Разбор контрольной работы

Общие комментарии по результатам проверки контрольной:

1. В вычислениях присутствует большое количество арифметических ошибок. Само по себе возникновение арифметических ошибок неизбежно. Поэтому для получения правильного ответа необходимо конечный результат, а также по возможности промежуточные результаты проверять на корректность. В простейшем виде такая проверка на корректность есть простое подставление ответа в условие задачи. Далее в рамках разбора решений задач указывается ряд тестов, которыми можно пользоваться для проверок.

2. В вычислениях многие не пользуются представлением элементов поля как степеней примитивного элемента. Из-за этого ряд выкладок значительно усложняется. Степенная запись позволяет легко вычислять произведение и частное элементов поля, в частности, поиск обратных элементов.

3. В решениях мало используется расширенный алгоритм Евклида. На практике зачастую он приводит к ответу гораздо быстрее, чем альтернативные методы. Здесь стоит упомянуть, в первую очередь, задачу поиска обратного элемента в поле и задачу поиска полинома локаторов ошибок для декодирования БЧХ кода.

4. Пусть $w(x)$ – некоторый многочлен над полем. В большом числе случаев его возведение в степень $w^k(x)$ удобнее вычислять как $w^i(x)w^j(x)$, где $i+j=k$, а не как $w(x)w^{k-1}(x)$.

5. Следует иметь в виду, что если многочлен $f(x)$ не имеет корней в поле, то это не значит, что он неприводим.

Далее разбирается решение некоторых задач из контрольной работы. Решение других задач либо присутствует в материалах по курсу, либо очевидно получается при умении решать задачи, разбираемые ниже.

Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(-2x^2+x+2)$ *построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля. С помощью данной таблицы вычислить выражение*

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)}.$$

Заданное поле имеет характеристику 3. Поэтому в вычислениях в данном поле все константы следует приводить по модулю 3. В частности, многочлен, используемый для построения поля, $-2x^2+x+2 = x^2+x+2$. В заданном поле все вычисления проводятся по модулю многочлена x^2+x+2. Следовательно, в этом поле

$$x^2+x+2=0 \;\Rightarrow\; x^2 = -x-2 = 2x+1. \tag{1}$$

Всего в поле $\mathbb{F}_3^2$ находится $3^2-1=8$ ненулевых элементов. Известно, что все ненулевые элементы поля могут быть представлены как $\alpha^i, i=1,\ldots,8$, где α – некоторый примитивный элемент поля.

Возьмём в качестве α элемент x и вычислим все его степени с учётом (1):

$$
\begin{aligned}
&x^2 = 2x + 1,\\
&x^3 = x \cdot x^2 = x(2x+1) = 2x^2 + x = 2(2x+1) + x = 2x + 2,\\
&x^4 = x \cdot x^3 = x(2x+2) = 2x^2 + 2x = 2(2x+1) + 2x = 2,\\
&x^5 = x \cdot x^4 = 2x,\\
&x^6 = x \cdot x^5 = 2x^2 = 2(2x+1) = x + 2,\\
&x^7 = x \cdot x^6 = x(x+2) = x^2 + 2x = 2x + 1 + 2x = x + 1,\\
&x^8 = x \cdot x^7 = x(x+1) = x^2 + x = 2x + 1 + x = 1.
\end{aligned}
$$

Последнее свойство $x^8 = 1$ следует из общих свойств поля и является проверкой на корректность проведённых вычислений.

Теперь вычислим значение выражения:

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} = \frac{x^8}{x^2} - \frac{(x^5)^7 x^4}{x^9 x^6} = x^6 - x^{35+4-9-6} = x^6 + 2x^{24} = x^6 + 2 = x + 2 + 2 = x + 1.$$

Заметим, что в общем случае элемент x не всегда является примитивным (эквивалентно, многочлен, используемый для построения поля, не является примитивным). В этом случае для построения таблицы соответствий между степенным и полиномиальным представлением необходимо сначала найти примитивный элемент – некоторый элемент, имеющий порядок $p^n - 1$. Рассмотрим решение следующей задачи:

Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(x^2+1)$ построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля.

В данном поле $x^2 + 1 = 0$, т.е. $x^2 = 2$. Найдём порядок элемента x. Для этого достаточно проверить степени, являющиеся делителями $3^2 - 1 = 8$, т.е. 2 и 4:

$$
\begin{aligned}
&x^2 = 2,\\
&x^4 = (x^2)^2 = 1.
\end{aligned}
$$

Следовательно, элемент x имеет порядок 4 и не является примитивным элементом. Также не являются примитивными все степени элемента x, т.е. элементы:

$$
\begin{aligned}
&x^2 = 2,\\
&x^3 = 2x,\\
&x^4 = 1.
\end{aligned}
$$

Возьмём элемент $x + 1$ и найдём его порядок:

$$
\begin{aligned}
&(x+1)^2 = x^2 + 2x + 1 = 2x,\\
&(x+1)^4 = (2x)^2 = 2.
\end{aligned}
$$

Значит, порядок $x + 1$ равен 8, т.е. он является примитивным элементом. Теперь вычислим все его степени:

$$
\begin{aligned}
&\alpha = x + 1,\\
&\alpha^2 = 2x,\\
&\alpha^3 = 2x(x+1) = 2x + 1,\\
&\alpha^4 = (\alpha^2)^2 = 2,\\
&\alpha^5 = 2(x+1) = 2x + 2,\\
&\alpha^6 = \alpha^2 \cdot \alpha^4 = x,\\
&\alpha^7 = x(x+1) = x + 2,\\
&\alpha^8 = (\alpha^4)^2 = 1.
\end{aligned}
$$

Заметим, что вычисление очередной степени α^i часто бывает удобным провести как $\alpha^j \cdot \alpha^k$, где $j + k = i$, а не как $\alpha \cdot \alpha^{i-1}$.

В фактор-кольце $\mathbb{F}_3[x]/(x^4+1)$ *найти все элементы главного идеала* (x^2+x+2).

Сначала проверим, является ли элемент x^2+x+2 делителем x^4+1:

$$x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2).$$

Так как элемент, порождающий идеал, является делителем многочлена, используемого при построении фактор-кольца, то

$$(x^2 + x + 2) = \{(x^2 + x + 2)(ax + b), a, b \in \mathbb{F}_3\}.$$

Проведём умножение:

$$(x^2 + x + 2)(ax + b) = ax^3 + (a + b)x^2 + (2a + b)x + 2b.$$

Теперь можно записать все элементы идеала, перебирая все возможные значения $a, b \in \mathbb{F}_3$:

a	b	элемент идеала
0	0	0
0	1	$x^2 + x + 2$
0	2	$2x^2 + 2x + 1$
1	0	$x^3 + x^2 + 2x$
1	1	$x^3 + 2x^2 + 2$
1	2	$x^3 + x + 1$
2	0	$2x^3 + 2x^2 + x$
2	1	$2x^3 + 2x + 2$
2	2	$2x^3 + x^2 + 1$

Заметим, что в полном соответствии с теорией в данном случае ненулевой элемент идеала минимальной степени совпадает с порождающим многочленом $x^2 + x + 2$.

В поле $\mathbb{F}_7[x]/(x^4+x^3+x^2+3)$ *найти обратный элемент для* x^2+x+3.

Проще всего обратный элемент можно найти путём решения уравнения

$$(x^4 + x^3 + x^2 + 3)a(x) + (x^2 + x + 3)b(x) = 1 \tag{2}$$

с помощью расширенного алгоритма Евклида. Тогда $b(x)$ будет искомым обратным элементом. Шаги алгоритма Евклида:

Шаг 0. $r_{-2}(x) = x^4 + x^3 + x^2 + 3$, // Инициализация
$r_{-1}(x) = x^2 + x + 3$,
$y_{-2}(x) = 0$,
$y_{-1}(x) = 1$.

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$, // Делим с остатком $r_{-2}(x)$ на $r_{-1}(x)$
$q_0(x) = x^2 + 5$,
$r_0(x) = 2x + 2$,
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = -x^2 - 5$.

Шаг 2. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$, // Делим с остатком $r_{-1}(x)$ на $r_0(x)$
$q_1(x) = 4x$,
$r_1(x) = 3$,
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) = 1 + 4x(x^2 + 5) = 4x^3 + 6x + 1$.

Заметим, что в итерациях алгоритма нет необходимости вычислять $x_i(x)$, т.е. коэффициент при $x^4 + x^3 + x^2 + 3$, т.к. нас интересует только коэффициент при $x^2 + x + 3$, т.е. $y_i(x)$. Алгоритм заканчивает свою работу на шаге 2, т.к. степень очередного остатка r_1 равна степени многочлена в правой части (2). Однако, сам остаток r_1 отличается от требуемого на константный множитель. Действительно, после шага 2 мы имеем

$$(x^4 + x^3 + x^2 + 3)x_1(x) + (x^2 + x + 3)y_1(x) = 3.$$

Чтобы получить решение уравнения (2), достаточно домножить последний результат на $3^{-1} = 5$:

$$b(x) = 5y_1(x) = 5(4x^3 + 6x + 1) = 6x^3 + 2x + 5.$$

Проверим, что найденный $b(x)$ действительно является обратным к $x^2 + x + 3$:

$$b(x)(x^2 + x + 3) = (6x^3 + 2x + 5)(x^2 + x + 3) = 6x^5 + 6x^4 + 6x^3 + 4x + 1 = \\ = 6x(-x^3 - x^2 - 3) + 6x^4 + 6x^3 + 4x + 1 = 1.$$

В поле $\mathbb{F}_5^2 = \mathbb{F}_5[x]/(x^2 + 3x + 3)$ *найти обратную для матрицы*

$$\begin{bmatrix} 3x + 4 & x + 2 \\ x + 3 & 3x + 2 \end{bmatrix}.$$

Для матриц размера 2×2 обратная матрица может быть записана как

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Сначала вычислим определитель заданной матрицы с учётом $x^2 = 2x + 2$:

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

Далее найдём обратный элемент к $4x + 3$ путём решения уравнения

$$(x^2 + 3x + 3)a(x) + (4x + 3)b(x) = 1$$

с помощью расширенного алгоритма Евклида:

Шаг 0. $r_{-2}(x) = x^2 + 3x + 3$, // Инициализация
$r_{-1}(x) = 4x + 3$,
$y_{-2}(x) = 0$,
$y_{-1}(x) = 1$.

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$, // Делим с остатком $r_{-2}(x)$ на $r_{-1}(x)$
$q_0(x) = 4x + 4$,
$r_0(x) = 1$,
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = -4x - 4 = x + 1$.

В результате $(4x + 3)^{-1} = y_0(x) = x + 1$. Наконец, вычислим обратную матрицу

$$\begin{bmatrix} 3x + 4 & x + 2 \\ x + 3 & 3x + 2 \end{bmatrix}^{-1} = (x + 1) \begin{bmatrix} 3x + 2 & 4x + 3 \\ 4x + 2 & 3x + 4 \end{bmatrix} = \begin{bmatrix} x + 3 & 1 \\ 4x & 3x \end{bmatrix}.$$

В конце убедимся в правильности проведённых вычислений непосредственной проверкой

$$\begin{bmatrix} 3x + 4 & x + 2 \\ x + 3 & 3x + 2 \end{bmatrix} \begin{bmatrix} x + 3 & 1 \\ 4x & 3x \end{bmatrix} = \begin{bmatrix} (3x + 4)(x + 3) + 4x(x + 2) & 3x + 4 + 3x(x + 2) \\ (x + 3)^2 + 4x(3x + 2) & x + 3 + 3x(3x + 2) \end{bmatrix} = \\ = \begin{bmatrix} 2x^2 + x + 2 & 3x^2 + 4x + 4 \\ 3x^2 + 4x + 4 & 4x^2 + 2x + 3 \end{bmatrix} = \begin{bmatrix} 2(2x + 2) + x + 2 & 3(2x + 2) + 4x + 4 \\ 3(2x + 2) + 4x + 4 & 4(2x + 2) + 2x + 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Разложить на неприводимые множители многочлен $f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.

Сначала пытаемся найти корни $f(x)$ в $\mathbb{F}_2$:

$$f(0) = 1,$$
$$f(1) = 1.$$

Значит, $f(x)$ не имеет корней в $\mathbb{F}_2$, т.е. не имеет линейных множителей в своём разложении над $\mathbb{F}_2$. Далее пытаемся найти неприводимые многочлены степени 2, являющиеся делителями $f(x)$. Над

$\mathbb{F}_2$ существует только один неприводимый многочлен степени 2: x^2+x+1. При делении $f(x)$ на x^2+x+1, получаем

$$f(x) = (x^2+x+1)(x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1).$$

Продолжая делить дальше на x^2+x+1, получаем

$$x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1 = (x^2+x+1)(x^7+x^4+x^3+x^2+x+1)+x.$$

Неприводимых многочленов степени 3 над $\mathbb{F}_2$ всего два: x^3+x+1 и x^3+x^2+1. Пробуем поделить на x^3+x+1:

$$x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1 = (x^3+x+1)(x^6+x^5+x^3+x^2+1).$$

Производя деления далее на многочлены третьей степени, получаем

$$x^6+x^5+x^3+x^2+1 = (x^3+x+1)(x^3+x^2+x+1)+x^2,$$
$$x^6+x^5+x^3+x^2+1 = (x^3+x^2+1)x^3+x^2+1.$$

Так как многочлен 6-ой степени $x^6+x^5+x^3+x^2+1$ не имеет делителей 3-ей и меньших степеней, то он является неприводимым (если бы он имел делитель, скажем, степени 4, то у него был бы и делитель степени 6-4=2). В итоге $f(x)$ раскладывается как

$$f(x) = (x^2+x+1)(x^3+x+1)(x^6+x^5+x^3+x^2+1).$$

Найти минимальное поле характеристики 3, в котором многочлен $f(x) = x^3+x+2 \in \mathbb{F}_3[x]$ раскладывается на линейные множители.

Найдём разложение многочлена на неприводимые множители над $\mathbb{F}_3$. Проверяем корни в $\mathbb{F}_3$:

$$f(0) = 2,$$
$$f(1) = 1,$$
$$f(2) = 0.$$

Отсюда получаем, что $x^3+x+2 = (x+1)(x^2+2x+2)$. Многочлен x^2+2x+2 не имеет корня $x=2$. Следовательно, он является неприводимым.

Известно, что любой неприводимый многочлен $f(x)$ степени n над конечным полем F из q элементов раскладывается на линейные множители в расширении F, построенном как $F[x]/(f(x))$. В этом расширении $f(x)$ имеет n корней $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^n}$, где α – произвольный корень $f(x)$ в построенном расширении F. При этом многочлен $f(x)$ не имеет корней ни в каком конечном поле, содержащим менее, чем q^n элементов, и имеющим ту же характеристику, что и F.

Рассмотрим расширение поля $\mathbb{F}_3$: $\mathbb{F}_3[x]/(x^2+2x+2)$. В этом расширении многочлен x^2+2x+2 имеет корни α и $\alpha^3 = \alpha\cdot\alpha^2 = \alpha(\alpha+1) = \alpha^2+\alpha = 2\alpha+1$. Кроме того, данное расширение содержит в себе корень 2, найденный ранее для $f(x)$. Таким образом, многочлен $f(x)$ в поле $\mathbb{F}_3[x]/(x^2+2x+2)$ раскладывается на линейные множители:

$$f(x) = x^3+x+2 = (x+1)(x+2\alpha)(x+\alpha+2).$$

В общем случае процесс получения всех корней некоторого многочлена $f(x)$ над конечным полем F из q элементов можно представить следующим образом:

1. Разложить $f(x)$ на неприводимые множители над F:

   $$f(x) = m_1(x)m_2(x)\ldots m_k(x).$$

   Пусть $d_i = \deg m_i$.

2. Для каждого $m_i(x)$ рассмотреть расширение $F[x]/(m_i(x))$ и взять в нём корни $\alpha, \alpha^q, \ldots, \alpha^{q^{d_i}}$.

3. Объединить все корни в одном общем расширении F. Данное расширение будет состоять из $q^{\text{НОК}(m_1,m_2,\ldots,m_k)}$ элементов.

Найти минимальный многочлен $m(x) \in \mathbb{F}_5[x]$, который имеет корень α^3, где α – примитивный элемент поля $\mathbb{F}_5^2 = \mathbb{F}_5[x]/(x^2+x+2)$.

Известно, что минимальный многочлен $m(x)$ в поле $\mathbb{F}_5^2$ содержит вместе с корнем α^3 все смежные с ним $(\alpha^3)^5, (\alpha^3)^{5^2}, \ldots$. С учётом $\alpha^{5^2-1} = \alpha^{24} = 1$ получаем, что смежный класс, образованный α^3, содержит только два элемента α^3 и α^{15}. Следовательно, минимальный многочлен имеет степень 2 и может быть представлен как

$$m(x) = (x-\alpha^3)(x-\alpha^{15}) = x^2 - (\alpha^3+\alpha^{15})x + \alpha^{18}.$$

Найдём коэффициенты многочлена с учётом $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}
&\alpha^3 = \alpha\cdot\alpha^2 = \alpha(4\alpha+3) = 4\alpha^2+3\alpha = 4(4\alpha+3)+3\alpha = 4\alpha+2,\\
&\alpha^{15} = (\alpha^3)^5 = (4\alpha+2)^5 = 4\alpha^5+2 = 4\alpha^2\alpha^3+2 = 4(4\alpha+3)(4\alpha+2)+2 =\\
&\qquad = 4(\alpha^2+1)+2 = 4(4\alpha+4)+2 = \alpha+3,\\
&\alpha^3+\alpha^{15} = 4\alpha+2+\alpha+3 = 0,\\
&\alpha^{18} = \alpha^3\alpha^{15} = (4\alpha+2)(\alpha+3) = 4(4\alpha+3)+4\alpha+1 = 3.
\end{aligned}$$

Заметим, что в полном соответствии с теорией значения коэффициентов $m(x)$ получились из $\mathbb{F}_5$. В итоге

$$m(x) = x^2+3.$$

Линейный код задан своей проверочной матрицей

$$H = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Требуется построить порождающую матрицу кода G для систематического кодирования, при котором биты исходного сообщения переходят в последние биты кодового слова. Найти систематическое кодирование для векторов $\boldsymbol{u}_1 = [1\ 1\ 0]^T$, $\boldsymbol{u}_2 = [1\ 0\ 1]^T$.

Порождающая матрица кода G, обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P \\ I_3 \end{bmatrix}$, где I_3 – единичная матрица размера 3×3. Такую матрицу можно получить, если привести проверочную матрицу H к виду $\begin{bmatrix} I_3 & P \end{bmatrix}$, т.е. с помощью эквивалентных преобразований строк выделить в первых трех колонках единичную матрицу:

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \xrightarrow{1\leftrightarrow 3} \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{1\leftarrow 1+2} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{1\leftarrow 1+3} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Теперь можно построить требуемую порождающую матрицу и осуществить кодирование для $\boldsymbol{u}_1$ и $\boldsymbol{u}_2$:

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad [\boldsymbol{v}_1, \boldsymbol{v}_2] = G[\boldsymbol{u}_1, \boldsymbol{u}_2] = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Циклический $(9,3)$-код задан своим порождающим полиномом $g(x) = x^6+x^3+1$. Требуется определить минимальное расстояние кода d, а также осуществить систематическое кодирование полинома $u(x) = x^2+x$.

Для определения минимального кодового расстояния d найдём все кодовые полиномы:

$$v(x) = g(x)(ax^2+bx+c) = (x^6+x^3+1)(ax^2+bx+c) = ax^8+bx^7+cx^6+ax^5+bx^4+cx^3+ax^2+bx+c,\ a,b,c \in \mathbb{F}_2.$$

В векторном виде все кодовые слова представляются как $[a,b,c,a,b,c,a,b,c]$. Следовательно, минимальный хэммингов вес ненулевого кодового слова равен 3, т.е. $d = 3$.

Систематическое кодирование полинома $u(x)$ вычисляем непосредственно

$$v(x) = x^6u(x) + \mathrm{mod}(x^6u(x), g(x)) = x^8 + x^7 + \mathrm{mod}(x^8 + x^7, x^6 + x^3 + 1) = x^8 + x^7 + x^5 + x^4 + x^2 + x.$$

Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом $\alpha \in \mathbb{F}_2[x]/(x^3 + x + 1)$. *Требуется декодировать полученный полином* $w(x) = x^7 + x^6 + x^2 + 1$.

Вычислим синдром с учётом $\alpha^3 = \alpha + 1$:

$$\begin{aligned} s = w(\alpha) &= \alpha^7 + \alpha^6 + \alpha^2 + 1 = \alpha(\alpha^3)^2 + (\alpha^3)^2 + \alpha^2 + 1 = \\ &= \alpha(\alpha+1)^2 + (\alpha+1)^2 + \alpha^2 + 1 = \alpha(\alpha^2+1) + \alpha^2 + 1 + \alpha^2 + 1 = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1. \end{aligned}$$

Далее необходимо найти полином ошибок вида $e(x) = x^k$ такой, что $e(\alpha) = s$, т.е. найти k: $\alpha^k = 1$. Очевидно, что $k = 0$. Следовательно, $\hat{v}(x) = w(x) + e(x) = x^7 + x^6 + x^2$.

Рассмотрим код БЧХ с нулями $\alpha^i,\ i = 1,\dots,4$, *где* α *– примитивный элемент поля* $\mathbb{F}_2[x]/(x^4 + x + 1)$. *Требуется найти полином локаторов ошибок* $\sigma(x)$ *для принятого полинома* $w(x) = x^{14} + x^{10} + x^5 + x^4$.

Для удобства вычислений в поле $\mathbb{F}_2^4$ построим таблицу соответствий между степенным и полиномиальным представлением элементов поля:

α	α
α^2	α^2
α^3	α^3
α^4	$\alpha + 1$
α^5	$\alpha^2 + \alpha$
α^6	$\alpha^3 + \alpha^2$
α^7	$\alpha^3 + \alpha + 1$
α^8	$\alpha^2 + 1$
α^9	$\alpha^3 + \alpha$
α^{10}	$\alpha^2 + \alpha + 1$
α^{11}	$\alpha^3 + \alpha^2 + \alpha$
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$
α^{13}	$\alpha^3 + \alpha^2 + 1$
α^{14}	$\alpha^3 + 1$
α^{15}	1

С помощью этой таблицы вычислим синдромы:

$$\begin{aligned} s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \alpha^7, \\ s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\ s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\ s_4 &= w(\alpha^4) = (w(\alpha^2))^2 = \alpha^{13}. \end{aligned}$$

В результате синдромный полином $s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1$. Синдромов всего четыре, следовательно, $t = 2$. Полином локаторов ошибок $\sigma(x)$ является решением уравнения

$$x^{2t+1}a(x) + s(x)\sigma(x) = \lambda(x),\ \deg\lambda(x) \le t.$$

Решим данное уравнение с помощью расширенного алгоритма Евклида:

Шаг 0. $r_{-2}(x) = x^5$, // Инициализация
$r_{-1}(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1$,
$y_{-2}(x) = 0$,
$y_{-1}(x) = 1$.

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$, // Делим с остатком $r_{-2}(x)$ на $r_{-1}(x)$
$q_0(x) = \alpha^2 x$,
$r_0(x) = \alpha x^3 + \alpha^9 x^2 + \alpha^2 x$,
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = \alpha^2 x$.

Шаг 2. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$, // Делим с остатком $r_{-1}(x)$ на $r_0(x)$
$q_1(x) = \alpha^{12}x + \alpha^5$,
$r_1(x) = \alpha^{14}x^2 + 1$,
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) = 1 + \alpha^2 x(\alpha^{12}x + \alpha^5) = \alpha^{14}x^2 + \alpha^7 x + 1$.

Таким образом, искомый полином локаторов ошибок $\sigma(x) = \alpha^{14}x^2 + \alpha^7 x + 1$.

Рассмотрим код БЧХ, нули которого определяются степенями α, где α – примитивный элемент поля $\mathbb{F}_2[x]/(x^4 + x + 1)$. Пусть для некоторого принятого слова $w(x)$ полином локаторов ошибок $\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1$. Требуется определить позиции ошибок в $w(x)$.

Найдём корни полинома локаторов ошибок полным перебором. Для вычислений будем пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов поля, вычисленной выше:

$$
\begin{aligned}
&\sigma(\alpha) = \alpha^4 + \alpha^7 + 1 = \alpha^3 + 1,\\
&\sigma(\alpha^2) = \alpha^6 + \alpha^8 + 1 = \alpha^3,\\
&\sigma(\alpha^3) = \alpha^8 + \alpha^9 + 1 = \alpha^3 + \alpha^2 + \alpha,\\
&\sigma(\alpha^4) = \alpha^{10} + \alpha^{10} + 1 = 1,\\
&\sigma(\alpha^5) = \alpha^{12} + \alpha^{11} + 1 = 0,\\
&\sigma(\alpha^6) = \alpha^{14} + \alpha^{12} + 1 = \alpha^2 + \alpha + 1,\\
&\sigma(\alpha^7) = \alpha + \alpha^{13} + 1 = \alpha^3 + \alpha^2 + 1,\\
&\sigma(\alpha^8) = \alpha^3 + \alpha^{14} + 1 = 0,\\
&\sigma(\alpha^9) = \alpha^5 + 1 + 1 = \alpha^2 + \alpha,\\
&\sigma(\alpha^{10}) = \alpha^7 + \alpha + 1 = \alpha^3,\\
&\sigma(\alpha^{11}) = \alpha^9 + \alpha^2 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,\\
&\sigma(\alpha^{12}) = \alpha^{11} + \alpha^3 + 1 = \alpha^2 + \alpha + 1,\\
&\sigma(\alpha^{13}) = \alpha^{13} + \alpha^4 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,\\
&\sigma(\alpha^{14}) = 1 + \alpha^5 + 1 = \alpha^2 + \alpha,\\
&\sigma(\alpha^{15}) = \alpha^2 + \alpha^6 + 1 = \alpha^3 + 1.
\end{aligned}
$$

Заметим, что полином локаторов ошибок $\sigma(x)$ является полиномом над полем $\mathbb{F}_2^4$. Поэтому здесь не выполняется свойство $\sigma(\alpha^2) = (\sigma(\alpha))^2$. Обратные элементы для обнаруженных корней α^5 и α^8 равны, соответственно, α^{10} и α^7. Отсюда получаем, что полином ошибок $e(x) = x^{10} + x^7$.