УДК 519.725

О простом алгоритме декодировании кодов БЧХ, кодов Рида–Соломона и кодов Гоппы

С. М. Рацеев, О. И. Череватенко

Гао получил простой и эффективный алгоритм декодирования кодов Рида–Соломона. В работе приводится описание применения данного алгоритма для декодирования обобщенных кодов Рида–Соломона, кодов Гоппы, кодов Боуза–Чоудхури–Хоквингема и кодов Рида–Соломона в случае ошибок и стираний.

Ключевые слова: помехоустойчивые коды, коды Рида–Соломона, коды Гоппы, коды Боуза–Чоудхури–Хоквингема, декодирование кода.

1. Введение

Коды Рида–Соломона (РС) являются важным частным случаем кодов Боуза–Чоудхури–Хоквингема (БЧХ), длины которых равны мощности мультипликативной группы поля, над которым они заданы. Важной особенностью кодов РС является возможность исправления многократных пакетов ошибок и тот факт, что они лежат на границе Синглтона. В настоящее время имеется несколько хорошо известных алгоритмов декодирования кодов РС. В силу специфики кодов РС эти алгоритмы позволяют восстановить количество искаженных данных, которое может доходить до половины количества избыточных данных. Наиболее известными алгоритмами декодирования кодов РС являются алгоритм Питерсона–Горенстейна–Цирлера, алгоритм Сугиямы–Касахары–Хирасавы–Намекавы, алгоритм на основе метода Берлекэмпа–Месси [1, 2]. Данные алгоритмы находят решение так называемого ключевого уравнения в четыре этапа: вычисление компонент синдромного вектора, вычисление многочлена локаторов ошибок, нахождение корней многочлена локаторов ошибок, вычисление значений ошибок. К данным алгоритмам можно также добавить алгоритм нахождения значений ошибок Форни.

Для кодов РС Гао [3] и Шиозаки [4] предложили более простой и естественный алгоритм декодирования. Асимптотическая сложность данного алгоритма оценивается величиной $O(n(\log n)^2)$, которая совпадает со сложностью лучших алгоритмов декодирования кода РС, причем его описание является самым простым из описаний известных алгоритмов. Данный алгоритм состоит из трех шагов: построение интерполяционного многочлена, применение незаконченного обобщенного алгоритма Евклида, деление многочленов.

Алгоритм Гао хорошо адаптируется для декодирования обобщенных кодов РС, кодов БЧХ, кодов Гоппы, декодирования кодов РС в случае ошибок и стираний, что и будет продемонстрировано в данной работе. Для каждого алгоритма приведен пример декодирования.

Заметим также, что важность исследования кодов Гоппы обусловлена еще и тем, что на их основе строятся перспективные постквантовые криптосистемы [5].

2. Алгоритм декодирования обобщенных кодов Рида–Соломона

Напомним определение обобщенного кода Рида–Соломона. 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 которых не превосходят $k-1$. При этом кодовое расстояние кода $GRS_k(\alpha, y)$ равно $d = n - k + 1$.

При описании нижеследующего алгоритма, а также его обоснования в виде теоремы 1 будем следовать работе [6].

Определим многочлен:

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

Например, если α_i пробегают все элементы поля $GF(q)$, то $m(x) = x^n - x$. Если $n \mid q-1$ и элемент α имеет порядок n (в мультипликативной группе $GF^*(q^m)$), то $m(x) = (x-1)(x-\alpha)\ldots(x-\alpha^{n-1}) = x^n - 1$.

Пусть кодовый вектор u получен на основе информационного многочлена $b(x) = b_0 + b_1 x + \ldots + b_{k-1} x^{k-1}$ с помощью (1), $v = u + e$ – полученный на приемном конце вектор, в котором t ошибок, $X_1 = \alpha_{i_1}, \ldots, X_t = \alpha_{i_t}$ – локаторы ошибок, $Y_1 = e_{i_1}, \ldots, Y_t = e_{i_t}$ – значения ошибок. Многочлен локаторов ошибок запишем в виде:

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

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

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

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

Обозначим $p(x) = \sigma(x) b(x)$. Заметим, что

$$\deg p(x) \leq \frac{d-1}{2} + k - 1 < \frac{n+k}{2}.$$

Тогда

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

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

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

Тогда из равенств

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

получаем сравнение:

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

Действительно, разделим с остатком $\sigma(x)f(x)$ и $p(x)$ на $m(x)$:

$$\sigma(x) f(x) = q(x) m(x) + r(x), \quad \deg r(x) < n,$$

$$p(x) = \widetilde{q}(x) m(x) + \widetilde{r}(x), \quad \deg \widetilde{r}(x) < n.$$

Так как $m(\alpha_i) = 0$, то:

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

Так как многочлены $r(x)$ и $\widetilde{r}(x)$ совпадают в n точках (причем $\alpha_i \neq \alpha_j$ при $i \neq j$) и имеют степень не более $n-1$, то $r(x) = \widetilde{r}(x)$. Следовательно, получаем сравнение (2).

Алгоритм 1 (алгоритм декодирования для обобщенных кодов РС).

Вход: принятый вектор v.

Выход: исходный информационный вектор b, если произошло не более $[(d-1)/2]$ ошибок, где $[\,]$ – целая часть числа.

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

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

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

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

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

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

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

Теорема 1. Если в кодовом векторе произошло не более $[(d-1)/2]$ ошибок, то алгоритм декодирования 1 всегда приводит к единственному решению, а именно, к исходному информационному вектору b.

Доказательство. Пусть $b(x)$ – исходный информационный многочлен (который соответствует вектору b), $u(x)$ – кодовый многочлен, полученный с помощью формулы (1). Пусть многочлен ошибок $e(x)$ имеет вес не более $[(d-1)/2]$, $v(x) = u(x) + e(x)$ – принятый на приемном конце многочлен. Заметим, что для $\sigma(x)$ и $p(x)$ (истинные значения), которые получены на основе исходных данных, сравнение (2) выполнено, причем $b(x) = p(x)/\sigma(x)$.

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

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

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

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

$$v_j(x) f(x) \equiv r_j(x) \pmod{m(x)}$$

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

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

Оценим сверху степени многочленов из левой и правой частей данного сравнения. Для многочлена из правой части сравнения:

$$\deg \sigma(x) r_j(x) < \frac{d-1}{2} + \frac{n+k}{2} = n.$$

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

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

получаем:

$$\deg v_j(x) = \deg m(x) - \deg r_{j-1}(x) \le n - \frac{n+k}{2} = \frac{d-1}{2}.$$

Поэтому

$$\deg v_j(x)p(x) < \frac{d-1}{2} + \frac{n+k}{2} = n.$$

Следовательно, из сравнения (3) получаем равенство:

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

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

Задача нахождения интерполяционного многочлена тесно связана с задачей обращения матрицы Вандермонда. Помимо классического метода Гаусса существуют алгоритмы обращения матрицы Вандермонда, которые учитывают ее структуру. В работе [7] приводятся формулы для вычисления обратной матрицы к матрице Вандермонда специального вида над конечным полем. В работе [8] приводится алгоритм со сложностью $O(n^3)$. В работах [9, 10, 11, 12, 13] приводятся алгоритмы со сложностью $O(n^2)$. В любом случае обращение матрицы Вандермонда является предвычислением и не влияет на сложность алгоритма декодирования.

Пример 1. Рассмотрим обобщенный код Рида–Соломона над полем $GF(7)$ с параметрами $n = 5$, $k = 3$, $d = 3$, $\alpha = (2, 3, 4, 5, 6)$, $y = (1, 2, 3, 2, 1)$. Для данного кода многочлен $m(x)$ примет вид:

$$m(x) = (x-2)(x-3)(x-4)(x-5)(x-6) = \frac{x^6-1}{x-1} = 1 + x + x^2 + x^3 + x^4 + x^5.$$

Ниже приведена матрица Вандермонда V на основе вектора α, обратная к ней матрица V^{-1} и диагональная матрица Y на основе вектора y:

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

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

Пусть $b = (2, 4, 1)$ – информационный вектор, который соответствует многочлену $b(x) = 2 + 4x + x^2$. Процесс кодирования можно записать в следующем виде:

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

После кодирования информационного вектора b получаем кодовый вектор $u = (0, 4, 4, 3, 6)$.

Предположим, что на приемном конце принят вектор $v = u + e = (0, 2, 4, 3, 6)$, где $e = (0, 5, 0, 0, 0)$ – вектор ошибок. Применим алгоритм декодирования 1.

1. Интерполяция. Вычисляем коэффициенты многочлена $f(x) = f_0 + f_1 x + \ldots + f_4 x^4$:

$$(f_0, f_1, f_2, f_3, f_4) = (0, 2, 4, 3, 6)Y^{-1}V^{-1} = (0, 6, 2, 3, 6).$$

2. Незаконченный обобщенный алгоритм Евклида. Полагаем $r_{-1}(x) = m(x)$, $r_0(x) = f(x)$, $v_{-1}(x) = 0$, $v_0(x) = 1$. После применения первого шага обобщенного алгоритма Евклида

$$r_{-1}(x) = r_0(x)(3+6x) + 1 + 4x + x^2 + x^3, \quad r_1(x) = 1 + 4x + x^2 + x^3,$$

$$v_1(x) = -(3+6x) = 4 + x$$

процесс останавливается, так как $\deg r_0(x) = 4$, $\deg r_1(x) = 3$, причем $(n+k)/2 = 4$.

3. Деление. Исходный информационный многочлен равен:

$$b(x) = \frac{r_1(x)}{v_1(x)} = 2 + 4x + x^2.$$

3. Декодирование кодов БЧХ

Для построения алгоритма декодирования для кодов БЧХ на основе метода Гао нам понадобится следующее хорошо известное утверждение.

Предложение 1. Пусть код БЧХ A над полем $F = GF(q)$ определяется последовательностью корней

$$\alpha^l,\ \alpha^{l+1}, \ldots, \alpha^{l+\delta-2} \in GF(q^m)$$

порождающего многочлена $g(x) \in F[x]$, где α – примитивный элемент поля $GF(q^m)$. Пусть $\widetilde{A}$ – код Рида–Соломона над полем $GF(q^m)$ с порождающим многочленом $\widetilde{g}(x) = (x-\alpha^l)(x-\alpha^{l+1})\ldots(x-\alpha^{l+\delta-2})$. Тогда код A является ограничением кода $\widetilde{A}$ на подполе $GF(q)$, т.е. код A состоит из всех таких $u \in \widetilde{A}$, компоненты которых принадлежат полю $GF(q)$.

Заметим, что предложение 1 верно для любого $\alpha \in GF^*(q)$. В этом случае длины кодов A и $\widetilde{A}$ равны порядку элемента α при $\delta > 2$. При этом код $\widetilde{A}$ уже будет подпадать под определение обобщенного кода Рида–Соломона.

Алгоритм 2 (декодирование кода БЧХ).

Вход: принятый вектор v.

Выход: исходный кодовый вектор $u \in A \subseteq \widetilde{A}$, если число ошибок не превышает $[(d-1)/2]$.

1. Вектор v декодируется с помощью алгоритма 1 для кода $\widetilde{A}$ (при этом полагается, что $m(x) = x^n - 1$), который возвращает информационной многочлен $b(x)$, соответствующий вектору u.

2. После этого остается получить вектор u на основе $b(x)$ с помощью формулы:

$$u = (b(1), b(\alpha), \ldots, b(\alpha^{n-1})).$$

Пример 2. Рассмотрим код БЧХ над полем $GF(2^3)$, построенным на основе многочлена $x^3 + x + 1$ с примитивным элементом α:

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

В качестве порождающего многочлена рассмотрим примитивный многочлен $g(x) = x^3 + x + 1$. Хорошо известно, что полученный код БЧХ является кодом Хэмминга с параметрами $n = 7$, $k = 4$, $d = 3$. С одной стороны, для данного кода существуют эффективные алгоритмы декодирования. С другой стороны, этот пример является иллюстрацией применения алгоритма Гао к кодам БЧХ.

Построим каноническую форму матрицы для нашего кода. Для этого разделим x^i с остатком на $g(x)$:

$$x^3 = g(x)\cdot 1 + 1 + x, \qquad x^4 = g(x)\cdot x + x + x^2,$$
$$x^5 = g(x)\cdot (1+x^2) + 1 + x + x^2, \quad x^6 = g(x)\cdot 1 + 1 + x^2.$$

Получаем порождающую матрицу G в каноническом виде:

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

Закодируем информационный вектор $i = (1,0,1,1)$:

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

Предположим, что на приемном конце получен вектор:

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

где вектор ошибок равен $e = (0,0,0,0,0,1,0)$.

Для декодирования многочлена $v(x) = 1+x^3+x^6$ применим алгоритм 2. Для этого сначала рассмотрим этот многочлен как искаженный кодовый многочлен $[7,5,3]$–кода Рида–Соломона над полем $GF(2^3)$ с порождающим многочленом $\widetilde{g}(x) = (x-\alpha)(x-\alpha^2)$. Матрица Вандермонда (в данном случае, в частности, матрица дискретного преобразования Фурье) для данного кода Рида–Соломона и ее обратная имеют вид:

$$V = \left(\alpha^{ij}\right) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{pmatrix},$$

$$V^{-1} = \frac{1}{n}\left(\alpha^{-ij}\right) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix}.$$

1. Интерполяция. Вычисляем многочлен $f(x)$:

$$(f_0, f_1, f_2, f_3, f_4, f_5, f_6) = vV^{-1} = (1, \alpha^6, \alpha^5, \alpha^6, \alpha^3, \alpha^3, \alpha^5),$$

$$f(x) = 1 + \alpha^6 x + \alpha^5 x^2 + \alpha^6 x^3 + \alpha^3 x^4 + \alpha^3 x^5 + \alpha^5 x^6.$$

2. Применение незаконченного обобщенного алгоритма Евклида. Полагаем $r_{-1}(x) = x^7 - 1$, $r_0(x) = f(x)$. Тогда

$$x^7 - 1 = f(x)(1 + \alpha^2 x) + x + \alpha^6 x^2 + \alpha^2 x^3 + x^4 + \alpha^2 x^5,$$
$$v_1(x) = -(1 + \alpha^2 x) = 1 + \alpha^2 x.$$

3. Деление:

$$b(x) = \frac{r_1(x)}{v_1(x)} = x + x^2 + x^4.$$

4. Находим кодовый многочлен

$$u = (b(1), b(\alpha), \ldots, b(\alpha^6)) = (0, 1, 1, 0, 1, 0, 0)V = (1, 0, 0, 1, 0, 1, 1),$$

из которого извлекаем исходный информационный вектор $i = (1, 0, 1, 1)$.

4. Декодирование кодов Рида–Соломона в случае ошибок и стираний

Пусть код РС над полем $GF(q)$ имеет параметры $[n, k, d = n - k + 1]$, $n = q - 1$, α – примитивный элемент поля $GF(q)$, $g(x) = (x - 1)(x - \alpha) \ldots (x - \alpha^{n-1})$ – порождающий многочлен. Пусть теперь в канале связи происходят ошибки и стирания, $d \geq 2t + r + 1$, где t и r – число ошибок и стираний соответственно. Предположим, что в принятом векторе v произошло t ошибок и r стираний, причем R – множество позиций в векторе v, на которых произошли стирания. Обозначим через $\widetilde{v}$ новый вектор длины $n - r$, который получен из вектора v путем удаления координат с номерами, принадлежащими множеству R. Тем самым мы рассматриваем новый обобщенный код Рида–Соломона длины $\widetilde{n} = n - r$, размерности $\widetilde{k} = k$ и с кодовым расстоянием $\widetilde{d} = \widetilde{n} - \widetilde{k} + 1$. Для декодирования информационного многочлена $b(x)$ можно применить алгоритм 1, который будет работать с вектором $\widetilde{v}$ и новыми параметрами $\widetilde{n}$, $\widetilde{k}$ и $\widetilde{d}$. Вектор y в данном алгоритме полагается состоящим из единиц. При этом рассматриваются такие степени α^i, для которых $i \notin R$, а многочлен $m(x)$ имеет такой вид:

$$m(x) = \prod_{\substack{0 \leq i \leq n-1, \\ i \notin R}} (x - \alpha^i).$$

Незаконченный алгоритм Евклида шага 2 алгоритма 1 будет работать до тех пор, пока не достигнется такое $r_j(x)$, что:

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

Так как для данного обобщенного кода Рида–Соломона выполнено $\widetilde{d} \geq 2t + 1$, то из теоремы 1 следует, что такой алгоритм декодирования однозначным образом возвратит исходный информационный многочлен $b(x)$.

Пример 3. Построим код РС над полем $GF(11)$ с параметрами $n = 10$, $k = 5$, $d = n - k + 1 = 6$. Число $\alpha = 2$ является примитивным элементом поля $GF(11)$ (иными словами, первообразным корнем кольца вычетов по модулю 11, так как по критерию первообразного корня для данного случая должно быть выполнено $\alpha^2 \not\equiv 1 \pmod{11}$ и $\alpha^5 \not\equiv 1 \pmod{11}$). Данный код может исправлять либо до двух ошибок и одно стирание, либо одну ошибку и до трех стираний, либо до пяти стираний.

Рассмотрим случай одной ошибки и трех стираний. Пусть $b = (7, 2, 8, 1, 4)$ – информационный вектор, который соответствует многочлену $b(x) = 7 + 2x + 8x^2 + x^3 + 4x^4$. После кодирования этого вектора получаем:

$$u = (b(1), b(\alpha), \ldots, b(\alpha^9)) = (0, 5, 10, 7, 4, 5, 3, 9, 7, 9).$$

Пусть на приемном конце получен вектор

$$v = (0, 5, 10, 7, 1, *, 3, *, 7, *),$$

т.е. произошла одна ошибка и три стирания (заметим, что на приемном конце исходный вектор u пока неизвестен).

Удалив в векторе v стертые символы, получим новый вектор

$$\widetilde{v} = (0, 5, 10, 7, 1, 3, 7),$$

в котором только одна ошибка. Сейчас будем рассматривать обобщенный код РС длины $\widetilde{n} = 7$, размерности $\widetilde{k} = 5$, с кодовым расстоянием $\widetilde{d} = 3$. Множество R позиций стертых символов равно $R = \{5, 7, 9\}$. Составляем многочлен $m(x)$:

$$m(x) = (x - \alpha^0)(x - \alpha^1)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)(x - \alpha^6)(x - \alpha^8) =$$

$$= (x - 1)(x - 2)(x - 4)(x - 8)(x - 5)(x - 9)(x - 3) =$$

$$= \frac{x^{10} - 1}{(x - 10)(x - 7)(x - 6)} = 6 + 10x + 10x^2 + 5x^5 + x^6 + x^7.$$

Построим матрицу Вандермонда V для вектора $(1, 2, 4, 8, 5, 9, 3)$ и ее обратную матрицу V^{-1}:

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

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

$$(f_0, f_1, \ldots, f_6) = (0, 5, 10, 7, 1, 3, 7)V^{-1} = (0, 8, 10, 8, 1, 2, 4).$$

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

$$m(x) = f(x)(7 + 3x) + 6 + 9x + 4x^2 + 2x^3 + 2x^4 + 10x^5,$$

$$v_1(x) = -(7 + 3x) = 4 + 8x.$$

После первого шага останавливаемся, так как $(\widetilde{n} + \widetilde{k})/2 = 6$, $\deg r_0(x) = 6$, $\deg r_1(x) = 5$.

3. Деление:

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

5. Декодирование кодов Гоппы

Определение кода Гоппы [14] с векторами длины n, каждая компонента которых принадлежит полю $GF(q)$, опирается на два объекта: многочлен $G(x)$ степени r 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 $\alpha_i \in L$. Обычно в качестве L выбирается подмножество всех элементов поля $GF(q^m)$, которые не являются корнями многочлена $G(x)$.

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 выполнено сравнение:

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

Хорошо известно, что для кодового расстояния кода $\Gamma(L, G)$ выполнено неравенство $d \geq r + 1$.

Следующее утверждение (см., напр., [15]) говорит о том, что коды Гоппы являются ограничениями кодов Рида–Соломона на подполе (т.е. альтернативными кодами).

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

$$y_i = G(\alpha_i) \prod_{\substack{0 \leq j \leq n-1, \\ j \neq i}} \frac{1}{\alpha_i - \alpha_j}, \quad i = 0, 1, \ldots, n-1. \tag{4}$$

Данная теорема означает, что к кодам Гоппы можно применять алгоритмы декодирования для обобщенных кодов Рида–Соломона.

Алгоритм 3 (декодирование кода Гоппы).

Вход: принятый вектор $v = u + e$, где $u \in \Gamma(L, G) \subseteq GRS_{n-r}(L, y)$.

Выход: исходный кодовый вектор u, если произошло не более $[r/2]$ ошибок, $[\,]$ – целая часть числа.

1. К вектору v применяется алгоритм 1, на выходе которого получаем многочлен $b(x)$.

2. Вычисление кодового вектора u:

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

Теорема 3. Если в кодовом векторе произошло не более $[r/2]$ ошибок, то алгоритм декодирования 3 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 $d \geq r + 1$, $r = \deg G(x)$. Пусть $u \in \Gamma(L, G)$. Так как код $\Gamma(L, G)$ является ограничением кода $GRS_k(L, y)$ на подполе $GF(q)$, то u можно получить с помощью кодирования некоторого информационного многочлена $b(x)$ кода $GRS_k(L, y)$ с помощью формулы (1). При этом кодовое расстояние кода $GRS_k(L, y)$ равно $d = n - k + 1 = r + 1$. Поэтому если в векторе u произошло не более $r/2$ ошибок, то их можно исправить на основе одного из алгоритмов декодирования кода $GRS_k(L, y)$. Учитывая теорему 1, пусть после применения алгоритма 1 получен информационный многочлен $b(x) = r_j(x)/v_j(x)$ кода $GRS_k(L, y)$. Тогда осталось найти исходный кодовый вектор u кода $\Gamma(L, G)$ на основе кодирования многочлена $b(x)$ кода $GRS_k(L, y)$ с помощью формулы (1). □

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., напр., [15]). Эти факты позволяют строить сепарабельный код $\Gamma(L, G) = \Gamma(L, \overline{G})$, а алгоритм декодирования 3 применять относительно кода $GRS_{n-2r}(\alpha, y)$, $r = \deg G(x)$.

Пусть след элемента $\beta_i \in GF(2^m)$ не равен нулю, $i = 1, \ldots, s$. Тогда хорошо известно, что многочлен $G(x) = \prod_{i=1}^{s}(x^2 + x + \beta_i)$ не имеет корней в $GF(2^m)$. Напомним, что для сепарабельности многочлена $G(x)$ необходимо отсутствие кратных корней.

Перед рассмотрением следующего примера заметим, что если $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\} = GF(q^m)$, $n = q^m$, q – четное, то $\prod_{\substack{0 \le j \le n-1, \\ j \ne i}} (\alpha_j - \alpha_i) = 1$ для любого $i = 0, 1, \ldots, n-1$. Действительно, для любого фиксированного $\beta \in GF(q^m)$ отображение $f_\beta : GF(q^m) \to GF(q^m)$, определенное равенством $f_\beta(x) = x - \beta$, $x \in GF(q^m)$, является биективным. Поэтому в произведении $\prod_{\substack{0 \le j \le n-1, \\ j \ne i}} (\alpha_j - \alpha_i)$ участвуют все ненулевые элементы поля, т.е. каждая скобка – это ненулевой элемент поля, причем все такие элементы различны. Осталось заметить, что все элементы из $GF^*(q^m)$ являются корнями многочлена $x^{n-1} - 1$.

Пример 4. Пусть $F = GF(2^3)$ – поле, построенное на основе многочлена $1 + x + x^3$ с примитивным элементом $\alpha \in GF(2^3)$ (см. пример 2). Построим $[8, 2]$-код Гоппы $\Gamma(L, G)$ над полем $GF(2)$, в котором множество L и многочлен $G(x)$ определены над $GF(2^3)$. Пусть $L = GF(2^3) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$, $G(x) = 1 + x + x^2$. Так как след единицы ненулевой, то многочлен $G(x)$ не имеет корней в поле $GF(2^3)$. Также вычислим $\overline{G}(x) = G^2(x) = 1 + x^2 + x^4$. Так как $d \ge 5$, то код может исправлять 1 и 2 ошибки.

Учитывая теорему 2, данный код является ограничением кода $GRS_4(L, y)$ на подполе $GF(2)$, где

$$y_i = \overline{G}(\alpha_i) \prod_{\substack{0 \le j \le 7, \\ j \ne i}} \frac{1}{\alpha_i - \alpha_j} = \overline{G}(\alpha_i), \quad i = 0, 1, \ldots, 7,$$

$$y = (1, 1, \alpha^3, \alpha^6, \alpha^3, \alpha^5, \alpha^5, \alpha^6).$$

Матрица Вандермонда V для кода $GRS_4(L, y)$, ее обратная V^{-1} и матрица Y имеют вид:

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

$$Y = \mathrm{Diag}(1, 1, \alpha^3, \alpha^6, \alpha^3, \alpha^5, \alpha^5, \alpha^6),$$

где Y – диагональная матрица.

Рассмотрим кодовый вектор $u = (0, 0, 1, 1, 1, 1, 1, 1) \in \Gamma(L, G) = \Gamma(L, \overline{G})$. Пусть на приемном конце после передачи вектора u получен вектор:

$$v = u + e = (0, 0, 0, 1, 1, 1, 0, 1), \quad e = (0, 0, 1, 0, 0, 0, 1, 0).$$

Будем декодировать вектор v с помощью алгоритма 1 для кода $GRS_4(L, y)$. В нашем случае

$$m(x) = \prod_{\beta \in GF(2^3)} (x - \beta) = x^8 - x.$$

Вычисляем коэффициенты интерполяционного многочлена $f(x)$:

$$(f_0, f_1, \ldots, f_7) = vY^{-1}V^{-1} = (0, \alpha^2, 0, 0, \alpha, \alpha, \alpha^4, \alpha),$$

$$f(x) = \alpha^2 x + \alpha x^4 + \alpha x^5 + \alpha^4 x^6 + \alpha x^7.$$

Полагаем $r_{-1}(x) = m(x)$, $r_0(x) = f(x)$ и применяем незаконченный обобщенный алгоритм Евклида:

$$m(x) = f(x)(\alpha^2 + \alpha^6 x) + \alpha^5 x + \alpha x^2 + \alpha^3 x^4 + \alpha x^5 + \alpha^2 x^6,$$
$$v_1(x) = -(\alpha^2 + \alpha^6 x) = \alpha^2 + \alpha^6 x,$$
$$f(x) = r_1(x)(\alpha^3 + \alpha^6 x) + \alpha^4 x + x^3 + \alpha^5 x^4,$$
$$v_2(x) = 1 - (\alpha^3 + \alpha^6 x)v_1(x) = \alpha^4 + \alpha^4 x + \alpha^5 x^2.$$

Так как для кода $GRS_4(L, y)$ $\widetilde{n} = 8$, $\widetilde{k} = 4$, $(\widetilde{n} + \widetilde{k})/2 = 6$, то после второго шага алгоритм Евклида останавливается ($\deg r_1(x) = 6$, $\deg r_2(x) < 6$).

Информационный многочлен $b(x)$ кода $GRS_4(L, y)$, который соответствует вектору u, имеет вид:

$$b(x) = \frac{r_2(x)}{v_2(x)} = \frac{\alpha^4 x + x^3 + \alpha^5 x^4}{\alpha^4 + \alpha^4 x + \alpha^5 x^2} = x + x^2.$$

Вычисляем сам вектор u:

$$u = (y_0 b(0), y_1 b(1), y_2 b(\alpha), \ldots, y_7 b(\alpha^6)) = (0, 0, 1, 1, 1, 1, 1, 1).$$

Литература

1. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. Перевод с англ.: И. И. Грушко, В. М. Блиновский. Под редакцией К .Ш. Зигангирова. М.: Мир, 1986. 576 с.
2. *W. Cary Huffman, Vera Pless.* Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003. 646 p.
3. *Gao S.* A new algorithm for decoding Reed–Solomon codes // Communications, Information and Network Security / V. Bhargava, H. V. Poor, V. Tarokh, and S. Yoon, Eds. Norwell, MA: Kluwer, 2003. V. 712. P. 55–68.
4. *Shiozaki A.* Decoding of redundant residue polynomial codes using Euclid's algorithm // IEEE Transactions on Information Theory. Sep. 1988. V. IT-34, № 5. P. 1351–1354.
5. 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`.
6. *Федоренко С. В.* Простой алгоритм декодирования алгебраических кодов // Информационно-управляющие системы. 2008. № 3. С. 23–27.
7. *Althaus H., Leake R.* Inverse of a finite-field Vandermonde matrix (Corresp.) // IEEE Transactions on Information Theory. 1969. V. 15, № 1. P. 173.
8. *Клейбанов С. Б., Норкин К. Б., Привальский В. Б.* Обращение матрицы Вандермонда // Автоматика и телемеханика. 1977. № 4. С. 176–177.
9. *Björck Å, Pereyra V.* Solution of Vandermonde systems of equations // Mathematics of Computation. 1970. V. 24, № 112. P. 893–903.
10. *Gohberg I., Olshevsky V.* The fast generalized Parker–Traub algorithm for inversion of Vandermonde and related matrices // Journal of Complexity. 1997. Vol. 13, № 2. P. 208–234.
11. *Parker F. D.* Inverses of Vandermonde matrices // The American Mathematical Monthly. 1964. V. 71, № 4. P. 410–411.
12. *Traub J. F.* Associated polynomials and uniform methods for the solution of linear problems // Siam Review. 1966. V. 8, № 3. P. 277–301.
13. *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.

14. *Гоппа В. Д.* Новый класс линейных корректирующих кодов // Пробл. передачи информ. 1970. Т. 6, № 3. С. 24–30.
15. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки: пер. с англ. М: Связь, 1979. 744 с.

Статья поступила в редакцию 15.03.2020;
переработанный вариант – 05.05.2020.

Рацеев Сергей Михайлович
д.ф.-м.н., профессор кафедры информационной безопасности и теории управления Ульяновского государственного университета (432017, Ульяновск, ул. Льва Толстого, 42), e-mail: ratseevsm@mail.ru).

Череватенко Ольга Ивановна
к.ф.-м.н., доцент кафедры высшей математики Ульяновского государственного педагогического университета имени И .Н. Ульянова (432071, Ульяновск, пл. Ленина, д. 4/5).

On a simple algorithm for decoding BCH codes, Reed–Solomon codes, and Goppa codes

S. M. Ratseev, O .I. Cherevatenko

Gao obtained a simple and efficient algorithm for decoding Reed-Solomon codes. In this paper we describe the use of this algorithm for decoding generalized Reed–Solomon codes, Goppa codes, Bose–Chaudhuri–Hocquenghem codes, and Reed–Solomon codes with errors and erasures.

Keywords: error-correcting codes, Reed–Solomon codes, Goppa codes, Bose–Chaudhuri–Hocquenghem codes, code decoding.