Челябинский физико-математический журнал. 2020. Т. 5, вып. 3. С. 327–341.

УДК 519.725 DOI: 10.47475/2500-0101-2020-15307

ОБ АЛГОРИТМАХ ДЕКОДИРОВАНИЯ КОДОВ ГОППЫ

С. М. Рацеев

Ульяновский государственный университет, Ульяновск, Россия
ratseevsm@mail.ru

Рассматриваются алгоритмы декодирования кодов Гоппы. Данные коды являются важнейшей составной частью некоторых перспективных постквантовых криптографических алгоритмов. Для декодирования кодов Гоппы хорошо известен алгоритм Паттерсона, но он применим только для двоичных кодов. Так как коды Гоппы можно задавать с помощью обобщённых кодов Рида — Соломона, то любой алгоритм декодирования таких кодов применим и для кодов Гоппы. В данной работе приводятся алгоритмы декодирования кодов Гоппы на основе алгоритма Сугиямы, алгоритма Гао, алгоритма Берлекэмпа — Месси (алгоритма Питерсона — Горенстейна — Цирлера). Также приводится алгоритм Паттерсона.

Ключевые слова: *помехоустойчивый код, код Гоппы, код Рида — Соломона, декодирование кода.*

Введение

Определение кода Гоппы [1] опирается на два объекта: многочлен $G(x)$ с коэффициентами из поля $GF(q^m)$, который называется многочленом Гоппы; подмножество $L = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ элементов поля $GF(q^m)$, таких, что $G(\alpha_i) \neq 0$ для всех $\alpha_i \in L$. Код Гоппы $\Gamma(L, G)$ состоит из всех векторов $u = (u_0, u_1, \ldots, u_{n-1})$ с компонентами из $GF(q)$, для которых

$$R_u = \sum_{i=0}^{n-1} \frac{u_i}{x - \alpha_i} \equiv 0 \pmod{G(x)}.$$

Если $G(x)$ неприводим, то код $\Gamma(L, G)$ называется неприводимым кодом Гоппы. Множество L называется множеством нумераторов позиций кодового слова. Имеют место следующие оценки параметров для кодов Гоппы (см., например, [1; 2]).

Теорема 1. *Параметры $[n, k, d]$-кода $\Gamma(L, G)$ над полем $GF(q)$, где $L \subseteq GF(q^m)$, связаны соотношениями*:

$$n = |L|, \quad k \geq n - mr, \quad r = \deg G(x), \quad d \geq r + 1,$$

где d — кодовое расстояние.

Пусть $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$, где α_i — различные элементы поля $GF(q^m)$, $y = (y_0, y_1, \ldots, y_{n-1})$ — ненулевые (не обязательно различные) элементы из $GF(q^m)$. Тогда обобщённый код Рида — Соломона, обозначаемый $GRS_k(\alpha, y)$, состоит из всех кодовых векторов вида $u = (y_0 b(\alpha_0), y_1 b(\alpha_1), \ldots, y_{n-1} b(\alpha_{n-1}))$, где $b(x)$ — информационные многочлены над полем $GF(q^m)$ степени не выше $k - 1$.

Нам понадобится следующее утверждение (см., например, [3]).

Теорема 2. *Код $\Gamma(L,G)$ представляет собой ограничение кода $GRS_{n-r}(L,y)$ на подполе $F=GF(q)$, т. е. $\Gamma(L,G)=GRS_{n-r}(L,y)\cap F^n$, где $r=\deg G(x)$, $y=(y_0,y_1,\ldots,y_{n-1})$,*

$$y_i=G(\alpha_i)\prod_{j\neq i}\frac{1}{\alpha_i-\alpha_j},\quad i=0,1,\ldots,n-1.$$

Следствие 1. *Проверочная матрица кода $GRS_{n-r}(L,y)$, который задаёт код $\Gamma(L,G)$, имеет вид*

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_0^{r-1} & \alpha_1^{r-1} & \ldots & \alpha_{n-1}^{r-1} \end{pmatrix} \begin{pmatrix} G(\alpha_0)^{-1} & 0 & \ldots & 0 \\ 0 & G(\alpha_1)^{-1} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & G(\alpha_{n-1})^{-1} \end{pmatrix},$$

т.е. совпадает с проверочной матрицей кода $\Gamma(L,G)$.

Таким образом, код $\Gamma(L,G)$ можно задать с помощью обобщённого кода Рида — Соломона (ОРС).

Пусть код $\Gamma(L,G)$ является двоичным. Если $G(x)$ не имеет кратных корней, то код $\Gamma(L,G)$ называется сепарабельным кодом Гоппы. Пусть $\overline{G}(x)$ — полный квадрат некоторого многочлена над $GF(2^m)$ наименьшей степени, делящийся на $G(x)$. В случае сепарабельного кода $\overline{G}(x)=G^2(x)$. Для минимального расстояния сепарабельного кода $\Gamma(L,G)$ верна оценка $d\geq 2r+1$ и выполнено равенство $\Gamma(L,G)=\Gamma(L,\overline{G})$ (см., например, [2]). Эти факты позволяют строить сепарабельный код $\Gamma(L,G)=\Gamma(L,\overline{G})$, а некоторые алгоритмы декодирования кодов Гоппы применять относительно кода $GRS_{n-2r}(\alpha,y)$, $r=\deg G(x)$.

В настоящее время имеются несколько хорошо известных алгоритмов декодирования (обобщённых) кодов Рида — Соломона. Например, алгоритм Питерсона — Горенстейна — Цирлера, алгоритм Берлекэмпа — Месси, алгоритм Сугиямы и др. [3; 4]. Для кодов РС Гао [5] и Шиозаки [6] предложили более простой и естественный алгоритм декодирования. Асимптотическая сложность данного алгоритма декодирования для кодов Рида — Соломона оценивается величиной $O(n\log^2 n)$, которая совпадает со сложностью лучших алгоритмов декодирования данных кодов, причём его описание является самым простым из описаний известных алгоритмов.

Для декодирования кодов Гоппы хорошо известен алгоритм Паттерсона [7]. Но он применим только для двоичных кодов Гоппы. При этом заметим, что любой алгоритм декодирования обобщённых кодов Рида — Соломона можно применить и для кодов Гоппы над любым полем.

Данная работа носит научно-методический характер. В ней собраны некоторые факты для ОРС кодов и применены для кодов Гоппы, в частности, приводятся алгоритмы декодирования кодов Гоппы на основе следующих алгоритмов: алгоритм Сугиямы, алгоритм Гао, алгоритм Берлекэмпа — Месси (алгоритм Питерсона — Горенстейна — Цирлера). Следует отметить, что для алгоритмов декодирования нужно учитывать то обстоятельство, что множество нумераторов позиций L может содержать нулевую компоненту. Также в работе приводится алгоритм Паттерсона.

Важность исследования алгоритмов декодирования кодов Гоппы обусловлена, в частности, тем, что на их основе строятся перспективные постквантовые криптосистемы [8]. При этом такие криптосистемы строятся не только на основе двоичных кодов, но и на основе кодов Гоппы над произвольным конечным полем.

1. Алгоритм декодирования Паттерсона для кодов Гоппы

Алгоритм Паттерсона [7] предназначен для декодирования двоичных неприводимых (из неприводимости следует сепарабельность) кодов Гоппы над $GF(2^m)$, так как построен на основе свойств полей вида $GF(2^m)$. В следующем предложении приводится одно из таких свойств, которое понадобится в дальнейшем.

Предложение 1. *Пусть $F = GF(2^m)$, $g(x) \in F[x]$ — некоторый неприводимый многочлен над F. Тогда для любого многочлена $a(x) \in F[x]$ найдётся такой многочлен $b(x) \in F[x]$, для которого $b^2(x) \equiv a(x) \pmod{g(x)}$.*

Доказательство данного несложного предложения строится на свойстве автоморфизма Фробениуса, определённого в поле $F[x]/(g(x))$.

Пусть многочлен $G(x)$ двоичного кода $\Gamma(L, G)$ является неприводимым. Предположим, что при передаче кодового вектора $u = (u_0, u_1, \ldots, u_{n-1})$ произошли некоторые ошибки, $e = (e_0, e_1, \ldots, e_{n-1})$ — вектор ошибок, $v = u + e$ — полученный вектор. Пусть ошибки произошли на позициях $i_1, \ldots, i_t$. Обозначим $X_1 = \alpha_{i_1}, \ldots, X_t = \alpha_{i_t}$ — локаторы ошибок, $\sigma(x)$ — многочлен локаторов ошибок:

$$\sigma(x) = \prod_{i=1}^{t}(x - X_i).$$

Взяв формальную производную от $\sigma(x)$, получим

$$\sigma'(x) = \sum_{i=1}^{t}\prod_{j\neq i}(x - X_j) = \sum_{i=1}^{t}\frac{1}{x - X_i}\prod_{j=1}^{t}(x - X_j) = \sigma(x)\sum_{i=1}^{t}\frac{1}{x - X_i}.$$

Так как $\sigma(x)$ не имеет кратных корней, то многочлены $\sigma(x)$ и $\sigma'(x)$ взаимно просты. Теперь найдём $R_v(x)$:

$$R_v(x) = \sum_{i=0}^{n-1}\frac{v_i}{x - \alpha_i} = \sum_{i=0}^{n-1}\frac{u_i}{x - \alpha_i} + \sum_{i=0}^{n-1}\frac{e_i}{x - \alpha_i} \equiv \sum_{i=0}^{n-1}\frac{e_i}{x - \alpha_i} = \sum_{i=1}^{t}\frac{1}{x - X_i} \pmod{G(x)}.$$

Обозначим $S(x) \equiv R_v(x) \pmod{G(x)}$. Получаем такое сравнение:

$$S(x)\sigma(x) \equiv \sigma'(x) \pmod{G(x)},$$

которое называется ключевым уравнением. Представим многочлен $\sigma(x)$ в виде $\sigma(x) = a^2(x) + xb^2(x)$ для некоторых многочленов $a(x)$ и $b(x)$. Так как $\deg\sigma(x) \leq t$, то $\deg a(x) \leq [t/2]$, $\deg b(x) \leq [(t-1)/2]$. Учитывая характеристику поля $GF(2^m)$, выразим $\sigma'(x)$ через $a(x)$ и $b(x)$:

$$\sigma'(x) = 2a(x)a'(x) + b^2(x) + 2xb(x)b'(x) = b^2(x).$$

Поэтому

$$b^2(x) \equiv \sigma'(x) \equiv S(x)\sigma(x) \equiv S(x)(a^2(x) + xb^2(x)) \pmod{G(x)}.$$

Следовательно,

$$a^2(x) \equiv b^2(x)(x + S^{-1}(x)) \pmod{G(x)},$$

где многочлен $S^{-1}(x)$, обратный к $S(x)$ по модулю $G(x)$, существует в силу того, что многочлен $G(x)$ неприводим, поэтому $GF(2^m)/G(x)$ является полем. Учитывая предложение 1, последнее сравнение можно записать в таком виде:

$$a(x) \equiv b(x)\sqrt{x + S^{-1}(x)} \pmod{G(x)}.$$

Алгоритм 1 (**декодирования Паттерсона для кодов Гоппы**).
Вход: вектор v.
Выход: исходный кодовый вектор u, *если произошло* $t \le r$ *ошибок,* $r = \deg G(x)$.
1. Вычисляется синдромный многочлен

$$S(x) \equiv \sum_{i=0}^{n-1} \frac{v_i}{x - \alpha_i} \pmod{G(x)}.$$

Если $S(x) = 0$, *то алгоритм завершается и возвращается* v.

2. Вычисляется $T(x) \equiv S^{-1}(x) \pmod{G(x)}$ *(т. е. находится решение сравнения* $S(x)T(x) \equiv 1 \pmod{G(x)}$*), используя обобщённый алгоритм Евклида. Если* $T(x) = x$, *то полагается* $\sigma(x) = x$ *и происходит переход в шаг 5.*

3. Вычисляется квадратный корень (см. замечание 2):

$$p(x) \equiv \sqrt{x + T(x)} \pmod{G(x)}.$$

4. Полагается $r_{-1}(x) = G(x)$, $r_0(x) = p(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. *Производится последовательность вычислений обобщённого алгоритма Евклида (*$i \ge 1$*)*

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

до тех пор, пока для некоторого j *не будут выполнены неравенства*

$$\deg r_{j-1}(x) > \left[\frac{r}{2}\right], \quad \deg r_j(x) \le \left[\frac{r}{2}\right].$$

В этом случае $a(x) = r_j(x)$, $b(x) = v_j(x)$, $\sigma(x) = r_j^2(x) + xv_j^2(x)$ *(с точностью до константы).*

5. Вычисляются корни многочлена $\sigma(x)$ *(например, методом Ченя), равные локаторам ошибок:* $X_1 = \alpha_{i_1}, \ldots, X_t = \alpha_{i_t}$, *где* $t = \deg \sigma(x)$. *После этого в векторе* v *исправляются ошибки на позициях* $i_1, \ldots, i_t$.

Замечание 1. Пусть на 4-м шаге алгоритма 1 для некоторого j выполнено $\deg r_{j-1}(x) > [r/2]$, $\deg r_j(x) \le [r/2]$. Тогда

$$\deg v_j(x) = \deg G(x) - \deg r_{j-1}(x) < r - \frac{r}{2} = \frac{r}{2}.$$

Поэтому $\deg v_j(x) \le \left[\frac{r-1}{2}\right]$.

Для ускорения работы алгоритма декодирования можно вычислить заранее многочлены $(x - \alpha_i)^{-1} \pmod{G(x)}$, $i = 0, 1, \ldots, n-1$, а в процессе вычисления синдромного многочлена $S(x)$ для полученного вектора v складывать над полем $GF(2^m)$ только те из них, которые соответствуют v_i, равным единице.

Замечание 2. Для нахождения многочлена $p(x)$ из 3-го шага алгоритма 1 заметим следующее. Пусть $r = \deg G(x)$. Тогда

$$x + T(x) = q_0 + q_1 x + \ldots + q_{r-1}x^{r-1} = \sum_{i=0}^{[(r-1)/2]} q_{2i}x^{2i} + x\left(\sum_{i=0}^{[r/2-1]} q_{2i+1}x^{2i}\right),$$

где обе суммы являются многочленами с чётными степенями. Так как для любого $a \in GF(2^m)$ выполнено $\left(a^{2^{m-1}}\right)^2 = a^{2^m} = a$, то $\sqrt{a} = a^{2^{m-1}}$. Поэтому

$$\sqrt{x + T(x)} \equiv \sum_{i=0}^{[(r-1)/2]} q_{2i}^{2^{m-1}} x^i + \sqrt{x}\left(\sum_{i=0}^{[r/2-1]} q_{2i+1}^{2^{m-1}} x^i\right) \pmod{G(x)}.$$

Пусть $s^2(x) \equiv x \pmod{G(x)}$ для некоторого $s(x)$. Тогда

$$\sqrt{x+T(x)} \equiv \sum_{i=0}^{[(r-1)/2]} q_{2i}^{2^{m-1}} x^i + \sum_{i=0}^{[r/2-1]} q_{2i+1}^{2^{m-1}} x^i s(x) \pmod{G(x)}.$$

Так как $G(x) \in GF(2^m)[x]$ и неприводим, то многочлен $G(x)$ делит многочлен $x^{(2^m)^r} - x$, т. е. $x^{2^{mr}} \equiv x \pmod{G(x)}$. Это означает, что $s(x) \equiv x^{2^{mr-1}} \pmod{G(x)}$.

Многочлен $s(x)$ можно также найти следующим образом. Пусть $G(x) = g_0^2(x) + xg_1^2(x)$. Тогда $s(x) \equiv g_0(x)g_1^{-1}(x) \pmod{G(x)}$. Действительно, так как характеристика поля $GF(2^m)$ равна двум, то $g_0^2(x) \equiv xg_1^2(x) \pmod{G(x)}$. Так как многочлен $G(x)$ неприводим, то многочлены $g_1^2(x)$ и $G(x)$ взаимно просты. Поэтому

$$(g_0(x)g_1^{-1}(x))^2 \equiv g_0^2(x)g_1^{-2}(x) \equiv x \pmod{G(x)}.$$

Пример 1. 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 $GF(2^4)$:

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

Пусть $L = GF(2^4) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$, $G(x) = x^2 + x + \alpha^3$. Так как след элемента α^3 в поле $GF(2^4)$ не равен нулю, то многочлен $G(x)$ в этом поле не имеет корней. Поэтому из неприводимости $G(x)$ над $GF(2^4)$ следует, что код $\Gamma(L, G)$ является сепарабельным, т. е. он исправляет до двух ошибок. Проверочная матрица H кода $\Gamma(L, G)$ примет вид

$$H = \begin{pmatrix} G(0)^{-1} & G(1)^{-1} & G(\alpha)^{-1} & \ldots & G(\alpha^{14})^{-1} \\ 0G(0)^{-1} & 1G(1)^{-1} & \alpha G(\alpha)^{-1} & \ldots & \alpha^{14}G(\alpha^{14})^{-1} \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^{12} & \alpha^{12} & \alpha^4 & \alpha^3 & \alpha^9 & \alpha^4 & \alpha & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^6 & \alpha & \alpha^2 & \alpha^2 & \alpha^8 & \alpha^9 \\ 0 & \alpha^{12} & \alpha^5 & \alpha^5 & \alpha^{12} & \alpha^8 & \alpha^6 & \alpha^{14} & \alpha^{13} & \alpha^{11} & 1 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha^6 & \alpha^8 \end{pmatrix} =$$

$$= \left(\begin{array}{cccccccccccccccc}
1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
\hline
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0
\end{array}\right).$$

Так как все строки матрицы H линейно независимы, то $n - k = 8$, $k = 8$. Выписав построчно фундаментальную систему решений системы однородных линейных

уравнений $HX = O$, находим порождающую матрицу кода $\Gamma(L, G)$:

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Пусть на приёмном конце принят вектор $v = (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$, в котором не более двух ошибок. Для декодирования данного вектора применим алгоритм 1.

1. Вычисляем синдромный многочлен

$$S(x) \equiv \sum_{i=0}^{15} \frac{v_i}{x - \alpha_i} \equiv \frac{1}{x-1} + \frac{1}{x-\alpha} + \frac{1}{x-\alpha^2} + \frac{1}{x-\alpha^3} + \frac{1}{x-\alpha^9} +$$

$$+ \frac{1}{x-\alpha^{10}} + \frac{1}{x-\alpha^{13}} + \frac{1}{x-\alpha^{14}} \equiv \alpha^{14} + \alpha^{12}x \pmod{G(x)}.$$

2. Вычисляем $T(x) \equiv (\alpha^{14} + \alpha^{12}x)^{-1} \equiv \alpha^{14} + \alpha^6 x \pmod{G(x)}$.

3. Вычисляем $s(x)$ и $p(x)$, учитывая замечание 2:

$$\begin{aligned} s(x) &\equiv x^{128} \equiv \alpha^9 + x \pmod{G(x)}, \\ p(x) &\equiv \sqrt{T(x) + x} \equiv \sqrt{\alpha^{14} + \alpha^{13}x} \equiv \\ &\equiv (\alpha^{14})^8 + (\alpha^{13})^8(\alpha^9 + x) \equiv \alpha^{11} + \alpha^{14}x \pmod{G(x)}. \end{aligned}$$

4. Полагаем $r_{-1}(x) = G(x)$, $r_0(x) = p(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. При $j = 0$ видно, что $\deg r_{-1}(x) = 2 > r/2$, $\deg r_0(x) = 1 \le r/2$. Поэтому с точностью до константы $\sigma(x) = r_0^2(x) + xv_0^2(x) = \alpha^7 + x + \alpha^{13}x^2$.

5. Корнями многочлена $\sigma(x)$ являются $X_1 = \alpha^3 = \alpha_4$, $X_2 = \alpha^6 = \alpha_7$, поэтому ошибки произошли на 4-й и 7-й позициях. Следовательно, исходный кодовый вектор равен $u = (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$. Так как столбцы матрицы G с номерами 7, 9–15 (при нумерации от нуля) образуют единичную матрицу, то из позиций вектора u с данными номерами извлекаем информационный вектор $i = (1, 0, 1, 1, 0, 0, 1, 1)$.

2. Декодирование кодов Гоппы на основе алгоритма Гао

Пусть до конца данной работы $\Gamma(L, G) = GRS_{n-r}(L, y) \cap F^n$, $F = GF(q)$, $r = \deg G(x)$, $\widetilde{k} = n - r$ — размерность кода $GRS_{n-r}(L, y)$ длины $\widetilde{n} = n$, $\overline{H}$ — проверочная матрица кода $GRS_{n-r}(L, y)$. Пусть $d, \widetilde{d}$ — кодовые расстояния соответственно кодов $\Gamma(L, G)$ и $GRS_{n-r}(L, y)$. Так как $d \ge r + 1$, $\widetilde{d} = n - \widetilde{k} + 1 = r + 1$, то если в кодовом векторе $u \in \Gamma(L, G)$ произошло не более $[r/2]$ ошибок, то для его декодирования можно применять алгоритмы декодирования для ОРС кодов.

Если же код $\Gamma(L, G)$ двоичный и сепарабельный, то $\Gamma(L, G) = GRS_{n-2r}(L, y) \cap F^n$, $F = GF(2)$, $\widetilde{k} = n - 2r$ — размерность кода $GRS_{n-2r}(L, y)$, $\overline{H}$ — проверочная матрица кода $GRS_{n-2r}(L, y)$. Также $d \ge 2r+1$, $\Gamma(L, G^2) \subseteq GRS_{n-2r}(L, y)$, $\widetilde{d} = 2r+1$, поэтому в этом случае алгоритмы декодирования для ОРС кодов можно применять для декодирования вектора u, в котором до r ошибок.

При описании следующего алгоритма будем следовать работе [9]. Определим многочлен

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

Пусть кодовый вектор $u \in \Gamma(L, G)$ получен с помощью кодирования информационного многочлена $b(x) = b_0 + b_1 x + \ldots + b_{\widetilde{k}-1} x^{\widetilde{k}-1}$ кода $GRS_{\widetilde{k}}(L, y)$:

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

Кроме того, пусть $v = u + e$ — полученный вектор, e — вектор ошибок, $X_1 = \alpha_{i_1}, \dots, X_t = \alpha_{i_t}$ — локаторы ошибок, $Y_1 = e_{i_1}, \dots, Y_t = e_{i_t}$ — значения ошибок. В данном алгоритме многочлен локаторов ошибок также запишем в виде

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

Если ошибок не было, то будем полагать, что $\sigma(x) = 1$.

Если $v_i = u_i$, то $v_i = y_i b(\alpha_i)$. Если $v_i \neq u_i$, то на позиции i произошла ошибка, поэтому $\sigma(\alpha_i) = 0$. Из этого следует, что

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

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

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

Построим интерполяционный многочлен Лагранжа $f(x)$ степени не выше $n-1$, проходящий через точки $(\alpha_0, y_0^{-1} v_0)$, $(\alpha_1, y_1^{-1} v_1)$, $\dots$, $(\alpha_{n-1}, y_{n-1}^{-1} v_{n-1})$:

$$f(\alpha_i) = y_i^{-1} v_i, \quad i = 0, 1, \dots, n-1, \quad \deg f(x) \leq n-1.$$

Тогда из равенств $\sigma(\alpha_i) f(\alpha_i) = p(\alpha_i)$, $i = 0, 1, \dots, n-1$, получаем сравнение

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

Следующий алгоритм декодирования относится к классу безсиндромных алгоритмов декодирования.

Алгоритм 2 (**декодирование кодов Гоппы на основе алгоритма Гао**).
Вход: принятый вектор v.

Выход: исходный кодовый вектор u, в котором произошло не более t ошибок, если $r \geq 2t$, $r = \deg G(x)$, $u \in \Gamma(L, G) \subseteq GRS_{n-r}(L, y)$ (для двоичного сепарабельного кода $r \geq t$, $u \in \Gamma(L, G) \subseteq GRS_{n-2r}(L, y)$).

1. Интерполяция. Строится интерполяционный многочлен $f(x)$, для которого $f(\alpha_i) = y_i^{-1} v_i$, $i = 0, 1, \dots, n-1$.

2. Незаконченный обобщённый алгоритм Евклида. Пусть $r_{-1}(x) = m(x)$, $r_0(x) = f(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. Производится последовательность действий обобщённого алгоритма Евклида

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

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

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

При этом на каждом i-м шаге выполнено сравнение $v_i(x)f(x) \equiv r_i(x) \pmod{m(x)}$.

3. Деление. Информационный многочлен равен $b(x) = r_j(x)/v_j(x)$.

4. Вычисление кодового вектора u с помощью кодирования информационного многочлена $b(x)$ с помощью формулы (1) для кода $GRS_{\widetilde{k}}(L, y)$:

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

Теорема 3. *Если в кодовом векторе произошло не более $[r/2]$ ошибок (не более r ошибок для двоичного сепарабельного кода), то алгоритм декодирования 2 всегда приводит к единственному решению.*

Доказательство данной теоремы аналогично доказательству подобной теоремы из работы [9] для кодов РС. При этом нужно учесть теоремы 1 и 2.

Пример 2. Продолжим рассмотрение кода $\Gamma(L, G)$ из примера 1. Так как этот код сепарабельный, то $\overline{G}(x) = G^2(x) = \alpha^6 + x^2 + x^4$, $\Gamma(L, G) = \Gamma(L, \overline{G})$. Учитывая теорему 2, данный код является ограничением кода $GRS_{12}(L, y)$ на подполе $GF(2)$, где

$$y_i = \overline{G}(\alpha_i) \prod_{j \neq i} \frac{1}{\alpha_i - \alpha_j} = \overline{G}(\alpha_i), \quad i = 0, 1, \ldots, 15,$$

$$y = (\alpha^6, \alpha^6, \alpha^7, \alpha^9, \alpha^{12}, \alpha^7, \alpha^{13}, \alpha^{14}, \alpha^3, \alpha^9, \alpha^3, \alpha^{13}, \alpha^{11}, \alpha^{11}, \alpha^{14}, \alpha^{12}).$$

Пусть $V = V(\alpha)$ — матрица Вандермонда, построенная на основе вектора α, V^{-1} — обратная к ней матрица, Y — диагональная матрица на основе вектора y:

$$Y = \mathrm{Diag}(\alpha^6, \alpha^6, \alpha^7, \alpha^9, \alpha^{12}, \alpha^7, \alpha^{13}, \alpha^{14}, \alpha^3, \alpha^9, \alpha^3, \alpha^{13}, \alpha^{11}, \alpha^{11}, \alpha^{14}, \alpha^{12}).$$

После кодирования информационного вектора $i = (1, 0, 1, 1, 0, 0, 1, 1)$ кода Гоппы $\Gamma(L, G) = \Gamma(L, \overline{G})$ с помощью порождающей матрицы G получен кодовый вектор

$$u = iG = (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1),$$

а на приёмном конце после передачи вектора u получен вектор

$$v = u + e = (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1),$$

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

Будем декодировать вектор v с помощью алгоритма 2. В нашем случае

$$m(x) = \prod_{\beta \in GF(2^4)} (x - \beta) = x^{16} - x.$$

Вычисляем коэффициенты интерполяционного многочлена $f(x)$:

$$(f_0, f_1, \ldots, f_{15}) = vY^{-1}V^{-1} = (0, \alpha^7, \alpha^3, \alpha^8, \alpha^{11}, \alpha^{12}, \alpha^{11}, \alpha^7, \alpha^4, \alpha^4, \alpha^3, \alpha^5, \alpha^6, \alpha^{10}, \alpha^{10}, \alpha^9),$$

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

$$+ \alpha^4 x^9 + \alpha^3 x^{10} + \alpha^5 x^{11} + \alpha^6 x^{12} + \alpha^{10} x^{13} + \alpha^{10} x^{14} + \alpha^9 x^{15}.$$

Полагаем $r_{-1}(x) = m(x)$, $r_0(x) = f(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$ и применяем неполный обобщённый алгоритм Евклида:

$$
\begin{aligned}
&r_{-1}(x) = r_0(x)q_0(x) + r_1(x),\\
&\quad q_0(x) = \alpha^7 + \alpha^6 x,\\
&\quad r_1(x) = \alpha^3 x + \alpha^9 x^2 + \alpha^7 x^3 + x^4 + \alpha^{10} x^5 + \alpha^{13} x^7 + \alpha^4 x^8 + \alpha^{14} x^9 + \alpha^8 x^{11} + \alpha^4 x^{12} +\\
&\qquad +\alpha^7 x^{13} + \alpha^5 x^{14},\\
&v_1(x) = v_{-1}(x) - v_0(x)q_0(x) = \alpha^7 + \alpha^6 x,\\
&r_0(x) = r_1(x)q_1(x) + r_2(x),\\
&\quad q_1(x) = \alpha^9 + \alpha^4 x,\\
&\quad r_2(x) = \alpha^2 x + \alpha^7 x^2 + \alpha^9 x^3 + \alpha^9 x^4 + \alpha^{12} x^5 + \alpha^{10} x^6 + \alpha^9 x^8 + \alpha^4 x^9 + \alpha x^{11} + \alpha^{11} x^{12},\\
&v_2(x) = v_0(x) - v_1(x)q_1(x) = \alpha^4 + \alpha^{12} x + \alpha^{10} x^2.
\end{aligned}
$$

Так как для кода $GRS_{12}(L, y)$ $\widetilde{n} = 16$, $\widetilde{k} = 12$, $(\widetilde{n} + \widetilde{k})/2 = 14$, то после второго шага алгоритма Евклида процесс останавливается ($\deg r_1(x) = 14$, $\deg r_2(x) < 14$).

Информационный многочлен $b(x)$ кода $GRS_{12}(L, y)$, который соответствует вектору u, имеет вид

$$
b(x) = \frac{r_2(x)}{v_2(x)} = \alpha^{13} x + \alpha^2 x^2 + \alpha x^3 + \alpha^{14} x^4 + \alpha^8 x^5 + \alpha^3 x^6 + \alpha^{10} x^7 + \alpha^2 x^8 + \alpha^2 x^9 + \alpha x^{10}.
$$

Вычисляем сам вектор u:

$$
u = (y_0 b(0), y_1 b(1), y_2 b(\alpha), \ldots, y_{15} b(\alpha^{14})) = (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1).
$$

Осталось из кодового вектора u извлечь информационный вектор

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

3. Декодирование кодов Гоппы на основе алгоритма Сугиямы

В данном и следующем параграфе рассмотрим алгоритмы синдромного декодирования кодов Гоппы. Пусть после отправления вектора $u \in \Gamma(L, G)$ на приёмном конце принят вектор $v = u + e$, где e — вектор ошибок веса не более t. Пусть ошибки произошли на позициях $i_1, \ldots, i_t$. Учитывая следствие 1, вычислим синдромный вектор:

$$
S = v\overline{H}^T = e\overline{H}^T = \begin{pmatrix} \ldots, & e_{i_1}, & \ldots, & e_{i_t}, & \ldots \end{pmatrix} \times
$$

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

$$
= \begin{pmatrix} e_{i_1} G(\alpha_{i_1})^{-1} + \ldots + e_{i_t} G(\alpha_{i_t})^{-1} \\ e_{i_1} G(\alpha_{i_1})^{-1} \alpha_{i_1} + \ldots + e_{i_t} G(\alpha_{i_t})^{-1} \alpha_{i_t} \\ \ldots \\ e_{i_1} G(\alpha_{i_1})^{-1} \alpha_{i_1}^{r-1} + \ldots + e_{i_t} G(\alpha_{i_t})^{-1} \alpha_{i_t}^{r-1} \end{pmatrix}^T.
$$

Пусть $X_1 = \alpha_{i_1}$, $X_2 = \alpha_{i_2}$, …, $X_t = \alpha_{i_t}$ — локаторы ошибок, $Y_1 = e_{i_1}$, $Y_2 = e_{i_2}$, …, $Y_t = e_{i_t}$ — значения ошибок. Обозначим $Z_j = Y_j G(\alpha_{i_j})^{-1}$, $j = 1, \ldots, t$. Тогда

$$
S_i = Z_1 X_1^i + \ldots + Z_t X_t^i, \quad i = 0, 1, \ldots, 2t-1, \quad S(x) = S_0 + S_1 x + \ldots + S_{2t-1} x^{2t-1}.
$$

Определим многочлен локаторов ошибок

$$\sigma(x) = (1 - X_1 x)(1 - X_2 x) \dots (1 - X_t x) = \sigma_0 + \sigma_1 x + \sigma_2 x^2 + \dots + \sigma_t x^t,$$

где $\sigma_0 = 1$. Выведем ключевое уравнение для обобщённых кодов РС. Для этого определим два многочлена $\omega(x)$ и $\Phi(x)$:

$$\omega(x) = \sum_{j=1}^{t} Z_j \prod_{s \neq j} (1 - X_s x) = \sum_{j=1}^{t} Z_j \frac{\sigma(x)}{1 - X_j x},$$

$$\Phi(x) = \sum_{j=1}^{t} Z_j X_j^{2t} \prod_{s \neq j} (1 - X_s x) = \sum_{j=1}^{t} Z_j X_j^{2t} \frac{\sigma(x)}{1 - X_j x},$$

где $\omega(x)$ называется многочленом значений ошибок для ОРС кодов. Тогда

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

$$= \sum_{j=1}^{t} Z_j \frac{1 - (X_j x)^{2t}}{1 - X_j x} = \sum_{j=1}^{t} \frac{Z_j}{1 - X_j x} - x^{2t} \sum_{j=1}^{t} \frac{X_j^{2t}}{1 - X_j x} = \frac{\omega(x)}{\sigma(x)} - x^{2t} \frac{\Phi(x)}{\sigma(x)}.$$

Таким образом, получаем ключевое уравнение

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

Алгоритм 3 (**декодирование кодов Гоппы на основе алгоритма Сугиямы**)**.**

Вход: принятый вектор v.

Выход: исходный кодовый вектор u, в котором произошло не более t ошибок, если $r \geq 2t$, $r = \deg G(x)$, $u \in \Gamma(L, G) \subseteq GRS_{n-r}(L, y)$ (для двоичного сепарабельного кода $r \geq t$, $u \in \Gamma(L, G) \subseteq GRS_{n-2r}(L, y)$).

1. Определяется $t = [r/2]$ ($t = r$ в случае двоичного сепарабельного кода Гоппы). Находятся первые $2t$ компонент $S_0, S_1, \dots, S_{2t-1}$ синдромного вектора $v\overline{H}^T$. Если они все равны нулю, то полагается, что ошибок нет и процедура окончена. Полученному вектору ставится в соответствие синдромный многочлен

$$S(x) = \sum_{i=0}^{2t-1} S_i x^i.$$

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

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

Процесс прекращается, как только для некоторого $r_j(x)$ выполняются условия

$$\deg r_{j-1}(x) \geq t, \quad \deg r_j(x) \leq t - 1. \tag{3}$$

Тогда $\sigma(x) = \lambda v_j(x)$, $\omega(x) = \lambda r_j(x)$, где константа $\lambda \in GF(q)$ задаётся так, чтобы удовлетворялось условие $\sigma(0) = 1$.

Пусть $s = \deg \sigma(x)$. Тогда вектор v содержит s ошибок.

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

4. Находятся $Z_1, \ldots, Z_s$, например, с помощью алгоритма Форни для ОРС кодов:

$$Z_i = \frac{\omega(X_i^{-1})}{\prod_{j \neq i}(1 - X_j X_i^{-1})}, \quad i = 1, \ldots, s. \tag{4}$$

После этого находятся значения ошибок $Y_j = Z_j G(X_j)$, $j = 1, \ldots, s$. У вектора v из i_j-го символа, $X_j = \alpha_{i_j}$, вычитается значение Y_j, $j = 1, \ldots, s$. При этом получаем вектор $\widetilde{u}$.

Если $\alpha_i = 0$ для некоторого i, то вычисляется значение Z_0, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы $\overline{H}$. Если $Z_0 \neq 0$, то вычисляется значение ошибки $Y_0 = Z_0 G(\alpha_i)$. Осталось в векторе $\widetilde{u}$ из i-го символа вычесть Y_0.

Теорема 4. *Пусть $r \geq 2t$ ($r \geq t$ для двоичного сепарабельного кода), $r = \deg G(x)$, $v_j(x)$ и $r_j(x)$ — многочлены из обобщённого алгоритма Евклида с условием (3). Тогда найдётся такая ненулевая константа $\lambda \in F$, для которой $\sigma(x) = \lambda v_j(x)$, $\omega(x) = \lambda r_j(x)$.*

Доказательство аналогичной теоремы для кодов РС можно найти, например, в [3]. При этом нужно учесть теоремы 1 и 2.

Пример 3. Продолжим рассмотрение предыдущего примера. Матрица $\overline{H}$ на основе многочлена $\overline{G}(x) = G^2(x) = x^4 + x^2 + \alpha^6$ примет вид

$$\overline{H} = \begin{pmatrix} \alpha^9 & \alpha^9 & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^8 & \alpha^2 & \alpha & \alpha^{12} & \alpha^6 & \alpha^{12} & \alpha^2 & \alpha^4 & \alpha^4 & \alpha & \alpha^3 \\ 0 & \alpha^9 & \alpha^9 & \alpha^8 & \alpha^6 & \alpha^{12} & \alpha^7 & \alpha^7 & \alpha^4 & \alpha^{14} & \alpha^6 & \alpha^{12} & 1 & \alpha & \alpha^{14} & \alpha^2 \\ 0 & \alpha^9 & \alpha^{10} & \alpha^{10} & \alpha^9 & \alpha & \alpha^{12} & \alpha^{13} & \alpha^{11} & \alpha^7 & 1 & \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{12} & \alpha \\ 0 & \alpha^9 & \alpha^{11} & \alpha^{12} & \alpha^{12} & \alpha^5 & \alpha^2 & \alpha^4 & \alpha^3 & 1 & \alpha^9 & \alpha^2 & \alpha^7 & \alpha^{10} & \alpha^{10} & 1 \end{pmatrix}.$$

Пусть на приёмном конце принят тот же вектор

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

Определяем $t = r = 2$, $r = \deg G(x)$. Находим синдромный вектор $S = v\overline{H}^T = (\alpha^9,\ \alpha^{10},\ \alpha^{10},\ \alpha^6)$. Тогда $S(x) = \alpha^9 + \alpha^{10}x + \alpha^{10}x^2 + \alpha^6 x^3$.

Определяем $r_{-1}(x) = x^4$, $r_0(x) = S(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. Применяем неполный обобщённый алгоритм Евклида:

$$\begin{aligned} r_{-1}(x) &= r_0(x)q_0(x) + r_1(x), \\ q_0(x) &= \alpha^{13} + \alpha^9 x, \\ r_1(x) &= \alpha^7 + \alpha^{13}x + \alpha^5 x^2, \\ v_1(x) &= v_{-1}(x) - v_0(x)q_0(x) = \alpha^{13} + \alpha^9 x, \\ r_0(x) &= r_1(x)q_1(x) + r_2(x), \\ q_1(x) &= \alpha^6 + \alpha x, \\ r_2(x) &= \alpha^{10} + x, \\ v_2(x) &= v_0(x) - v_1(x)q_1(x) = \alpha + \alpha^3 x + \alpha^{10} x^2. \end{aligned}$$

Так как $\deg r_1(x) = 2 = t$, $\deg r_2(x) = 1 < t$, то останавливаемся на втором шаге. При этом $\sigma(x) = \lambda v_2(x) = \lambda(\alpha + \alpha^3 x + \alpha^{10} x^2)$, $\omega(x) = \lambda r_2(x) = \lambda(\alpha^{10} + x)$. При $\lambda = \alpha^{14}$ получаем $\sigma(0) = 1$, поэтому $\sigma(x) = 1 + \alpha^2 x + \alpha^9 x^2$. Корнями многочлена

$\sigma(x)$ являются $x_1 = \alpha^{12}$ и $x_2 = \alpha^9$, поэтому $X_1 = x_1^{-1} = \alpha^3 = \alpha_4$, $X_2 = x_2^{-1} = \alpha^6 = \alpha_7$. Таким образом, ошибки произошли на 4-й и 7-й позициях. После исправления ошибок получаем вектор $\widetilde{u} = (0,1,1,1,0,0,0,1,0,0,1,1,0,0,1,1)$. Вычисляя значение Z_0, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы $\overline{H}$, получаем 0, поэтому ошибок на 0-й позиции не происходило. Следовательно, $u = \widetilde{u}$ — исходный кодовый вектор.

4. Декодирование кода Гоппы на основе алгоритма Берлекэмпа — Месси

Рассмотрим сравнение (2). Так как $\deg S(x)\sigma(x) \le 3t-1$, $\deg \omega(x) \le t-1$, то сравнение (2) имеет место, если коэффициент многочлена $S(x)\sigma(x)$ при x^i, $i = t, t+1, \ldots, 2t-1$, равен нулю. Учитывая, что $\sigma_0 = 0$, получаем систему уравнений

$$\begin{cases} \sigma_1 S_{t-1} + \sigma_2 S_{t-2} + \ldots + \sigma_t S_0 = -S_t, \\ \sigma_1 S_t + \sigma_2 S_{t-1} + \ldots + \sigma_t S_1 = -S_{t+1}, \\ \ldots \\ \sigma_1 S_{2t-2} + \sigma_2 S_{2t-3} + \ldots + \sigma_t S_{t-1} = -S_{2t-1}. \end{cases}$$

Запишем данную систему в матричном виде:

$$\begin{pmatrix} S_0 & S_1 & \ldots & S_{t-2} & S_{t-1} \\ S_1 & S_2 & \ldots & S_{t-1} & S_t \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ S_{t-1} & S_t & \ldots & S_{2t-3} & S_{2t-2} \end{pmatrix} \begin{pmatrix} \sigma_t \\ \sigma_{t-1} \\ \ldots \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} -S_t \\ -S_{t+1} \\ \ldots \\ -S_{2t-1} \end{pmatrix}. \tag{5}$$

Матрицу данной системы обозначим через M_t.

Теорема 5. *Матрица M_t невырождена тогда и только тогда, когда произошло t ошибок.*

Доказательство. Пусть

$$A = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_t \\ \ldots & \ldots & \ldots & \ldots \\ X_1^{t-1} & X_2^{t-1} & \ldots & X_t^{t-1} \end{pmatrix}, \quad B = \begin{pmatrix} Z_1 & 0 & \ldots & 0 \\ 0 & Z_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & Z_t \end{pmatrix}.$$

Тогда доказательство следует из равенства $M_t = ABA^T$ и критерия равенства нулю определителя Вандермонда. □

Следствие 2. *Система уравнений* (5) *имеет единственное решение тогда и только тогда, когда произошло t ошибок.*

Алгоритм 4 (**декодирование кода Гоппы на основе алгоритма Берлекэмпа — Месси**)**.**

Вход: принятый вектор v.

Выход: исходный кодовый вектор u, в котором произошло не более t ошибок, если $r \ge 2t$, $r = \deg G(x)$, $u \in \Gamma(L,G) \subseteq GRS_{n-r}(L,y)$ (для двоичного сепарабельного кода $r \ge t$, $u \in \Gamma(L,G) \subseteq GRS_{n-2r}(L,y)$).

1. Определяется $t = [r/2]$ ($t = r$ в случае двоичного сепарабельного кода Гоппы). Находятся первые $2t$ компонент $S_0, S_1, \ldots, S_{2t-1}$ синдромного вектора $v\overline{H}^T$. Если они все равны нулю, то полагается, что ошибок нет и процедура окончена.

2. Цикл: пока $|M_t| = 0$, переопределяется $t := t - 1$.

Находятся $\sigma_1, \ldots, \sigma_t$ — решение системы (5). Это можно сделать с помощью алгоритма Берлекэмпа — Месси (или методом Гаусса). После этого составляется многочлен $\sigma(x)$. Пусть $s = \deg \sigma(x)$.

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

4. Находятся $Z_1, \ldots, Z_s$, например, с помощью алгоритма Форни (4). После этого находятся значения ошибок $Y_j = Z_j G(X_j)$, $j = 1, \ldots, s$. У вектора v из i_j-го символа, $X_j = \alpha_{i_j}$, вычитается значение Y_j, $j = 1, \ldots, s$. При этом получаем вектор $\widetilde{u}$.

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

Пример 4. Продолжим рассмотрение предыдущего примера. Путь на приёмном конце принят тот же вектор v. Определяем $t = r = 2$. Составляем матрицу системы (5):

$$\left(\begin{array}{cc|c} S_0 & S_1 & -S_2 \\ S_1 & S_2 & -S_3 \end{array}\right) = \left(\begin{array}{cc|c} \alpha^9 & \alpha^{10} & \alpha^{10} \\ \alpha^{10} & \alpha^{10} & \alpha^6 \end{array}\right).$$

Так как $|M_2| \neq 0$, то полученный вектор v содержит две ошибки. Находим значения $\sigma_1 = \alpha^2$, $\sigma_2 = \alpha^9$, поэтому $\sigma(x) = 1 + \alpha^2 x + \alpha^9 x^2$. Дальнейшие шаги декодирования совпадают с шагами предыдущего примера, разве что не нужно проверять, происходила ли ошибка на 0-й позиции, так как $\deg \sigma(x) = 2 = t$.

Список литературы

1. **Гоппа, В. Д.** Новый класс линейных корректирующих кодов / В. Д. Гоппа // Проблемы передачи информации. — 1970. — Т. 6, вып. 3. — С. 24–30.
2. **Мак-Вильямс, Ф. Дж.** Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. — М. : Связь, 1979. — 744 с.
3. **Блейхут, Р.** Теория и практика кодов, контролирующих ошибки / Р. Блейхут. — М. : Мир, 1986. — 576 с.
4. **Cary Huffman, W.** Fundamentals of Error-Correcting Codes / W. Cary Huffman. — Cambridge University Press, 2003. — 646 p.
5. **Gao, S.** A new algorithm for decoding Reed — Solomon codes / S. Gao // Communications, Information and Network Security; eds V. Bhargava, H. V. Poor, V. Tarokh, S. Yoon. Norwell : Kluwer, 2003. — P. 55–68.
6. **Shiozaki, A.** Decoding of redundant residue polynomial codes using Euclid's algorithm / A. Shiozaki // IEEE Transactions on Information Theory. — 1988. — Vol. IT-34, no. 5. — P. 1351–1354.
7. **Patterson, N. J.** The algebraic decoding of Goppa codes / N. J. Patterson // IEEE Transactions on Information Theory. — 1975. — Vol. 21, no. 2. — P. 203–207.
8. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology. Internal Report 8240. — January, 2019. — 27 p. — https://doi.org/10.6028/NIST.IR.8240
9. **Федоренко, С. В.** Простой алгоритм декодирования алгебраических кодов / С. В. Федоренко // Информационно-управляющие системы. — 2008. — № 3. — С. 23–27.

Поступила в редакцию 21.04.2020
После переработки 15.07.2020

Сведения об авторе

Рацеев Сергей Михайлович, доктор физико-математических наук, доцент, профессор кафедры информационной безопасности и теории управления, Ульяновский государственный университет, Ульяновск, Россия; e-mail: ratseevsm@mail.ru.

Chelyabinsk Physical and Mathematical Journal. 2020. Vol. 5, iss. 3. P. 327–341.

DOI: 10.47475/2500-0101-2020-15307

ON DECODING ALGORITHMS FOR GOPPA CODES

S.M. Ratseev

Ulyanovsk State University, Ulyanovsk, Russia
ratseevsm@mail.ru

The paper is devoted to the decoding algorithms for Goppa codes. These codes are an important part of some promising post-quantum cryptographic algorithms. The Patterson algorithm is well known for decoding Goppa codes, but it is only applicable for binary codes. Since Goppa codes can be specified using generalized Reed — Solomon codes, any decoding algorithm for such codes is also applicable to Goppa codes. The algorithms for decoding Goppa codes based on the algorithm Sugiyama algorithm, Gao algorithm, Berlekamp — Massey algorithm (Peterson — Gorenstein — Zierler algorithm) are given. The Patterson algorithm is also given.

Keywords: *error-correcting code, Goppa code, Reed — Solomon code, code decoding.*

References

1. **Goppa V.D.** A new class of linear correcting codes. *Problemy Peredachi Informatsii* [Problems of information transmission], 1970, vol. 6, pp. 207–212. (In Russ.).
2. **MacWilliams F.J., Sloane N.J.A.** *The Theory of Error Correcting Codes.* New York : North-Holland Publ., 1977. 762 p.
3. **Blahut R.E.** *Theory and Practice of Error Control Codes.* Reading : Addison-Wesley Publ., 1983. 500 p.
4. **Cary Huffman W.** *Fundamentals of Error-Correcting Codes.* Cambridge University Press, 2003. 646 p.
5. **Gao S.** A new algorithm for decoding Reed — Solomon codes. *Communications, Information and Network Security*; eds V. Bhargava, H. V. Poor, V. Tarokh, S. Yoon. Norwell : Kluwer, 2003. 382 p. Pp. 55–68.
6. **Shiozaki A.** Decoding of redundant residue polynomial codes using Euclid's algorithm. *IEEE Transactions on Information Theory*, 1988, vol. IT-34, no. 5, pp. 1351–1354.
7. **Patterson N.J.** The algebraic decoding of Goppa codes. *IEEE Transactions on Information Theory*, 1975, vol. 21, no. 2, pp. 203–207.
8. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology. Internal Report 8240. January, 2019. 27 p. https://doi.org/10.6028/NIST.IR.8240.
9. **Fedorenko S.V.** Prostoy algoritm dekodirovaniya algebraicheskikh kodov [Simple algorithm for decoding algebraic codes]. *Informatsionno-upravlyayushchiye sistemy* [Information and Control Systems], 2008, no. 3, pp. 23–27. (In Russ.).

Accepted article received 21.04.2020
Corrections received 15.07.2020