Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2021, № 1, с. 67–86.
Поступила: 15.01.2021
Окончательный вариант: 30.05.2021

УДК 519.725

Об алгоритмах декодирования кодов Рида-Соломона на случай ошибок и стираний

Рацеев С.М.

ratseevsm@mail.ru
УлГУ, Ульяновск, Россия

В работе рассматриваются алгоритмы декодирования кодов Рида-Соломона на случай ошибок и стираний. Данные алгоритмы строятся на основе алгоритма Гао, алгоритма Сугиямы, алгоритма Питерсона-Горенстейна-Цирлера, алгоритма Берлекэмпа–Месси. Первый из данных алгоритмов относится к алгоритмам безсиндромного декодирования, остальные — к алгоритмам синдромного декодирования. Актуальность данных алгоритмов состоит в том, что они применимы для декодирования кодов Гоппы, которые лежат в основе некоторых перспективных постквантовых криптосистем.

Ключевые слова: помехоустойчивые коды, коды Рида-Соломона, декодирование кода.

Введение

Пусть $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$, где α_i — различные элементы конечного поля $F = GF(q)$, $y = (y_0, y_1, \ldots, y_{n-1})$ — ненулевые (не обязательно различные) элементы из F. Тогда обобщенный код Рида-Соломона, обозначаемый $GRS_k(\alpha, y)$, состоит из всех кодовых векторов вида:

$$u = (y_0 b(\alpha_0), y_1 b(\alpha_1), \ldots, y_{n-1} b(\alpha_{n-1})), \tag{1}$$

где $b(x)$ — информационные многочлены над полем F степени не выше $k-1$. Кодовое расстояние кода $GRS_k(\alpha, y)$ равно $d = n - k + 1$. Если $n = q - 1$, вектор y состоит из единиц и $\alpha_i = \alpha^i$, $i = 0, 1, \ldots, n-1$, где α — примитивный элемент поля F, то в этом случае получаем код Рида-Соломона (РС).

Для декодирования кодов Рида-Соломона хорошо известны следующие алгоритмы [1, 2, 3]: алгоритм Гао, алгоритм Сугиямы, алгоритм Берлекэмпа–Месси, алгоритм Питерсона-Горенстейна-Цирлера. В дополнение к этим алгоритмам можно добавить алгоритм поиска

ошибок Форни. Для обобщенных кодов Рида-Соломона и кодов Гоппы подобные алгоритмы рассматривались в работах [4, 5, 6, 7].

В данной работе рассматриваются алгоритмы декодирования для кодов РС на случай ошибок и стираний: декодирование на основе алгоритма Гао, на основе алгоритма Сугиямы, на основе алгоритма Питерсона-Горенстейна-Цирлера, на основе алгоритма Берлекэмпа–Месси.

1 Декодирование кодов РС на основе алгоритма Гао на случай ошибок и стираний (первый вариант)

При описании нижеследующего алгоритма декодирования будем следовать работам [8, 5].

Пусть код Рида-Соломона A над полем $GF(q)$ имеет параметры $[n, k, d = n - k + 1]$, $n = q - 1$, α — примитивный элемент поля $GF(q)$. Будем полагать, что $A = GRS_k(\gamma, y)$, где $\gamma = (1, \alpha, \ldots, \alpha^{n-1})$, $y = (1, \ldots, 1)$. Пусть кодовый вектор $u \in A$ получен на основе информационного многочлена $b(x) = b_0 + b_1 x + \ldots + b_{k-1}x^{k-1}$ с помощью (1).

Пусть в канале связи происходят ошибки и стирания, $d \geq 2t+s+1$, где t и s — число ошибок и стираний соответственно. Предположим, что в принятом векторе v произошли t ошибок и s стираний, причем S — множество позиций в векторе v, на которых произошли стирания. На основе векторов v, γ, y составим соответствующие векторы $\widetilde{v}$, β, z путем удаления всех компонент с номерами из множества S. Рассмотрим код $GRS_k(\beta, z)$ длины $\widetilde{n} = n - s$ и размерности $\widetilde{k} = k$, который получается из кода $GRS_k(\gamma, y)$ путем выкалывания компонент с номерами из множества S. Для кодового расстояния кода $GRS_k(\beta, z)$ выполнено равенство $\widetilde{d} = \widetilde{n} - \widetilde{k} + 1 = n - s - k + 1$. Если $d \geq 2t + s + 1$, то для кодового расстояния $\widetilde{d}$ кода $GRS_k(\beta, z)$ выполнено неравенство $\widetilde{d} \geq 2t + 1$. Тогда вектор $\widetilde{v}$, в котором только ошибки, можно декодировать.

На основе компонент вектора β определим многочлен:

$$m(x) = (x - \beta_0)(x - \beta_1)\ldots(x - \beta_{\widetilde{n}-1}).$$

Пусть $X_1 = \beta_{i_1}, \ldots, X_t = \beta_{i_t}$ — локаторы ошибок. В данном алгоритме многочлен локаторов ошибок запишем в виде:

$$\sigma(x) = (x - X_1)\ldots(x - X_t).$$

Если ошибок не было, то будем полагать, что $\sigma(x) = 1$. Пусть $\widetilde{u}$ — вектор, полученный из u, путем выкалывания компонент с номерами из S. Понятно, что $\widetilde{u} \in GRS_k(\beta, z)$. Так как $n-k+1 = d \geq 2t+s+1$, то $n-s \geq 2t+k \geq k$, поэтому вектор $\widetilde{u}$ получен с помощью кодирования информационного многочлена $b(x) = b_0 + b_1 x + \ldots + b_{k-1}x^{k-1}$ с помощью правила:

$$\widetilde{u} = (b(\beta_0), b(\beta_1), \ldots, b(\beta_{\widetilde{n}-1})).$$

Если $\widetilde{v}_i = \widetilde{u}_i$, то $\widetilde{v}_i = b(\beta_i)$. Если $\widetilde{v}_i \neq \widetilde{u}_i$, то на позиции i произошла ошибка, поэтому $\sigma(\beta_i) = 0$. Из этого следует, что:

$$\sigma(\beta_i)\widetilde{v}_i = \sigma(\beta_i)b(\beta_i), \quad i = 0, 1, \ldots, \widetilde{n} - 1.$$

Обозначим $p(x) = \sigma(x)b(x)$. Тогда:

$$\sigma(\beta_i)\widetilde{v}_i = p(\beta_i), \quad i = 0, 1, \ldots, \widetilde{n} - 1.$$

Построим интерполяционный многочлен Лагранжа $f(x)$ степени не выше $\widetilde{n} - 1$, проходящий через точки $(\beta_0, \widetilde{v}_0)$, $(\beta_1, \widetilde{v}_1)$,..., $(\beta_{\widetilde{n}-1}, \widetilde{v}_{\widetilde{n}-1})$:

$$f(\beta_i) = \widetilde{v}_i, \quad i = 0, 1, \ldots, \widetilde{n} - 1, \quad \deg f(x) \leq \widetilde{n} - 1.$$

Тогда из равенств:

$$\sigma(\beta_i)f(\beta_i) = p(\beta_i), \quad i = 0, 1, \ldots, \widetilde{n} - 1,$$

получаем сравнение:

$$\sigma(x)f(x) \equiv p(x) \pmod{m(x)}. \tag{2}$$

Алгоритм 1 (**декодирование кодов РС на основе алгоритма Гао на случай ошибок и стираний**).

Вход: принятый вектор v.

Выход: исходный информационный вектор b, если в соответствующем кодовом векторе u произошло s стираний и не более t ошибок при $d \geq 2t + s + 1$.

1. Пусть S — позиции стертых символов в векторе v. На основе векторов v, γ составить соответствующие векторы $\widetilde{v}$, β путем удаления всех компонент с номерами из множества S. После этого вектор $\widetilde{v}$ рассматривается как вектор, в котором только ошибки, и который соответствует некоторому кодовому вектору кода $GRS_k(\beta, z)$ длины $\widetilde{n} = n - s$ и размерности $\widetilde{k} = k$. Определяется многочлен:

$$m(x) = \prod_{i=0}^{\widetilde{n}-1}(x - \beta_i).$$

2. Интерполяция. Строится интерполяционный многочлен $f(x)$, для которого:

$$f(\beta_i) = \widetilde{v}_i, \quad i = 0, 1, \ldots, \widetilde{n} - 1.$$

3. Незаконченный обобщенный алгоритм Евклида. Пусть $r_{-1}(x) = m(x)$, $r_0(x) = f(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. Производится последовательность действий обобщенного алгоритма Евклида:

$$r_{i-2}(x) = r_{i-1}(x)q_{i-1}(x) + r_i(x),$$
$$v_i(x) = v_{i-2}(x) - v_{i-1}(x)q_{i-1}(x), \quad i \geq 1,$$

до тех пор, пока не достигается такого $r_j(x)$, для которого:

$$\deg r_{j-1}(x) \geq \frac{\widetilde{n} + \widetilde{k}}{2}, \quad \deg r_j(x) < \frac{\widetilde{n} + \widetilde{k}}{2}.$$

4. Деление. Информационный многочлен кода $GRS_k(\beta, z)$, соответствующий кодовому вектору u, равен $b(x) = \frac{r_j(x)}{v_j(x)}$.

Теорема 1. Если в кодовом векторе произошло t ошибок и s стираний, причем $d \geq 2t + s + 1$, то алгоритм декодирования 1 всегда приводит к единственному решению, а именно, к исходному информационному вектору b.

Доказательство следует из теоремы 1 работы [5].

Пример 1. Рассмотрим код РС над полем $GF(11)$ с параметрами $n = 10$, $k = 4$, $d = 7$, $\alpha = 2$. Данный $[10, 4, 7]$-код может исправлять до трех ошибок, либо до двух ошибок и до двух стираний, либо одну ошибку и до четырех стираний, либо до шести стираний. Рассмотрим случай одной ошибки и четырех стираний. При этом данный код можно рассматривать как обобщенный код $GRS_4(\gamma, y)$, где $\gamma = (1, 2, 4, 8, 5, 10, 9, 7, 3, 6)$, вектор y состоит из единиц.

Пусть $b = (5, 3, 8, 2)$ — информационный вектор, который соответствует многочлену $b(x) = 5 + 3x + 8x^2 + 2x^3$. После кодирования вектора b получаем кодовый вектор:

$$u = (b(1), b(2), b(4), \ldots, b(6)) = (7, 4, 9, 3, 8, 8, 4, 4, 8, 6).$$

Пусть после отправки вектора u на приемном конце получен вектор v:

$$v = (*, *, *, *, 8, 8, 4, 4, 2, 6),$$

т.е. произошла ошибка на 8-й позиции (нумеруя с нуля) и четыре стирания с 0-й по 3-ю позиции. Для декодирования применим алгоритм 1.

1. Удалив в векторе v стертые символы, получим новый вектор:

$$\widetilde{v} = (8, 8, 4, 4, 2, 6),$$

в котором только одна ошибка. Множество S позиций стертых символов равно $S = \{0, 1, 2, 3\}$. Пусть β и z — векторы длины 6, которые получаются соответственно из векторов γ и y путем удаления компонент с номерами из множества S:

$$\beta = (5, 10, 9, 7, 3, 6).$$

Составляем многочлен $m(x)$:

$$m(x) = (x - 5)(x - 10)(x - 9)(x - 7)(x - 3)(x - 6) =$$

$$= 6 + 3x + 8x^2 + 9x^3 + x^4 + 4x^5 + x^6.$$

Ниже приведена матрица Вандермонда V на основе вектора β и обратная к ней матрица V^{-1}:

$$V = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 5 & 10 & 9 & 7 & 3 & 6 \\ 3 & 1 & 4 & 5 & 9 & 3 \\ 4 & 10 & 3 & 2 & 5 & 7 \\ 9 & 1 & 5 & 3 & 4 & 9 \\ 1 & 10 & 1 & 10 & 1 & 10 \end{pmatrix}, \quad V^{-1} = \begin{pmatrix} 4 & 5 & 10 & 8 & 3 & 4 \\ 3 & 4 & 0 & 10 & 7 & 6 \\ 8 & 0 & 7 & 3 & 9 & 10 \\ 10 & 8 & 4 & 3 & 0 & 3 \\ 5 & 6 & 5 & 0 & 10 & 3 \\ 4 & 10 & 7 & 9 & 4 & 7 \end{pmatrix}.$$

2. Интерполяция. Вычисляем коэффициенты многочлена $f(x) = f_0 + f_1 x + \ldots + f_5 x^5$:

$$(f_0, f_1, \ldots, f_5) = \widetilde{v} V^{-1} = (8, 0, 0, 2, 6, 4),$$

$$f(x) = 8 + 2x^3 + 6x^4 + 4x^5.$$

3. Применение неполного обобщенного алгоритма Евклида. Определяем $r_{-1}(x) = m(x)$, $r_0(x) = f(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$ и применяем алгоритм Евклида:

$$\begin{aligned} r_{-1}(x) &= r_0(x)q_0(x) + r_1(x), \\ q_0(x) &= 2 + 3x, \\ r_1(x) &= 1 + x + 8x^2 + 5x^3 + 5x^4, \\ v_1(x) &= v_{-1}(x) - q_0(x)v_0(x) = 9 + 8x. \end{aligned}$$

Так как $(\widetilde{n} + \widetilde{k})/2 = 5$, $\deg r_0(x) = 5$, $\deg r_1(x) = 4$, то после первого шага алгоритма Евклида останавливаемся.

4. Деление:

$$b(x) = \frac{r_1(x)}{v_1(x)} = 5 + 3x + 8x^2 + 2x^3.$$

2 Декодирование кодов РС на основе алгоритма Гао на случай ошибок и стираний (второй вариант)

Пусть после передачи кодового вектора u на приемной стороне получен вектор v, в котором t ошибок и s стираний, причем $d \geq 2t + s + 1$. Заменим в векторе v стертые символы, например, нулями. Получим при этом вектор $\widetilde{v}$. Пусть ошибки произошли на позициях $i_1, \ldots, i_t$, а стирания на позициях $i_{t+1}, \ldots, i_{t+s}$. Пусть $X_1 = \alpha^{i_1}, \ldots X_t = \alpha^{i_t}$ — неизвестные локаторы ошибок, $X_{t+1} = \alpha^{i_{t+1}}, \ldots, X_{t+s} = \alpha^{i_{t+s}}$ — известные локаторы стираний.

Определим многочлен локаторов ошибок $\sigma(x)$ и многочлен локаторов стираний $\nu(x)$ следующим образом:

$$\sigma(x) = (x - X_1) \ldots (x - X_t), \quad \nu(x) = (x - X_{t+1}) \ldots (x - X_{t+s}).$$

Обозначим $\widetilde{\sigma}(x) = \sigma(x)\nu(x)$. Если ошибок и стираний не было, то будем полагать, что $\widetilde{\sigma}(x) = 1$.

Если $\widetilde{v}_i = u_i$, то $\widetilde{v}_i = b(\alpha^i)$. Если $\widetilde{v}_i \neq u_i$, то на позиции i произошла ошибка или стирание, поэтому $\widetilde{\sigma}(\alpha^i) = 0$. Из этого следует, что:

$$\widetilde{\sigma}(\alpha^i)\widetilde{v}_i = \widetilde{\sigma}(\alpha^i)b(\alpha^i), \quad i = 0, 1, \ldots, n-1.$$

Обозначим $\widetilde{p}(x) = \widetilde{\sigma}(x)b(x)$. Тогда:

$$\widetilde{\sigma}(\alpha^i)\widetilde{v}_i = \widetilde{p}(\alpha^i), \quad i = 0, 1, \ldots, n-1.$$

Построим интерполяционный многочлен Лагранжа $f(x)$ степени не выше $n-1$, проходящий через точки $(1, \widetilde{v}_0)$, $(\alpha, \widetilde{v}_1)$,..., $(\alpha^{n-1}, \widetilde{v}_{n-1})$:

$$f(\alpha^i) = \widetilde{v}_i, \quad i = 0, 1, \ldots, n-1, \quad \deg f(x) \leq n-1.$$

Тогда из равенств:

$$\widetilde{\sigma}(\alpha^i)f(\alpha^i) = \widetilde{p}(\alpha^i), \quad i = 0, 1, \ldots, n-1,$$

получаем сравнение:

$$\widetilde{\sigma}(x)f(x) \equiv \widetilde{p}(x) \pmod{x^n - 1}.$$

После обозначения $\widetilde{f}(x) = f(x)\nu(x)$ данное сравнение приобретает вид:

$$\sigma(x)\widetilde{f}(x) \equiv \widetilde{p}(x) \pmod{x^n - 1}. \tag{3}$$

Заметим, что:

$$\deg\sigma(x) \le \frac{n-k-s}{2}, \quad \deg\widetilde{p}(x) < \frac{n+k+s}{2}, \tag{4}$$

так как:

$$\deg\sigma(x) \le t \le \frac{d-s-1}{2} = \frac{n-k-s}{2},$$
$$\deg\widetilde{p}(x) = \deg\sigma(x) + \deg\nu(x) + \deg b(x) \le$$
$$\le \frac{n-k-s}{2} + s + k - 1 < \frac{n+k+s}{2}.$$

Алгоритм 2 (**декодирование кодов РС на основе метода Гао на случай ошибок и стираний**)**.**

Вход: принятый вектор v.

Выход: исходный информационный вектор b, если в соответствующем кодовом векторе u произошло s стираний и t ошибок при $d \ge 2t + s + 1$.

1. Определяется $t = [(d-s-1)/2]$. В векторе v все стирания заменяются нулями, получая тем самым вектор $\widetilde{v}$. Вычисляются значения локаторов стираний $X_{t+1} = \alpha^{i_{t+1}}, \ldots, X_{t+s} = \alpha^{i_{t+s}}$ на основе известных позиций стираний $i_{t+1}, \ldots, i_{t+s}$. Также вычисляется многочлен локаторов стираний $\nu(x) = (x - X_{t+1}) \ldots (x - X_{t+s})$.

2. Интерполяция. Строится интерполяционный многочлен $f(x)$, для которого:

$$f(\alpha^i) = \widetilde{v}_i, \quad i = 0, 1, \ldots, n-1.$$

Вычисляется многочлен $\widetilde{f}(x) = f(x)\nu(x)$.

3. Незаконченный обобщенный алгоритм Евклида. Пусть $r_{-1}(x) = x^n - 1$, $r_0(x) = \widetilde{f}(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. Производится последовательность действий обобщенного алгоритма Евклида:

$$r_{i-2}(x) = r_{i-1}(x)q_{i-1}(x) + r_i(x),$$
$$v_i(x) = v_{i-2}(x) - v_{i-1}(x)q_{i-1}(x), \quad i \ge 1,$$

до тех пор, пока не достигается такого $r_j(x)$, для которого:

$$\deg r_{j-1}(x) \ge \frac{n+k+s}{2}, \quad \deg r_j(x) < \frac{n+k+s}{2}. \tag{5}$$

4. Деление. Информационный многочлен равен $b(x) = \dfrac{r_j(x)}{v_j(x)\nu(x)}$.

Теорема 2. Если в кодовом векторе произошло t ошибок и s стираний, причем $d \ge 2t + s + 1$, то алгоритм декодирования 2 всегда приводит к единственному решению, а именно, к исходному информационному вектору b.

Доказательство. Пусть $b(x)$ — исходный информационный многочлен, $u(x)$ — кодовый многочлен, полученный с помощью формулы (1). Заметим, что для $\sigma(x)$ и $\widetilde{p}(x)$ (истинные значения), которые получены на основе исходных данных, сравнение (3) выполнено, причем $b(x) = \widetilde{p}(x)/(\sigma(x)\nu(x))$.

Пусть с помощью алгоритма 2 получены значения $r_j(x)$ и $v_j(x)$, причем выполнено (5). Покажем, что $r_j(x)$ делится на $v_j(x)\nu(x)$, причем $r_j(x)/(v_j(x)\nu(x)) = b(x)$. Домножив первое из приведенных ниже сравнений:

$$\sigma(x)\widetilde{f}(x) \equiv \widetilde{p}(x) \pmod{x^n - 1},$$

$$v_j(x)\widetilde{f}(x) \equiv r_j(x) \pmod{x^n - 1}$$

на $v_j(x)$, а второе — на $\sigma(x)$, получим:

$$v_j(x)\widetilde{p}(x) \equiv \sigma(x)r_j(x) \pmod{x^n - 1}. \tag{6}$$

Оценим сверху степени многочленов из левой и правой частей данного сравнения. Учитывая неравенства (4) и (5) получаем:

$$\deg \sigma(x)r_j(x) < \frac{n-k-s}{2} + \frac{n+k+s}{2} = n.$$

Так как:

$$\deg v_j(x) = \deg(x^n - 1) - \deg r_{j-1}(x) \le n - \frac{n+k+s}{2} = \frac{n-k-s}{2},$$

то:

$$\deg v_j(x)\widetilde{p}(x) < \frac{n-k-s}{2} + \frac{n+k+s}{2} = n.$$

Следовательно, из сравнения (6) получаем равенство:

$$v_j(x)\widetilde{p}(x) = \sigma(x)r_j(x).$$

Так как $\widetilde{p}(x) = \sigma(x)\nu(x)b(x)$, то $r_j(x) = v_j(x)\nu(x)b(x)$. □

Пример 2. Построим поле $GF(2^3)$ на основе примитивного многочлена $x^3 + x + 1$ с примитивным элементом α. Так как $\alpha^3 = \alpha + 1$, то:

$$\begin{array}{rrrrrr}
\alpha^0 = & 1 & & & = & 100, \\
\alpha^1 = & & \alpha & & = & 010, \\
\alpha^2 = & & & \alpha^2 & = & 001, \\
\alpha^3 = & 1 & +\alpha & & = & 110, \\
\alpha^4 = & & \alpha & +\alpha^2 & = & 011, \\
\alpha^5 = & 1 & +\alpha & +\alpha^2 & = & 111, \\
\alpha^6 = & 1 & & +\alpha^2 & = & 101, \\
\alpha^7 = & 1 & & & = & 100.
\end{array}$$

Рассмотрим код Рида-Соломона над полем $GF(2^3)$ с параметрами $n = 7$, $k = 3$, $d = 5$. Так как $d = 5$, то данный код может исправлять либо до двух ошибок, либо одну ошибку и до двух стираний, либо до четырех стираний.

Ниже приведена матрица Вандермонда V на основе вектора $\gamma = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$ и обратная к ней матрица V^{-1}:

$$V = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{pmatrix}, \; V^{-1} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix}.$$

Рассмотрим случай одной ошибки и двух стираний. Пусть $b = (\alpha^4, \alpha^3, \alpha)$ — информационный вектор, который соответствует многочлену $b(x) = \alpha^4 + \alpha^3 x + \alpha x^2$. После кодирования вектора b получаем кодовый вектор (который можно получить несколькими способами):

$$u = (b(1), b(\alpha), \ldots, b(\alpha^6)) = (\alpha^4, \alpha^3, \alpha, 0, 0, 0, 0)V = (\alpha^5, \alpha^3, \alpha^4, \alpha, \alpha^3, \alpha, \alpha^5).$$

Пусть на приемном конце получен вектор:

$$v = (\alpha^5, *, \alpha^4, \alpha, \alpha^2, *, \alpha^5),$$

т.е. произошли два стирания на 1-й и 5-й позициях и одна ошибка на 4-й позиции (нумерация с нуля).

Применим алгоритм декодирования 2.

1. Полагаем $s = 2$, $t = [(d - s - 1)/2] = 1$. Заменив в векторе v стертые символы нулями, получаем $\widetilde{v} = (\alpha^5, 0, \alpha^4, \alpha, \alpha^2, 0, \alpha^5)$. Также вычисляем многочлен локаторов стираний $\nu(x) = (x - \alpha)(x - \alpha^5) = \alpha^6 + \alpha^6 x + x^2$.

2. Интерполяция. Вычисляем коэффициенты многочлена $f(x) = f_0 + f_1 x + \ldots + f_6 x^6$:

$$(f_0, f_1, \ldots, f_6) = \widetilde{v}V^{-1} = (0, \alpha^4, 1, 1, \alpha, \alpha^2, \alpha^5),$$

$$f(x) = \alpha^4 x + x^2 + x^3 + \alpha x^4 + \alpha^2 x^5 + \alpha^5 x^6.$$

Вычисляем $\widetilde{f}(x) = f(x)\nu(x) = \alpha^3 x + \alpha^4 x^2 + \alpha^4 x^3 + \alpha^6 x^4 + \alpha x^5 + \alpha^4 x^6 + \alpha x^7 + \alpha^5 x^8$.

3. Незаконченный обобщенный алгоритм Евклида. Полагаем $r_{-1}(x) = 1 + x^7$, $r_0(x) = \widetilde{f}(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. Применяем обобщенный алгоритм Евклида:

$$\begin{aligned} r_{-1}(x) &= r_0(x)q_0(x) + r_1(x), \\ q_0(x) &= 0, \\ r_1(x) &= 1 + x^7, \\ v_1(x) &= v_{-1}(x) - v_0(x)q_0(x) = 0, \\ r_0(x) &= r_1(x)q_1(x) + r_2(x), \\ q_1(x) &= \alpha + \alpha^5 x, \\ r_2(x) &= \alpha + \alpha^2 x + \alpha^4 x^2 + \alpha^4 x^3 + \alpha^6 x^4 + \alpha x^5 + \alpha^4 x^6, \\ v_2(x) &= v_0(x) - v_1(x)q_1(x) = 1, \\ r_1(x) &= r_2(x)q_2(x) + r_3(x), \\ q_2(x) &= 1 + \alpha^3 x, \\ r_3(x) &= \alpha^3 + \alpha x + x^2 + \alpha^5 x^3 + \alpha^2 x^4 + \alpha^4 x^5, \\ v_3(x) &= v_1(x) - v_2(x)q_2(x) = 1 + \alpha^3 x. \end{aligned}$$

После третьего шага процесс останавливается, так как $\deg r_2(x) = 6$, $\deg r_3(x) = 5$, причем $(n+k+s)/2 = 6$.

4. Деление. Исходный информационный многочлен равен:

$$b(x) = \frac{r_3(x)}{v_3(x)\nu(x)} = \alpha^4 + \alpha^3 x + \alpha x^2.$$

3 Декодирование кодов РС на основе алгоритма Сугиямы на случай ошибок и стираний

Пусть v — полученный на приемной стороне вектор, в котором могут быть ошибки и стирания. Пусть t — максимальное число возможных ошибок при фиксированном числе стираний s в векторе v, $d \geq 2t+s+1$, $t = [(d-s-1)/2]$. Так как позиции стертых символов известны, то заменим эти символы в векторе v, например, на нули и будем обращаться с полученным вектором $\widetilde{v}$, как с вектором, содержащим только ошибки. Пусть ошибки произошли на позициях $i_1, \ldots, i_t$, а стирания на позициях $i_{t+1}, \ldots, i_{t+s}$. При этом известны только позиции $i_{t+1}, \ldots, i_{t+s}$. После того, как на данные позиции поместили нули, с какими-то позициями могли угадать (если в кодовом векторе там действительно стояли нули). Поэтому $\widetilde{v} = u + e$, где e — вектор ошибок веса не более $t+s$.

Пусть $X_1 = \alpha^{i_1}, \ldots X_t = \alpha^{i_t}$ — неизвестные локаторы ошибок, $X_{t+1} = \alpha^{i_{t+1}}, \ldots, X_{t+s} = \alpha^{i_{t+s}}$ — известные локаторы стираний, $Y_1 = e_{i_1}, \ldots, Y_{t+s} = e_{i_{t+s}}$ — значения ошибок. Найдем компоненты синдромного вектора:

$$\begin{aligned}
&S_0 = \widetilde{v}(\alpha) = Y_1X_1 + \ldots + Y_tX_t + Y_{t+1}X_{t+1} + \ldots + Y_{t+s}X_{t+s},\\
&S_1 = \widetilde{v}(\alpha^2) = Y_1X_1^2 + \ldots + Y_tX_t^2 + Y_{t+1}X_{t+1}^2 + \ldots + Y_{t+s}X_{t+s}^2,\\
&\ldots\\
&S_{2t+s-1} = \widetilde{v}(\alpha^{2t+s}) = Y_1X_1^{2t+s} + \ldots + Y_tX_t^{2t+s} + Y_{t+1}X_{t+1}^{2t+s} + \ldots + Y_{t+s}X_{t+s}^{2t+s}.
\end{aligned}$$

Запишем синдромный многочлен в виде:

$$S(x) = \sum_{i=0}^{2t+s-1} S_i x^i = \sum_{i=0}^{2t+s-1} \left(\sum_{j=1}^{t+s} Y_j X_j^{i+1} \right) x^i = \sum_{j=1}^{t+s} Y_j X_j \left(\sum_{i=0}^{2t+s-1} (X_j x)^i \right) =$$

$$= \sum_{j=1}^{t+s} Y_j X_j \frac{1-(X_j x)^{2t+s}}{1-X_j x} = \sum_{j=1}^{t+s} \frac{Y_j X_j}{1-X_j x} - x^{2t+s} \sum_{j=1}^{t+s} \frac{Y_j X_j^{2t+s+1}}{1-X_j x}.$$

Полагая:

$$\widetilde{\sigma}(x) = \prod_{i=1}^{t+s}(1-X_i x) = \sum_{i=0}^{t+s} \widetilde{\sigma}_i x^i, \quad \widetilde{\sigma}_0 = 1,$$

$$\widetilde{\omega}(x) = \sum_{i=1}^{t+s} Y_i X_i \prod_{\substack{1 \leq j \leq t+s,\\ j \neq i}} (1-X_j x), \quad \widetilde{\Phi}(x) = \sum_{i=1}^{t+s} Y_i X_i^{2t+s+1} \prod_{\substack{1 \leq j \leq t+s,\\ j \neq i}} (1-X_j x),$$

после приведения всех дробей к общему знаменателю, получим:

$$S(x) = \frac{\widetilde{\omega}(x)}{\widetilde{\sigma}(x)} - x^{2t+s} \frac{\widetilde{\Phi}(x)}{\widetilde{\sigma}(x)}.$$

Тогда:

$$S(x)\widetilde{\sigma}(x) = \widetilde{\omega}(x) - x^{2t+s}\widetilde{\Phi}(x).$$

Данное выражение называют ключевым уравнением, которому можно придать иной вид:

$$\widetilde{\sigma}(x)S(x) \equiv \widetilde{\omega}(x) \pmod{x^{2t+s}}. \tag{7}$$

Заметим, что $\widetilde{\sigma}(x) = \sigma(x)\nu(x)$, где $\sigma(x)$ — это многочлен неизвестных локаторов ошибок, $\nu(x)$ — многочлен известных локаторов стираний:

$$\widetilde{\sigma}(x) = \prod_{i=1}^{t}(1 - X_i x)\prod_{i=1}^{s}(1 - X_{t+i}x) = \sigma(x)\nu(x).$$

Введем в рассмотрение многочлен $\widetilde{S}(x) = S(x)\nu(x)$ — модифицированный синдромный многочлен. Тогда ключевое уравнение (7) примет вид:

$$\sigma(x)\widetilde{S}(x) \equiv \widetilde{\omega}(x) \pmod{x^{2t+s}}, \tag{8}$$

где:

$$\deg\sigma(x) \le t, \quad \deg\widetilde{\omega}(x) \le t + s - 1, \quad \sigma(0) = 1. \tag{9}$$

Рассмотрим сравнение:

$$a(x)\widetilde{S}(x) \equiv b(x) \pmod{x^{2t+s}} \tag{10}$$

относительно неизвестных многочленов $a(x), b(x) \in F[x]$ с условием:

$$\deg a(x) \le t,\ \deg b(x) \le t + s - 1,\ a(0) = 1. \tag{11}$$

Из (8) и (9) следует, что сравнение (10) с условием (11) имеет решение.

Теорема 3. 1. Многочлены $a(x)$ и $b(x)$ являются решением сравнения (10) с условием (11) тогда и только тогда, когда для некоторого многочлена $\mu(x) \in F[x]$ выполнены равенства $a(x) = \mu(x)\sigma(x)$, $b(x) = \mu(x)\widetilde{\omega}(x)$.

2. Многочлены $\sigma(x)$ и $\widetilde{\omega}(x)$ являются единственным решением сравнения (10) с условием (11) и условием взаимной простоты.

Доказательство. 1. Если $a(x) = \mu(x)\sigma(x)$, $b(x) = \mu(x)\widetilde{\omega}(x)$, то:

$$a(x)\widetilde{S}(x) \equiv \mu(x)\sigma(x)\widetilde{S}(x) \equiv \mu(x)\widetilde{\omega}(x) \equiv b(x) \pmod{x^{2t+s}}.$$

Обратно, пусть $a(x)$ и $b(x)$ — некоторое решение сравнения (10) с условием (11). Рассмотрим два сравнения:

$$b(x) \equiv a(x)\widetilde{S}(x) \pmod{x^{2t+s}}, \quad \widetilde{\omega}(x) \equiv \sigma(x)\widetilde{S}(x) \pmod{x^{2t+s}}.$$

Умножив первое сравнение на $\sigma(x)$, а второе на $a(x)$, получим:

$$b(x)\sigma(x) \equiv a(x)\sigma(x)\widetilde{S}(x) \equiv \widetilde{\omega}(x)a(x) \pmod{x^{2t+s}}.$$

Учитывая первые два неравенства из условия (11) для многочленов $a(x)$, $b(x)$, $\sigma(x)$, $\widetilde{\omega}(x)$, из сравнения $b(x)\sigma(x) \equiv \widetilde{\omega}(x)a(x) \pmod{x^{2t+s}}$ следует равенство:

$$b(x)\sigma(x) = \widetilde{\omega}(x)a(x). \tag{12}$$

Так как $\sigma(x) \,|\, \widetilde{\omega}(x)a(x)$ и $\sigma(x)$ и $\widetilde{\omega}(x)$ взаимно просты, то $\sigma(x) \,|\, a(x)$. Поэтому найдется многочлен $\mu(x)$, для которого $a(x) = \mu(x)\sigma(x)$. При этом из (12) следует, что:

$$\frac{b(x)}{\widetilde{\omega}(x)} = \frac{a(x)}{\sigma(x)} = \mu(x).$$

Таким образом, $a(x) = \mu(x)\sigma(x)$, $b(x) = \mu(x)\widetilde{\omega}(x)$.

2. Пусть $a(x)$ и $b(x)$ — некоторое решение сравнения (10) с условием (11), причем $a(x)$ и $b(x)$ взаимно просты. Из пункта 1 следует, что для некоторого многочлена $\mu(x)$ выполнено $a(x) = \mu(x)\sigma(x)$, $b(x) = \mu(x)\widetilde{\omega}(x)$. В силу взаимной простоты $a(x)$ и $b(x)$ многочлен $\mu(x)$ должен являться константой. А в силу условия $\sigma(0) = a(0) = 1$ эта константа равна единице, поэтому $\alpha(x) = \sigma(x)$, $b(x) = \widetilde{\omega}(x)$. □

Определим для обобщенного алгоритма Евклида следующие многочлены:

$$r_{-1}(x) = x^{2t+s},\ r_0(x) = \widetilde{S}(x),$$
$$u_{-1}(x) = 1,\ u_0(x) = 0, \quad v_{-1}(x) = 0,\ v_0(x) = 1.$$

Произведем последовательность действий обобщенного алгоритма Евклида ($i \geq 1$):

$$\begin{aligned} r_{i-2}(x) &= r_{i-1}(x)q_i(x) + r_i(x), \\ u_i(x) &= u_{i-2}(x) - u_{i-1}(x)q_{i-1}(x), \\ v_i(x) &= v_{i-2}(x) - v_{i-1}(x)q_{i-1}(x). \end{aligned}$$

При этом будем получать такие равенства:

$$u_i(x)x^{2t+s} + v_i(x)\widetilde{S}(x) = r_i(x),$$

из которых следуют сравнения:

$$r_i(x) \equiv v_i(x)\widetilde{S}(x) \pmod{x^{2t+s}}.$$

Учитывая, что степени остатков $r_i(x)$ строго убывают, будем применять алгоритм Евклида до тех пор, пока не достигнем такого $r_j(x)$, что:

$$\deg r_{j-1}(x) \geq t+s, \quad \deg r_j(x) \leq t+s-1. \tag{13}$$

Тогда в качестве $a(x)$ и $b(x)$ возьмем такие многочлены:

$$a(x) = \lambda v_j(x), \quad b(x) = \lambda r_j(x), \tag{14}$$

где константа $\lambda \in F$ задается так, чтобы удовлетворялось условие $a(0) = 1$ (в теореме 4 приводится обоснование того, что $v_j(0) \neq 0$, поэтому такая константа существует). В этом случае:

$$b(x) \equiv \lambda r_j(x) \equiv \lambda v_j(x)\widetilde{S}(x) \equiv a(x)\widetilde{S}(x) \pmod{x^{2t+s}},$$
$$\deg b(x) = \deg r_j(x) \leq t+s-1,$$
$$\deg a(x) = \deg v_j(x) = \deg x^{2t+s} - \deg r_{j-1}(x) \leq 2t+s-t-s = t.$$

Поэтому такой алгоритм приводит к решению $a(x)$ и $b(x)$ сравнения (10) с условием (11).

Теорема 4. Пусть $v_j(x)$ и $r_j(x)$ — многочлены из обобщенного алгоритма Евклида с условием (13). Тогда найдется такая ненулевая константа $\lambda \in F$, для которой $\sigma(x) = \lambda v_j(x)$, $\widetilde{\omega}(x) = \lambda r_j(x)$.

Доказательство. Для многочленов $v_j(x)$ и $r_j(x)$, а также для многочленов $\sigma(x)$ и $\widetilde{\omega}(x)$ выполнены равенства:

$$u_j(x)x^{2t+s} + v_j(x)\widetilde{S}(x) = r_j(x), \tag{15}$$

$$\widetilde{\Phi}(x)x^{2t+s} + \sigma(x)\widetilde{S}(x) = \widetilde{\omega}(x). \tag{16}$$

Домножив обе части первого равенства на $\sigma(x)$, а второго — на $v_j(x)$, получим:

$$\begin{aligned} \sigma(x)u_j(x)x^{2t+s} + \sigma(x)v_j(x)\widetilde{S}(x) &= \sigma(x)r_j(x), \\ v_j(x)\widetilde{\Phi}(x)x^{2t+s} + v_j(x)\sigma(x)\widetilde{S}(x) &= v_j(x)\widetilde{\omega}(x). \end{aligned} \tag{17}$$

Из данных равенств следует сравнение:

$$\sigma(x)r_j(x) \equiv v_j(x)\widetilde{\omega}(x) \pmod{x^{2t+s}}.$$

Учитывая степени многочленов в данном сравнении, получаем равенство:

$$\sigma(x)r_j(x) = v_j(x)\widetilde{\omega}(x).$$

Поэтому из (17) с учетом последнего равенства следует такое равенство:

$$\sigma(x)u_j(x) = v_j(x)\widetilde{\Phi}(x).$$

Из свойства взаимной простоты многочленов $u_j(x)$ и $v_j(x)$ следует, что $v_j(x) \,|\, \sigma(x)$, поэтому для некоторого многочлена $\mu(x)$ выполнено $\sigma(x) = \mu(x)v_j(x)$. Подставим это равенство в (16):

$$\widetilde{\Phi}(x)x^{2t+s} + \mu(x)v_j(x)\widetilde{S}(x) = \widetilde{\omega}(x).$$

Теперь домножим равенство (15) на $\mu(x)$:

$$\mu(x)u_j(x)x^{2t+s} + \mu(x)v_j(x)\widetilde{S}(x) = \mu(x)r_j(x).$$

Учитывая степени многочленов $\omega(x)$, $\mu(x)$ и $r_j(x)$, из последних двух равенств следует равенство $\widetilde{\omega}(x) = \mu(x)r_j(x)$.

Таким образом, $\sigma(x) = \mu(x)v_j(x)$, $\widetilde{\omega}(x) = \mu(x)r_j(x)$. Так как многочлены $\sigma(x)$ и $\widetilde{\omega}(x)$ взаимно просты, то многочлен $\mu(x)$ является ненулевой константой. □

Алгоритм 3 (декодирование кодов РС на основе алгоритма Сугиямы на случай ошибок и стираний).

Вход: принятый вектор v, в котором s стираний и не более t ошибок.

Выход: исходный кодовый вектор u, если $d \geq 2t + s + 1$.

1. Определяется $t = [(d-s-1)/2]$, где $[\,]$ — целая часть числа. В векторе v все стирания заменяются нулями, получая тем самым вектор $\widetilde{v}$. Находятся компоненты $S_0, S_1, \ldots, S_{2t+s-1}$ синдромного вектора: $S_i = \widetilde{v}(\alpha^{i+1})$, $i = 0, 1, \ldots, 2t + s - 1$. Если они все равны нулю, то возвращается вектор $\widetilde{v}$ и процедура окончена.

   Вычисляются значения локаторов стираний $X_{t+1} = \alpha^{i_{t+1}}, \ldots, X_{t+s} = \alpha^{i_{t+s}}$ на основе известных позиций стираний $i_{t+1}, \ldots, i_{t+s}$. Вычисляются коэффициенты модифицированного синдромного многочлена $\widetilde{S}(x)$.

2. Пусть $r_{-1}(x) = x^{2t+s}$, $r_0(x) = \widetilde{S}(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. С помощью обобщенного алгоритма Евклида производится последовательность вычислений ($i \geq 1$):

$$r_{i-2}(x) = r_{i-1}(x)q_{i-1}(x) + r_i(x),$$

$$v_i(x) = v_{i-2}(x) - v_{i-1}(x)q_{i-1}(x).$$

Процесс прекращается, как только для некоторого $r_j(x)$ будет выполнено:

$$\deg r_{j-1}(x) \geq t + s, \quad \deg r_j(x) \leq t + s - 1.$$

Тогда:

$$\sigma(x) = \lambda v_j(x), \quad \widetilde{\omega}(x) = \lambda r_j(x),$$

где константа $\lambda \in F$ задается так, чтобы удовлетворялось условие $\sigma(0) = 1$. Пусть $l = \deg \sigma(x)$.

3. Отыскиваются l корней многочлена $\sigma(x)$ последовательной подстановкой в него ненулевых элементов поля F. При этом локаторы ошибок — это величины, обратные корням многочлена $\sigma(x)$.

4. Определяется множество $M = \{1, \ldots, l\} \cup \{t + 1, \ldots, t + s\}$. По формулам Форни:

$$Y_j = \frac{X_j^{-1}\widetilde{\omega}(X_j^{-1})}{\prod\limits_{i \in M \setminus \{j\}} (1 - X_i X_j^{-1})}, \quad j \in M, \tag{18}$$

где $\widetilde{\omega}(x) \equiv \sigma(x)\widetilde{S}(x) \pmod{x^{2t+s}}$, находятся значения ошибок Y_j, $j \in M$. У вектора $\widetilde{v}$ из i_j-го символа, $X_j = \alpha^{i_j}$, вычитается значение Y_j, $j \in M$. При этом получается кодовый вектор u.

Пример 3. Рассмотрим поле $GF(3^2)$ на основе многочлена $x^2 + 2x + 2$ с примитивным элементом α:

В виде степени	В троичном виде	Минимальный многочлен элемента
α^0	10	$x - 1$
α^1	01	$x^2 + 2x + 2$
α^2	11	$x^2 + 1$
α^3	12	$x^2 + 2x + 2$
α^4	20	$x + 1$
α^5	02	$x^2 + x + 2$
α^6	22	$x^2 + 1$
α^7	21	$x^2 + x + 2$
α^8	10	$x - 1$

Рассмотрим $[8, 4]$-код РС над $GF(3^2)$ с кодовым расстоянием $d = 5$. Данный код может исправлять либо любые две ошибки и менее, либо любую ошибку и одновременно два и менее стираний, либо четыре и менее стираний. Рассмотрим случай одной ошибки и двух и менее стираний.

Пусть принят вектор:

$$v = \left(\begin{array}{cccccccc} 0, & \alpha^2, & *, & 1, & \alpha, & 1, & 0, & 0 \end{array} \right).$$

1. Как мы видим, произошло одно стирание символа. Известный локатор стирания $X_2 = \alpha^2$, поэтому $\nu(x) = 1 - \alpha^2 x$. Заменив * на 0, получим:

$$\widetilde{v} = \left(\begin{array}{cccccccc} 0, & \alpha^2, & 0, & 1, & \alpha, & 1, & 0, & 0 \end{array} \right).$$

Определим $s = 1$, $t = [(d - s - 1)/2] = 1$. Вычисляем компоненты синдромного вектора:

$$\begin{array}{l} S_0 = \widetilde{v}(\alpha) = \alpha^3 + \alpha^3 + \alpha^5 + \alpha^5 = \alpha^6, \\ S_1 = \widetilde{v}(\alpha^2) = \alpha^4 + \alpha^6 + \alpha + \alpha^2 = \alpha^7, \\ S_2 = \widetilde{v}(\alpha^3) = \alpha^5 + \alpha + \alpha^5 + \alpha^7 = \alpha^4, \\ S_3 = \widetilde{v}(\alpha^4) = \alpha^6 + \alpha^4 + \alpha + \alpha^4 = 0. \end{array}$$

Вычисляем $\widetilde{S}(x) = S(x)\nu(x) = (\alpha^6 + \alpha^7 x + \alpha^4 x^2)(1 + \alpha^6 x) = \alpha^6 + \alpha^2 x + \alpha^6 x^2 + \alpha^2 x^3$.

2. Определяем $r_{-1}(x) = x^{2t+s} = x^3$, $r_0(x) = \widetilde{S}(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. Применяем неполный обобщенный алгоритм Евклида:

$$\begin{array}{l} r_{-1}(x) = r_0(x)q_0(x) + r_1(x), \\ \qquad q_0(x) = \alpha^6, \\ \qquad r_1(x) = 1 + \alpha^4 x + x^2, \\ v_1(x) = v_{-1}(x) - q_0(x)v_0(x) = \alpha^2, \\ r_0(x) = r_1(x)q_1(x) + r_2(x), \\ \qquad q_1(x) = \alpha^2 x, \\ \qquad r_2(x) = \alpha^6, \\ v_2(x) = v_0(x) - q_1(x)v_1(x) = 1 + x. \end{array}$$

Так как $t + s = 2$, $\deg r_1(x) = 2$, $\deg r_2(x) < 2$, то после второго шага останавливаемся. Тогда:

$$\sigma(x) = \lambda v_2(x), \quad \widetilde{\omega}(x) = \lambda r_2(z).$$

При $\lambda = 1$ получаем:

$$\sigma(x) = 1 + x, \quad \widetilde{\omega}(x) = \alpha^6.$$

3. Локатор ошибки равен $X_1 = \alpha^4$.

4. По формулам (18) для локаторов $X_1 = \alpha^4$ и $X_2 = \alpha^2$ находим значения ошибок $Y_1 = \alpha^3$, $Y_2 = \alpha^7$. Таким образом,

$$e = \left(\begin{array}{cccccccc} 0, & 0, & \alpha^7, & 0, & \alpha^3, & 0, & 0, & 0 \end{array} \right),$$

$$u = \widetilde{v} - e = \left(\begin{array}{cccccccc} 0, & \alpha^2, & \alpha^3, & 1, & \alpha^6, & 1, & 0, & 0 \end{array} \right).$$

Предположим, что кодовый вектор u получен на основе информационного вектора i с помощью дискретного преобразования Фурье. Тогда информационные символы из кодового многочлена:

$$u(x) = \alpha^2 x + \alpha^3 x^2 + x^3 + \alpha^6 x^4 + x^5$$

получаются следующим образом:

$$u(1) = \alpha^2 + \alpha^3 + 1 + \alpha^6 + 1 = \alpha^5,$$
$$u(\alpha^{-1}) = u(\alpha^7) = \alpha + \alpha + \alpha^5 + \alpha^2 + \alpha^3 = \alpha^7,$$
$$u(\alpha^{-2}) = u(\alpha^6) = 1 + \alpha^7 + \alpha^2 + \alpha^6 + \alpha^6 = \alpha^4,$$
$$u(\alpha^{-3}) = u(\alpha^5) = \alpha^7 + \alpha^5 + \alpha^7 + \alpha^2 + \alpha = \alpha^4,$$

$$i = \left(-\alpha^5, \ -\alpha^7, \ -\alpha^4, \ -\alpha^4 \right) = \left(\alpha, \ \alpha^3, \ 1, \ 1 \right).$$

4 Декодирование кодов РС на основе алгоритма Питерсона-Горенстейна-Цирлера и алгоритма Берлекэмпа-Месси

Продолжим рассмотрение сравнения (8). Пусть $d \geq 2t + s + 1$,

$$\widetilde{S}(x) = \widetilde{S}_0 + \widetilde{S}_1 x + \ldots + \widetilde{S}_{2t+2s-1} x^{2t+2s-1} =$$

$$= S(x)\nu(x) = (S_0 + S_1 x + \ldots + S_{2t+s-1} x^{2t+s-1})(\nu_0 + \nu_1 x + \ldots + \nu_s x^s),$$

где $\nu_0 = 1$, $\nu_i = (-1)^i \sigma_i(X_{t+1}, \ldots, X_{t+s})$ — элементарный симметрический многочлен от $X_{t+1}, \ldots, X_{t+s}$, $i = 1, \ldots, s$.

Так как в сравнении (8) $\deg \widetilde{\omega}(x) \leq t + s - 1$, $\deg \widetilde{S}(x) \leq 2t + 2s - 1$, $\deg \sigma(x) \leq t$, то необходимым условием выполнения данного сравнения является тот факт, что коэффициенты многочлена $\sigma(x)\widetilde{S}(x)$ при степенях $j = t + s, t + s + 1, \ldots, 2t + s - 1$ равны нулю. Поэтому получаем такую систему линейных уравнений:

$$\begin{cases} \sigma_0 \widetilde{S}_{s+t} + \sigma_1 \widetilde{S}_{s+t-1} + \ldots + \sigma_t \widetilde{S}_s = 0, \\ \sigma_0 \widetilde{S}_{s+t+1} + \sigma_1 \widetilde{S}_{s+t} + \ldots + \sigma_t \widetilde{S}_{s+1} = 0, \\ \ldots \\ \sigma_0 \widetilde{S}_{s+2t-1} + \sigma_1 \widetilde{S}_{s+2t-2} + \ldots + \sigma_t \widetilde{S}_{s+t-1} = 0. \end{cases}$$

Так как $\sigma_0 = 1$, то данная система в матричной форме примет такой вид:

$$\begin{pmatrix} \widetilde{S}_s & \widetilde{S}_{s+1} & \ldots & \widetilde{S}_{s+t-1} \\ \widetilde{S}_{s+1} & \widetilde{S}_{s+2} & \ldots & \widetilde{S}_{s+t} \\ \ldots & \ldots & \ldots & \ldots \\ \widetilde{S}_{s+t-1} & \widetilde{S}_{s+t} & \ldots & \widetilde{S}_{s+2t-2} \end{pmatrix} \begin{pmatrix} \sigma_t \\ \sigma_{t-1} \\ \ldots \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} -\widetilde{S}_{s+t} \\ -\widetilde{S}_{s+t+1} \\ \ldots \\ -\widetilde{S}_{s+2t-1} \end{pmatrix}. \tag{19}$$

Обозначим матрицу этой системы через $M(t, s)$. Выясним, в каком случае эта система разрешима.

Лемма 1. Для любого $j = 0, 1, \ldots, 2t - 2$ выполнено равенство:

$$\widetilde{S}_{s+j} = \sum_{k=1}^{t} Y_k X_k^{j+1} \prod_{i=1}^{s} (X_k - X_{t+i}).$$

Доказательство. Пусть, как и ранее, $\nu_i = (-1)^i \sigma_i(X_{t+1}, \ldots, X_{t+s})$ — элементарный симметрический многочлен от $X_{t+1}, \ldots, X_{t+s}$. Обозначим $\sigma_i = \sigma_i(X_{t+1}, \ldots, X_{t+s})$. Учитывая определение многочлена $\widetilde{S}(x)$ и равенство:

$$\sum_{i=0}^{s} (-1)^{s-i} \sigma_{s-i} X_k^i = \begin{cases} 0, & t+1 \le k \le t+s, \\ \prod_{i=1}^{s} (X_k - X_{t+i}), & \text{иначе}, \end{cases}$$

получаем:

$$\widetilde{S}_{s+j} = \sum_{i=0}^{s} S_{j+i} \nu_{s-i} = \sum_{i=0}^{s} \sum_{k=1}^{t+s} Y_k X_k^{j+i+1} (-1)^{s-i} \sigma_{s-i} =$$

$$= \sum_{k=1}^{t+s} Y_k X_k^{j+1} \sum_{i=0}^{s} X_k^i (-1)^{s-i} \sigma_{s-i} = \sum_{k=1}^{t} Y_k X_k^{j+1} \sum_{i=0}^{s} X_k^i (-1)^{s-i} \sigma_{s-i} =$$

$$= \sum_{k=1}^{t} Y_k X_k^{j+1} \prod_{i=1}^{s} (X_k - X_{t+i}).$$

□

Теорема 5. Пусть произошло s стираний. Матрица $M(t,s)$ невырождена тогда и только тогда, когда произошло t ошибок.

Доказательство. Обозначим через A, B, C следующие квадратные матрицы порядка t:

$$A = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_t \\ \ldots & \ldots & \ldots & \ldots \\ X_1^{t-1} & X_2^{t-1} & \ldots & X_t^{t-1} \end{pmatrix}, B = \begin{pmatrix} Y_1 X_1 & 0 & \ldots & 0 \\ 0 & Y_2 X_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & Y_t X_t \end{pmatrix},$$

$$C = \begin{pmatrix} \prod_{i=1}^{s} (X_1 - X_{t+i}) & 0 & \ldots & 0 \\ 0 & \prod_{i=1}^{s} (X_2 - X_{t+i}) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \prod_{i=1}^{s} (X_t - X_{t+i}) \end{pmatrix}.$$

Покажем, что $M(t,s) = ABCA^T$. По лемме 1 элемент матрицы $M(t,s)$ с индексами i и j равен:

$$(M(t,s))_{ij} = \widetilde{S}_{s+i+j-2} = \sum_{k=1}^{t} Y_k X_k^{i+j-1} \prod_{l=1}^{s} (X_k - X_{t+l}).$$

Учитывая, что:

$$(A)_{ij} = X_j^{i-1}, \quad (BC)_{ij} = \delta_{ij} Y_i X_i \prod_{k=1}^{s} (X_i - X_{t+k}),$$

где δ_{ij} — символ Кронекера, найдем элемент с соответствующими индексами матрицы $ABCA^T$:

$$(ABCA^T)_{ij} = \sum_{m=1}^{t} (ABC)_{im} (A^T)_{mj} = \sum_{m=1}^{t} \sum_{k=1}^{t} A_{ik} (BC)_{km} A_{jm} =$$

$$= \sum_{m=1}^{t} \sum_{k=1}^{t} X_k^{i-1} \delta_{km} Y_k X_k \prod_{l=1}^{s} (X_k - X_{t+l}) X_m^{j-1} = \sum_{k=1}^{t} Y_k X_k^{i+j-1} \prod_{l=1}^{s} (X_k - X_{t+l}).$$

Следовательно, $M(t,s) = ABCA^T$.

Если произошло t ошибок, то все $X_1, \ldots, X_{t+s}$ различные, а все $Y_1, \ldots, Y_t$ отличны от нуля, поэтому определитель матрицы $ABCA^T$ отличен от нуля. Если произошло менее чем t ошибок, то хотя бы один диагональный элемент матрицы B равен нулю, поэтому матрица $ABCA^T$ будет вырожденной. □

Алгоритм 4 (**декодирование кодов РС на основе алгоритма Питерсона-Горенстейна-Цирлера на случай ошибок и стираний**).

Вход: принятый вектор v, в котором s стираний и не более t ошибок.

Выход: исходный кодовый вектор u, если $d \geq 2t + s + 1$.

1. Определяется $t = [(d-s-1)/2]$. В векторе v все стирания заменяются нулями, получая тем самым вектор $\widetilde{v}$. Находятся компоненты $S_0, S_1, \ldots, S_{2t+s-1}$ синдромного вектора: $S_i = \widetilde{v}(\alpha^{i+1})$, $i = 0, 1, \ldots, 2t+s-1$. Если они все равны нулю, то возвращается вектор $\widetilde{v}$ и процедура окончена.

   Вычисляются значения локаторов стираний $X_{t+1} = \alpha^{i_{t+1}}, \ldots, X_{t+s} = \alpha^{i_{t+s}}$ на основе известных позиций стираний $i_{t+1}, \ldots, i_{t+s}$. Вычисляются коэффициенты модифицированного синдромного многочлена $\widetilde{S}(x)$.

2. Определяется $h := t$.

   Цикл: пока $|M(h,s)| = 0$, переопределить $h := h - 1$.

   Если $h > 0$, то находятся $\sigma_1, \ldots, \sigma_h$ — решение системы (19). Это можно сделать, например, с метода Гаусса. После этого составляется многочлен $\sigma(x)$. Пусть $l = \deg \sigma(x)$.

3. Отыскиваются l корней многочлена $\sigma(x)$ последовательной подстановкой в него ненулевых элементов поля F. При этом локаторы ошибок — это величины, обратные корням многочлена $\sigma(x)$.

4. Определяется множество:

   $$M = \{1, \ldots, l\} \cup \{t+1, \ldots, t+s\}.$$

   По формуле (18) находятся значения ошибок Y_j, $j \in M$. У вектора $\widetilde{v}$ из i_j-го символа, $X_j = \alpha^{i_j}$, вычитается значение Y_j, $j \in M$. При этом получается кодовый вектор u.

Пример 4. Рассмотрим расширение поля $GF(2) \subset GF(2^4)$. Пусть поле $GF(2^4)$ строится на основе примитивного многочлена $p(x) = x^4 + x + 1$, α — примитивный элемент поля $GF(2^4)$:

$$\begin{array}{llll}
\alpha^0 = 1 = 1000, & \alpha^1 = \alpha = 0100, \\
\alpha^2 = \alpha^2 = 0010, & \alpha^3 = \alpha^3 = 0001, \\
\alpha^4 = 1 + \alpha = 1100, & \alpha^5 = \alpha + \alpha^2 = 0110, \\
\alpha^6 = \alpha^2 + \alpha^3 = 0011, & \alpha^7 = 1 + \alpha + \alpha^3 = 1101, \\
\alpha^8 = 1 + \alpha^2 = 1010, & \alpha^9 = \alpha + \alpha^3 = 0101, \\
\alpha^{10} = 1 + \alpha + \alpha^2 = 1110, & \alpha^{11} = \alpha + \alpha^2 + \alpha^3 = 0111, \\
\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3 = 1111, & \alpha^{13} = 1 + \alpha^2 + \alpha^3 = 1011, \\
\alpha^{14} = 1 + \alpha^3 = 1001, & \alpha^{15} = 1 = 1000.
\end{array}$$

Рассмотрим код Рида-Соломона с параметрами $n = 15$, $k = 7$, $d = 9$. В этом случае код может исправить четыре и менее ошибок, либо три и менее ошибок и два и менее стираний, либо две и менее ошибок и четыре и менее стираний, либо одну ошибку и шесть и менее стираний, либо восемь и менее стираний.

Рассмотрим случай возможности исправления до двух ошибок и до четырех стираний. Пусть на приемном конце получен вектор:

$$v = \left(\alpha^{12},\ \alpha^{7},\ 0,\ \alpha^{9},\ \alpha^{12},\ \alpha^{5},\ \alpha^{2},\ *,\ \alpha^{3},\ *,\ *,\ \alpha,\ *,\ \alpha^{7},\ \alpha^{4} \right),$$

в котором не более двух ошибок и четыре стирания. Применим алгоритм декодирования 4.

1. Полагаем $s = 4$, $t = [(d - s - 1)/2] = 2$. В данном случае нам известно, что:

$$X_3 = \alpha^7, X_4 = \alpha^9, X_5 = \alpha^{10}, X_6 = \alpha^{12}.$$

Поэтому:

$$\nu(x) = (1 - \alpha^7 x)(1 - \alpha^9 x)(1 - \alpha^{10} x)(1 - \alpha^{12} x) =$$
$$= 1 + \alpha^{14} x + x^2 + \alpha^3 x^3 + \alpha^8 x^4.$$

Заменим в векторе v $*$ на 0:

$$\widetilde{v} = \left(\alpha^{12},\ \alpha^{7},\ 0,\ \alpha^{9},\ \alpha^{12},\ \alpha^{5},\ \alpha^{2},\ 0,\ \alpha^{3},\ 0,\ 0,\ \alpha,\ 0,\ \alpha^{7},\ \alpha^{4} \right).$$

Вычислим компоненты синдрома для вектора $\widetilde{v}$:

$$S_0 = \widetilde{v}(\alpha) = \alpha^9,\ S_1 = \widetilde{v}(\alpha^2) = 0,\ S_2 = \widetilde{v}(\alpha^3) = \alpha^5,$$

$$S_3 = \widetilde{v}(\alpha^4) = \alpha^5,\ S_4 = \widetilde{v}(\alpha^5) = \alpha^{11},\ S_5 = \widetilde{v}(\alpha^6) = \alpha^{12},$$
$$S_6 = \widetilde{v}(\alpha^7) = \alpha^8,\ S_7 = \widetilde{v}(\alpha^8) = \alpha^3.$$

Поэтому синдромный многочлен имеет такой вид:

$$S(x) = \alpha^9 + \alpha^5 x^2 + \alpha^5 x^3 + \alpha^{11} x^4 + \alpha^{12} x^5 + \alpha^8 x^6 + \alpha^3 x^7.$$

Тогда:

$$\widetilde{S}(x) = S(x)\nu(x) = \widetilde{S}_0 + \widetilde{S}_1 x + \ldots + \widetilde{S}_{11} x^{11} =$$
$$= \alpha^9 + \alpha^8 x + \alpha^6 x^2 + \alpha^9 x^3 + \alpha^{12} x^4 + \alpha^7 x^5 + \alpha^{13} x^6 +$$
$$+ \alpha^3 x^7 + \alpha^4 x^8 + \alpha^{11} x^{10} + \alpha^{11} x^{11}.$$

2. В матричном виде система относительно неизвестных σ_1, σ_2 примет вид:

$$\begin{pmatrix} \widetilde{S}_4 & \widetilde{S}_5 \\ \widetilde{S}_5 & \widetilde{S}_6 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} -\widetilde{S}_6 \\ -\widetilde{S}_7 \end{pmatrix},$$

$$\begin{pmatrix} \alpha^{12} & \alpha^{7} \\ \alpha^{7} & \alpha^{13} \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} \alpha^{13} \\ \alpha^{3} \end{pmatrix},$$

которая имеет решение $\sigma_1 = \alpha^{14}$, $\sigma_2 = \alpha^3$, так как $|M(2,4)| \neq 0$.

3. Корнями многочлена локаторов ошибок:

$$\sigma(x) = 1 + \alpha^{14}x + \alpha^3 x^2$$

являются $x_1 = 1$, $x_2 = \alpha^{12}$, поэтому $X_1 = 1$, $X_2 = \alpha^3$.

4. После того, как все локаторы ошибок известны, можно воспользоваться формулой Форни для кодов РС:

$$Y_i = \frac{X_i^{-1}\widetilde{\omega}(X_i^{-1})}{\prod\limits_{\substack{1\le j\le t+s,\\ j\ne i}} (1 - X_j X_i^{-1})}, \quad i = 1, 2, \ldots, t+s,$$

где:

$$\widetilde{\omega}(x) \equiv \sigma(x)\widetilde{S}(x) \equiv$$
$$\equiv \alpha^9 + \alpha^3 x^2 + \alpha^7 x^3 + \alpha^7 x^4 + \alpha^7 x^5 + \alpha^{12} x^6 + \alpha^{10} x^7 \pmod{x^8}.$$

Находим значения ошибок: $Y_1 = \alpha^8, Y_2 = \alpha^3, Y_3 = \alpha^5$, $Y_4 = \alpha^8, Y_5 = \alpha^6$, $Y_6 = \alpha^{12}$. Таким образом:

$$e = \left(\alpha^8,\ 0,\ 0,\ \alpha^3,\ 0,\ 0,\ 0,\ \alpha^5,\ 0,\ \alpha^8,\ \alpha^6,\ 0,\ \alpha^{12},\ 0,\ 0 \right),$$

$$u = \left(\alpha^9,\ \alpha^7,\ 0,\ \alpha,\ \alpha^{12},\ \alpha^5,\ \alpha^2,\ \alpha^5,\ \alpha^3,\ \alpha^8,\ \alpha^6,\ \alpha,\ \alpha^{12},\ \alpha^7,\ \alpha^4 \right).$$

Замечание 1. Если второй шаг алгоритма 4 заменить тем, что на вход алгоритма Берлекэмпа-Месси подается последовательность $\widetilde{S}_s$, $\widetilde{S}_{s+1}, \ldots$, $\widetilde{S}_{s+2t-1}$, то на выходе данного алгоритма получается многочлен $\sigma(x)$. Этим самым получим новый алгоритм декодирования кодов РС на основе алгоритма Берлекэмпа-Месси на случай ошибок и стираний.

Список литературы

[1] Блейхут Р. Теория и практика кодов, контролирующих ошибки. Перевод с англ.: И.И. Грушко, В.М. Блиновский. Под редакцией: К.Ш. Зигангирова. М.: Мир, 1986. 576 с.

[2] Gao S. A new algorithm for decoding Reed—Solomon codes // Communications, Information and Network Security / V. Bhargava, H. V. Poor, V. Tarokh, and S. Yoon, Eds. Norwell, MA: Kluwer, 2003. Vol. 712. P. 55–68.

[3] W. Cary Huffman, Vera Pless. Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003. 646 p.

[4] Рацеев С.М. Об алгоритмах декодирования кодов Гоппы // Челяб. физ.-матем. журн. 2020. Т. 5, № 3. С. 327–341.

[5] Рацеев С.М., Череватенко О.И. О простом алгоритме декодировании кодов БЧХ, кодов Рида-Соломона и кодов Гоппы // Вестник СибГУТИ. 2020. № 3. С. 3–14.

[6] Рацеев С.М., Череватенко О.И. Об алгоритмах декодирования обобщенных кодов Рида-Соломона // Системы и средства информатики. 2020. Т. 30, № 4. С. 83–94.

[7] Рацеев С.М., Череватенко О.И. Об алгоритмах декодирования обобщенных кодов Рида-Соломона на случай ошибок и стираний // Вестник Самарского университета. Естественнонаучная серия. 2020. Т. 26, № 3. С. 17–29.

[8] Федоренко С.В. Простой алгоритм декодирования алгебраических кодов // Информационно-управляющие системы. 2008. № 3. С. 23–27.