое $C(x)$.

Сообщение с ненулевым синдромом — искажено:

$$\widetilde{C}(x) = C(x) + e(x), \tag{1.11}$$

необходима коррекция. Степень $e(x)$ в общем случае может быть равна степени $C(x)$, но число ненулевых коэффициентов $e(x)$ (количество ошибок u) не превышает $u_{\max} = \left\lfloor \frac{\kappa}{2} \right\rfloor$ (κ выбиралось так, что вероятностью $u > \frac{\kappa}{2}$ можно пренебречь).

При этом, так как $C(\beta^{i+1}) = 0$ ($C(x)$ делится на $g(x)$, то есть делится и на все его делители $x - \beta^{i+1}$), то синдром характеризует только ошибку $e(x)$:

$$s_i = \widetilde{C}(\beta^{i+1}) = C(\beta^{i+1}) + e(\beta^{i+1}) = e(\beta^{i+1}) \tag{1.12}$$

1.4.2. Ошибки рассматриваемого кода

Для (1.2) $u_{\max} = 1$, то есть ошибка $e(x)$ либо равна 0 (и делится на $g(x)$), либо имеет только один ненулевой коэффициент и имеет вид

$$e(x) = Ax^k, \tag{1.13}$$

где $0 \leqslant k \leqslant \mu - 1$, $A \neq 0$.

При делении на $g(x)$ все возможные $e(x)$ дают разные остатки (таблица 1.1).

Возможные остатки от деления $e(x) = Ax^k$ на $g(x)$

Таблица 1.1

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
$A=1$	1	x	$5x+1$	$5x+5$	$2x+5$	$x+2$
$A=2$	2	$2x$	$3x+2$	$3x+3$	$4x+3$	$2x+4$
$A=3$	3	$3x$	$x+3$	$x+1$	$6x+1$	$3x+6$
$A=4$	4	$4x$	$6x+4$	$6x+6$	$x+6$	$4x+1$
$A=5$	5	$5x$	$4x+5$	$4x+4$	$3x+4$	$5x+3$
$A=6$	6	$6x$	$2x+6$	$2x+2$	$5x+2$	$6x+5$

Рассмотрим остатки от деления $e(x) = Ax^k$ на $x-3$ и $x-2$ (таблица 1.2). По теореме Безу $e(x) \bmod (x-a) = e(a) = Aa^k$. Видно, что ни для одного

Возможные остатки от деления $e(x) = Ax^k$ на двучлены $x-3$ и $x-2$

Таблица 1.2

$Ax^k \bmod (x-3) = A \cdot 3^k$	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
$A=1$	1	3	2	6	4	5
$A=2$	2	6	4	5	1	3
$A=3$	3	2	6	4	5	1
$A=4$	4	5	1	3	2	6
$A=5$	5	1	3	2	6	4
$A=6$	6	4	5	1	3	2
$Ax^k \bmod (x-2) = A \cdot 2^k$	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
$A=1$	1	2	4	1	2	4
$A=2$	2	4	1	2	4	1
$A=3$	3	6	5	3	6	5
$A=4$	4	1	2	4	1	2
$A=5$	5	3	6	5	3	6
$A=6$	6	5	3	6	5	3

$e(x) = Ax^k$ не совпадают оба остатка $Ax^k \bmod (x-3) = A \cdot 3^k$ и $Ax^k \bmod (x-2) = A \cdot 2^k$, то есть по остатку от деления на $g(x)$ или по значениям $e(3)$ и $e(2)$ (коэффициентам синдрома) можно найти $e(x)$.

1.4.3. Синдром рассматриваемого кода

Для (1.2) с $\kappa = 2$ синдром линеен:

$$s(x) = \widetilde{C}(\beta^1)x^0 + \widetilde{C}(\beta^2)x^1 = \widetilde{C}(\beta) + \widetilde{C}(\beta^2)x = \widetilde{C}(3) + \widetilde{C}(2)x. \qquad (1.14)$$

1.4.4. Исправление сообщения с ненулевым синдромом

Если у полученного сообщения $\widetilde{C}(x)$ ненулевой синдром, то при передаче произошло u ошибок, $1 \leqslant u \leqslant u_{\max} = \left\lfloor \frac{\kappa}{2} \right\rfloor$.

Для исправления необходимо найти два полинома:

1. Многочлен локаторов $L(x)$ степени u вида:

$$L(x) = (1 - xX_1)(1 - xX_2)\dots(1 - xX_u) \qquad (1.15)$$

где константа $X_i \in \mathbb{Z}_7 \setminus \{0\}$ — *локатор ошибки:* $X_i = \beta^\ell$ указывает, что коэффициент при x^ℓ был передан с ошибкой.

2. Многочлен ошибок $W(x)$ степени $u-1$.

Оба многочлена — $L(x)$ и $W(x)$ — находятся из соотношения:

$$L(x) \cdot S(x) = W(x) \mod x^{\kappa}, \tag{1.16}$$

причём поиск их коэффициентов — самая сложная часть исправления ошибок. Неизвестная степень u вначале полагается равной $u_{\max} = \frac{\kappa}{2}$; при вычислении часть коэффициентов может оказаться нулевой.

После вычисления $L(x)$ и $W(x)$ для каждого локатора X_i находим значение, которое необходимо добавить к соответствующему коэффициенту для исправления ошибки

$$Y_i = \frac{W(X_i^{-1})}{L'(X_i^{-1})}, \tag{1.17}$$

где штрих — производная по x; тогда

$$C(c) = \widetilde{C}(x) + \sum Y_i \cdot x^{\ell_i}. \tag{1.18}$$

1.4.5. Многочлены локаторов и ошибок рассматриваемого кода

В общем случае для (1.2) с $\kappa = 2$, исправляющего $u_{\max} = 1$ ошибку, многочлен локаторов линеен:

$$L(x) = 1 - xX_1 = 1 - ax, \tag{1.19}$$

а многочлен ошибок степени $u_{\max} - 1$ представляет собой константу:

$$W(x) = c. \tag{1.20}$$

Таким образом $L'(x) = -a$, и выражение (1.17) для коррекции ошибки в месте локатора X_i:

$$Y_1 = \frac{W(X_i^{-1})}{L'(X_i^{-1})} = \frac{c}{-a}. \tag{1.21}$$

1.5. Проверка и декодирование конкретного сообщения

Для неискажённого $C(x) = x^5 + x^4 + x^3 + x^2 + x + 1$ синдром равен $0 + 0x$ (выше проверено $C(3) = C(2) = 0$).

Внесём искажение: пусть получено

$$\widetilde{C}(x) = x^5 + x^4 + x^3 + x^2 + x + 3 \tag{1.22}$$

его синдром

$$s(x) = \widetilde{C}(3) + \widetilde{C}(2)x = 2 + 2x. \tag{1.23}$$

отличен от нуля, то есть надо найти коэффициенты многочленов $L(x) = 1 - ax$ и $W(x) = c$ из соотношения (1.16):

$$(1 - ax) \cdot S(x) = c \mod x^2, \tag{1.24}$$

то есть

$$(1 - ax) \cdot (2 + 2x) = c \mod x^2, \tag{1.25}$$

$$2 + 2x - 2ax - 2ax^2 = c \mod x^2, \tag{1.26}$$

получаем систему уравнений:

$$\begin{cases} 2 = c \\ 2 - 2a = 0 \end{cases} \tag{1.27}$$

откуда $a = 1$ и $c = 2$.

Так как локатор единственной ошибки $X_1 = a = 1 = 3^0$ — ошибка в коэффициенте при x^0 (свободном члене); добавить к нему, согласно (1.21), необходимо величину

$$Y_1 = \frac{c}{-a} = \frac{2}{-1} = -2 = 5. \tag{1.28}$$

Действительно,

$$\widetilde{C}(x)+Y_1x^0 = x^5+x^4+x^3+x^2+x+3-2 = x^5+x^4+x^3+x^2+x+1 = C(x) \tag{1.29}$$