МАТЕМАТИКА
MATHEMATICS

Научная статья
DOI: 10.18287/2541-7525-2021-27-2-7-15

УДК 519.725

Дата: поступления статьи: 05.02.2021
после рецензирования: 10.03.2021
принятия статьи: 28.05.2021

С.М. Рацеев
Ульяновский государственный университет,
г. Ульяновск, Российская Федерация
E-mail: ratseevsm@mail.ru. ORCID: https://orcid.org/0000-0003-4995-9418
О.И. Череватенко
Ульяновский государственный педагогический университет
имени И.Н. Ульянова, г. Ульяновск, Российская Федерация
E-mail: choi2008@mail.ru. ORCID: https://orcid.org/0000-0003-3931-9425

ОБ АЛГОРИТМАХ ДЕКОДИРОВАНИЯ ОБОБЩЕННЫХ КОДОВ РИДА — СОЛОМОНА НА СЛУЧАЙ ОШИБОК И СТИРАНИЙ. II

АННОТАЦИЯ

Статья является продолжением работы авторов «Об алгоритмах декодирования обобщенных кодов Рида — Соломона на случай ошибок и стираний».

В данной работе приводится еще одна модификация алгоритма Гао и алгоритма Берлекэмпа — Месси. Первый из данных алгоритмов относится к алгоритмам бессиндромного декодирования, второй — 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; коды Гоппы; декодирование кода.

Цитирование. Рацеев С.М., Череватенко О.И. Об алгоритмах декодирования обобщенных кодов Рида — Соломона на случай ошибок и стираний. II // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 27, № 2. С. 7–15. DOI: http://doi.org/10.18287/2541-7525-2021-27-2-7-15.

Информация о конфликте интересов: авторы и рецензенты заявляют об отсутствии конфликта интересов.

Сергей Михайлович Рацеев — доктор физико-математических наук, доцент, профессор кафедры информационной безопасности и теории управления, Ульяновский государственный университет, 432017, Российская Федерация, г. Ульяновск, ул. Льва Толстого, 42.

Ольга Ивановна Череватенко — кандидат физико-математических наук, доцент, доцент кафедры высшей математики, Ульяновский государственный педагогический университет имени И.Н. Ульянова, 432071, Российская Федерация, г. Ульяновск, пл. Ленина, 4/5.

Введение

Пусть $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$, где α_i — различные элементы 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

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

где $b(x)$ — информационные многочлены над полем F степени не выше $k-1$.

В данной статье приводятся алгоритмы декодирования для обобщенных кодов РС на случай ошибок и стираний: декодирование на основе алгоритма Гао [1] и на основе алгоритма Берлекэмпа — Месси [2]. В работе [3] в алгоритме декодирования на основе метода Гао компоненты искаженного кодового вектора, содержащие стирания, удалялись. В приводимом ниже алгоритме значения данных компонент будут заменяться нулевыми значениями. Достоинство данного метода заключается в том, что многочлен $m(x)$ не нужно пересчитывать в зависимости от позиций стертых символов. Матрицу Вандермонда V в новом алгоритме пересчитывать тоже не нужно. Это значит, что, учитывая работу [4], при $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\} = GF(q)\backslash\{0\}$ представленный алгоритм будет иметь сложность $O(n(\log n)^2)$. Так как в работе [3] алгоритм декодирования на основе алгоритма Берлекэмпа — Месси в явном виде не приводился, то для полноты картины этот алгоритм приводится в данной работе. Более того, приведем обоснование корректности его использования для случая ошибок и стираний. При этом, в отличие от кодов РС, в обобщенных кодах РС одна из компонент вектора α может быть нулевой, это нужно учитывать для алгоритма декодирования на основе алгоритма Берлекэмпа — Месси.

Напомним, что актуальность данных алгоритмов состоит в том, что они применимы для декодирования кодов Гоппы [5–8], которые лежат в основе некоторых перспективных постквантовых криптосистем [9; 10].

1. Декодирование ОРС-кодов на основе алгоритма Гао на случай ошибок и стираний

Предположим, что в канале связи действуют ошибки и стирания. Пусть после передачи кодового вектора $u \in GRS_k(\alpha, y)$ на приемной стороне получен вектор v, в котором t ошибок и s стираний, причем $d \geqslant 2t+s+1$. Заменим в векторе v стертые символы, например, нулями. Получим при этом вектор $\widetilde{v}$. Пусть ошибки произошли на позициях $i_1, \dots, i_t$, а стирания — на позициях $i_{t+1}, \dots, i_{t+s}$. Пусть $X_1 = \alpha_{i_1}, \dots X_t = \alpha_{i_t}$ — неизвестные локаторы ошибок, $X_{t+1} = \alpha_{i_{t+1}}, \dots, X_{t+s} = \alpha_{i_{t+s}}$ — известные локаторы стираний.

Определим многочлен:

$$m(x) = (x-\alpha_0)(x-\alpha_1)\dots(x-\alpha_{n-1}).$$

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

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

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 $\widetilde{v}_i = y_i b(\alpha_i)$. 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

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

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

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

Построим интерполяционный многочлен Лагранжа $f(x)$ степени не выше $n-1$, проходящий через точки $(\alpha_0, y_0^{-1}\widetilde{v}_0)$, $(\alpha_1, y_1^{-1}\widetilde{v}_1)$,..., $(\alpha_{n-1}, y_{n-1}^{-1}\widetilde{v}_{n-1})$:

$$f(\alpha_i) = y_i^{-1}\widetilde{v}_i, \quad i = 0, 1, \dots, n-1, \quad \deg f(x) \leqslant n-1.$$

Тогда из равенств:

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

получаем сравнение:

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

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

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

Заметим, что

$$\deg \sigma(x) \leqslant \frac{n-k-s}{2}, \quad \deg \widetilde{p}(x) < \frac{n+k+s}{2}, \tag{3}$$

так как

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

Алгоритм 1 (декодирование ОРС кодов методом 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 $d \geqslant 2t+s+1$.

1. Определяется $t = [(d-s-1)/2]$. В векторе v все стирания заменяют 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

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

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

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

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

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

$$\deg r_{j-1}(x) \geqslant \frac{n+k+s}{2}, \quad \deg r_j(x) < \frac{n+k+s}{2}. \tag{4}$$

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

Теорема 1. Если в кодовом векторе произошло t ошибок и s стираний, причем $d \geqslant 2t + s + 1$, то алгоритм декодирования 1 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 (2) выполнено, причем $b(x) = \widetilde{p}(x)/(\sigma(x)\nu(x))$.

Пусть с помощью алгоритма 1 получены значения $r_j(x)$ и $v_j(x)$, причем выполнено (4). 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

$$\sigma(x)\widetilde{f}(x) \equiv \widetilde{p}(x) \pmod{m(x)},$$
$$v_j(x)\widetilde{f}(x) \equiv r_j(x) \pmod{m(x)}$$

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

$$v_j(x)\widetilde{p}(x) \equiv \sigma(x) r_j(x) \pmod{m(x)}. \tag{5}$$

Оценим сверху степени многочленов из левой и правой частей данного сравнения. Учитывая неравенства (3) и (4), получаем

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

Так как

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

то

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

Следовательно, из сравнения (5) 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 1. Рассмотрим обобщенный код Рида — Соломона над полем $GF(7)$ с параметрами $n = 7$, $k = 3$, $d = 5$, $\alpha = (0, 1, 2, 3, 4, 5, 6)$, $y = (2, 1, 3, 1, 4, 1, 5)$. Так как $d = 5$, то данный код может исправлять либо до двух ошибок, либо одну ошибку и до двух стираний, либо до четырех стираний.

Так как вектор α содержит все элементы поля $GF(7)$, то $m(x) = x^7 - x$. Ниже приведена матрица Вандермонда V на основе вектора α, обратная к ней матрица V^{-1} и диагональная матрица Y на основе вектора y:

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

$$Y = \mathrm{Diag}(2, 1, 3, 1, 4, 1, 5).$$

Заметим, что первые $k = 3$ строки матрицы VY образуют порождающую матрицу G нашего кода.

Рассмотрим случай одной ошибки и двух стираний. Пусть $b = (3, 5, 2)$ — информационный вектор, который соответствует многочлену $b(x) = 3 + 5x + 2x^2$. После кодирования вектора b получаем кодовый вектор (который можно получить несколькими способами):

$$u = (y_0 b(0), y_1 b(1), \ldots, y_6 b(6)) = bG =$$
$$= (b_0, b_1, b_2, 0, 0, 0, 0)VY = (6, 3, 0, 1, 3, 1, 0).$$

Пусть на приемном конце получен вектор

$$v = (*, 3, 5, 1, *, 1, 0),$$

т. е. произошли два стирания и одна ошибка.

Применим алгоритм декодирования 1.

1. Полагаем $s = 2$, $t = [(d - s - 1)/2] = 1$. Заменив в векторе v стертые символы нулями, получаем $\widetilde{v} = (0, 3, 5, 1, 0, 1, 0)$. Также вычисляем многочлен локаторов стираний $\nu(x) = (x - 0)(x - 4) = 3x + x^2$.

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

$$(f_0, f_1, \ldots, f_6) = \widetilde{v} Y^{-1} V^{-1} = (0, 1, 4, 2, 3, 2, 5),$$
$$f(x) = x + 4x^2 + 2x^3 + 3x^4 + 2x^5 + 5x^6.$$

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

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

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

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

$$b(x) = \frac{r_3(x)}{v_3(x)\nu(x)} = 3 + 5x + 2x^2.$$

2. Декодирование ОРС-кодов на основе алгоритма Берлекэмпа — Месси

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, $d \geqslant 2t + s + 1$, $t = [(d - s - 1)/2]$, m — реальное число ошибок, $m \leqslant t$. 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 $i_1, \ldots, i_m$, а стирания — на позициях $i_{m+1}, \ldots, i_{m+s}$. При этом известны только позиции $i_{m+1}, \ldots, i_{m+s}$. 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 $m + s$.

Вычисляя синдромный вектор, получаем:

$$S = \widetilde{v}H^T = eH^T = \begin{pmatrix} \ldots, & e_{i_1}, & \ldots, & e_{i_{m+s}}, & \ldots \end{pmatrix} \times$$

$$\times \left(\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_0^{n-k-1} & \alpha_1^{n-k-1} & \ldots & \alpha_{n-1}^{n-k-1} \end{pmatrix} \begin{pmatrix} w_0 & 0 & \ldots & 0 \\ 0 & w_1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & w_{n-1} \end{pmatrix} \right)^T =$$

$$= \begin{pmatrix} e_{i_1}w_{i_1} + \ldots + e_{i_{m+s}}w_{i_{m+s}} \\ e_{i_1}w_{i_1}\alpha_{i_1} + \ldots + e_{i_{m+s}}w_{i_{m+s}}\alpha_{i_{m+s}} \\ \ldots \\ e_{i_1}w_{i_1}\alpha_{i_1}^{n-k-1} + \ldots + e_{i_{m+s}}w_{i_{m+s}}\alpha_{i_{m+s}}^{n-k-1} \end{pmatrix}^T.$$

Пусть $X_1 = \alpha_{i_1}, \ldots X_m = \alpha_{i_m}$ — неизвестные локаторы ошибок, $X_{m+1} = \alpha_{i_{m+1}}, \ldots, X_{m+s} = \alpha_{i_{m+s}}$ — известные локаторы стираний, $Y_1 = e_{i_1}, \ldots, Y_{m+s} = e_{i_{m+s}}$ — значения ошибок в векторе $\widetilde{v}$. Обозначим $Z_j = Y_j w_{i_j}$, $j = 1, \ldots, m+s$. Тогда

$$\begin{aligned} &S_0 = Z_1 + \ldots + Z_m + Z_{m+1} + \ldots + Z_{m+s}, \\ &S_1 = Z_1X_1 + \ldots + Z_mX_m + Z_{m+1}X_{m+1} + \ldots + Z_{m+s}Z_{m+s}, \\ &\ldots \\ &S_{2t+s-1} = Z_1X_1^{2t+s-1} + \ldots + Z_mX_m^{2t+s-1} + Z_{m+1}X_{m+1}^{2t+s-1} + \ldots + Z_{m+s}X_{m+s}^{2t+s-1}. \end{aligned}$$

Запишем синдромный многочлен в виде

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

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

Полагая

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

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

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

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

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

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

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

$$\sigma(x)\widetilde{S}(x) \equiv \widetilde{\omega}(x) \pmod{x^{2t+s}}, \tag{6}$$

где

$$\deg \sigma(x) \leqslant m, \quad \deg \widetilde{\omega}(x) \leqslant m + s - 1, \quad \sigma(0) = 1. \tag{7}$$

Пусть
$$\widetilde{S}(x) = \widetilde{S}_0 + \widetilde{S}_1 x + \ldots + \widetilde{S}_{2t+2s-1} x^{2t+2s-1} =$$
$$= S(x)\nu(x) = (S_0 + S_1 x + \ldots + S_{2t+s-1} x^{2t+s-1})(\nu_0 + \nu_1 x + \ldots + \nu_s x^s),$$
где $\nu_0 = 1$, $\nu_i = (-1)^i \sigma_i(X_{m+1}, \ldots, X_{m+s})$ — элементарный симметрический многочлен от $X_{m+1}, \ldots, X_{m+s}$, $i = 1, \ldots, s$.

Так как в сравнении (6) $\deg \widetilde{\omega}(x) \leqslant m + s - 1$, $\deg \widetilde{S}(x) \leqslant 2t + 2s - 1$, $\deg \sigma(x) \leqslant m$, то необходимым условием выполнения данного сравнения является тот факт, что коэффициенты многочлена $\sigma(x)\widetilde{S}(x)$ при степенях $j = m+s, m+s+1, \ldots, 2t+s-1$ равны нулю. Поэтому получаем такую систему линейных уравнений:
$$\begin{cases} \sigma_0 \widetilde{S}_{s+m} + \sigma_1 \widetilde{S}_{s+m-1} + \ldots + \sigma_m \widetilde{S}_s = 0, \\ \sigma_0 \widetilde{S}_{s+m+1} + \sigma_1 \widetilde{S}_{s+m} + \ldots + \sigma_m \widetilde{S}_{s+1} = 0, \\ \ldots \\ \sigma_0 \widetilde{S}_{s+2t-1} + \sigma_1 \widetilde{S}_{s+2t-2} + \ldots + \sigma_m \widetilde{S}_{s+2t-m-1} = 0. \end{cases}$$
Так как $\sigma_0 = 1$, то данная система в матричной форме примет такой вид:
$$\begin{pmatrix} \widetilde{S}_{s+m-1} & \widetilde{S}_{s+m-2} & \ldots & \widetilde{S}_s \\ \widetilde{S}_{s+m} & \widetilde{S}_{s+m-1} & \ldots & \widetilde{S}_{s+1} \\ \ldots & \ldots & \ldots & \ldots \\ \widetilde{S}_{s+2t-2} & \widetilde{S}_{s+2t-3} & \ldots & \widetilde{S}_{s+2t-m-1} \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \ldots \\ \sigma_m \end{pmatrix} = \begin{pmatrix} -\widetilde{S}_{s+m} \\ -\widetilde{S}_{s+m+1} \\ \ldots \\ -\widetilde{S}_{s+2t-1} \end{pmatrix}. \tag{8}$$

Для нахождения решения системы (8) применим следующий алгоритм.

Алгоритм 2 (алгоритм Берлекэмпа — Месси)
Вход: последовательность $a_1, \ldots, a_n$ над некоторым полем.
Выход: LFSR $(L, f(x))$ минимальной длины L, для которого
$$-a_j = \sum_{i=1}^{L} f_i a_{j-i}, \quad j = L+1,\, L+2, \ldots, n.$$

1. Определить $r := 0$, $f(x) := 1$, $b(x) := 1$, $L := 0$.
2. Цикл $r := 1, \ldots, n$
   - 2.1. Определить $\Delta := a_r + \sum\limits_{i=1}^{L} f_i a_{r-i}$.
   - 2.2. Если $\Delta = 0$, то $b(x) := x \cdot b(x)$.
   - 2.3. Если $\Delta \neq 0:$
     - 2.3.1. Если $2L < r$:
       $buf(x) := f(x) - \Delta \cdot x \cdot b(x)$,
       $b(x) := \Delta^{-1} \cdot f(x)$,
       $f(x) := buf(x)$,
       $L := r - L$.
     - 2.3.2. Иначе (т. е. выполнено $2L \geqslant r$):
       $f(x) := f(x) - \Delta \cdot x \cdot b(x)$,
       $b(x) := x \cdot b(x)$.

Теорема 2. Пусть $d \geqslant 2t + s + 1$. Если на вход алгоритма 2 подать последовательность $\widetilde{S}_s$, $\widetilde{S}_{s+1}, \ldots, \widetilde{S}_{s+2t-1}$, то на выходе алгоритма будет верное значение многочлена локаторов ошибок $\sigma(x)$.

Доказательство. Пусть $\widetilde{\sigma}(x)$ — многочлен, полученный после применения алгоритма 2. Так как коэффициенты многочлена локаторов ошибок $\sigma(x)$ являются решением системы (8), то по свойству алгоритма Берлекэмпа — Месси $L \leqslant m$. Удалив в системе (8) $2t - 2m$ последних уравнений, получим новую систему с квадратной матрицей системы порядка m. Из теоремы 5 работы [3] следует, что данная матрица невырождена, поэтому полученная новая система имеет единственное решение. Это значит, что $\widetilde{\sigma}(x) = \sigma(x)$ и $L = m$. □

Алгоритм 3 (декодирование ОРС-кодов на основе алгоритма Берлекэмпа — Месси на случай ошибок и стираний).

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

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

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 $\widetilde{v}H^T$. 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. На вход алгоритма 2 подается последовательность $\widetilde{S}_s$, $\widetilde{S}_{s+1}, \ldots$, $\widetilde{S}_{s+2t-1}$. На выходе данного алгоритма получается многочлен $\sigma(x)$. Пусть $l = \deg \sigma(x)$.

3. Если $l > 0$, то 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. При вычислении значений ошибок выполняется один из следующих пунктов.

4.1. Если среди локаторов стираний $X_{t+1}, \ldots, X_{t+s}$ имеется нулевое значение (в противном случае переходим в пункт 4.2), скажем, $X_p = 0$, то пусть

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

Находятся Z_j, $j \in M$, например, с помощью алгоритма Форни для обобщенных кодов РС:

$$Z_j = \frac{\widetilde{\omega}(X_j^{-1})}{\prod_{i \in M \backslash \{j\}} (1 - X_i X_j^{-1})}, \quad j \in M. \tag{9}$$

После этого находятся значения ошибок $Y_j = Z_j / w_{i_j}$, $j \in M$. У вектора $\widetilde{v}$ из i_j-го символа, $X_j = \alpha_{i_j}$, вычитается значение Y_j, $j \in M$. При этом получается вектор $\widetilde{u}$. Пусть для некоторого i выполнено $\alpha_i = 0$. Вычисляется значение Z_p, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы H. Вычисляется значение ошибки $Y_p = Z_p / w_i$. Осталось в векторе $\widetilde{u}$ из i-го символа вычесть Y_p.

4.2. Если условие 4.1 не выполнено, то пусть $M = \{1, \ldots, l\} \cup \{t+1, \ldots, t+s\}$. По формуле (9) находятся значения Z_j, затем значения ошибок $Y_j = Z_j / w_{i_j}$, $j \in M$. У вектора $\widetilde{v}$ из i_j-го символа, $X_j = \alpha_{i_j}$, вычитается значение Y_j, $j \in M$. При этом получается вектор $\widetilde{u}$.

Если $\alpha_i = 0$ для некоторого i и $\deg \sigma(x) < L$, то вычисляется значение Z_0, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы H, а затем вычисляется значение ошибки $Y_0 = Z_0 / w_i$. Осталось в векторе $\widetilde{u}$ из i-го символа вычесть Y_0.

Пример 2. Продолжим рассматривать пример 3 работы [3]. Пусть на приемной стороне получен тот же вектор $v = (1, 3, 6, 10, 9, 1, 10, *, 8)$. После замены стертых символов нулями получаем вектор $\widetilde{v} = (1, 3, 6, 10, 9, 1, 10, 0, 8)$. Компоненты синдромного вектора $\widetilde{S}$ равны: $\widetilde{S} = (4, 10, 5, 9, 3, 8)$. Определяем $s = 1$, $t = [(d - s - 1)/2] = 2$. Поэтому на вход алгоритма 2 передаем значения $\widetilde{S}_1 = 10$, $\widetilde{S}_2 = 5$, $\widetilde{S}_3 = 9$, $\widetilde{S}_4 = 3$. Получаем

r	Δ	$f(x)$	$b(x)$	L
0		1	1	0
1	10	$1+x$	10	1
2	4	$1+5x$	$10x$	1
3	1	$1+5x+x^2$	$1+5x$	2
4	9	$1+7x$	$x+5x^2$	2

Следовательно, $\sigma(x) = 1 + 7x$.

Заключение

В данной статье приводится еще одна модификация алгоритма Гао и алгоритма Берлекэмпа — Месси. Первый из данных алгоритмов относится к алгоритмам бессиндромного декодирования, второй — 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.

Литература

[1] Gao S. A new algorithm for decoding Reed — Solomon codes // In: Bhargava V.K., Poor H.V., Tarokh V., Yoon S. (eds) Communications, Information and Network Security. The Springer International Series in Engineering and Computer Science (Communications and Information Theory). Boston, MA.: Springer, 2003, vol. 712, pp. 55–68. DOI: https://doi.org/10.1007/978-1-4757-3789-9_5.

[2] Massey J.L. Shift-register synthesis and BCH decoding // IEEE Trans. Inf. Theory. 1969. Vol. IT. 15, № 1. P. 122–127. URL: https://crypto.stanford.edu/ mironov/cs359/massey.pdf.

[3] 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. DOI: http://doi.org/10.18287/2541-7525-2020-26-3-17-29.

[4] Федоренко С.В. Простой алгоритм декодирования алгебраических кодов // Информационно-управляющие системы, 2008. № 3(34). С. 23–27. URL: https://elibrary.ru/item.asp?id=10607208.

[5] Гоппа В.Д. Новый класс линейных корректирующих кодов // Пробл. передачи информ. 1970. Т. 6, № 3. С. 24–30. URL: http://mi.mathnet.ru/ppi1748; http://xn–80af7aea.xn–p1ai/Publications/linear_correcting_codes.pdf.

[6] Рацеев С.М. Элементы высшей алгебры и теории кодирования: учеб. пособие для вузов. Санкт-Петербург: Лань, 2022. 656 с. URL: https://reader.lanbook.com/book/187575?demoKey=9c43d0c829634cd713016a7fb3743823#1.

[7] Рацеев С.М. Об алгоритмах декодирования кодов Гоппы // Челяб. физ.-матем. журн. 2020. Т. 5, № 3. С. 327–341. DOI: http://doi.org/10.47475/2500-0101-2020-15307.

[8] Patterson N.J. The algebraic decoding of Goppa codes // IEEE Transactions on Information Theory. 1975. Vol. 21, Issue 2. P. 203–207. DOI: http://doi.org/10.1109/TIT.1975.1055350

[9] Bernstein D., Chou T., Lange T., Maurich I., Misoczki R., Niederhagen R., Persichetti E., Peters C., Schwabe P., Sendrier N., Szefer J., Wang W. Classic McEliece: conservative code-based cryptography. Project documentation: [Электронный ресурс]. URL: https://classic.mceliece.org/nist/mceliece-20190331.pdf, свободный. Яз. англ. (дата обращения: 22.12.2020).

[10] Рацеев С.М. Математические методы защиты информации: учеб. пособие для вузов. Санкт-Петербург: Лань, 2022. 544 с. URL: https://e.lanbook.com/book/193323.

Scientific article

DOI: 10.18287/2541-7525-2021-27-2-7-15

Submited: 05.02.2021
Revised: 10.03.2021
Accepted: 28.05.2021

S.M. Ratseev
Ulyanovsk State University, Ulyanovsk, Russian Federation
E-mail: ratseevsm@mail.ru. ORCID: https://orcid.org/0000-0003-4995-9418
O.I. Cherevatenko
Ulyanovsk State University of Education, Ulyanovsk, Russian Federation
E-mail: chai@pisem.net. ORCID: https://orcid.org/0000-0003-3931-9425

ON DECODING ALGORITHMS FOR GENERALIZED REED — SOLOMON CODES WITH ERRORS AND ERASURES. II

ABSTRACT

The article is a continuation of the authors' work «On decoding algorithms for generalized Reed —Solomon codes with errors and erasures». In this work, another modification of the Gao algorithm and the Berlekamp — Massey algorithm is given. The first of these algorithms is a syndrome-free decoding algorithm, the second is a syndrome decoding algorithm. The relevance of these algorithms is that they are applicable for decoding Goppa codes, which are the basis of some promising post-quantum cryptosystems.

Key words: error-correcting codes; Reed — Solomon codes; Goppa codes; code decoding.

Citation. Ratseev S.M., Cherevatenko O.I. On decoding algorithms for generalized Reed-Solomon codes with errors and erasures. II. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2021, vol. 27, no. 2, pp. 7–15. DOI: http://doi.org/10.18287/2541-7525-2021-27-2-7-15. (In Russ.)

Information about the conflict of interests: authors and reviewers declare no conflict of interests.

Sergey M. Ratseev — Doctor of Physical and Mathematical Sciences, associate professor, Department of Information Security and Control Theory, Ulyanovsk State University, 42, Leo Tolstoy Street, Ulyanovsk, 432017, Russian Federation.

Olga I. Cherevatenko — Candidate of Physical and Matheatical Sciences, associate professor, Department of Higher Mathematics, Ulyanovsk State University of Education, 4/5, Lenin Square, Ulyanovsk, 432063, Russian Federation.

References

[1] Gao S. A new algorithm for decoding Reed—Solomon codes. In: Bhargava V.K., Poor H.V., Tarokh V., Yoon S. (Eds.) Communications, Information and Network Security. The Springer International Series in Engineering and Computer Science (Communications and Information Theory). Boston, MA.: Springer, 2003, vol. 712, pp. 55–68. DOI: http://doi.org/10.1007/978-1-4757-3789-9_5.

[2] Massey J.L. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 1969, vol. IT. 15, no. 1, pp. 122–127. Available at: https://crypto.stanford.edu/ mironov/cs359/massey.pdf.

[3] Ratseev S.M., Cherevatenko O.I. On decoding algorithms for generalized Reed-Solomon codes with errors and erasures. *Vestnik Samarskogo universiteta. Estestvennonauchnaia seriia = Vestnik of Samara University. Natural Science Series*, 2020, vol. 26, no. 3, pp. 17–29. DOI: http://doi.org/10.18287/2541-7525-2020-26-3-17-29. (In Russ.)

[4] Fedorenko S.V. A simple algorithm for decoding algebraic codes. *Information and Control Systems*, 2008, no. 3 (34), pp. 23–27. Available at: https://elibrary.ru/item.asp?id=10607208. (In Russ.)

[5] Goppa V.D. A New Class of Linear Correcting Codes. *Probl. Peredachi Inf.* [Problems of Information Transmission], 1970, vol. 6, issue 3, pp. 207–212. Available at: http://mi.mathnet.ru/ppi1748; http://xn–80af7aea.xn–p1ai/Publications/linear_correcting_codes.pdf. (In Russ.)

[6] Ratseev S.M. Elements of higher algebra and coding theory. St. Petersburg: Lan', 2022, 656 p. Available at: https://reader.lanbook.com/book/187575?demoKey=9c43d0c829634cd713016a7fb3743823#1 (In Russ.)

[7] Ratseev S.M. On decoding algorithms for Goppa codes. *Chelyabinskiy Fizilko-Matematicheskiy Zhurnal = Chelyabinsk Physical and Mathematical Journal*, 2020, vol. 5, no. 3, pp. 327–341. DOI: http://doi.org/10.47475/2500-0101-2020-15307. (In Russ.)

[8] Patterson N.J. The algebraic decoding of Goppa codes. *IEEE Transactions on Information Theory*, 1975, vol. 21, issue 2, pp. 203–207. DOI: http://doi.org/10.1109/TIT.1975.1055350

[9] Bernstein D., Chou T., Lange T., Maurich I., Misoczki R., Niederhagen R., Persichetti E., Peters C., Schwabe P., Sendrier N., Szefer J., Wang W. Classic McEliece: conservative code-based cryptography. Project documentation. Available at: https://classic.mceliece.org/nist/mceliece-20190331.pdf (accessed 22.12.2020).

[10] Ratseev S.M. Mathematical methods of information security: textbook. Saint Petersburg: Lan', 2022, 544 p. Available at: https://e.lanbook.com/book/193323. (In Russ.)