С. М. Рацеев, О. И. Череватенко, Об алгоритмах декодирования кодов Гоппы на случай ошибок и стираний, *Изв. Сарат. ун-та. Нов. сер. Сер.: Математика. Механика. Информатика*, 2022, том 22, выпуск 1, 28–47

DOI: 10.18500/1816-9791-2022-22-1-28-47

Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2022. Т. 22, вып. 1. С. 28–47
Izvestiya of Saratov University. Mathematics. Mechanics. Informatics, 2022, vol. 22, iss. 1, pp. 28–47
https://mmi.sgu.ru https://doi.org/10.18500/1816-9791-2022-22-1-28-47

Научная статья
УДК 519.725

Об алгоритмах декодирования кодов Гоппы на случай ошибок и стираний

С. М. Рацеев[1]✉, **О. И. Череватенко**[2]

[1]Ульяновский государственный университет, Россия, 432017, г. Ульяновск, ул. Льва Толстого, д. 42
[2]Ульяновский государственный педагогический университет имени И. Н. Ульянова, Россия, 432071, г. Ульяновск, пл. Ленина, д. 4/5

Рацеев Сергей Михайлович, доктор физико-математических наук, профессор кафедры информационной безопасности и теории управления, ratseevsm@mail.ru, https://orcid.org/0000-0003-4995-9418
Череватенко Ольга Ивановна, кандидат физико-математических наук, доцент кафедры высшей математики, choi2008@yandex.ru, https://orcid.org/0000-0003-3931-9425

Аннотация. В 1978 г. Мак-Элис построил первую кодовую криптосистему с открытым ключом, которая основана на применении помехоустойчивых кодов. Данная криптосистема именно на основе кодов Гоппы считается перспективной и криптостойкой с учетом квантовых вычислений. При этом эффективные атаки на секретные ключи этой криптосистемы до сих пор не найдены. В работе исследуются алгоритмы декодирования кодов Гоппы на случай ошибок и стираний. Приводятся четыре алгоритма декодирования на основе алгоритмов для кодов Рида – Соломона, предложенных Гао, Берлекэмпом и Месси, Сугиямой и др. Первые два алгоритма строятся на основе алгоритма Гао и относятся к алгоритмам бессиндромного декодирования, остальные — к алгоритмам синдромного декодирования. При этом любой из этих алгоритмов применим и для случая канала связи только с ошибками. Также приводятся примеры декодирования сепарабельных кодов Гоппы с использованием данных алгоритмов.

Ключевые слова: помехоустойчивые коды, коды Рида – Соломона, коды Гоппы, декодирование кода

Для цитирования: *Рацеев С. М., Череватенко О. И.* Об алгоритмах декодирования кодов Гоппы на случай ошибок и стираний // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2022. Т. 22, вып. 1. С. 28–47. https://doi.org/10.18500/1816-9791-2022-22-1-28-47

Article

Decoding algorithms for Goppa codes with errors and erasures

S. M. Ratseev[1]✉, **O. I. Cherevatenko**[2]

[1]Ulyanovsk State University, 42 Leo Tolstoy St., Ulyanovsk 432017, Russia
[2]Ilya Ulyanov State Pedagogical University, 4/5 Ploshchad' Lenina, Ulyanovsk 432071, Russia

Sergey M. Ratseev, ratseevsm@mail.ru, https://orcid.org/0000-0003-4995-9418
Olga I. Cherevatenko, choi2008@yandex.ru, https://orcid.org/0000-0003-3931-9425

Abstract. In 1978, McEliece built the first public key cryptosystem based on error-correcting codes. This cryptosystem based on Goppa codes is considered promising and cryptographically stable, taking into account quantum computing. At the same time, effective attacks on the secret keys of this cryptosystem have not yet been found. In the paper, algorithms for decoding Goppa codes in the case of errors and erasures are investigated. Four decoding algorithms based on the algorithms for Reed–Solomon codes proposed by Gao, Berlekamp and Massey, Sugiyama, and others are given. The first two algorithms are based on Gao algorithm and related to syndrome-free decoding algorithms, the rest are related to syndrome decoding algorithms. Moreover, any of these algorithms is also applicable for the case of a communication channel with errors only. Examples of decoding separable Goppa codes using these algorithms are also given.
Keywords: error-correcting codes, Reed–Solomon codes, Goppa codes, code decoding
For citation: Ratseev S. M., Cherevatenko O. I. Decoding algorithms for Goppa codes with errors and erasures. *Izvestiya of Saratov University. Mathematics. Mechanics. Informatics*, 2022, vol. 22, iss. 1, pp. 28–47 (in Russian). https://doi.org/10.18500/1816-9791-2022-22-1-28-47

Введение

Важность исследования кодов Гоппы обусловлена, в частности, тем, что на их основе строятся перспективные постквантовые криптосистемы [1]. Хорошо известно, что некоторые классические коды Гоппы лежат на границе Варшамова–Гильберта.

Определение кода Гоппы [2] 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, [2, 3]).

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

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

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 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 $GF(q^m)$ степени не выше $k - 1$.

Нам понадобится следующее утверждение (см., например, [4]).

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

$$y_i = G(\alpha_i) \prod_{j \neq i} \frac{1}{\alpha_i - \alpha_j}, \quad i = 0, 1, \ldots, n-1. \tag{2}$$

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

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

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

Таким образом, код $\Gamma(L,G)$ можно задать с помощью обобщенного кода Рида–Соломона (ОРС). Для декодирования кодов Рида–Соломона на случай ошибок хорошо известны следующие алгоритмы [4–6]: алгоритм Гао, алгоритм Сугиямы, алгоритм Берлекэмпа–Месси, алгоритм Питерсона–Горенстейна–Цирлера. Для кодов Гоппы подобные алгоритмы рассматривались в работе [7].

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 $d \geqslant 2r+1$ и выполнено равенство $\Gamma(L,G) = \Gamma(L,\overline{G})$ (см., например, [3]). Эти факты позволяют строить сепарабельный код $\Gamma(L,G) = \Gamma(L,\overline{G})$, а некоторые алгоритмы декодирования кодов Гоппы применять относительно кода $GRS_{n-2r}(\alpha,y)$, $r = \deg G(x)$.

Пусть до конца данной работы $[n,k,d]$-код $\Gamma(L,G)$ задается на основе ОРС кода: $\Gamma(L,G) = GRS_{n-r}(L,y) \cap F^n$, $F = GF(q)$, $r = \deg G(x)$, $\widetilde{k} = n-r$ — размерность кода $GRS_{n-r}(L,y)$ длины 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 $d \geqslant r+1$, $\widetilde{d} = n - \widetilde{k} + 1 = r+1$, то если в кодовом векторе $u \in \Gamma(L,G)$ произошло t ошибок и s стираний, причем $r \geqslant 2t+s$, 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 $d \geqslant 2r+1$, $\Gamma(L,G^2) \subseteq GRS_{n-2r}(L,y)$, $\widetilde{d} = 2r+1$, поэтому в этом случае алгоритмы декодирования для ОРС кодов можно применять для декодирования вектора u, в котором t ошибок и s стираний, причем $2r \geqslant 2t+s$.

1. Декодирование кодов Гоппы на основе алгоритма Гао (первый вариант)

Предположим, что в канале связи действуют ошибки и стирания. Пусть кодовый вектор $u \in \Gamma(L,G)$ получен на основе информационного вектора b с помощью правила (1), а после передачи вектора u на приемной стороне получен вектор v, в котором t ошибок и s стираний.

При описании следующего алгоритма будем учитывать работы [5, 8]. Пусть S — позиции стертых символов в векторе v. На основе векторов v, L, y составим соответствующие векторы $\widetilde{v}$, β, z путем удаления всех компонент с номерами из множества S. Рассмотрим код $GRS_{\widetilde{k}}(\beta,z)$ длины $\widetilde{n} = n-s$ и размерности $\widetilde{k}$, который получается из кода $GRS_{\widetilde{k}}(L,y)$ путем выкалывания компонент с номерами из множества S.

Для кодового расстояния кода $GRS_{\widetilde{k}}(\beta, z)$ выполнено равенство $\widehat{d} = \widetilde{n} - \widetilde{k} + 1 = n - s - \widetilde{k} + 1$. Предположим, что для $\widehat{d}$ выполнено неравенство $\widehat{d} \geqslant 2t + 1$. Тогда вектор $\widetilde{v}$, в котором только ошибки, можно декодировать.

На основе компонент вектора β определим многочлен

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

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

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

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 $\widetilde{u} \in GRS_{\widetilde{k}}(\beta, z)$. Так как $n - \widetilde{k} + 1 = d \geqslant 2t + s + 1$, то $n - s \geqslant 2t + \widetilde{k} \geqslant \widetilde{k}$, поэтому вектор $\widetilde{u}$ получен с помощью кодирования информационного многочлена $b(x) = b_0 + b_1 x + \ldots + b_{k-1} x^{k-1}$ (на основе которого получен вектор u) с помощью правила

$$\widetilde{u} = \left(z_0 b(\beta_0), z_1 b(\beta_1), \dots, z_{\widetilde{n}-1} b(\beta_{\widetilde{n}-1})\right).$$

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

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

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

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

Построим интерполяционный многочлен Лагранжа $f(x)$ степени не выше $\widetilde{n} - 1$, проходящий через точки $(\beta_0, z_0^{-1}\widetilde{v}_0)$ $(\beta_1, z_1^{-1}\widetilde{v}_1)$,. . . , $(\beta_{\widetilde{n}-1}, z_{\widetilde{n}-1}^{-1}\widetilde{v}_{\widetilde{n}-1})$:

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

Тогда из равенств

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

получаем сравнение

$$\sigma(x) f(x) \equiv p(x) \pmod{m(x)}. \tag{3}$$

Алгоритм 1 (декодирование кода Гоппы на основе алгоритма Гао на случай ошибок и стираний).

Вход: принятый вектор v.

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

1. Пусть S — позиции стертых символов в векторе v. На основе векторов v, L, y составляются соответствующие векторы $\widetilde{v}$, β, z 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 $GRS_{\widetilde{k}}(\beta, z)$ длины $\widetilde{n} = n - s$. Определяется многочлен

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

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

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

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:

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

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

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

4. Деление. Информационный многочлен кода $GRS_{\widetilde{k}}(\beta, z)$, соответствующий кодовому вектору u, равен $b(x) = \dfrac{r_j(x)}{v_j(x)}$.
5. 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 t ошибок и s стираний, причем $r \geqslant 2t + s$ ($2r \geqslant 2t + s$ для двоичного сепарабельного кода), $r = \deg G(x)$, то алгоритм декодирования* 1 *всегда приводит к единственному решению, а именно к исходному кодовому вектору u кода $\Gamma(L, G)$.*

Доказательство. Пусть код $\Gamma(L, G)$ имеет кодовое расстояние $d \geqslant r+1$ ($d \geqslant 2r+1$ для двоичного сепарабельного кода), $r = \deg G(x)$. Пусть $u \in \Gamma(L, G)$. Так как по теореме 1 код $\Gamma(L, G)$ является ограничением кода $GRS_{\widetilde{k}}(L, y)$ на подполе $GF(q)$, то u можно получить с помощью кодирования некоторого информационного многочлена $b(x)$ кода $GRS_{\widetilde{k}}(L, y)$ с помощью формулы (1). При этом кодовое расстояние кода $GRS_{\widetilde{k}}(L, y)$ равно $\widetilde{d} = n - \widetilde{k} + 1 = r + 1$ ($\widetilde{d} = 2r + 1$ в случае двоичного сепарабельного кода Гоппы). Предположим, что при передаче вектора u произошло t ошибок и s стираний, $r \geqslant 2t + s$ ($2r \geqslant 2t + s$), а на приемной стороне получен вектор v. Как и ранее, выколем из векторов u, v, α, y компоненты с номерами стертых компонент вектора v, получив при этом $\widetilde{u}$, $\widetilde{v}$, β и z. Теперь $\widetilde{u}$ принадлежит коду $GRS_{\widetilde{k}}(\beta, z)$ длины $\widetilde{n} = n - s$ и с кодовым расстоянием $\widehat{d} = \widetilde{n} - \widetilde{k} + 1 = n - s + \widetilde{k} + 1$. Так как

$$2t + 1 \leqslant \widetilde{d} - s = n - s - \widetilde{k} + 1 = \widehat{d}, \tag{4}$$

то код $GRS_{\widetilde{k}}(\beta, z)$ может исправить t ошибок в векторе $\widetilde{v}$.

Заметим, что для $\sigma(x)$ и $p(x)$ (истинные значения), которые получены на основе исходных данных, сравнение (3) выполнено, причем $b(x) = p(x)/\sigma(x)$.

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

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

Покажем, что $v_j(x)$ делится на $r_j(x)$, причем $r_j(x)/v_j(x) = b(x)$. Домножив первое из приведенных ниже сравнений:

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

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

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

Учитывая, что для любого i-го шага обобщенного алгоритма Евклида выполнено

$$\deg v_i(x) = \deg m(x) - \deg r_{i-1}(x),$$

степени многочленов в обеих частях сравнения (5) строго меньше $\widetilde{n} = \deg m(x)$. Следовательно, получаем равенство

$$v_j(x)p(x) = \sigma(x)r_j(x).$$

Так как $p(x) = \sigma(x)b(x)$, то $r_j(x) = v_j(x)b(x)$.

Поскольку кодовый вектор $\widetilde{u}$ кода $GRS_{\widetilde{k}}(\beta, z)$ получен с помощью многочлена $b(x)$, то, учитывая неравенство $n - s \geqslant \widetilde{k}$ из (4), вектор u кода $GRS_{\widetilde{k}}(L, y)$ получен с помощью этого же многочлена. Поэтому исходный кодовый вектор u кода $\Gamma(L, G)$ можно найти на основе кодирования многочлена $b(x)$ кода $GRS_{\widetilde{k}}(L, y)$ с помощью формулы (1). □

Задача нахождения интерполяционного многочлена тесно связана с задачей обращения матрицы Вандермонда. В работах [9, 10] приводятся алгоритмы нахождения обратной матрицы со сложностью $O(n^2)$. В работе [11] приводятся точные формулы обратной матрицы Вандермонда через элементарные симметрические многочлены. Приведем эти формулы. Пусть $V = V(a_1, \ldots, a_n)$ — матрица Вандермонда:

$$V = V(a_1, \ldots, a_n) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ \ldots & \ldots & \ldots & \ldots \\ a_1^{n-1} & a_2^{n-1} & \ldots & a_n^{n-1} \end{pmatrix},$$

где $a_1, \ldots, a_n$ — элементы произвольного поля F. Пусть

$$\sigma_k = \sigma_k(a_1, \ldots, a_n) = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} a_{i_1} \ldots a_{i_k}$$

— элементарный симметрический многочлен от $a_1, \ldots, a_n$, $k = 1, \ldots, n$. При этом

$$\sigma_0 = \sigma_0(a_1, \ldots, a_n) = 1.$$

Также определим

$$\sigma_{k,j} = \sigma_k(a_1, \ldots, \widehat{a}_j, \ldots, a_n), \quad k = 1, \ldots, n-1, \quad j = 1, \ldots, n,$$

где $\widehat{\ }$ означает, что элемент пропущен. Тогда (i, j)-й элемент матрицы V^{-1} равен

$$(V^{-1})_{ij} = (-1)^{i+j} \frac{\sigma_{n-j,i}}{\prod_{k=1}^{i-1}(a_i - a_k) \prod_{k=i+1}^{n}(a_k - a_i)}. \tag{6}$$

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 $L = GF(2^4) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$. Рассмотрим квадратный многочлен $x^2 + x + \alpha^3$. Так как след элемента α^3 в $GF(2^4)$ не равен нулю, то этот многочлен в поле $GF(2^4)$ не имеет корней. Поэтому определим $G(x) = x^2 + x + \alpha^3$. Поскольку многочлен $G(x)$ сепарабельный, то $\Gamma(L, G) = \Gamma(L, \overline{G})$, где $\overline{G}(x) = x^4 + x^2 + \alpha^6$. Проверочная матрица H кода $\Gamma(L, G)$ примет такой вид:

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

После замены каждого элемента матрицы H столбцовым двоичным вектором длины 4, представляющим этот элемент, получим матрицу H_2 размера 8×16. Так как все строки полученной двоичной матрицы H_2 линейно независимы, то $n - k = 8$, $k = 8$. Выписав построчно фундаментальную систему решений однородной системы линейных уравнений $H_2 X = O$, находим порождающую матрицу кода $\Gamma(L, G)$:

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

Для данного $[16, 8]$-кода кодовое расстояние $d = 5$, поэтому код может исправлять до двух ошибок, либо одну ошибку и до двух стираний, либо до четырех стираний. Рассмотрим случай одной ошибки и двух стираний.

Учитывая теорему 1, код $\Gamma(L, G)$ является ограничением кода $GRS_{12}(L, y)$ на подполе $GF(2)$, где

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

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

причем равенство $\prod_{j \neq i} (\alpha_i - \alpha_j) = 1$ выполнено в силу того, что корнями многочлена $x^{n-1} - 1$ являются все ненулевые элементы поля $GF(2^m)$.

Пусть после кодирования информационного вектора $i = (1, 0, 0, 1, 1, 1, 0, 1)$ получен кодовый вектор кода $\Gamma(L, G)$

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

а на приемном конце получен вектор

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

т. е. произошла одна ошибка на 3-й позиции (нумеруя позиции с нуля) и два стирания на 10-й и 12-й позициях. При этом на приемной стороне известны только позиции стираний. Для декодирования вектора v применим алгоритм 1.

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

$$\widetilde{v} = (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1),$$

в котором только одна ошибка. Для декодирования данного вектора будем рассматривать код $GRS_{12}(\beta, z)$ длины $\widetilde{n} = 14$, β и y — векторы длины 14, которые получаются соответственно из векторов L и y путем удаления 10-й и 12-й компонент:

$$\beta = (0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^{10}, \alpha^{12}, \alpha^{13}, \alpha^{14}),$$
$$z = (\alpha^6, \alpha^6, \alpha^7, \alpha^9, \alpha^{12}, \alpha^7, \alpha^{13}, \alpha^{14}, \alpha^3, \alpha^9, \alpha^{13}, \alpha^{11}, \alpha^{14}, \alpha^{12}).$$

Множество S позиций стертых символов равно $S = \{10, 12\}$. Составляем многочлен $m(x)$:

$$m(x) = \frac{x^{16} - x}{(x - \alpha^9)(x - \alpha^{11})} = \alpha^{10}x + \alpha^7x^2 + \alpha^8x^3 + \alpha x^4 + \alpha^8x^5 +$$
$$+\alpha^3x^6 + \alpha^{14}x^7 + \alpha^4x^8 + \alpha^3x^9 + \alpha^3x^{10} + \alpha^6x^{11} + \alpha^8x^{12} + \alpha^2x^{13} + x^{14}.$$

Пусть $V = V(\beta)$ — матрица Вандермонда, построенная на основе вектора β, V^{-1} — обратная к ней матрица (построенная, например, с помощью формулы (6)), Z — диагональная матрица на основе вектора z:

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

2. Интерполяция. Вычисляем коэффициенты многочлена $f(x) = f_0 + f_1x + \ldots + f_{13}x^{13}$:

$$(f_0, f_1, \ldots, f_{13}) = \widetilde{v}Z^{-1}V^{-1} = (0,\ \alpha^9,\ \alpha^8,\ \alpha^{10},\ 0,\ \alpha^3,\ \alpha^{13},\ \alpha^4,\ \alpha^7,\ \alpha^2,\ \alpha^5,\ \alpha^4,\ 0,\ \alpha^{11}),$$
$$f(x) = \alpha^9x + \alpha^8x^2 + \alpha^{10}x^3 + \alpha^3x^5 + \alpha^{13}x^6 + \alpha^4x^7 + \alpha^7x^8 + \alpha^2x^9 + \alpha^5x^{10} + \alpha^4x^{11} + \alpha^{11}x^{13}.$$

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:

$$r_{-1}(x) = r_0(x)(\alpha^6 + \alpha^4x) + r_1(x),$$
$$r_1(x) = \alpha^5x + \alpha^{12}x^2 + \alpha^3x^3 + \alpha^7x^4 + \alpha^{12}x^5 + \alpha^9x^7 + \alpha^7x^8 + \alpha^4x^9 + \alpha^9x^{10} + x^{11},$$
$$v_1(x) = -(\alpha^6 + \alpha^4x) = \alpha^6 + \alpha^4x.$$

Так как $(\widetilde{n} + \widetilde{k})/2 = 13$, $\deg r_0(x) = 13$, $\deg r_1(x) = 11$, то после первого шага алгоритма Евклида останавливаемся.

4. Деление:

$$b(x) = \frac{r_1(x)}{v_1(x)} = \alpha^{14}x + \alpha^4x^2 + \alpha^7x^3 + \alpha^2x^4 +$$
$$+\alpha^{13}x^5 + \alpha^{11}x^6 + \alpha x^7 + \alpha^7x^8 + \alpha^7x^9 + \alpha^{11}x^{10}.$$

5. Вычисление исходного кодового вектора u с помощью кодирования информационного многочлена $b(x)$ в кодовый вектор кода $GRS_{14}(L, y)$:

$$u = (y_0b(0), y_1b(1), y_2b(\alpha), \ldots, y_{15}b(\alpha^{14})) = (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1).$$

С учетом того, что столбцы матрицы G с номерами 7, 9–15 (нумеруя с нуля) образуют единичную матрицу, из этих позиций вектора u извлекаем информационный вектор $i = (1, 0, 0, 1, 1, 1, 0, 1)$.

2. Декодирование кодов Гоппы на основе алгоритма Гао (второй вариант)

Пусть кодовый вектор $u \in \Gamma(L, G)$ получен на основе информационного вектора b с помощью правила (1), а после передачи вектора u на приемной стороне получен вектор v, в котором t ошибок и s стираний.

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:

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

Также 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 $\widetilde{v}_i = y_ib(\alpha_i)$. 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

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

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

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

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

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

Тогда из равенств

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

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

$$\sigma(x)\widetilde{f}(x) \equiv \widetilde{p}(x) \pmod{m(x)}. \tag{7}$$

Заметим, что

$$\deg\sigma(x) \leqslant \frac{n-\widetilde{k}-s}{2}, \quad \deg\widetilde{p}(x) < \frac{n+\widetilde{k}+s}{2}, \tag{8}$$

так как

$$\deg\sigma(x) \leqslant t \leqslant \frac{d-s-1}{2} = \frac{n-\widetilde{k}-s}{2},$$

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

Алгоритм 2 (декодирование кода Гоппы на основе алгоритма Гао на случай ошибок и стираний).

Вход: принятый вектор v.

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

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

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

   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

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

4. Деление. Информационный многочлен равен $b(x) = \dfrac{r_j(x)}{v_j(x)\nu(x)}$.
5. 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 4. *Если в кодовом векторе произошло t ошибок и s стираний, причем $r \geqslant 2t+s$ ($2r \geqslant 2t+s$ для двоичного сепарабельного кода), $r = \deg G(x)$, то алгоритм декодирования 2 всегда приводит к единственному решению, а именно к исходному кодовому вектору u кода $\Gamma(L,G)$.*

Доказательство аналогично доказательству теоремы 3.

Пример 2. Продолжим рассмотрение примера 1. Пусть после кодирования информационного вектора $i=(1,0,1,1,0,0,1,1)$ получен кодовый вектор кода $\Gamma(L,G)$

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

а на приемном конце получен вектор

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

т. е. произошла одна ошибка на 3-й позиции (нумеруя позиции с нуля) и два стирания на 10-й и 12-й позициях. При этом на приемной стороне известны только позиции стираний. Для декодирования вектора v применим алгоритм 2.

1. Полагаем $s=2$, $t=[(d-s-1)/2]=1$. Заменив в векторе v стертые символы нулями, получаем $\widetilde{v}=(0,1,1,0,0,0,0,1,0,0,0,1,0,0,1,1)$. Также вычисляем многочлен локаторов стираний $\nu(x)=(x-\alpha_{10})(x-\alpha_{12})=(x-\alpha^9)(x-\alpha^{11})=\alpha^5+\alpha^2x+x^2$. Пусть $V=V(L)$ — матрица Вандермонда, построенная на основе вектора L, V^{-1} — обратная к ней матрица, Y — диагональная матрица на основе вектора y.
2. Интерполяция. Вычисляем коэффициенты многочлена $f(x)=f_0+f_1x+\ldots+f_{15}x^{15}$:
$$(f_0,f_1,\ldots,f_{15}) = \widetilde{v}Y^{-1}V^{-1} =$$
$$= (0,\ \alpha^5,\ \alpha^9,\ \alpha,\ \alpha^3,\ \alpha^2,\ \alpha^9,\ \alpha^5,\ \alpha^4,\ 0,\ \alpha^{12},\ 1,\ \alpha^8,\ \alpha^5,\ \alpha^{14},\ \alpha^4),$$
$$f(x) = \alpha^5x+\alpha^9x^2+\alpha x^3+\alpha^3x^4+\alpha^2x^5+\alpha^9x^6+\alpha^5x^7+\alpha^4x^8+$$
$$+\alpha^{12}x^{10}+x^{11}+\alpha^8x^{12}+\alpha^5x^{13}+\alpha^{14}x^{14}+\alpha^4x^{15}.$$
Вычисляем $\widetilde{f}(x)=f(x)\nu(x)$:
$$\widetilde{f}(x) = \alpha^{10}x+\alpha x^2+\alpha^2x^3+\alpha^{10}x^4+\alpha^{12}x^5+\alpha x^6+\alpha^{13}x^7+\alpha^7x^8+\alpha^9x^9+$$
$$+\alpha^{10}x^{10}+\alpha^{12}x^{11}+\alpha^5x^{12}+x^{13}+\alpha^{13}x^{14}+\alpha^{11}x^{15}+\alpha^8x^{16}+\alpha^4x^{17}.$$
3. Применение неполного обобщенного алгоритма Евклида. Определяем $r_{-1}(x)=m(x)=x^{16}-x$, $r_0(x)=\widetilde{f}(x)$, $v_{-1}(x)=0$, $v_0(x)=1$ и применяем алгоритм Евклида:
$$\begin{aligned}
&r_{-1}(x) = r_0(x)q_0(x)+r_1(x),\\
&\quad q_0(x)=0,\\
&\quad r_1(x)=x+x^{16},\\
&v_1(x)=v_{-1}(x)-v_0(x)q_0(x)=0,\\
&r_0(x)=r_1(x)q_1(x)+r_2(x),\\
&\quad q_1(x)=\alpha^8+\alpha^4x,\\
&\quad r_2(x)=\alpha x+x^2+\alpha^2x^3+\alpha^{10}x^4+\alpha^{12}x^5+\alpha x^6+\alpha^{13}x^7+\alpha^7x^8+\alpha^9x^9+\\
&\quad +\alpha^{10}x^{10}+\alpha^{12}x^{11}+\alpha^5x^{12}+x^{13}+\alpha^{13}x^{14}+\alpha^{11}x^{15},\\
&v_2(x)=v_0(x)-v_1(x)q_1(x)=1,\\
&r_1(x)=r_2(x)q_2(x)+r_3(x),\\
&\quad q_2(x)=\alpha^6+\alpha^4x,\\
&\quad r_3(x)=\alpha^9x+\alpha^9x^2+\alpha^5x^3+\alpha^{11}x^4+x^5+\alpha^{14}x^6+\alpha^8x^7+\alpha^{14}x^8+\alpha^{12}x^9+\\
&\quad +\alpha^{12}x^{10}+x^{11}+\alpha^6x^{12}+\alpha^5x^{13},\\
&v_3(x)=v_1(x)-v_2(x)q_2(x)=\alpha^6+\alpha^4x.
\end{aligned}$$

Так как $(n+\widetilde{k}+s)/2=15$, $\deg r_2(x)=15$, $\deg r_3(x)=13$, то после третьего шага алгоритма Евклида останавливаемся.

4. Деление:

$$b(x)=\frac{r_3(x)}{v_3(x)\nu(x)}=\alpha^{13}x+\alpha^2x^2+\alpha x^3+\alpha^{14}x^4+\alpha^8x^5+\alpha^3x^6+\alpha^{10}x^7+\alpha^2x^8+\alpha^2x^9+\alpha x^{10}.$$

5. Вычисление исходного кодового вектора u с помощью кодирования информационного многочлена $b(x)$ в кодовый вектор кода $GRS_{12}(L,y)$:

$$u=(y_0b(0),y_1b(1),y_2b(\alpha),\ldots,y_{15}b(\alpha^{14}))=(0,1,1,1,0,0,0,1,0,0,1,1,0,0,1,1).$$

С учетом того, что столбцы матрицы G с номерами 7, 9–15 (нумеруя с нуля) образуют единичную матрицу, из этих позиций вектора u извлекаем информационный вектор $i=(1,0,1,1,0,0,1,1)$.

3. Декодирование кодов Гоппы на основе алгоритма Сугиямы

Пусть v — полученный на приемной стороне вектор, в котором могут быть ошибки и стирания. Пусть $\widetilde{d}\geqslant 2t+s+1$. 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 $t+s$.

Вычисляя синдромный вектор, получаем

$$S=\widetilde{v}\,\overline{H}^T=e\overline{H}^T=\left(\ \ldots,\ \ e_{i_1},\ \ \ldots,\ \ e_{i_{t+s}},\ \ \ldots\ \right)\times$$

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

$$=\begin{pmatrix}e_{i_1}G(\alpha_{i_1})^{-1}+\ldots+e_{i_{t+s}}G(\alpha_{i_{t+s}})^{-1}\\ e_{i_1}G(\alpha_{i_1})^{-1}\alpha_{i_1}+\ldots+e_{i_{t+s}}G(\alpha_{i_{t+s}})^{-1}\alpha_{i_{t+s}}\\ \ldots\\ e_{i_1}G(\alpha_{i_1})^{-1}\alpha_{i_1}^{n-k-1}+\ldots+e_{i_{t+s}}G(\alpha_{i_{t+s}})^{-1}\alpha_{i_{t+s}}^{n-k-1}\end{pmatrix}^T.$$

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, причем локаторы принадлежат полю $GF(q^m)$, а значения ошибок — полю $GF(q)$. Обозначим $Z_j=Y_jG(\alpha_{i_j})^{-1}$, $j=1,\ldots,t+s$. Тогда

$$\begin{aligned}&S_0=Z_1+\ldots+Z_t+Z_{t+1}\ldots+Z_{t+s},\\ &S_1=Z_1X_1+\ldots+Z_tX_t+Z_{t+1}X_{t+1}+\ldots+Z_{t+s}Z_{t+s},\\ &\ldots\\ &S_{2t+s-1}=Z_1X_1^{2t+s-1}+\ldots+Z_tX_t^{2t+s-1}+Z_{t+1}X_{t+1}^{2t+s-1}+\ldots+Z_{t+s}X_{t+s}^{2t+s-1}.\end{aligned}\tag{9}$$

Запишем синдромный многочлен в виде

$$S(x)=\sum_{i=0}^{2t+s-1}S_ix^i=\sum_{i=0}^{2t+s-1}\left(\sum_{j=1}^{t+s}Z_jX_j^i\right)x^i=\sum_{j=1}^{t+s}Z_j\left(\sum_{i=0}^{2t+s-1}(X_jx)^i\right)=$$

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

Полагая

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

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

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:

$$\widetilde{\sigma}(x)S(x)\equiv\widetilde{\omega}(x)\ (\mathrm{mod}\ \ x^{2t+s}). \tag{10}$$

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

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

Введем в рассмотрение многочлен $\widetilde{S}(x)=S(x)\nu(x)$ — модифицированный синдромный многочлен. Тогда ключевое уравнение (10) примет вид

$$\sigma(x)\widetilde{S}(x)\equiv\widetilde{\omega}(x)\ (\mathrm{mod}\ \ x^{2t+s}), \tag{11}$$

где

$$\deg\sigma(x)\leqslant t,\quad \deg\widetilde{\omega}(x)\leqslant t+s-1,\quad \sigma(0)=1. \tag{12}$$

Алгоритм 3 (декодирование кода Гоппы на основе алгоритма Сугиямы на случай ошибок и стираний).

Вход: принятый вектор v.

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

1. Определяется $t = [(r-s)/2]$ ($t = [(2r-s)/2]$ в случае двоичного сепарабельного кода Гоппы). 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 $\widetilde{v}\overline{H}^T$. 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. 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 ($i \geqslant 1$):
$$r_{i-2}(x) = r_{i-1}(x)q_{i-1}(x) + r_i(x),$$
$$v_i(x) = v_{i-2}(x) - v_{i-1}(x)q_{i-1}(x).$$
   Процесс прекращается, как только для некоторого $r_j(x)$ будет выполнено
$$\deg r_{j-1}(x) \geqslant t+s, \quad \deg r_j(x) \leqslant t+s-1.$$
   Тогда
$$\sigma(x) = \lambda v_j(x), \quad \widetilde{\omega}(x) = \lambda r_j(x),$$
   где константа $\lambda \in GF(q^m)$ 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 $GF(q^m)$. 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
$$M = \{1, \ldots, l\} \cup \{t+1, \ldots, t+s\} \backslash \{p\}$$
   — множество индексов локаторов ошибок и стираний без учета индекса p. Находятся Z_j, $j \in M$, например, с помощью алгоритма Форни для обобщенных кодов РС:
$$Z_j = \frac{\widetilde{\omega}(X_j^{-1})}{\prod_{i \in M \backslash \{j\}}(1 - X_i X_j^{-1})}, \quad j \in M. \tag{13}$$
   После этого находятся значения ошибок $Y_j = Z_j G(X_j)$, $j \in M$. 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 $\alpha_i = 0$ (в противном случае все локаторы стираний были бы ненулевые). Вычисляется значение Z_p, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы $\overline{H}$. Вычисляется значение ошибки $Y_p = Z_p G(\alpha_i)$. 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 (13) находятся значения Z_j, затем значения ошибок $Y_j = Z_j G(X_j)$, $j \in M$. 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, 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 5. *Если в кодовом векторе* $u \in \Gamma(L,G)$ *произошло* t *ошибок и* s *стираний, причем* $r \geqslant 2t+s$ ($2r \geqslant 2t+s$ *в случае двоичного сепарабельного кода Гоппы*), $r = \deg G(x)$, *то алгоритм декодирования* 3 *всегда приводит к единственному решению, а именно к исходному кодовому вектору* u *кода* $\Gamma(L,G)$.

Доказательство. Пусть $\Gamma(L,G) = GRS_{\widetilde{k}}(L,y) \cap F^n$. Из неравенства $r \geqslant 2t+s$ ($2r \geqslant 2t+s$) следует, что $\widetilde{d} \geqslant 2t+s+1$. Поэтому для декодирования вектора $u \in \Gamma(L,G)$ можно применить любой алгоритм декодирования для ОРС кодов, так как $u \in GRS_{\widetilde{k}}(L,y)$. В этом случае остается применить теорему 4 из работы [12]. □

Пример 3. Продолжим рассмотрение примеров 1 и 2. В данном случае $\Gamma(L,G) \subseteq \subseteq GRS_{12}(L,y)$, при этом проверочная матрица $\overline{H}$ кода $GRS_{12}(L,y)$, учитывая следствие 1, имеет 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, как и ранее, на приемном конце получен вектор

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

в котором одна ошибка и два стирания. Применим к этому вектору алгоритм декодирования 3.

1. Пусть $s=2$, $t=[(2r-s)/2]=1$. Заменив стертые символы на 0, получим вектор $\widetilde{v}$:
$$\widetilde{v} = (0,1,0,0,1,0,0,1,0,0,0,1,0,1,0,1).$$
Найдем компоненты синдромного вектора $\widetilde{v}\overline{H}^T$:
$$(S_0,S_1,S_2,S_3) = (\alpha^{12},\alpha^2,\alpha^{14},\alpha^2).$$
Вычисляем известные локаторы стираний:
$$X_2 = \alpha_{10} = \alpha^9, \quad X_3 = \alpha_{12} = \alpha^{11}.$$
Поэтому
$$\widetilde{S}(x) = S(x)\nu(x) = (\alpha^{12}+\alpha^2 x+\alpha^{14}x^2+\alpha^2x^3)(1-\alpha^9x)(1-\alpha^{11}x) = \\ = \alpha^{12}+\alpha^{13}x+\alpha^{11}x^2+\alpha^{13}x^3+\alpha^7x^5.$$
2. Определяем $r_{-1}(x)=x^4$, $r_0(x)=\widetilde{S}(x)$, $v_{-1}(x)=0$, $v_0(x)=1$. Выполняем неполный алгоритм Евклида:
$$\begin{aligned} r_{-1}(x) &= r_0(x)q_0(x)+r_1(x), \\ q_0(x) &= 0, \\ r_1(x) &= x^4, \\ v_1(x) &= v_{-1}(x)-q_0(x)v_0(x) = 0, \\ r_0(x) &= r_1(x)q_1(x)+r_2(x), \\ q_1(x) &= \alpha^7 x, \\ r_2(x) &= \alpha^{12}+\alpha^{13}x+\alpha^{11}x^2+\alpha^{13}x^2, \\ v_2(x) &= v_0(x)-q_1(x)v_1(x) = 1, \\ r_1(x) &= r_2(x)q_2(x)+r_3(x), \\ q_2(x) &= 1+\alpha^2x, \\ r_3(x) &= \alpha^{12}+\alpha^2x+\alpha^{12}x^2, \\ v_3(x) &= v_1(x)-q_2(x)v_2(x) = 1+\alpha^2x. \end{aligned}$$

Так как $t+s=3$, $\deg r_2(x)=3$, $\deg r_3(x)<3$, то после третьего шага останавливаемся. Тогда

$$\sigma(x)=\lambda v_3(x),\quad \widetilde{\omega}(x)=\lambda r_3(x).$$

При $\lambda=1$ получаем $\sigma(0)=1$, поэтому

$$\sigma(x)=1+\alpha^2x,\quad \widetilde{\omega}(x)=\alpha^{12}+\alpha^2x+\alpha^{12}x^2.$$

3. Корнем многочлена $\sigma(x)$ является $x_1=\alpha^{13}$, поэтому $X_1=x_1^{-1}=\alpha^2=\alpha_3$. Это значит, что ошибка произошла на 3-й позиции. Итак, на 3-й позиции вектора $\widetilde{v}$ точно имеется ошибка, а на позициях 10 и 12, возможно, есть ошибки (после замены стертых символов нулями мы могли поставить некоторые символы верно).
4. Так как среди локаторов стираний нет нулевых значений, то переходим к пункту 4.2 алгоритма 3 декодирования. Поскольку код $\Gamma(L,G)$ двоичный, то $Y_1=1$. Найдем Y_2 и Y_3. Используем алгоритм Форни:

$$Z_2=\frac{\widetilde{\omega}(X_2^{-1})}{(1-X_1X_2^{-1})(1-X_3X_2^{-1})}=0,\quad Y_2=Z_2G(\alpha_{10})=0,$$

$$Z_3=\frac{\widetilde{\omega}(X_3^{-1})}{(1-X_1X_3^{-1})(1-X_2X_3^{-1})}=\alpha^4,\quad Y_3=Z_3G(\alpha_{12})=1.$$

Таким образом, в векторе $\widetilde{v}$ две ошибки — на 3-й и 12-й позициях. Поэтому

$$\widetilde{u}=(0,1,0,1,1,0,0,1,0,0,0,1,1,1,0,1).$$

Так как $\alpha_0=0$, то проверяем, была ли ошибка на 0-й позиции. Скалярное произведение вектора $\widetilde{u}$ на первую строку матрицы $\overline{H}$ дает ноль, поэтому исходный кодовый вектор равен $u=\widetilde{u}$.

4. Декодирование кодов Гоппы на основе алгоритма Берлекэмпа – Месси

Продолжим рассмотрение сравнения (11). 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, $\widetilde{d}\geqslant 2t+s+1$, $t=[(\widetilde{d}-s-1)/2]$, m — реальное число ошибок, $m\leqslant t$. В этом случае $\deg\omega(x)\leqslant m+s-1$, и необходимым условием выполнения данного сравнения является то, что коэффициент многочлена $\sigma(x)\widetilde{S}(x)$ при x^i, $i=m+s,m+s+1,\ldots,2t+s-1$, равен нулю. Учитывая, что $\sigma_0=0$, получаем систему уравнений:

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

Запишем данную систему в матричном виде:

$$\begin{pmatrix}\widetilde{S}_{s+m-1} & \widetilde{S}_{s+m-2} & \ldots & \widetilde{S}_s\\ \widetilde{S}_{s+m} & \widetilde{S}_{s+m-1} & \ldots & \widetilde{S}_{s+1}\\ \ldots & \ldots & \ldots & \ldots\\ \widetilde{S}_{s+2t-2} & \widetilde{S}_{s+2t-3} & \ldots & \widetilde{S}_{s+2t-m-1}\end{pmatrix}\begin{pmatrix}\sigma_1\\ \sigma_2\\ \ldots\\ \sigma_m\end{pmatrix}=\begin{pmatrix}-\widetilde{S}_{s+m}\\ -\widetilde{S}_{s+m+1}\\ \ldots\\ -\widetilde{S}_{s+2t-1}\end{pmatrix}. \qquad (14)$$

Удалив в системе (14) $2t-2m$ последних уравнений, получим новую систему с квадратной матрицей системы порядка m. Матрицу данной системы обозначим через $M(m,s)$.

Теорема 6. *Пусть произошло s стираний. Матрица $M(m,s)$ невырождена тогда и только тогда, когда произошло m ошибок.*

Доказательство следует из теоремы 5 работы [12].

Для нахождения решения системы (14) применим следующий алгоритм.

Алгоритм 4 (алгоритм Берлекэмпа–Месси)
Вход: последовательность $a_1,\dots,a_n$ над некоторым полем.
Выход: LFSR $(L,f(x))$ минимальной длины L, для которого

$$-a_j=\sum_{i=1}^{L} f_i a_{j-i},\quad j=L+1,\,L+2,\dots,n.$$

1. Определить $r:=0$, $f(x):=1$, $b(x):=1$, $L:=0$.
2. Цикл $r:=1,\dots,n$
   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 7. *Пусть $\widetilde{d}\geqslant 2t+s+1$. Если на вход алгоритма 4 подать последовательность $\widetilde{S}_s$, $\widetilde{S}_{s+1}$,..., $\widetilde{S}_{s+2t-1}$, то на выходе алгоритма будет верное значение многочлена локаторов ошибок $\sigma(x)$.*

Доказательство. Пусть $\widetilde{\sigma}(x)$ — многочлен, полученный после применения алгоритма 4. Так как коэффициенты многочлена локаторов ошибок $\sigma(x)$ являются решением системы (14), то по свойству алгоритма Берлекэмпа–Месси будет выполнено неравенство $L\leqslant m$ (в данном случае L — длина регистра). Удалив в системе (14) $2t-2m$ последних уравнений, получим новую систему с квадратной матрицей системы порядка m. Из теоремы 6 следует, что данная матрица невырождена, поэтому полученная новая система имеет единственное решение. Это значит, что $\widetilde{\sigma}(x)=\sigma(x)$. □

Алгоритм 5 (декодирование кода Гоппы на основе алгоритма Берлекэмпа–Месси на случай ошибок и стираний).

Вход: принятый вектор v.

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

1. Определяется $t = [(r-s)/2]$ ($t = [(2r-s)/2]$ в случае двоичного сепарабельного кода Гоппы). 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 $\widetilde{v}\overline{H}^T$. 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 4 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. Отыскиваются l 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. 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
   $$M = \{1, \ldots, l\} \cup \{t+1, \ldots, t+s\} \backslash \{p\}$$
   — множество индексов локаторов ошибок и стираний без учета индекса p. Находятся Z_j, $j \in M$, например, с помощью алгоритма Форни (13) для обобщенных кодов РС. После этого находятся значения ошибок $Y_j = Z_j G(X_j)$, $j \in M$. 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 $\alpha_i = 0$ (в противном случае все локаторы стираний были бы ненулевые). Вычисляется значение Z_p, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы $\overline{H}$. Вычисляется значение ошибки $Y_p = Z_p G(\alpha_i)$. 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 (13) находятся значения Z_j, затем значения ошибок $Y_j = Z_j G(X_j)$, $j \in M$. 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 $\deg \sigma(x)$ строго меньше длины LFSR (полученного на выходе алгоритма 4), то вычисляется значение Z_0, равное скалярному произведению вектора $\widetilde{u}$ на первую строку матрицы $\overline{H}$, а затем 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 рассматривать примеры 1, 2 и 3. Пусть на приемной стороне получен все тот же вектор $v = (0,1,0,0,1,0,0,1,0,0,*,1,*,1,0,1)$. После замены стертых символов нулями получаем вектор $\widetilde{v} = (0,1,0,0,1,0,0,1,0,0,0,1,0,1,0,1)$. Компоненты синдромного вектора $\widetilde{S}$ вычислены в предыдущем примере: $\widetilde{S}_0 = \alpha^{12}$, $\widetilde{S}_1 = \alpha^{13}$, $\widetilde{S}_2 = \alpha^{11}$, $\widetilde{S}_3 = \alpha^{13}$, $\widetilde{S}_4 = \alpha^7$. Определяем $s = 2$, $t = [(2r-s)/2] = 1$. На вход алгоритма 4 подаем последовательность $\widetilde{S}_2 = \alpha^{11}$, $\widetilde{S}_3 = \alpha^{13}$. Получаем $\sigma(x) = 1 + \alpha^2 x$, $L = 2$. Многочлен $\widetilde{\omega}(x)$ можно найти из сравнения $\widetilde{\omega}(x) \equiv \sigma(x)\widetilde{S}(x) \pmod{x^4}$. После этого осталось повторить шаги 3 и 4 предыдущего примера.

Список литературы

1. 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

2. *Гоппа В. Д.* Новый класс линейных корректирующих кодов // Проблемы передачи информации. 1970. Т. 6, № 3. С. 24–30.
3. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки : пер. с англ. Москва : Связь, 1979. 744 с.
4. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки / пер. с англ. И. И. Грушко, В. М. Блиновский ; под ред. К. Ш. Зигангирова. Москва : Мир, 1986. 576 с.
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, MA : Kluwer, 2003. Vol. 712. P. 55–68.
6. *Huffman W. C., Pless V.* Fundamentals of Error-Correcting Codes. New York ; Cambridge : Cambridge University Press, 2003. 646 p.
7. *Рацеев С. М.* Элементы высшей алгебры и теории кодирования : учеб. пособие для вузов. Санкт-Петербург : Лань, 2022. 656 с.
8. *Федоренко С. В.* Простой алгоритм декодирования алгебраических кодов // Информационно-управляющие системы. 2008. № 3. С. 23–27.
9. *Gohberg I., Olshevsky V.* The fast generalized Parker–Traub algorithm for inversion of Vandermonde and related matrices // Journal of Complexity. 1997. Vol. 13, iss. 2. P. 208–234. https://doi.org/10.1006/jcom.1997.0442
10. *Yan S., Yang A.* Explicit algorithm to the inverse of Vandermonde matrix // 2009 International Conference on Test and Measurement. Hong Kong, 2009. P. 176–179. https://doi.org/10.1109/ICTM.2009.5413083
11. *Rawashdeh E. A.* A simple method for finding the inverse matrix of Vandermonde matrix // MATEMATIČKI VESNIK. 2019. Vol. 71, № 3. P. 207–213.
12. *Рацеев С. М., Череватенко О. И.* Об алгоритмах декодирования обобщенных кодов Рида–Соломона на случай ошибок и стираний // Вестник Самарского университета. Естественнонаучная серия. 2021. Т. 26, № 3. С. 17–29. http://doi.org/10.18287/2541-7525-2020-26-3-17-29

References

1. *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
2. Goppa V. D. A New Class of Linear Correcting Codes. *Problems of Information Transmission*, 1970, vol. 6, iss. 3, pp. 207–212.
3. MacWilliams F. J., Sloane N. J. A. *The Theory of Error Correcting Codes*. Amsterdam, New York, North-Holland Pub. Co, 1977. 762 p. (Russ. ed.: Moscow, Sviaz', 1979. 744 p.).
4. Blahut R. E. *Theory and Practice of Error Control Codes*. Reading, Mass., Addison-Wesley Pub. Co., 1983. 500 p. (Russ. ed.: Moscow, Mir, 1986. 576 p.).
5. Gao S. A new algorithm for decoding Reed—Solomon codes. In: V. Bhargava, H. V. Poor, V. Tarokh, S. Yoon, eds. *Communications, Information and Network Security*. Norwell, MA, Kluwer, 2003, vol. 712, pp. 55–68.
6. Huffman W. C., Pless V. *Fundamentals of Error-Correcting Codes*. New York, Cambridge, Cambridge University Press, 2003. 646 p.
7. Ratseev S. M. *Elementy vysshei algebry i teorii kodirovaniya* [Elements of Higher Algebra and Coding Theory]. St. Petersburg, Lan', 2022. 656 p. (in Russian).
8. Fedorenko S. V. Simple algorithm for decoding algebraic codes. *Informatsionno-upravlyayushchie sistemy* [Information and Control Systems], 2008, no. 3, pp. 23–27 (in Russian).

9. Gohberg I., Olshevsky V. The fast generalized Parker–Traub algorithm for inversion of Vandermonde and related matrices. *Journal of Complexity*, 1997, vol. 13, iss. 2, pp. 208–234. https://doi.org/10.1006/jcom.1997.0442
10. Yan S., Yang A. Explicit algorithm to the inverse of Vandermonde matrix. *2009 International Conference on Test and Measurement*. Hong Kong, 2009, pp. 176–179. https://doi.org/10.1109/ICTM.2009.5413083
11. Rawashdeh E. A. A simple method for finding the inverse matrix of Vandermonde matrix. *MATEMATIČKI VESNIK*, 2019, vol. 71, no. 3, pp. 207–213.
12. 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 (in Russian). http://doi.org/10.18287/2541-7525-2020-26-3-17-29

Поступила в редакцию / Received 25.08.2021
Принята к публикации / Accepted 28.09.2021
Опубликована / Published 31.03.2022