1. ©2002-2013 Ри-РТФ лектор Крохин А.Л. Указания и задачи по циклическим кодам

1.1. Циклические коды

Разработка эффективных информационных технологий невозможна без привлечения математики. Воображение исследователя или инженера — вещь хорошая, но наиболее важные технологии были получены в рамках изощренных математических моделей. Одна из них — это *циклический код*.

Пусть набор символов, алфавита нашей коммуникационной системы нашей моделируется полем $\mathbb{F}_q$. В этом случае полный набор сообщений-команд, представляющих собой упорядоченные наборы элементов $\mathbb{F}_q$ фиксированной длины k рассматривается как линейное пространство $\mathbb{F}_q^k$. Кодирование моделируем линейным преобразованием $\varphi : \mathbb{F}_q^k \mapsto \mathbb{F}_q^n$. В этом случае набор образов векторов-сообщений переходит в линейное подпространство $\mathcal{C}$ — *линейный код*. Мы уже знаем (см. предыдущие задачи из ИДЗ), что исправляющие свойства полученного кода определяются a posteriori свойствами проверочной матрицы H.

Значительно более плодотворной оказывается *полиномиальная интерпретация* и наложение на подпространство $\mathcal{C}$ условия замкнутости относительно *циклической перестановки*. При этом мы интерпретируем слово $(v_0,\ v_1,\ \ldots, v_{n-1})$, как коэффициенты многочлена над полем $\mathbb{F}_q$, записанным в порядке возрастания степени.(Можно записать многочлен и по возрастающим степеням — некоторые авторы так и делают!) Это позволяет нам получить полезные результаты и алгоритмы обсчета элементов слова, которые иначе совершенно неочевидны.

Пусть $\mathbf{v} = (v_0,\ v_1,\ \ldots, v_{n-1})$. Тогда вектор $\mathbf{v}^{(1)} = (v_{n-1},\ v_0,\ v_1,\ \ldots, v_{n-2})$ называют правым циклическим сдвигом $\mathbf{v}$. Повторив операцию i раз, получим $\mathbf{v}^{(i)} = (v_{n-i-1},\ v_{n-i+1)}, \ldots, v_{n-i+1})$.

Определение. Линейный код $\mathcal{C}$ такой, что $\forall \mathbf{v} \in \mathcal{C} \quad \forall i = 1 \ldots n-1,\ \mathbf{v}^{(i)} \in \mathcal{C}$ называют *циклическим.*

Для работы с циклическими кодами удобно применять полиномиальную интерпретацию. В частности, оператор правого сдвига на одну позицию, $D^{(1)}\mathbf{v} = \mathbf{v}^{(1)} = (v_n,\ v_0,\ v_1,\ \ldots, v_{n-1})$ сводится к умножению $v^{(1)}(x) = x(v(x))(\mod x^n - 1)$.

Множество многочленов, составляющих циклический код можно получить, используя только один из них — ненулевой нормированный многочлен. Его называют *порождающим*, $g(x)$. Каждый многочлен из $v(x) \in \mathcal{C}$ единственным образом представляется в виде $v(x) = m(x)g(x)$. Циклический код длины n существует тогда, и только тогда, когда $g(x) \mid x^n - 1$.

В полиномиальной интерпретации декодирование циклического кода (если кодирование производилось умножением на $g(x)$) производится делением на порождающий многочлен.

Принят (прошедший по каналу связи) многочлен $u^*(x)$, производим деление и получаем $u^*(x) = a(x)\cdot g(x) + s(x)$, $\deg s(x) < n - k = \deg g(x)$.

Определение. *Синдромным многочленом* вектора $\mathbf{u}^*$ (а также и многочлена $u(x)^*$) относительно $\mathcal{C}$ называется остаток от деления $u^*(x)$ на $g(x)$.

Слова "относительно $\mathcal{C}$" опускают, если код известен.

$$v(x) = m(x)g(x) + s(x), \quad \deg s(x) < \deg g(x).$$

Теорема. Пусть $\mathcal{C}$ — циклический код $V(n, \mathbb{F}_q)$. Два слова из $V(n, \mathbb{F}_q)$ имеют один и тот же синдром т.и.т.т., когда они лежат в одном смежном классе по $\mathcal{C}$.

При использовании циклического кода можно применять вместо синдромной таблицы декодирования полиномиально-синдромную таблицу.

Лидеры смежных классов (многочлены ошибок)	Синдромные многочлены
$e_1(x)$	$s_1(x)$
$e_2(x)$	$s_2(x)$

Замечу, что при $\deg e(x) < \deg g(x) \quad e(x) = s(x)$. В других случаях можно циклическим сдвигом "загнать" ошибочные символы в младшие разряды — циклическое свойство синдромов и ошибок.

При наличии ошибки $u^*(x) = u(x) + e(x)$, где $u(x)$ — кодовый многочлен, отправленный в канал связи, а $e(x)$ — многочлен ошибки. Заметим, что синдром $e(x)$ равен синдрому $u^*(x)$, поскольку $u(x) = m(x)g(x)$, а значит

$\text{res}\left(u^*(x)/g(x)\right) = res\big((u(x)+e(x))/g(x)\big) = \text{res}\left(e(x)/g(x)\right) = s(x)$.

Пример 1. Код $C(7,\ 3)$ порождается многочленом $g(x) = x^3 + x + 1$. Построить таблицу лидеров и синдромов.

Решение Данный код имеет $d^* = 3$, исправляет одиночные ошибки. $e_i(x) = x^i$. Синдромы ошибок $s_i(x) = \text{res}\left(e_i(x)/g(x)\right)$.

лидер	синдром
1	1
x	x
x^2	x^2
x^3	$x+1$
x^4	x^2+x
x^5	x^2+x+1
x^6	x^2+1

В случае большой длины кодового слова и $d^* >> 3$ таблица синдромов становится очень большой, такие коды могут исправлять не только одиночные ошибки. Скажем, $n = 32$ и нас интересуют синдромы одиночных и двойных ошибок. Общее количество синдромных многочленов легко подсчитать,

это $32 + C_{32}^2 = 32 + \dfrac{32 \cdot 31}{2} = 32 + 496 = 528$. Циклические коды обладают замечательным свойством, позволяющим облегчить декодирование.

Теорема 1. *Пусть принято слово, соответствующее многочлену* $r(x)$*, синдром которого* $\operatorname{res}\big(r(x)/g(x)\big) = s(x)$.

Тогда синдром $xr(x)$ *равен* $\operatorname{res}\big(xs(x)/g(x)$.

Доказательство

По определению синдромного многочлена $r(x) = a(x)g(x) + s(x)$, $\deg s(x) < \deg g(x)$. $xr(x) = r^c(x) + r_{n-1}(x^n - 1)$. Тогда

$$r^c(x) = -r_{n-1}(x^n-1)+xr(x) = x\Big(a(x)g(x)+s(x)\Big)-r_{n-1}(x^n-1)$$

с одной стороны, и

$$r^c(x) = b(x)g(x) + s^*(x),\ s^*(x) = \operatorname{res}\big(r^c(x)/g(x)\big)$$

с другой стороны.

Разделим $r^c(x)$ на $g(x)$, получим

$$\operatorname{res}\left(\frac{x\Big(a(x)g(x)+s(x)\Big) - r_{n-1}(x^n-1)}{g(x)}\right) = \operatorname{res}\left(\frac{xs(x)}{g(x)}\right).$$

$s^*(x) = \operatorname{res}\big(xs(x)/g(x)\big)$ — синдром циклически сдвинутого принятого слова. Остатки от деления на порождающий многочлен $r^c(x)$ и $xr(x)$ равны, т.к. $g(x)|(x^n - 1)$. Итак, синдром $xr(x)$ равен $\operatorname{res}\big(xs(x)/g(x)$.$\square$

Доказанное свойство позволяет предложить такую методику декодирования.

1. Вычисляем синдром принятого многочлена, если он нулевой — ошибки нет. Иначе идем дальше.

2. Вес синдрома не больше максимального числа ошибок, $wt(s(x)) \le t$, исправляемых данным кодом. $s(x) = e(x)$ — синдром совпадает с многочленом ошибки. Исправляем ошибку.

3. $wt(s(x)) > t$. Последовательно находим остатки от деления $s_i(x) = x^i s(x)$, $i = 1 \dots n-1$, на $g(x)$(это синдромы "сдвинутых" многочленов), пока не будет $wt\Big(\text{res}\left(s_i(x)/g(x)\right)\Big) \leq t$.

4. Полная "прокрутка" не приводит к указанному условию — ошибка не может быть исправлена.

Пример 2. Код $C(15, 7)$ порождается многочленом $g(x) = x^8 + x^7 + x^6 + x^4 + 1$, $d^* = 5$. Декодировать принятое слово (011010111010010).

Решение Принятому слову соответствует многочлен $x + x^2 + x^4 + x^6 + x^7 + x^8 + x^{10} + x^{13}$.

Найдем синдромный многочлен $s(x)$.

$x + x^2 + x^4 + x^6 + x^7 + x^8 + x^{10} + x^{13} \equiv s(x) \pmod{x^8 + x^7 + x^6 + x^4 + 1} \Rightarrow s(x) = x^7 + x^4 + x^2 + 1$. Вес синдрома больше 2, используем свойство циклического сдвига. Последовательно находим $s_i(x) = x^i s(x) \pmod{g(x)}$, пока вес $wt(s_i(x)) \leq 2$.

$$s_1(x) = xs(x) \pmod{g(x)} = x^7+x^6+x^5+x^4+x^3+x+1 (xs(x) = x^8+x^5+x^3+x).$$

$$s_2(x) = x^2 s(x) \pmod{g(x)} = xS_1(x) \pmod{g(x)} = 1+x+x^2+x^5.$$

$$s_3(x) = x^3 s(x) \pmod{g(x)} = xs_2(x) \pmod{g(x)} = x+x^2+x^3+x^6.$$

$$s_4(x) = x^4 s(x) \pmod{g(x)} = xs_3(x) \pmod{g(x)} = x^2+x^3+x^4+x^7.$$

$$s_5(x) = x^5 s(x) \pmod{g(x)} = xs_4(x) \pmod{g(x)} = 1+x^3+x^5+x^6+x^7.$$

$$s_6(x) = x^6 s(x) \pmod{g(x)} = xs_5(x) \pmod{g(x)} = x+1.$$

Поскольку $wt(x+1) = 2$, это многочлен двойной ошибки(в первом и втором символах) для кодового многочлена, циклически сдвинутого на 6 позиций относительно исходного. Настоящий многочлен ошибки будет $e(x) = x^{15-6}(x+1) = x^9 + x^{10}$. Исправляем полученный многочлен и получаем посланный кодовый

$(x+x^2+x^4+x^6+x^7+x^8+x^{10}+x^{13})+(x^9+x^{10}) = x+x^2+x^4+x^6+x^7+x^8+x^9+x^{13}$.

Осталось восстановить сообщение $m(x)$:

$$m(x) = \frac{x+x^2+x^4+x^6+x^7+x^8+x^9+x^{13}}{g(x)} = x+x^2+x^4+x^5.$$

Задача решена, было послано сообщение (0110110).

Это интересно, но можно пропустить

Для построения порождающего многочлена потребуется разложить x^n-1 на неприводимые сомножители над основным полем $\mathbf{GF}(q)$(символы которого используются при кодировании). Методика разложения основана на том факте, что корни многочлена x^n-1 будут иметь различные минимальные многочлены над $\mathbf{GF}(q)$. Найдя все минимальные многочлены, мы и получим искомое разложение. Корнями одного минимального многочлена (сопряженными элементами) будут степени примитивного элемента, показатели которых составляют *циклотомический класс.*

Определение. Множество целых чисел по модулю p^m-1 относительно операции умножения на p распадается на подмножества, которые называются *циклотомическими классами по модулю* p^m-1.

Циклотомический класс , содержащий s, состоит из чисел

$\{s, ps, p^2s, p^3s, \ldots sp^{m_s-1}\}$, где m_s — наименьшее положительное целое число такое, что $p^{m_s}\cdot s \equiv s \pmod{p^m-1}$.

Например, циклотомическими классами по модулю 15 (для $p=2, m=4$) являются: $C_0 = \{0\}$; $C_1 = \{1, 2, 4, 8\}$; $C_3 = \{3, 6, 12, 9\}$; $C_6 = \{5, 10\}$, $C_7 = \{7, 14, 13, 11\}$.

Наши обозначения выбраны так, что если s — наименьшее число в классе, то класс обозначается через C_s. Индексы s называются *представителями* классов по модулю $p^m - 1$.

Минимальные многочлены строим с использованием циклотомических классов.

Пример 3. В F_{16}, элементы $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ имеют один и тот же МП: $m_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) = x^4 + (\alpha+\alpha^2+\alpha^4+\alpha^8)x^3 + (\alpha^3+\alpha^5+\alpha^9+\alpha^6+\alpha^{10}+\alpha^{12})x^2 + (\alpha^7+\alpha^{11}+\alpha^{13}+\alpha^{14})x + 1$.

Поскольку МП принадлежит $F_{16}[x]$, преобразуем коэффициенты в соответствие с таблицами Кэли.

C_i	$m_i(x)$
$C_0 = \{0\}$	$m_0(x) = x + 1$
$C_1 = \{1, 2, 4, 8\}$	$m_1(x) = x^4 + x + 1$
$C_3 = \{3, 6, 9, 12\}$	$m_3(x) = x^4 + x^3 + x^2 + x + 1$
$C_5 = \{5, 10\}$	$m_5(x) = x^2 + x + 1$
$C_7 = \{7, 11, 13, 14\}$	$m_7(x) = x^4 + x^3 + 1$

Согласно теореме БЧХ циклический код, порождающий многочлен которого, имеет своими корнями s последовательных степеней примитивного элемента, имеет минимальное расстояние не менее $s + 1$. Значит число ошибок $t : 2t + 1 \geq s + 1$. Так можно оценить исправляющие свойства построенного вами кода.

Второй метод декодирования состоит в следующем.

Порождающий многочлен — делитель любого кодового многочлена, а любой многочлен $m(x)g(x) \pmod{x^n - 1}$ кодовый. Поэтому **все** корни порождающего многочлена будут корнями кодового. Обратно, если многочлен из $\mathbb{F}_q[x]/(x^n - 1)$ будет иметь своими корнями все корни порождающего, то он нацело на него делится. Левая часть условия обращения в ноль многочлена при каждом значении корня

$$f(\alpha_i) = 0 \Rightarrow f_0 + f_1\alpha_i + f_2\alpha_i^2 + \cdots + f_{n-1}\alpha_i^{n-1} = 0, \quad i \in \overline{1,\, n-k} \tag{1}$$

совпадает с результатом матричного умножения $H \cdot (f_0,\, f_1, \ldots,\, f_{n-1})^T$.

$$H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha_{n-k} & \alpha_{n-k}^2 & \ldots & \alpha_{n-k}^{n-1} \end{pmatrix} \tag{2}$$

Равенство (1) означает также, что вектор $(f_0,\, f_1, \ldots,\, f_{n-1})$ принадлежит нуль-пространству матрицы (2).

ИДЕЯ. Векторный синдром, который имеет длину $n-k$, для циклических кодов можно заменить на более простой объект. Мы выше убедились, что проверочными соотношениями для многочлена $f(x)$ могут быть равенства $f(\alpha) = 0$, где α — примитивный корень $n-$ой степени из единицы в F_{q_m}. Заметим, кстати, что порождающий многочлен делит $x^n - 1$, поэтому все его корни являются корнями из единицы.

Пусть порождающий многочлен будет минимальным многочленом α над F_q.

Моделируем возникновение ошибки при передаче кодового многочлена

$$u^*(x) = u(x) + e(x).$$

Многочлен ошибки содержит ненулевые коэффициенты только при тех степенях, которые соответствуют позициям кодового слова, искаженным при передаче. Причем само искажение символа $u_i \to u_i^*$ описываем $u_i^* = u_i + e_i$.

Многочлен ошибок

$$e(x) = e_0 + e_1 x + e_2 x^2 + \cdots + e_{n-1} x^{n-1} \tag{3}$$

в интересующем нас случае, т. е. когда ошибки можно исправить содержит $0 \le \nu \le t$ ненулевых коэффициентов. Отразим этот факт в записи

$$e(x) = e_{i_1}x^{i_1} + e_{i_2}x^{i_2} + \cdots + e_{i_\nu}x^{i_\nu} \tag{4}$$

Значение ошибки в $i+1$-ой позиции e_i равно единичке для бинарного случая.

Пусть порождающий многочлен имеет корни α, α^2, $\ldots \alpha^{2t}$. Значение полученного многочлена в корне, как уже отмечалось, равно нулю

$$u * (\alpha^l) = e(\alpha^l) \neq 0,$$

получаем систему уравнений

$$e_{i_1}\alpha^{l(i_1)} + e_{i_2}\alpha^{l(i_2)} + \cdots + e_{i_\nu}\alpha^{li_\nu} = S_l.$$

Пример 4. Построим циклический бинарный код с помощью корня неприводимого (примитивного) многочлена $x^4 + x + 1 \in F_2[x]$. Минимальные многочлены элементов α и α^3 перемножим и возьмем произведение в качестве порождающего многочлена (минимальные многочлены делят $x^{15} - 1$).

Поскольку порождающий многочлен делит многочлен $f \in F_2[x]/(x^{15} - 1)$ титт, когда $f(\alpha) = f(\alpha^3) = 0$, то проверочную матрицу можно взять в виде

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \ldots & \alpha^{42} \end{pmatrix}.$$

Компоненты векторного синдрома многочлена $v(x)$ обозначим

$$S_1 = \sum_{i=0}^{14} v_i\alpha^i,\ S_3 = \sum_{i=0}^{14} v_i\alpha^{3i},\ v_i \in F_2. \tag{5}$$

$$v(x) = \sum_{i=0}^{14} v_i x^i \text{ — многочлен из } F_2[x]/(x^{15} - 1).$$

В соответствии с определением синдромного многочлена, величины S_1 и S_3 равны значениям полученного многочлена при

$x = \alpha$ и $x = \alpha^3$. При отсутствии ошибки полученный многочлен совпадает с кодовым и $S_1 = S_3 = 0$. При наличии ошибок (5) равны соответствующим значениям многочлена ошибки.

Пусть теперь многочлен двойной ошибки имеет вид

$$e(x) = x^{i_1} + x^{i_2}, \quad 0 \le i_1,\, i_2 \le 14,\, i_1 \ne i_2.$$

Синдромные компоненты

$$S_1 = \alpha^{i_1} + \alpha^{i_2}, \quad S_3 = \alpha^{3i_1} + \alpha^{3i_2}$$

Синдром для α^2 ничего не дает, поскольку $e(\alpha^2) = e^2(\alpha)$.

Локаторы ошибок $X_1 = \alpha^{i_1}$, $X_2 = \alpha^{i_2}$. Связь синдромов и локаторов:

$$S_1 = X_1 + X_2,\; S_3 = X_1^3 + X_2^3 \Rightarrow \frac{X_1^3 + X_2^3}{X_1 + X_2} = X_1^2 + X_1X_2 + X_2^2 = (X_1 + X_2)^2 + X_1X_2.$$

Или

$$\begin{aligned} X_1 + X_2 &= S_1 \\ X_1 \cdot X_2 &= \frac{S_3 + S_1^3}{S_1}. \end{aligned}$$

По теореме Виета составляем квадратное уравнение. Локаторы ошибок — корни квадратного уравнения

$$z^2 + S_1 z + (S_1^2 + S_3 S_1^{-1}) = z^2 + \Lambda_1 z + \Lambda_2 = 0.$$

Возможные случаи:

1. синдромы нулевые, значит ошибок нет;
2. $S_1 \ne 0$, $S_3 = S_1^3$, один корень нулевой, второй S_1, одна ошибка;
3. два различные корня, две ошибки;

4. корней в поле $\mathbf{GF}(16)$ нет, ошибок более, чем две.

Обычно рассматривают уравнение для величин, обратных по отношению к локаторам

$$1 + S_1 x + (S_1^2 + S_3 S_1^{-1})x^2 = 1 + \Lambda_1 x + \Lambda_2 x^2 = 0,\ z = x^{-1}.$$

Пример 5. (Лидл-Нидеррайтер) Получено слово (100111000000000).

Найдем синдром (многочлен $u(x) = 1 + x^3 + x^4 + x^5$.)

$$H(u^*)^T = S = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix} = \begin{pmatrix} 1 + \alpha^3 + \alpha^4 + \alpha^5 \\ 1 + \alpha^9 + \alpha^{12} + \alpha^{15}. \end{pmatrix} = \begin{pmatrix} \alpha^2 + \alpha^3 \\ 1 + \alpha^2 \end{pmatrix}.$$

Учтено, что примитивный элемент удовлетворяет соотношению $\alpha^4 + \alpha + 1 = 0$.

Многочлен локаторов ошибки

$$1 + (\alpha^2 + \alpha^3)x + \left((\alpha^2 + \alpha^3)^2 + (1 + \alpha^2)(\alpha^2 + \alpha^3)^{-1}\right) x^2 = \quad (6)$$
$$= 1 + (\alpha^2 + \alpha^3)x + \left(1 + \alpha + \alpha^3\right) x^2 \quad (7)$$

Коэффициент при x^2 посчитан так. Сначала находим элемент $(\alpha^3 + \alpha^2)^{-1}$.

$\alpha^4 + \alpha + 1$		0	1
$\alpha^3 + \alpha^2$		1	0
$\alpha^2 + \alpha + 1$	$\alpha + 1$	$\alpha + 1$	1
α	α	$\alpha^2 + \alpha + 1$	
1	$\alpha + 1$	$\alpha^3 + \alpha$	

$(\alpha^2 + \alpha^3)^{-1} = \alpha + \alpha^3$.

$$(\alpha^2+\alpha^3)^2+(1+\alpha^2)(\alpha^2+\alpha^3)^{-1} = \alpha^4(1+\alpha^2)+(1+\alpha^2)(\alpha+\alpha^3) =$$
$$= (1+\alpha)(1+\alpha^2)+\alpha(1+\alpha^2)(1+\alpha^2) = 1+\alpha+\alpha^2+\alpha^3+\alpha(1+\alpha^4) =$$
$$= 1 + \alpha + \alpha^2 + \alpha^3 + \alpha\alpha = 1 + \alpha + \alpha^3.$$

Решение (6) подбором α, α^7, а локаторы — обратные величины, т. е. $X_1 = \alpha^{14}$, $X_2 = \alpha^8$.

Исправив ошибки, получаем кодовый многочлен(вектор) $\mathbf{u} = (100111001000001)$. Затем делим на порождающий многочлен и получаем сообщение $u(x)/g(x) = 1+x^3+x^5+x^6 \Rightarrow (1001011)$.

Задание по циклическим кодам

~~1 часть (если совсем невмоготу~~ **можно не делать**~~, но выполнение существенно улучшит вашу интеллектуальную ауру)~~

Построить циклический код (n,k) по номеру варианта N.

N	n,k	N	n,k	N	n,k	N	n,k
1	15,4	6	31,11	11	15,7	16	31,10
2	15,7	7	15,6	12	12,4	17	31,5
3	15,6	8	15,6	13	12,4	18	21,6
4	15,8	9	15,7	14	31,5	19	21,6
5	31,4	10	15,7	15	31,10	20	21,6

- построить подходящий (при заданных n и k) многочлен $g(x)$;
- записать соответствующие матрицы G и H;
- записать матрицы G_{syst} и H_{syst}, соответствующие систематическому варианту кодирования (делением);
- оценить исправляющие свойства кода, подсчитать количество синдромов.

2 часть (надо делать всем!)

Ниже вам предлагаются по одному принятому слову, закодированному умножением на многочлен $g(x) = (x^4+x^3+x^2+x+1)*(x^4+x^3+1)*(x^2+x+1) = 1+x^8+x^5+x^2+x^{10}+x^6+x^9$ (код C(15,5,7) ->(n,k,d)) провести декодирование двумя способами, как описано в руководстве. Получить вектор ошибки, исправленный вектор кода и исходное сообщение.

Вариант №1

$$r_1 := 1 + x^7 + x^4 + x^2 + x^6 + x + x^{14} + x^{15}$$

Вариант №2

$$r_2 := 1 + x + x^9 + x^2 + x^7 + x^{12} + x^{10}$$

Вариант №3

$$r_3 := 1 + x^7 + x^4 + x^2 + x^6 + x$$

Вариант №4

$$r_4 := 1 + x + x^9 + x^2 + x^{13} + x^7 + x^{12} + x^{11} + x^{15}$$

Вариант №5

$$r_5 := 1 + x^7 + x^4 + x^2 + x^{10} + x^6 + x + x^{14} + x^{13} + x^8$$

Вариант №6

$$r_6 := 1 + x + x^2 + x^7 + x^{12}$$

Вариант №7

$$r_7 := 1 + x^4 + x^2 + x^{10} + x^6 + x + x^{14} + x^{13}$$

Вариант №8

$$r_8 := 1 + x + x^9 + x^2 + x^7 + x^{12} + x^6$$

Вариант №9

$$r_9 := 1 + x^7 + x^4 + x^2 + x^6 + x + x^{14} + x^9$$

Вариант №10

$$r_{10} := 1 + x + x^9 + x^2 + x^{13} + x^7 + x^{12} + x^{10} + x^8$$

Вариант №11

$$r_{11} := 1 + x^4 + x^2 + x^6 + x + x^{14}$$

Вариант №12

$$r_{12} := 1 + x + x^9 + x^2 + x^{13} + x^7 + x^{12} + x^{10} + x^6$$

Вариант №13

$$r_{13} := 1 + x^7 + x^4 + x^2 + x^6 + x + x^{14} + x^5$$

Вариант №14

$$r_{14} := 1 + x + x^9 + x^2 + x^{13} + x^7 + x^{12} + x^{14} + x^8$$

Вариант №15

$$r_{15} := 1 + x^7 + x^4 + x^2 + x^{10} + x^6 + x + x^9$$

Вариант №16

$$r_{16} := 1 + x + x^9 + x^2 + x^{13} + x^{12} + x^{14}$$

Вариант №17

$$r_{17} := 1 + x^7 + x^4 + x^2 + x^6 + x + x^{14} + x^8$$

Вариант №18

$$r_{18} := 1 + x + x^9 + x^2 + x^{13} + x^7 + x^{12} + x^5 + x^8$$

Вариант №19

$$r_{19} := 1 + x^7 + x^4 + x^2 + x^{10} + x^6 + x + x^3$$

Вариант №20

$$r_{20} := 1 + x + x^9 + x^2 + x^7 + x^{12} + x^3$$

Разложения на неприводимые сомножители

```
> Factor(x^8-1) mod 3;
```

$$(x^2+1)\,(x+1)\,(x^2+x+2)\,(x+2)\,(x^2+2\,x+2)$$

```
> Factor(x^(15)+1) mod 2;
```

$$(x^4+x+1)\,(x+1)\,(x^4+x^3+1)\,(x^4+x^3+x^2+x+1)\,(x^2+x+1)$$

```
> Factor(x^(12)+1) mod 2;
```

$$(x+1)^4\,(x^2+x+1)^4$$

```
> Factor(x^(21)-1) mod 2;
```

$$(x^6+x^5+x^4+x^2+1)\,(x^3+x+1)\,(x+1)\,(x^3+x^2+1)\,(x^6+x^4+x^2+x+1)\,(x^2+x+1)$$

```
> Factor(x^(256)+x) mod 2;
```

$$(x^8+x^4+x^3+x^2+1)\,(x^8+x^7+x^6+x+1)\,(x^4+x+1)\,(x^8+x^7+x^6+x^3+x^2+x+1)$$
$$(x^8+x^5+x^3+x^2+1)\,(x+1)\,(x^8+x^7+x^6+x^5+x^4+x^2+1)\,(x^8+x^7+x^5+x^4+1)$$
$$(x^4+x^3+1)\,(x^8+x^5+x^3+x+1)\,(x^8+x^7+x^2+x+1)$$
$$(x^8+x^6+x^5+x^4+x^3+x+1)\,(x^8+x^7+x^5+x^3+1)\,(x^8+x^7+x^6+x^5+x^2+x+1)$$
$$(x^8+x^6+x^5+x^4+1)\,(x^8+x^6+x^5+x^3+1)\,(x^8+x^7+x^6+x^4+x^2+x+1)$$
$$(x^8+x^4+x^3+x+1)\,(x^4+x^3+x^2+x+1)\,(x^8+x^5+x^4+x^3+1)$$
$$(x^8+x^6+x^5+x^4+x^2+x+1)\,x\,(x^8+x^7+x^6+x^5+x^4+x+1)$$
$$(x^8+x^7+x^6+x^4+x^3+x^2+1)\,(x^8+x^5+x^4+x^3+x^2+x+1)$$
$$(x^8+x^7+x^6+x^5+x^4+x^3+1)\,(x^8+x^6+x^4+x^3+x^2+x+1)\,(x^2+x+1)$$
$$(x^8+x^7+x^4+x^3+x^2+x+1)\,(x^8+x^7+x^5+x+1)\,(x^8+x^7+x^3+x+1)$$
$$(x^8+x^7+x^5+x^4+x^3+x^2+1)\,(x^8+x^6+x^5+x^2+1)\,(x^8+x^6+x^5+x+1)$$
$$(x^8+x^7+x^3+x^2+1)\,(x^8+x^6+x^3+x^2+1)$$

```
> Factor(x^(8)+x) mod 2;
```

$$(x^3+x+1)\,(x+1)\,(x^3+x^2+1)\,x$$

```
> Factor(x^(16)+x) mod 2;
```

$$(x^4+x+1)\,(x+1)\,(x^4+x^3+1)\,(x^4+x^3+x^2+x+1)\,x\,(x^2+x+1)$$

```
> Factor(x^(32)+x) mod 2;
```

$$(x^5+x^4+x^3+x+1)\,(x+1)\,(x^5+x^3+x^2+x+1)\,(x^5+x^2+1)\,x\,(x^5+x^3+1)$$
$$(x^5+x^4+x^2+x+1)\,(x^5+x^4+x^3+x^2+1)$$

2. дополнения (декабрь 2008) для мануала к выполнению ИДЗ по циклическим кодам (А.Л.Крохин)

В данном документе более подробно прописаны две возможных "ручных" методик решения уравнения для локаторов. Перебор облегчается рекуррентной процедурой Ченя (21) или вычислением значений многочлена по схеме Горнера (16) $a_0+x(a_1+x(a_2+xa_3)))$**. Ваш лектор будет благодарен за вопросы или сообщения о каких-либо ошибках! (alkrochinGAVyandex.ru)**

Расширение с помощью неприводимого многочлена $f(x)$.

Множество классов вычетов по модулю произвольного многочлена образует кольцо. $[a(x)] + [b(x)] = [a(x) + b(x)]$, поскольку степень многочлена не повышается. $[a(x)] * [b(x)] = \mathrm{res}(a(x)b(x)/f(x))$, если степень произведения становится равной или большей степени модуля, находим остаток. Пусть многочлен приводим, т. е. $f(x) = f_1(x)f_2(x), \quad \deg f_i(x) < \deg f(x)$. Тогда в обозначениях классов вычетов $[f(x)] = [0] = [f_1(x)] * [f_2(x)]$. В поле не может быть делителей нуля! Если же многочлен-модуль неприводим, то делителей нуля нет. НОД $(f(x), r(x)) = 1$ для любого многочлена-остатка. И тогда существование мультипликативного обратного элемента следует из расширенного алгоритма Евклида.

Описание поля $\mathbf{GF}(2^4) = \mathbf{GF}(2)[x]/f(x)$, $f(x) = x^4 + x^3 + 1$.

Можно использовать несколько способов представления этого поля: а) множество многочленов-остатков; б) расширение поля $\mathbf{GF}(2)$ при помощи примитивного элемента α, минимальным многочленом которого является многочлен $x^4 + x^3 + 1$. Поскольку степени примитивного элемента, начиная с четвертой выражаются в виде линейных комбинаций элементов $\{1, \alpha, \alpha^2, \alpha^3\}$, то поле $\mathbf{GF}(2^4)$ можно еще рассматривать как линейное пространство над полем $\mathbf{GF}(2)$. Итак, каждый элемент $\mathbf{GF}(2^4)$ можно записывать в виде степени примитивного элемента, что удобно для выполнения умножения, или в виде линейной комбинации базисных элементов $\{1, \alpha, \alpha^2, \alpha^3\}$. Коэффициенты линейных комбинаций можно интерпретировать двоичными четырехразрядными числами (шестнадцатитичными) или даже соответствующими десятичными.

Второй примитивный многочлен четвертой степени — x^4+x+1. Можно использовать его корень при построении поля $\mathbf{GF}(2^4)$, что и делают некоторые авторы. Однако, соответствие между степенями примитивного многочлена и линейными комбинациями будет **другое**! Еще больше

произвола в записи двоичных(и десятичных) представлений — в представленной таблице коэффициенты при младших степенях стоят в качестве младших двоичных разрядов. При этом получается более "естественно" — $\alpha = 2$, $\alpha^2 = 4$, $\alpha^3 = 8$.

Примитивный многочлен $x^4 + x^3 + 1$				Примитивный многочлен $x^4 + x + 1$			
0	0000	0	0	0	0000	0	0
1	0001	α^0	1	1	0001	α^0	1
2	0010	α^1	α	2	0010	α^1	α
4	0100	α^2	α^2	4	0100	α^2	α^2
8	1000	α^3	α^3	8	1000	α^3	α^3
9	1001	α^4	$\alpha^3 + 1$,	3	0011	α^4	$1 + \alpha$,
11	1011	α^5	$\alpha^3 + \alpha + 1$,	6	0110	α^5	$\alpha + \alpha^2$,
15	1111	α^6	$\alpha^3 + \alpha^2 + \alpha + 1$,	12	1100	α^6	$\alpha^2 + \alpha^3$,
7	0111	α^7	$\alpha^2 + \alpha + 1$,	11	1011	α^7	$1 + \alpha + \alpha^3$,
14	1110	α^8	$\alpha^3 + \alpha^2 + \alpha$,	5	0101	α^8	$1 + \alpha^2$,
5	0101	α^9	$\alpha^2 + 1$,	10	1010	α^9	$\alpha + \alpha^3$,
10	1010	α^{10}	$\alpha^3 + \alpha$,	7	0111	α^{10}	$1 + \alpha + \alpha^2$,
13	1101	α^{11}	$\alpha^3 + \alpha^2 + 1$,	14	1110	α^{11}	$\alpha + \alpha^2 + \alpha^3$,
3	0011	α^{12}	$\alpha + 1$,	15	1111	α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$,
6	0110	α^{13}	$\alpha^2 + \alpha$,	13	1101	α^{13}	$1 + \alpha^2 + \alpha^3$,
12	1100	α^{14}	$\alpha^3 + \alpha^2$	9	1001	α^{14}	$1 + \alpha^3$

Локаторы ошибок $X_1 = \alpha^{i_1}$, $X_2 = \alpha^{i_2}$. Связь синдромов и локаторов:

$$S_1 = X_1 + X_2,\ S_3 = X_1^3 + X_2^3 \Rightarrow \frac{X_1^3 + X_2^3}{X_1 + X_2} = X_1^2 + X_1X_2 + X_2^2 = (X_1 + X_2)^2 + X_1X_2.$$

Или

$$\begin{aligned} X_1 + X_2 &= S_1 \\ X_1 \cdot X_2 &= \frac{S_3 + S_1^3}{S_1}. \end{aligned}$$

По теореме Виета локаторы ошибок — корни квадратного уравнения

$$z^2 + \Lambda_1 z + \Lambda_2.$$

Возможные случаи:

1. синдромы нулевые, значит ошибок нет;

2. $S_1 \neq 0$, $S_3 = S_1^3$, один корень нулевой, второй S_1, одна ошибка;

3. два различные корня, две ошибки;

4. корней в поле $\mathbf{GF}(16)$ нет, ошибок более, чем две.

———————————————————————

В этом примере использовать вторую таблицу, т.е. $\alpha^4 + \alpha + 1 = 0$.

Пример 6. Получено слово (100111000000000).

Найдем синдром

$$H(u^*)^T = S = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix} = \begin{pmatrix} 1+\alpha^3+\alpha^4+\alpha^5 \\ 1+\alpha^9+\alpha^{12}+\alpha^{15}. \end{pmatrix} = \begin{pmatrix} \alpha^2+\alpha^3 \\ 1+\alpha^2 \end{pmatrix}.$$

Учтено, что примитивный элемент удовлетворяет соотношению $\alpha^4 + \alpha + 1 = 0$.

Многочлен локаторов ошибки

$$1 + (\alpha^2+\alpha^3)x + \left((\alpha^2+\alpha^3)^2 + (1+\alpha^2)(\alpha^2+\alpha^3)^{-1}\right)x^2 = \\ = 1 + (\alpha^2+\alpha^3)x + \left(1+\alpha+\alpha^3\right)x^2$$

Решение получаем перебором, используя алгоритм Ченя (21),

i	$\gamma_{0,i}$	$\gamma_{1,i}$	$\gamma_{2,i}$	$\gamma_{0,i}+\gamma_{1,i}+\gamma_{2,i}$
0	1	α^6	α^7	
1	1	$\alpha^6\cdot\alpha$	$\alpha^9\cdot\alpha^2$	0
2	1	$\alpha^7\cdot\alpha$	$\alpha^{11}\cdot\alpha^2$	$\alpha+1$
3	1	$\alpha^8\cdot\alpha$	$\alpha^{13}\cdot\alpha^2$	$\alpha+\alpha^2$
4	1	$\alpha^9\cdot\alpha$	$\alpha^0\cdot\alpha^2$	$1+\alpha+\alpha^2$
5	1	$\alpha^{10}\cdot\alpha$	$\alpha^2\cdot\alpha^2$	$1+\alpha+\alpha^3$
6	1	$\alpha^{11}\cdot\alpha$	$\alpha^4\cdot\alpha^2$	$1+\alpha^2+\alpha^3$
7	1	$\alpha^{12\cdot}\alpha$	$\alpha^6\cdot\alpha^2$	0

$\{\alpha, \alpha^7\}$, а локаторы ошибок равны обратным величинам, т. е. $X_1 = \alpha^{14}$, $X_2 = \alpha^8$.

Можно и иначе. Решаем перебором по схеме Горнера:

α^i	$\alpha^7\alpha^i$	$() + \alpha^2 + \alpha^3$	$()\cdot\alpha^i$	$()+1$	$=?$
α	α^8	$1+\alpha^2+\alpha^2+\alpha^3$	$\alpha+\alpha^4$	$\alpha+\alpha^4+1$	0
α^2	α^9	$\alpha+\alpha^3+\alpha^2+\alpha^3$	$\alpha+\alpha^2$		
α^3	α^{10}				
α^7	α^{14}	$1+\alpha^2+\alpha^2+\alpha^3$	$\alpha^7+\alpha^9$	$1+\alpha+\alpha^3+\lvert al+\alpha^3+1$	$=0$

(8)

Исправив ошибки, получаем кодовый многочлен(вектор) $\mathbf{u} = (100111001000001)$. Затем делим на порождающий многочлен и получаем сообщение $u(x)/g(x) = 1 + x^3 + x^5 + x^6 \Rightarrow (1001011)$.

Пример. Рассмотрим БЧХ-код с конструктивным расстоянием $d = 5$, который может исправлять любую одиночную и двойную ошибку. В этом случае положим $b = 1$, $n = 15$, $q = 2$. Если через $m_i(x)$ обозначить минимальный многочлен над полем F_2 элемента α^i, где примитивный элемент $\alpha \in F_{16}$ является корнем многочлена $x^4 + x + 1$, то

$$m_1(x) = n_2(x) = m_4(x) = m_8(x) = 1 + x + x^4,$$
$$m_3(x) = m_6(x) = m_{12}(x) = m_9(x) = 1 = x + x^2 + x^3 + x^4.$$

Таком образом, порождающий многочлен рассматриваемого БЧХ-кода имеет вид

$$g(x) = m_1(x) \cdot m_3(x) = 1 + x^4 + x^6 + x^7 + x^8.$$

Уравнение для локаторов

$$s(x) = 1 + x + \alpha x^2.$$

Решаем по схеме Горнера перебором

α^i	$\alpha\alpha^i$	$\underbrace{(\alpha\alpha^i)}+1$	$\underbrace{(1+\alpha\alpha^i)}\cdot\alpha$	$()+1$	$=?$
α	α^2	$1+\alpha^2$	$\alpha^2+\alpha^4$	$\alpha^2+1+\alpha+1$	α
α^2	α^3	$1+\alpha^3$	$\alpha^5+\alpha^2$	$1+\alpha^2+\alpha+\alpha^2$	$=1+\alpha$
α^3	α^4	$1+\alpha^4$	α^4	$1+\alpha+1$	α
α^4	α^5	$1+\alpha^5$	$\alpha^4+\alpha^9$	$1+\alpha+\alpha+\alpha^3$	$=1+\alpha^3$
α^5	α^6	$1+\alpha^6$	$\alpha^5+\alpha^{11}$	$1+\alpha+\alpha^2+\alpha+\alpha^2+\alpha^3$	$=1+\alpha^3$
α^6	α^7	$1+\alpha^7$	$\alpha^6+\alpha^{13}$	$1+\alpha^2+\alpha^3+1+\alpha^2+\alpha^3$	$=0$
α^7	α^8	$1+\alpha^8$	α^7+1	$1+1+1+\alpha+\alpha^3$	$=1+\alpha+\alpha^3$
α^8	α^9	$1+\alpha^9$	$\alpha^8+\alpha^2$	$1+\alpha^2+1+\alpha^2$	$=0$

(9)

$\eta_1^{-1} = \alpha^8$, $\eta_2^{-1} = \alpha^6 \Rightarrow \eta_1 = \alpha^7$, $\eta_2 = \alpha^9$. Исправляем ошибки $w(x) = v(x) - e(x) = 1 + x^3 + x^6 + x^7 + x^{12} + x^7 + x^9 = 1 + x^3 + x^6 + x^{12} + x^9$. Для нахождения сообщения делим на порождающий многочлен. Результат $1 + x^3 + x^4$.

Пример 7. (Блейхут стр. 200) БЧХ-код (15,5), исправляющий три ошибки с порождающим многочленом $g(x) = 1+x+x^2+x^4+x^5+x^8+x^{10}$. Многочлен ошибки $e(x) = x^7+x^2$. Выполнить декодирование (хотя ответ и известен!!).

Решение Вычислим компоненты синдрома, используя арифметику в поле **GF**(16):

$$\begin{aligned} S_1 &= \alpha^7 + \alpha^2 = \alpha^{12} && (10)\\ S_2 &= \alpha^{14} + \alpha^4 = \alpha^9 && (11)\\ S_3 &= \alpha^{21} + \alpha^6 = 0 && (12)\\ S_4 &= \alpha^{28} + \alpha^8 = \alpha^3 && (13)\\ S_5 &= \alpha^{35} + \alpha^{10} = \alpha^0 && (14)\\ S_6 &= \alpha^{42} + \alpha^{12} = 0 && (15) \end{aligned}$$

Работаем по алгоритму Петерсона и др.

Пусть $\nu = 3$, тогда

$$M = \begin{vmatrix} S_1 & S_2 & S_3 \\ S_2 & S_2 & S_4 \\ S_3 & S_4 & S_5 \end{vmatrix} = \begin{vmatrix} \alpha^{12} & \alpha^6 & 0 \\ \alpha^9 & 0 & \alpha^3 \\ 0 & \alpha^3 & \alpha^0 \end{vmatrix}, \quad \det(M) = 0.$$

Ошибок не три, пусть $\nu = 2$.

$$M = \begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} = \begin{pmatrix} \alpha^{12} & \alpha^9 \\ \alpha^9 & 0 \end{pmatrix}, \quad \det(M) = -\alpha^{18} = \alpha^3.$$

Ошибок две.

$$\begin{pmatrix} \Lambda_2 \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} 0 & \alpha^6 \\ \alpha^6 & \alpha^3 \end{pmatrix} \begin{pmatrix} \alpha^9 \\ \alpha^{12} \end{pmatrix}.$$

Многочлен будет $\Lambda(z) = \alpha^9 z^2 + \alpha^{12} z + 1$. Решаем по схеме Горнера перебором

α^i	$\alpha^7\alpha^i$	$() + \alpha^2 + \alpha^3$	$() \cdot \alpha^i$	$() + 1$	$=?$
α	α^8	$1 + \alpha^2 + \alpha^2 + \alpha^3$	$\alpha + \alpha^4$	$\alpha + \alpha^4 + 1$	0
α^2	α^9	$\alpha + \alpha^3 + \alpha^2 + \alpha^3$	$\alpha + \alpha^2$		
α^3	α^{10}				
α^7	α^{14}	$1 + \alpha^2 + \alpha^2 + \alpha^3$	$\alpha^7 + \alpha^9$	$1 + \alpha + \alpha^3 + \alpha + \alpha^3 + 1$	$= 0$

(16)

$$(\alpha^7 z + 1)(\alpha^2 z + 1) = \alpha^9 (z + \alpha^8)(z + \alpha^{13}).$$

Решения $\{\alpha^8, \alpha^{13}\}$, находим обратные элементы — локаторы ошибок. $e(x) = x^2 + x^7$.

Решение, используя алгоритм Ченя (21).

i	$\gamma_{0,i}$	$\gamma_{1,i}$	$\gamma_{2,i}$	$\gamma_{0,i}+\gamma_{1,i}+\gamma_{2,i}$	$=?$
0	1	α^{12}	α^9	$1+\alpha^{12}+\alpha^9$	$=\alpha^2$
1	1	$\alpha^{12}\cdot\alpha$	$\alpha^9\cdot\alpha^2$	$\not1+\not1+\not\alpha^2+\not\alpha^3+\alpha+\not\alpha^2+\not\alpha^3$	$=\alpha$
2	1	$\alpha^{13}\cdot\alpha$	$\alpha^{11}\cdot\alpha^2$	$\not1+\not1+\not\alpha^3+\alpha^2+1+\not\alpha^3$	$=1+\alpha^2$
3	1	$\alpha^{14}\cdot\alpha$	$\alpha^{13}\cdot\alpha^2$	$\not1+\not1+1$	$=1$
4	1	$\alpha^0\cdot\alpha$	$\alpha^0\cdot\alpha^2$	$1+\alpha+\alpha^2$	$=\alpha^{10}$
5	1	$\alpha^1\cdot\alpha$	$\alpha^2\cdot\alpha^2$	$\not1+\alpha+\not1+\alpha^2$	$=\alpha+\alpha^2$
6	1	$\alpha^2\cdot\alpha$	$\alpha^4\cdot\alpha^2$	$1+\alpha^2+\not\alpha^3+\not\alpha^3$	$=1+\alpha^2$
7	1	$\alpha^3\cdot\alpha$	$\alpha^6\cdot\alpha^2$	$\not1+\not1+\alpha+1+\alpha^2$	$1+\alpha+\alpha^2$
8	1	$\alpha^4\cdot\alpha$	$\alpha^8\cdot\alpha^2$	$\not1+\not1+\not\alpha^2+\not\alpha+\not\alpha^2+\not\alpha$	$=0$
9	1	$\alpha^5\cdot\alpha$	$\alpha^{10}\cdot\alpha^2$	$1+\alpha^2+\alpha^3+1+\alpha+\alpha^2+\alpha^3$	$=\alpha$
10	1	$\alpha^6\cdot\alpha$	$\alpha^{12}\cdot\alpha^2$	$\not1+\not\alpha^3+\not1+\alpha+1+\not\alpha^2+\not\alpha^2+\not\alpha^3$	$=1+\alpha$
11	1	$\alpha^7\cdot\alpha$	$\alpha^{14}\cdot\alpha^2$	$\not1+\not1+\alpha+\alpha^2$	$=\alpha+\alpha^2$
12	1	$\alpha^8\cdot\alpha$	$\alpha^1\cdot\alpha^2$	$1+\alpha+\not\alpha^3+\not\alpha^3$	$=1+\alpha$
13	1	$\alpha^9\cdot\alpha$	$\alpha^3\cdot\alpha^2$	$\not1+\not1+\not\alpha+\not\alpha^2+\not\alpha+\not\alpha^2$	$=0$

Корни уравнения $\{\alpha^{13}, \alpha^8\}$, а локаторы ошибок равны обратным величинам, т. е. $X_1=\alpha^2$, $X_2=\alpha^7$.

Процедура Ченя (R.T.Chien, "Cyclic Decoding Procedure for the Bose-Chaudhuri-Hocquenghem Codes,IEEE Transactions on Information Theory, Vol. IT-10, pp.357-363,October 1964.")

Требуется найти корни полинома (над конечным полем $\mathbf{GF}(q)$)

$$\Lambda(x)=\lambda_0+\lambda_1 x+\lambda_2 x^2+\dots\lambda_t x^t.$$

В конечном поле небольшого порядка это можно сделать простым перебором, но есть возможность ускорить вычисления. Каждый ненулевой элемент поля $\mathbf{GF}(q)$ выражается некоторой степенью примитивного элемента α^i, $\quad 0\le i\le N-1$.

Вычисляем значения многочлена $\Lambda(x)$ для двух последовательных степеней α

разные способы записи

$$\begin{aligned}\Lambda(\alpha^i) &= \lambda_0+\lambda_1(\alpha^i)+\lambda_2(\alpha^i)^2+\dots\lambda_t(\alpha^i)^t &(17)\\ &\triangleq \gamma_{0,i}+\gamma_{1,i}+\gamma_{2,i}\cdots+\gamma_{t,i}. &(18)\end{aligned}$$

$$\begin{aligned}\Lambda(\alpha^i)=\lambda_0+\lambda_1(\alpha^i)+\lambda_2(\alpha^i)^2+\dots\lambda_t(\alpha^i)^t &(19)\\ \gamma_{0,i}+\gamma_{1,i}+\gamma_{2,i}\cdots+\gamma_{t,i}. &(20)\end{aligned}$$

$$\begin{aligned}\Lambda(\alpha^{i+1}) &= \lambda_0 + \lambda_1(\alpha^{i+1}) + \lambda_2(\alpha^{i+1})^2 + \dots \lambda_t(\alpha^{i+1})^t \\ &= \lambda_0 + \lambda_1(\alpha^i)\alpha + \lambda_2(\alpha^i)^2\alpha^2 + \dots \lambda_t(\alpha^i)^t\alpha^t \\ &= \gamma_{0,i} + \gamma_{1,i}\alpha + \gamma_{2,i}\alpha^2 \cdots + \gamma_{t,i}\alpha^t \\ &\triangleq \gamma_{0,i+1} + \gamma_{1,i+1} + \gamma_{2,i+1} \cdots + \gamma_{t,i+1}.\end{aligned}$$

Замечаем, что вычисления можно провести, используя рекуррентное соотношение

$$\gamma_{j,i+1} = \gamma_{j,i}\alpha^j,\ \gamma_{j,0} = \lambda_j \tag{21}$$

$$\gamma_{j,0} = \lambda_j,\ \gamma_{j,1} = \lambda_j\alpha^j,\ \gamma_{j,2} = \gamma_{j,1}\alpha^j.$$