УДК 519.725

Ф.Г. Фейзиев, д-р физ.-мат. наук
Сумгаитский госуниверситет
(Азербайджан, AZ5008, Сумгаит , 43 квартал, ул. Баку, 1,
тел.(+994018) 6448906, e-mail: FeyziyevFikratGul@gmail.com),
М.Р. Мехтиева, канд. физ.-мат. наук
Бакинский госуниверситет
(Азербайджан, AZ1148, Баку, ул. Академика Захида Халилова, 23,
тел.(+994012) 5390535)

Модификация метода Питерсона—Горенстейна—Цирлера приведением матрицы к треугольному виду

Для обнаружения и исправления произошедших ошибок в q-ичных кодах Боуза—Чоудхури—Хоквингема предложена модификация метода Питерсона—Горенстейна—Цирлера на основе приведения матрицы к треугольному виду. Разработана методика ускорения вычисления согласно этой модификации. Приведен алгоритм декодирования принятых сообщений, основанный на предложенной модификации.

К л ю ч е в ы е с л о в а: q-ичные коды Боуза—Чоудхури—Хоквингема, метод Питерсона—Горенстейна—Цирлера, треугольные матрицы, примитивный элемент конечного поля, локатор ошибок.

Для виявлення та виправлення помилок, що сталися в q-ічних кодах Боуза—Чоудхурі—Хоквінгема, запропоновано модифікацію методу Пітерсона—Горенстейна—Цирлера на основі приведення матриці до трикутної форми. Розроблено методику прискорення обчислень за цією модифікацією. Наведено алгоритм декодування отриманих повідомлень, базований на запропонованій модифікації.

К л ю ч о в і с л о в а: q-ічні коди Боуза—Чоудхурі—Хоквінгема, метод Пітерсона—Горенстейна—Цирлера, трикутні матриці, примітивний елемент скінченного поля, локатор помилок.

Коды Боуза—Чоудхури—Хоквингема (БЧХ) являются эффективными помехоустойчивыми кодами [1—3]. Код БЧХ строится для заданного натурального числа, которое представляет собой максимальное число исправляемых ошибок. Для декодирования кодов БЧХ, т.е. обнаружения ошибок в принятых сообщениях, их исправления и выделения из них информационных сообщений, используются различные методы, например метод Питерсона—Горенстейна—Цирлера (ПГЦ) [1], основанный на решении специальной системы линейных алгебраических уравнений (СЛАУ) относительно неизвестных локаторов ошибок с применением обращения матрицы.

В работе [4] предложена модификация алгоритма ПГЦ, в которой для решения СЛАУ вместо метода обращения матрицы применен метод Гаусса. В модификации метода ПГЦ, как и в самом методе ПГЦ, число произошедших ошибок предполагается равным максимально возможному числу ℓ ошибок. Строится СЛАУ с ℓ неизвестными и проверяется, имеет ли она решение. Если нет, то из числа ошибок вычитается единица. Снова строится СЛАУ и проверяется, имеет ли она решение и так далее. В работе [5] в случае двоичных кодов БЧХ на основе приведения матрицы к треугольному виду предложена новая модификация метода ПГЦ, в которой нахождение числа ошибок осуществляется непосредственно, т.е. без последовательного выбора и проверки.

Представим новую модификацию метода ПГЦ, описанного в работе [5], и обобщим его на случай недвоичных кодов БЧХ.

Постановка задачи. Пусть m — заданное натуральное число; q — простое число ($q \geq 3$); α — примитивный элемент поля $GF(q^m)$ [3], т.е. элемент порядка $n = q^m - 1$; $P(x)$ — примитивный многочлен над полем $GF(q)$ степени m, с помощью которого построено поле $GF(q^m)$. В поле $GF(q^m)$ примитивному элементу α соответствует многочлен x [1].

Рассмотрим код БЧХ, исправляющий максимум ℓ ошибок, который является циклическим кодом длины n с порождающим многочленом $g(x)$. Пусть $k = n - \deg g(x)$ и $i = (i_0, i_1, ..., i_{k-1})$ есть k-мерный произвольный информационный вектор над полем $GF(q)$. Вектор i может быть закодирован посредством операции $c(x) = i(x)\,g(x)$ в кодовый многочлен $c(x) = c_{n-1}x^{n-1} + ... + c_1 x + c_0$, где $i(x) = i_{k-1}x^{k-1} + ... + i_1 x + i_0$.

Пусть по каналу связи передан многочлен $c(x)$, на другом конце канала принят многочлен $\upsilon(x) = \upsilon_{n-1}x^{n-1} + ... + \upsilon_1 x + \upsilon_0$, а $e(x) = e_{n-1}x^{n-1} + ... + e_1 x + e_0$ есть многочлен ошибок и не более ℓ коэффициентов отлично от нуля. Предположим, что в данный момент произошло ν ошибок, где $0 \leq \nu \leq \ell$, и этим ошибкам соответствуют неизвестные позиции $p_1, p_2, ..., p_\nu$. В этом случае $e(x) = e_{p_1}x^{p_1} + e_{p_2}x^{p_2} + ... + e_{p_\nu}x^{p_\nu}$. Здесь коэффициент e_{p_β} есть величина β-й ошибки, $\beta = \overline{1, \nu}$. Заметим, что число ν произошедших ошибок, показатели степеней (номеров индексов) $p_1, p_2, ..., p_\nu$ и $e_{p_1}, ..., e_{p_\nu}$ — величины соответственно 1, ..., ν-й ошибки неизвестны. Для обнаружения и исправления ошибок необходимо найти эти неизвестные, для чего используются компоненты синдрома $S_1, ..., S_{2\ell}$, где [1]

$$S_\beta = \upsilon(\alpha^\beta) = c(\alpha^\beta) + e(\alpha^\beta) =$$
$$= e(\alpha^\beta) = e_{p_1}(\alpha^{p_1})^\beta + e_{p_2}(\alpha^{p_2})^\beta + ... + e_{p_\nu}(\alpha^{p_\nu})^\beta. \qquad (1)$$

Вычисления S_β по формуле (1) проводятся над полем $GF(q^m)$. Это означает, что после выполнения операций, указанных в правой части ра-

венства, полученный результат делится на многочлен $P(\alpha)$ и берется остаточный многочлен. Ясно, что если $S_\beta = 0, \beta = \overline{1,2\ell}$, то в принятом сообщении ошибок нет, в противном случае — ошибки (искажения) есть.

Пусть $Y_\beta = e_{p_\beta}$ (значение ошибок) и $X_\beta = \alpha^{p_\beta}$ (локаторы ошибок) $\beta = 1, ..., \nu$. Поскольку порядок элемента α равен n, все локаторы рассматриваемой конфигурации ошибок различны. Для каждой ошибки $\beta = 1, ..., 2\ell$ из (1) находим $S_\beta = \upsilon(\alpha^\beta) = Y_1 X_1^\beta + Y_2 X_2^\beta + ... Y_\nu X_\nu^\beta$. Таким образом, получается следующая система из 2ℓ уравнений относительно неизвестных локаторов ошибок $X_1, ..., X_\nu$ и неизвестных значений ошибок $Y_1, ..., Y_\nu$:

$$Y_1 X_1^\beta + Y_2 X_2^\beta + ... + Y_\nu X_\nu^\beta = S_\beta, \quad \beta = \overline{1,2\ell}. \tag{2}$$

Систему нелинейных уравнений (2) решают косвенным путем [1]. Для этого используют многочлен локаторов ошибок $\Lambda(x) = \Lambda_\nu x^\nu + \Lambda_{\nu-1} x^{\nu-1} + ... + \Lambda_1 x + 1$, корнями которого являются X_β^{-1}, $\beta = 1, ..., \nu$. Если коэффициенты многочлена $\Lambda(x)$ известны, то для вычисления локаторов ошибок необходимо найти его корни. В [1] получены СЛАУ, связывающие компоненты синдрома с коэффициентами многочлена $\Lambda(x)$. Эта система уравнений имеет следующий матричный вид:

$$A \operatorname{col}(\Lambda_\nu, \Lambda_{\nu-1}, ..., \Lambda_1) = \operatorname{col}(-S_{\nu+1}, -S_{\nu+2}, ..., -S_{2\nu}). \tag{3}$$

Здесь $A = (a_{\rho,\beta})\, S_{\rho-1+\beta}, \rho = \overline{1,\nu}, \beta = \overline{1,\nu}$, где $a_{\rho,\beta} = S_{\rho-1+\beta}$.

Модификация метода ПГЦ. Компоненты $S_1, ..., S_{2\ell}$ можно вычислить по алгоритму, приведенному в [4].

Теорема 1 [5]. Пусть $M = (a_{\rho,\beta}), \rho, \beta = \overline{1,\ell}$, где $a_{\rho,\beta} = S_{\rho-1+\beta}$ и пусть матрица M с помощью элементарных операций над строками приводится к полутреугольному виду:

$$\overline{M} = \begin{pmatrix} d_{11} & d_{12} & \cdots & d_{1k} & d_{1,k+1} & \ldots & d_{1\ell} \\ 0 & d_{22} & \cdots & d_{2k} & d_{2,k+1} & \ldots & d_{2\ell} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \cdots & d_{kk} & d_{k,k+1} & \ldots & d_{k\ell} \\ 0 & 0 & \cdots & 0 & d_{k+1,k+1} & \ldots & d_{k+1,\ell} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \cdots & 0 & d_{\ell,k+1} & \ldots & d_{\ell\ell} \end{pmatrix},$$

где $d_{ii} \neq 0$, $i = \overline{1,k}$, и вектор-столбец $d = \operatorname{col}(d_{k+1,k+1}, ..., d_{\ell,k+1})$ суть нулевой вектор-столбец. Тогда при передаче информации число произошедших ошибок равно k.

Теорема 2. Пусть при передаче информации число произошедших ошибок равно ν и СЛАУ (3) имеет треугольный вид $\overline{A}\,\mathrm{col}\,(\Lambda_\nu, \Lambda_{\nu-1}, \ldots$ $\ldots, \Lambda_1) = \overline{b}$, где

$$\overline{A} = \begin{pmatrix} d_{11} & d_{12} & d_{13} & \cdots & d_{1\nu} \\ 0 & d_{22} & d_{23} & \cdots & d_{2\nu} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & d_{\nu\nu} \end{pmatrix}, \quad \overline{b} = \mathrm{col}\,(\vartheta_1, \ldots, \vartheta_\nu).$$

Тогда решение СЛАУ (3) относительно $\Lambda_1, \Lambda_2, \ldots, \Lambda_\nu$ можно представить в виде следующих рекуррентных соотношений:

$$\Lambda_1 = (d_{\nu\nu})^{-1}\vartheta_\nu,$$

$$\Lambda_\rho = (d_{\nu-\rho+1,\,\nu-\rho+1})^{-1}\left\{\vartheta_{\nu-\rho+1} - \sum_{\sigma=1}^{\rho-1} d_{\nu-\rho+1,\,\nu-\rho+1+\sigma}\Lambda_{\rho-\sigma}\right\}, \ \rho = 2, 3, \ldots, \nu. \tag{4}$$

Д о к а з а т е л ь с т в о. Учитывая вид матрицы $\overline{A}$ и вектора $\overline{b}$, СЛАУ

$$\overline{A}\,\mathrm{col}\,(\Lambda_\nu, \Lambda_{\nu-1}, \ldots, \Lambda_1) = \overline{b} \tag{5}$$

можно записать в виде

$$\begin{aligned} d_{11}\Lambda_\nu + d_{12}\Lambda_{\nu-1} + d_{13}\Lambda_{\nu-2} + \ldots + d_{1\rho}\Lambda_{\nu-(\rho-1)} + \ldots + d_{1,\nu-1}\Lambda_2 + d_{1\nu}\Lambda_1 &= \vartheta_1, \\ d_{22}\Lambda_{\nu-1} + d_{23}\Lambda_{\nu-2} + \ldots + d_{2\rho}\Lambda_{\nu-(\rho-1)} + \ldots + d_{2,\nu-1}\Lambda_2 + d_{2\nu}\Lambda_1 &= \vartheta_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ d_{\nu-\rho+1,\nu-\rho+1}\Lambda_\rho + \ldots + d_{\nu-\rho+1,\nu-1}\Lambda_2 + d_{\nu-\rho+1,\nu}\Lambda_1 &= \vartheta_{\nu-\rho+1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ d_{\nu-1,\nu-1}\Lambda_2 + d_{\nu-1,\nu}\Lambda_1 &= \vartheta_{\nu-1}, \\ d_{\nu\nu}\Lambda_1 &= \vartheta_\nu. \end{aligned} \tag{6}$$

Из последнего уравнения (6) неизвестный компонент Λ_1 можно найти по формуле

$$\Lambda_1 = (d_{\nu\nu})^{-1}\vartheta_\nu. \tag{7}$$

При известном Λ_1 из предпоследнего уравнения (6) неизвестный Λ_2 можно найти по формуле $\Lambda_2 = (d_{\nu-1,\nu-1})^{-1}\{\vartheta_{\nu-1} - d_{\nu-1,\nu}\Lambda_1\}$. Продолжая такие вычисления, последовательно из третьего, четвертого и так далее до $(\rho-1)$-го уравнения с конца СЛАУ (6) найдем неизвестные $\Lambda_3, \Lambda_4, \ldots, \Lambda_{\rho-1}$. Тогда не-

известный Λ_ρ можно определить из ρ-го уравнения с конца СЛАУ (6), которое в более расширенной форме имеет вид

$$d_{\nu-\rho+1,\nu-\rho+1}\Lambda_\rho + d_{\nu-\rho+1,\nu-\rho+2}\Lambda_{\rho-1} + ... + d_{\nu-\rho+1,\nu-1}\Lambda_2 + d_{\nu-\rho+1,\nu}\Lambda_1 = \vartheta_{\nu-\rho+1}. \quad (8)$$

Из уравнения (8), где $\Lambda_1, \Lambda_2, ..., \Lambda_{\rho-1}$ уже известны, а Λ_ρ неизвестное, получаем формулу для определения Λ_ρ:

$$\Lambda_\rho = (d_{\nu-\rho+1,\nu-\rho+1})^{-1}\{\vartheta_{\nu-\rho+1} -$$
$$-(d_{\nu-\rho+1,\nu-\rho+2}\Lambda_{\rho-1} + ... + d_{\nu-\rho+1,\nu-1}\Lambda_2 + d_{\nu-\rho+1,\nu}\Lambda_1)\},$$

или

$$\Lambda_\rho = (d_{\nu-\rho+1,\nu-\rho+1})^{-1}\left\{\vartheta_{\nu-\rho+1} - \sum_{\sigma=1}^{\rho-1} d_{\nu-\rho+1,\nu-\rho+1+\sigma}\Lambda_{\rho-\sigma}\right\}. \quad (9)$$

Формулы (7), (9) идентичны формулам (4). Теорема 2 доказана.

Если число ошибок ν и локаторы ошибок $X_1, ..., X_\nu$ известны, то неизвестные значения ошибок $Y_1, ..., Y_\nu$ могут быть найдены в результате решения следующих СЛАУ относительно $Y_1, ..., Y_\nu$:

$$Y_1 X_1^\beta + Y_2 X_2^\beta + ... + Y_\nu X_\nu^\beta = S_\beta, \ \beta = \overline{1,\nu}. \quad (10)$$

Теорема 3. Если число ошибок ν и локаторы ошибок $X_1, ..., X_\nu$ известны, то неизвестные значения ошибок $Y_1, ..., Y_\nu$ могут быть найдены из СЛАУ (10) с помощью следующих рекуррентных соотношений:

$$Y_\nu = (B_\nu^{(\nu-1)} X_\nu)^{-1} S_\nu^{(\nu-1)},$$

$$Y_\beta = (B_\beta^{(\beta-1)} X_\beta)^{-1}\left[S_\beta^{(\beta-1)} - \sum_{\sigma=\beta+1}^{\nu} B_\sigma^{(\beta-1)} X_\sigma Y_\sigma\right], \ \beta = \nu-1, \nu-2, ..., 1,$$

где $B_i^{(0)} = 1$; $S_i^{(0)} = S_i$, $i = 1, ..., \nu$; $B_i^{(\beta)} = B_i^{(\beta-1)}(X_i - X_\beta)$; $S_i^{(\beta)} = S_i^{(\beta-1)} - X_\beta S_{i-1}^{(\beta-1)}$, $i = \beta + 1, ..., \nu, \beta = 1, ..., \nu-1$.

Доказательство. Запишем СЛАУ (10) в открытом виде:

$$\begin{aligned} &Y_1 X_1 + Y_2 X_2 + ... + Y_\nu X_\nu = S_1, \\ &Y_1 X_1^2 + Y_2 X_2^2 + ... + Y_\nu X_\nu^2 = S_2, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &Y_1 X_1^\nu + Y_2 X_2^\nu + ... + Y_\nu X_\nu^\nu = S_\nu. \end{aligned} \quad (11)$$

Детерминант системы (11) есть детерминант Вандермонда и, так как $X_i \neq X_j$ при $i \neq j$, этот детерминант отличен от нуля. Поэтому СЛАУ (11) имеет единственное решение. В (11) из v-го уравнения вычитаем $(v-1)$-е уравнение, умноженное на X_1, из $(\nu-1)$-го уравнения вычитаем $(\nu-2)$-е уравнение, умноженное на X_1,…, из второго уравнения вычитаем первое уравнение, умноженное на X_1. Тогда получаем

$$\begin{gathered} X_1 Y_1 + X_2 Y_2 + ... + X_\nu Y_v = S_1 , \\ B_2' \; X_2 Y_2 + ... + B_v' X_\nu Y_v = S_2' , \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ B_2' \; X_2^{\nu-1} Y_2 + ... + B_v' X_\nu^{\nu-1} Y_v = S_\nu' , \end{gathered} \tag{12}$$

где $B_i' = X_i - X_1$; $S_i' = S_i - X_1 S_{i-1}$, $i = 2, ..., \nu$. В (12) из ν-го уравнения вычитаем $(\nu-1)$-е уравнение, умноженное на X_2, из $(\nu-1)$-го уравнения вычитаем $(\nu-2)$-е уравнение, умноженное на X_2, …, из третьего уравнения вычитаем второе уравнение, умноженное на X_2. Тогда запишем

$$\begin{gathered} X_1 Y_1 + X_2 Y_2 + X_3 Y_3 + ... + X_\nu Y_v = S_1 , \\ B_2' \; X_2 Y_2 + B_3' \; X_3 Y_3 + ... + B_v' X_\nu Y_v = S_2' , \\ B_3'' \; X_3 Y_3 + ... + B_v'' X_\nu Y_v = S_3'' , \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ B_3'' \; X_3^{\nu-2} Y_3 + ... + B_v'' X_\nu^{\nu-2} Y_v = S_\nu'' , \end{gathered}$$

где $B_i'' = B_i'(X_i - X_2)$; $S_i'' = S_i' - X_2 S_{i-1}'$, $i = 3, ..., \nu$. Продолжая описанную процедуру, на β-м шаге получим $(1 \le \beta \le \nu-1)$ следующее:

$$\begin{gathered} X_1 Y_1 + X_2 Y_2 + \; ... + X_\beta Y_\beta + X_{\beta+1} Y_{\beta+1} + ... + X_\nu Y_v = S_1 , \\ B_2' \; X_2 Y_2 + ... + B_\beta' \; X_\beta Y_\beta + B_{\beta+1}' X_{\beta+1} Y_{\beta+1} + ... + B_v' X_\nu Y_v = S_2' , \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ B_\beta^{(\beta-1)} X_\beta Y_\beta + B_{\beta+1}^{(\beta-1)} X_{\beta+1} Y_{\beta+1} + ... + B_\nu^{(\beta-1)} X_\nu Y_v = S_\beta^{(\beta-1)}, \\ B_{\beta+1}^{(\beta)} X_{\beta+1} Y_{\beta+1} + ... + B_v^{(\beta)} X_v Y_v = S_{\beta+1}^{(\beta)}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ B_{\beta+1}^{(\beta)} X_{\beta+1}^{\nu-\beta} Y_{\beta+1} + ... + B_\nu^{(\beta)} X_\nu^{\nu-\beta} Y_v = S_\nu^{(\beta)}, \end{gathered}$$

где $B_i^{(\beta)} = B_i^{(\beta-1)}(X_i - X_\beta)$; $S_i^{(\beta)} = S_i^{(\beta-1)} - X_2 S_{i-1}^{(\beta-1)}$, $i = \beta+1, ..., \nu$. Наконец, на $(\nu-1)$-м шаге получаем

$$\begin{gathered} X_1 Y_1 + X_2 Y_2 + \ldots + X_{\nu-1} Y_{\nu-1} + X_\nu Y_\nu = S_1 , \\ B'_2 X_2 Y_2 + \ldots + B'_{\nu-1} X_{\nu-1} Y_{\nu-1} + B'_\nu X_\nu Y_\nu = S'_2 , \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ B_{\nu-1}^{(\nu-2)} X_{\nu-1} Y_{\nu-1} + B_\nu^{(\nu-2)} X_\nu Y_\nu = S_{\nu-1}^{(\nu-2)}, \\ B_\nu^{(\nu-1)} X_\nu Y_\nu = S_\nu^{(\nu-1)}, \end{gathered} \tag{13}$$

где $B_i^{(\beta)} = B_i^{(\beta-1)}(X_i - X_\beta)$; $S_i^{(\beta)} = S_i^{(\beta-1)} - X_\beta S_{i-1}^{(\beta-1)}$, $i = \beta+1, ..., \nu$, $\beta = 1, ..., \nu-1$. Из последнего уравнения системы (13) получаем

$$Y_\nu = (B_\nu^{(\nu-1)} X_\nu)^{-1} S_\nu^{(\nu-1)}, \tag{14}$$

из предпоследнего уравнения системы (13) получаем $Y_{\nu-1} = (B_{\nu-1}^{(\nu-2)} X_{\nu-1})^{-1} \times$ $\times [S_{\nu-1}^{(\nu-2)} - B_\nu^{(\nu-2)} X_\nu Y_\nu]$ и так далее. Пусть найдены $Y_\nu, Y_{\nu-1}, ..., Y_{\beta+1}$. Ясно, что β-е уравнение в (13) имеет вид $B_\beta^{(\beta-1)} X_\beta Y_\beta + B_{\beta+1}^{(\beta-1)} X_{\beta+1} Y_{\beta+1} + \ldots$ $\ldots + B_\nu^{(\beta-1)} X_\nu Y_\nu = S_\beta^{(\beta-1)}$. Отсюда находим

$$B_\beta^{(\beta-1)} X_\beta Y_\beta = S_\beta^{(\beta-1)} - (B_{\beta+1}^{(\beta-1)} X_{\beta+1} Y_{\beta+1} + \ldots + B_\nu^{(\beta-1)} X_\nu Y_\nu),$$

или

$$B_\beta^{(\beta-1)} X_\beta Y_\beta = S_\beta^{(\beta-1)} - \sum_{\sigma=\beta+1}^{\nu} B_\sigma^{(\beta-1)} X_\sigma Y_\sigma. \tag{15}$$

Из (15) получаем

$$Y_\beta = (B_\beta^{(\beta-1)} X_\beta)^{-1} \left[S_\beta^{(\beta-1)} - \sum_{\sigma=\beta+1}^{\nu} B_\sigma^{(\beta-1)} X_\sigma Y_\sigma \right], \beta = \nu-1, \nu-2, ..., 1, \tag{16}$$

где очевидно, что $\beta_\gamma^{(0)} = 1$, $\gamma = \overline{1, \nu}$. Соотношения (14), (16) являются рекуррентными соотношениями для нахождения неизвестных значений ошибок $Y_1, ..., Y_\nu$. Теорема 3 доказана.

На основании теорем 1—3, используя методику приведения матрицы к треугольной форме, можно описать модификацию метода ПГЦ с помощью следующего алгоритма.

А л г о р и т м 1.

Ш а г 0. Используя принятое значение $\upsilon(x)$, вычислить $S_\beta = \upsilon(\alpha^\beta)$, $\beta = \overline{1, 2\ell}$, по формуле (1). Если все числа S_1, ..., $S_{2\ell}$ равны нулю, то перейти к шагу 13, иначе — к шагу 1.

Ш а г 1. Построить матрицу $A=(a_{\rho,\beta}),\rho,\beta=\overline{1,\ell}$ и вектор $b=\mathrm{col}(b_1,...,b_\ell)$, где $a_{\rho,\beta}=S_{\rho-1+\beta}$, $\rho,\beta=\overline{1,\ell}$; $b_\rho=-S_{\rho+\ell}$, $\rho=\overline{1,\ell}$. Принять $j=1$ и перейти к шагу 2.

Ш а г 2. Если $j+1>\ell$, то принять $v=j$ и перейти к шагу 7, иначе наименьший элемент множества $Q=\{\xi\,|\,\xi\in\{j,...,\ell\},\ a_{\xi j}\neq 0\}$ обозначить через σ. В случае $\sigma\neq j$ поменять местами j-ю и σ-ю строки матрицы A и j-й и σ-й компоненты вектора b, т.е. принять последовательно: $c=a_{j\beta}$, $a_{j\beta}=a_{\sigma\beta}, a_{\sigma\beta}=c,\beta=j,...,\ell; c=b_j, b_j=b_\sigma, b_\sigma=c.$ Принять $v=j+1$ и перейти к шагу 3.

Ш а г 3. Умножить j-ю строку матрицы A на $-a_{vj}/a_{jj}$ и прибавить к v-й строке:

$$a_{v\beta}:=a_{v\beta}-(a_{vj}/a_{jj})a_{j\beta},\ GF(q),\ \beta=j,...,\ell, \tag{17}$$

умножить j-ю компоненту вектора b на $-a_{vj}/a_{jj}$ и прибавить к v-й компоненте вектора b:

$$b_v:=b_v-(a_{vj}/a_{jj})b_j,\ GF(q). \tag{18}$$

Ш а г 4. Принять $v:=v+1$. Если $v\le\ell$, то перейти к шагу 3, иначе — к шагу 5.

Ш а г 5. Если $j+1>\ell$, то принять $v=j$ и перейти к шагу 7, иначе — проверить вектор-столбец $d=\mathrm{col}(a_{j+1,j+1},a_{j+2,j+1},...,a_{\ell,j+1},)$. Если он суть нулевой, то принять $v=j$ и перейти к шагу 7, иначе — к шагу 6.

Ш а г 6. $j:=j+1$. Если $j<\ell$, то перейти к шагу 2, иначе принять $v=j$ и перейти к шагу 7.

Ш а г 7. Решить СЛАУ (5) и определить коэффициенты $\Lambda_1,\Lambda_2,...,\Lambda_v$ многочлена $\Lambda(x)$ по формулам

$$\Lambda_1=(a_{vv})^{-1}b_v, \tag{19}$$

$$\Lambda_\rho=(a_{v-\rho+1,v-\rho+1})^{-1}\left\{b_{v-\rho+1}-\sum_{\sigma=1}^{\rho-1}a_{v-\rho+1,v-\rho+1+\sigma}\Lambda_{\rho-\sigma}\right\},\ \rho=2,3,...,v,\ GF(q), \tag{20}$$

где $\overline{A}=(a_{\rho,\beta}),\rho,\beta=\overline{1,v}$ и $\overline{b}=\mathrm{col}\,(b_1,...,b_v)$.

Ш а г 8. Найти корни $x_1,...,x_v$ многочлена локаторов ошибок, локаторы ошибок найти по формуле $X_\beta=x_\beta^{-1}$, $\beta=\overline{1,...,v}$. Найти $p_1,...,p_v$.

Ш а г 9. Определить B_i^β, $S_i^{(\beta)}$, $i=\beta+1,...,v,\beta=0,1,...,v-1$, по следующим рекуррентным формулам:

$$B_i^{(0)}=1,\quad S_i^{(0)}=S_i,\ i=1,...,v, \tag{21}$$

$$B_i^{(\beta)} = B_i^{(\beta-1)}(X_i - X_\beta),\ S_i^{(\beta)} = S_i^{(\beta-1)} - X_\beta S_{i-1}^{(\beta-1)},\ GF(q),\ i = \beta+1, ..., v,$$
$$\beta = 1, ..., v-1. \tag{22}$$

Ш а г 10. Определить $Y_1, ..., Y_v$ по рекуррентным формулам

$$Y_v = (B_v^{(v-1)} X_v)^{-1} S_v^{(v-1)},$$
$$Y_\beta = (B_\beta^{(\beta-1)} X_\beta)^{-1}\left[S_\beta^{(\beta-1)} - \sum_{\sigma=\beta+1}^{v} B_\sigma^{(\beta-1)} X_\sigma Y_\sigma \right],\ GF(q), \tag{23}$$
$$\beta = \nu-1, \nu-2, ..., 1.$$

Ш а г 11. Исправить ошибки по формулам $\upsilon_{p_\beta} := \upsilon_{p_\beta} - Y_\beta$, $GF(q)$ $\beta = 1, ..., v$.

Ш а г 12. Определить информационный многочлен по формуле $i(x) = \upsilon(x)/g(x)$.

Ш а г 13. Конец.

Методика ускорения вычисления в модификации метода ПГЦ. Элементы матрицы A в (3) есть элементы поля $GF(q^m)$. Ненулевые элементы поля $GF(q^m)$ являются степенью примитивного элемента. Для выполнения операций сложения и умножения элементов поля $GF(q^m)$ можно использовать соответствующие таблицы, что позволит сократить время выполнения этих операций. Компоненты $S_1, ..., S_{2\ell}$ принимают значения из поля $GF(q^m)$. Поэтому они являются нулевым элементом или степенью примитивного элемента α. Введем числа N_β, $\beta = \overline{1,2\ell}$:

$$N_\beta = \begin{cases} -1, \text{ если } S_\beta = 0, \\ k, \text{ если } S_\beta = \alpha^k,\ k \in \{0, ..., q^m - 2\}. \end{cases} \tag{24}$$

Введем массивы $M1$ и $M2$. Элемент $M1(u, \beta, v)$ массива $M1$, где $u \in GF(q)$, $v \in GF(q)$ и $\beta \in \{0, ..., q^m - 2\}$, используемый для нахождения показателя степени числа $u + \alpha^\beta v$, определяется так:

$$M1(u, \beta, v) = \begin{cases} -1, \text{ если } u + \alpha^\beta v = 0, \\ k, \text{ если } u + \alpha^\beta v = \alpha^k, k \in \{0, ..., q^m - 2\}. \end{cases}$$

Элемент $M2(\tau, v)$ массива $M2$, где $\tau \in \{-1, 0, ..., q^m - 2\}$ и $v \in GF(q)$, используется для нахождения показателя степени числа $\alpha^\tau + v$ и определяется так:

$$M2(\tau, v) = \begin{cases} \tau, \text{ если } v = 0, \\ -1, \text{ если } v = 0 \text{ и } \tau = -1, \\ \sigma, \text{ если } v \neq 0 \text{ и } \alpha^\tau + v = \alpha^\sigma, \sigma \in \{0, ..., q^m - 2\}. \end{cases}$$

Для нахождения показателя степени в представлении произведений $\alpha^x\alpha^y$ при $x,\ y\in\{-1,\ 0,\ ...,\ q^m-2\}$ в виде степени примитивного элемента α поля $GF(q^m)$ введем операцию $*$:

$$x*y=\begin{cases}-1, \text{если } x=-1 \text{ или } (u)\ y=-1\ ,\\ x+y-(q^m-1), \text{если } x\neq -1,\ y\neq -1,\ x+y\geq q^m-1,\\ x+y, \text{если } x\neq -1,\ y\neq -1,\ x+y<q^m-1.\end{cases}$$

Если предварительно построены массивы $M1$ и $M2$, то аналогично по алгоритму, приведенному в [4], можно вычислить $N_1,...,N_{2\ell}$. Если числа N_β, $\beta=\overline{1,\ 2\ell}$, вычислены, то

$$S_\beta=\begin{cases}0, \quad \text{если } N_\beta=-1,\\ \alpha^k, \text{ если } N_\beta=k, k\in\{0,...,q^m-2\}.\end{cases}$$

Поэтому в дальнейшем вместо $S_1,...,S_{2\ell}$ можно использовать $N_1,...,N_{2\ell}$.

В формулах (4)—(23) операции проводятся над многочленами. Рассмотрим преобразование этих формул к формулам, в которых вместо многочлена используются показатели соответствующих степеней примитивного элемента. Для этого на основе матрицы A и вектора b введем матрицу $Z=(z_{\rho\beta})$, $\rho=\overline{1,v}$, $\beta=\overline{1,v}$, и вектор $\eta=\mathrm{col}(\eta_1,...,\eta_v)$, где

$$z_{\rho\beta}=\begin{cases}-1, \text{если } a_{\rho\beta}=0,\\ \sigma, \text{ если } a_{\rho\beta}=\alpha^\sigma, \sigma\in\{0,...,q^m-2\}.\end{cases} \tag{25}$$

$$\eta_\rho=\begin{cases}-1, \text{если } b_\rho=0,\\ \sigma, \text{ если } b_\rho=\alpha^\sigma, \sigma\in\{0,...,q^m-2\}.\end{cases} \tag{26}$$

Используя примитивный элемент α, можно записать формулы (17) и (18) с учетом (25) и (26) в виде

$$\alpha^{z_{\nu\beta}}:=\alpha^{z_{\nu\beta}}-(\alpha^{z_{\nu j}}/\alpha^{z_{jj}})\alpha^{z_{j\beta}}, \tag{27}$$

$$\alpha^{\eta_\nu}:=\alpha^{\eta_\nu}-(\alpha^{z_{\nu j}}/\alpha^{z_{jj}})\alpha^{\eta_j}. \tag{28}$$

Используя формулу (24), можно определить $z_{\rho\beta}$, $\rho=\overline{1,v}$, $\beta=\overline{1,v}$ и η_ρ, $\rho=\overline{1,v}$, по формулам $z_{\rho\beta}=N_{\rho-1+\beta}$ и $\eta_\rho=MP(N_{\rho+\nu})$ соответственно, где $MP(x)$ — показатель степени (на основании α) многочлена, являющегося противоположным многочлену α^x:

$$MP(x)=\begin{cases}1, \quad \text{если } x=-1,\\ \sigma, \text{ если } x\neq -1, \alpha^\sigma+\alpha^x=0, \sigma\in\{0,...,q^m-2\}.\end{cases}$$

Поскольку $(\alpha^{z_{jj}})^{-1} = \alpha^{2^m-1-z_{jj}}$, (27) и (28) можно записать в виде $\alpha^{z_{v\beta}} := \alpha^{z_{v\beta}} - \alpha^{q^m-1-z_{jj}}\alpha^{z_{vj}}\alpha^{z_{j\beta}}$, $\alpha^{\eta_v} := \alpha^{\eta_v} - \alpha^{q^m-1-z_{jj}}\alpha^{z_{vj}}\alpha^{\eta_j}$. Из этих соотношений получаем

$$z_{v\beta} := MF(z_{v\beta}, (q^m - 1 - z_{jj}) * z_{vj} * z_{j\beta}),$$

$$\eta_v := MF(\eta_v, (q^m - 1 - z_{jj}) * z_{vj} * \eta_v),$$

где $MF(x, y)$ — показатель степени (на основании α) $\alpha^x - \alpha^y$, определяемый по формуле

$$MF(x,y) = \begin{cases} x, & \text{если } y = -1,\ x \geq 0, \\ MP(y), & \text{если } x = -1,\ y \geq 0, \\ -1, & \text{если } y = -1,\ x = -1, \\ \sigma, & \text{если } y \neq -1,\ x \neq -1,\ \alpha^x - \alpha^y = \alpha^\sigma,\ \sigma \in \{0, ..., q^m - 2\}, \\ -1, & \text{если } y \neq -1,\ x \neq -1,\ \alpha^x - \alpha^y = 0. \end{cases}$$

Для каждого $\rho \in \{1, 2, ..., v\}$ введем обозначение

$$\lambda_\rho = \begin{cases} -1, \text{если } \Lambda_\rho = 0, \\ \sigma, \text{ если } \Lambda_\rho = \alpha^\sigma, \sigma \in \{0, ..., q^m - 2\}. \end{cases} \tag{29}$$

На основании (25)—(29) формулы (19) и (20) можно записать в виде

$$\lambda_1 = (q^m - 1 - z_{vv}) * \eta_v, \tag{30}$$

$$\lambda_\rho = (q^m - 1 - z_{v-\rho+1, v-\rho+1}) * MF(\eta_{v-\rho+1}, \gamma_\rho),\ \rho = 2, 3, ..., v. \tag{31}$$

В (31) γ_ρ является показателем степени (на основании α) выражения $J_\rho = \sum_{\sigma=1}^{\rho-1} a_{v-\rho+1, v-\rho+1-\sigma}\Lambda_{\rho-\sigma}$, т.е. $J_\rho = \alpha^{\gamma_\rho}$. Поэтому γ_ρ можно определить рекуррентно: $\gamma_\rho := MC(\gamma_\rho, z_{v-\rho+1, v-\rho+1+\sigma} * \lambda_{\rho-\sigma}), \sigma = 1, ..., \rho - 1$, где $MC(x, y)$ — значение показателя суммы $\alpha^x + \alpha^y$, определяемое по формуле

$$MC(x,y) = \begin{cases} y, & \text{если } x = -1, \\ x, & \text{если } y = -1, \\ -1, & \text{если } \alpha^x - \alpha^y = 0, \\ \tau, & \text{если } \alpha^x + \alpha^y = \alpha^\tau, \tau \in \{0, ..., q^m - 2\}. \end{cases}$$

При известных коэффициентах $\Lambda_1, \Lambda_2, ..., \Lambda_v$ для определения корней многочлена $\Lambda(x)$ надо вычислить $\Lambda(x)$ для каждого элемента $x \in GF(q^m)$ и выделить те значения x, при которых $\Lambda(x)$ равно нулю. Приняв Λ_0:=1, $\Lambda(x) := \Lambda_v x + \Lambda_{v-1}$, с использованием схемы Горнера значение $\Lambda(x)$ вычисляется рекуррентно в такой последовательности:

$$\Lambda(x) := \Lambda(x)\, x + \Lambda_\xi,\ \xi = v-2, v-3, ..., 0. \qquad (32)$$

Для ускорения вычисления вместо x можно использовать его описание в виде $x = \alpha^\beta$. Тогда схему (32) запишем в виде

$$\lambda_0 := 0,\ \lambda(\beta) := MC((\lambda_v * \beta),\ \lambda_{v-1}),$$
$$\lambda(\beta) := MC((\lambda(\beta) * \beta),\ \lambda_\xi),\ \xi = v-2, v-3, ..., 0,$$

где

$$\lambda(\beta) = \begin{cases} -1, \text{ если } \Lambda(\alpha^\beta) = 0, \\ \sigma, \text{ если } \Lambda(\alpha^\beta) = \alpha^\sigma,\ \sigma \in \{0, ..., q^m - 2\}. \end{cases}$$

По определению для каждого $\beta = 1, ..., v$

$$p_\beta = \begin{cases} -1, \text{ если } X_\beta = 0, \\ \sigma, \text{ если } X_\beta = \alpha^\sigma, \sigma \in \{0, ..., q^m - 2\}. \end{cases}$$

Пусть

$$\theta_i^{(\beta)} = \begin{cases} -1, \text{ если } B_i^{(\beta)} = 0, \\ k, \text{ если } B_i^{(\beta)} = \alpha^k, k \in \{0, ..., q^m - 2\}, \end{cases}$$

$$s_i^{(\beta)} = \begin{cases} -1, \text{ если } S_i^{(\beta)} = 0, \\ k, \text{ если } S_i^{(\beta)} = \alpha^k, k \in \{0, ..., q^m - 2\}, \end{cases}$$

$$y_\beta = \begin{cases} -1, \text{ если } Y_\beta = 0, \\ k, \text{ если } Y_\beta = \alpha^k, k \in \{0, ..., q^m - 2\}. \end{cases}$$

Тогда $\theta_i^{(0)}$, $i = 1, 2, ..., v$, и $\theta_i^{(\beta)}$, $i = \beta+1, ..., v, \beta = 1, ..., v-1$ и на основании (21) и (22) могут быть вычислены с помощью рекуррентных формул соответственно $\theta_i^{(0)} = 0$, $i = 1, 2, ..., v$, и $\theta_i^{(\beta)} = \theta_i^{(\beta-1)} * MF(d_i, d_\beta)$, $i = \beta+1, ..., v$, $\beta = 1, ..., v-1$, а $s_i^{(0)}$, $i = 1, 2, ..., v$, и $s_i^{(\beta)}$, $i = \beta+1, ..., v, \beta = 1, ..., v-1$, — с помощью рекуррентных формул соответственно $s_i^{(0)} = N_i$, $i = 1, 2, ..., v$, и $s_i^{(\beta)} = MF(s_i^{(\beta-1)}, d_\beta * s_{i-1}^{(\beta-1)})$, $i = \beta+1, ..., v$, $\beta = 1, ..., v-1$.

Согласно (23) $y_v = (q^m - 1 - (\theta_v^{(v-1)} * \ p_v)) * s_v^{(v-1)})$. В правой части формулы (23) выражения $J_\beta = \sum_{\sigma=\beta+1}^{v} B_\sigma^{(\beta-1)} X_\sigma Y_\sigma$ можно вычислить рекуррентно:

$$J_\beta := 0,\ J_\beta := J_\beta + B_\sigma^{(\beta-1)} X_\sigma Y_\sigma,\ \sigma = \beta+1, ..., v.$$

Если $J_\beta = \alpha^{\gamma_\beta}$, то показатель степени γ_ℓ также можно вычислить по формуле $\gamma_\beta := -1,\ \gamma_\beta := MC(\gamma_\beta, \theta_\sigma^{(\beta-1)} * \ p_\sigma * \ y_\sigma)$. Таким образом,

$$y_\beta = (q^m - 1 - \theta_\beta^{(\beta-1)} * \ p_\beta) * MF(s_\beta^{(\beta-1)},\ \gamma_\beta).$$

Алгоритм обнаружения и исправления ошибок в принятом многочлене. Предположим, что массивы (таблицы) $M1$, $M2$, MC предварительно составлены. Тогда алгоритм декодирования следующий.

А л г о р и т м 2.

Ш а г 0. Выбрать $\upsilon_{n-1}, \upsilon_{n-2}, ..., \upsilon_1, \upsilon_0$. Принять $\beta = 1$.

Ш а г 1. $N_\beta = M1(\upsilon_{n-1}, \beta, \upsilon_{n-2}),\ \gamma = 1$.

Ш а г 2. $N_\beta := M2((N_\beta * \beta), \upsilon_{n-2-\gamma})$.

Ш а г 3. $\gamma := \gamma + 1$. Если $n - 2 - \gamma \geq 0$, то перейти к шагу 2, иначе — к шагу 4.

Ш а г 4. $\beta := \beta + 1$. Если $\beta \leq 2\ell$, то перейти к шагу 1, иначе — к шагу 5.

Ш а г 5. Если все числа $N_1, ..., N_{2\ell}$ равны -1, то перейти к шагу 51, иначе — к шагу 6.

Ш а г 6. Построить матрицу $D = (z_{\rho\beta}),\ \rho = \overline{1, \ell},\ \beta = \overline{1, \ell}$, где $z_{\rho\beta} = N_{\rho-1+\beta}$, $\rho = \overline{1, \ell}, \beta = \overline{1, \ell}$. Построить вектор $\eta = (\eta_1, \eta_2, ..., \eta_\ell)$, где $\eta_\rho = MP(N_{\rho+\ell}),\ \rho = \overline{1, \ell}$. Принять $j = 1$ и перейти к шагу 7.

Ш а г 7. Если $j + 1 > \ell$, то принять $v = j$ и перейти к шагу 19, иначе — найти $\sigma = \min\{\xi | \xi \in \{j, ..., \ell\},\ z_{\xi j} \neq -1\}$. Если $\sigma \neq j$, то принять $\beta = j$ и перейти к шагу 8, иначе — к шагу 10.

Ш а г 8. Последовательно принять: $c = z_{j\beta},\ z_{j\beta} = a_{\sigma\beta},\ z_{\sigma\beta} = c$.

Ш а г 9. $\beta := \beta + 1$. Если $\beta \leq \ell$, то перейти к шагу 8, иначе — принять последовательно $c = \eta_j,\ \eta_j = \eta_\sigma,\ \eta_\sigma = c$ и перейти к шагу 10.

Ш а г 10. Принять $v = j + 1$. Если $v \leq \ell$, то перейти к шагу 11, иначе — к шагу 15.

Ш а г 11. Принять $\beta = j$.

Ш а г 12. Принять $z_{v\beta} := MF(z_{v\beta}, (q^m - 1 - z_{jj}) * z_{vj} * z_{j\beta})$.

Ш а г 13. Принять $\beta := \beta + 1$. Если $\beta \leq \ell$, то перейти к шагу 12, иначе — принять $\eta_v := MF(\eta_v, (q^m - 1 - z_{jj}) * z_{vj} * \eta_v)$ и перейти к шагу 14.

Ш а г 14. $v := v + 1$. Если $v \leq \ell$, то перейти к шагу 11, иначе — к шагу 15.

Ш а г 15. Если $j + 1 > \ell$, то принять $v = j$ и перейти к шагу 19, иначе — принять $\rho = j + 1,\ \beta = j + 1$ и перейти к шагу 16.

Ш а г 16. Если $z_{\rho\beta} \neq -1$, то перейти к шагу 18, иначе — к шагу 17.

Ш а г 17. $\rho := \rho + 1$. Если $\rho \leq \ell$, то перейти к шагу 16, иначе — принять $v = j$ и перейти к шагу 19.

Ш а г 18. $j := j + 1$. Если $j < \ell$, то перейти к шагу 7, иначе — принять $v = j$ и перейти к шагу 19.

Ш а г 19. Принять $\lambda_1 = (q^m - 1 - z_{vv}) * \eta_v$. Если $v > 1$, то перейти к шагу 20, иначе — к шагу 26.

Ш а г 20. $\rho := 2$.

Ш а г 21. $\gamma := -1; \sigma = 1$.

Ш а г 22. $\gamma := MC(\gamma, z_{v-\rho+1, v-\rho+1+\sigma} * \lambda_{\rho-\sigma})$.

Ш а г 23. $\sigma := \sigma + 1$. Если $\sigma \leq \rho - 1$, то перейти к шагу 22, иначе — к шагу 24.

Ш а г 24. $\lambda_\rho := (q^m - 1 - z_{v-\rho+1, v-\rho+1}) * MC(\eta_{v-\rho+1}, \gamma)$.

Ш а г 25. $\rho := \rho + 1$. Если $\rho \leq v$, то перейти к шагу 21, иначе — к шагу 26.

Ш а г 26. $\beta = -1, \lambda_0 = 0, \sigma = 0$.

Ш а г 27. $\lambda(\beta) := MC((\lambda_v * \beta), \lambda_{v-1})$, $\xi = v - 2$. Если $\xi < 0$, то перейти к шагу 30, иначе — к шагу 28.

Ш а г 28. $\lambda(\beta) := MC((\lambda(\beta) * \beta), \lambda_\xi)$.

Ш а г 29. $\xi := \xi - 1$. Если $\xi \geq 0$, то перейти к шагу 28, иначе — к шагу 30.

Ш а г 30. Если $\lambda(\beta) \neq -1$, то перейти к шагу 32, иначе — к шагу 31.

Ш а г 31. $\sigma := \sigma + 1$, $x_\sigma = \beta$. Если $\sigma \geq v$, то перейти к шагу 33, иначе — к шагу 32.

Ш а г 32. $\beta := \beta + 1$. Если $\beta \leq q^m - 2$, то перейти к шагу 27, иначе — к шагу 33.

Шаг 33. Для каждого $\xi = 1, ..., v$ определить p_ξ по формуле $p_\xi = q^m - 1 - x_\xi$.

Шаг 34. $i = 1$.

Шаг 35. $\theta_i^{(0)} = 0, s_i^{(0)} = N_i$.

Шаг 36. $i := i + 1$. Если $i \leq v$, то перейти к шагу 35, иначе — к шагу 37.

Шаг 37. $\beta = 1$.

Шаг 38. $i = \beta + 1$.

Шаг 39. Если $i \leq v$, то перейти к шагу 40, иначе — к шагу 41.

Шаг 40. Принять: $\theta_i^{(\beta)} = \theta_i^{(\beta-1)} * MF(p_i, p_\beta)$, $s_i^{(\beta)} = MF(s_i^{(\beta-1)}, p_\beta * s_{i-1}^{(\beta-1)})$. Сначала принять $i := i + 1$ и перейти к шагу 39.

Шаг 41. $\beta := \beta + 1$. Если $\beta \leq v - 1$, то перейти к шагу 38, иначе — к шагу 42.

Шаг 42. Принять $y_v = (q^m - 1 - (\theta_v^{(v-1)} * p_v)) * s_v^{(v-1)})$ и $\beta = v$. Перейти к шагу 43.

Шаг 43. $\beta := \beta - 1$. Если $\beta = 0$, то перейти к шагу 48, иначе — к шагу 44.

Шаг 44. $\gamma_\beta := -1$, $\sigma = \beta + 1$. Перейти к шагу 45.

Шаг 45. Если $\sigma \leq v$, то перейти к шагу 46, иначе — к шагу 47.

Шаг 46. Принять $\gamma_\beta := MC(\gamma_\beta, (\theta_\sigma^{(\beta-1)} * p_\sigma * y_\sigma))$, $\sigma := \sigma + 1$ и перейти к шагу 45.

Шаг 47. Принять $y_\beta := (q^m - 1 - (\theta_\beta^{(\beta-1)} * p_\beta)) * MF(s_\beta^{(\beta-1)}, \gamma_\beta)$ и перейти к шагу 43.

Шаг 48. $\beta = 1$.

Шаг 49. Принять $\upsilon_{p_\beta} := \upsilon_{p_\beta} - \alpha^{y_\beta}$, $GF(q)$, $\ell = 1, ..., v$.

Шаг 50. $\beta := \beta + 1$. Если $\beta \le v$, то перейти к шагу 49, иначе — к шагу 51.

Шаг 51. Делить многочлен $\upsilon(x)$ на многочлен $g(x) = g_{n-k}x^{n-k} + ... + g_1 x + g_0$ по следующей схеме [6]:

$$y_\alpha[0] = \upsilon_\alpha, \ \alpha = 0, 1, ..., n-1;$$

$$y_{n-\beta-\alpha}[\beta] = y_{n-\beta-\alpha}[\beta-1] - y_{n-\beta}[\beta-1]\, g_{n-k-\alpha}, \ \ \alpha = 1, ..., n-k, GF(q),$$

$$y_{n-\beta-\alpha}[\beta] = y_{n-\beta-\alpha}[\beta-1], \ \ \alpha = n-k+1, ..., n-\beta,$$

$$I_{k-\beta}[\beta] = y_{n-\beta}[\beta-1], \ \beta = 1, 2, ..., k-1;$$

$$y_{n-k-\alpha}[k] = y_{n-k-\alpha}[k-1] - y_{n-k}[k-1]\, g_{n-k-\alpha}, \alpha = 1, ..., n-k, GF(q),$$

$$I_o[k] = y_{n-k}[k-1].$$

Шаг 52. Определить компоненты информационного вектора по формуле $i_{k-\beta} = I_{k-\beta}[\beta], \beta = 1, 2, ..., k$.

Шаг 53. Конец.

Выводы

Таким образом, предложенная модификация метода ПГЦ, основанная на приведении матрицы к треугольному виду, может быть применена для ускорения обнаружения и исправления ошибок в q-ичных кодах БЧХ. Разработанный подробный алгоритм для обнаружения и исправления ошибок в принятом многочлене можно реализовать программно на языке Ассемблер.

СПИСОК ЛИТЕРАТУРЫ

1. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986, 576 с.
2. *William C.H., Vera P.* Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003, 662 p.
3. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. М.: Мир, 1976, 400 с.
4. *Фейзиев Ф.Г.* Модификация алгоритма Питерсона—Горенстейна—Цирлера и ее эффективная реализация// Электрон. моделирование, 2015, **37**, № 3, с. 3 —16.
5. *Фейзиев Ф.Г., Мехтиева М.Р., Самедова З.А.* Модификация метода Питерсона—Горенстейна—Цирлера приведением матрицы к треугольному виду (двоичный случай)// Электрон. моделирование, 2016, **38**, № 5, с. 11— 21.
6. *Фейзиев Ф.Г., Бабаванд Араблу М.А.* Описание декодирования p-ичных циклических кодов в классе последовательностных машин// Изв. НАН Азербайджана. Серия физ.-техн. и мат. наук: Информатика и проблемы управления, 2012, **XXXII**, № 6, с. 3—9.

Поступила 22.11.17;
после доработки 23.12.17

REFERENCES

1. Blahut, R. (1986), *Teoriya i praktika kodov, kontroliriyushikh oshibki* [Theory and Practice of Error Control Codes], Translated by I.I. Grushina and V.M. Blinov, Mir, Moscow, Russia.
2. William, C.H. and Vera, P. (2003), Fundamentals of error-correcting codes, Cambridge University Press, Cambridge, UK.
3. Birkoff, G. and Barti, T. (1976), *Sovremennaya prikladnaya algebra* [Modern applied algebra], Translated by Yu.I. Manina, Mir, Moscow, Russia.
4. Feyziyev, F.G. (2015), "On one modification of algorithm Peterson–Gorenstein–Zierler and its effective realization", *Elektronnoe modelirovanie,* Vol. 37, no. 3, pp. 3-16.
5. Feyziyev, F.G., Mekhtiyeva, M.R. and Samedova, Z.A. (2016), "Modification of Peterson–Gorenstein–Zierler method, bringing the matrix to triangular form (binary case)", *Elektronnoe modelirovanie,* Vol. 38, no. 5, pp. 11-21.
6. Feyziyev, F.G. and Babavand Arablou, M.A. (2012), "Description of decoding of p-nary cyclic codes in the class of sequential machines", *Izvestiya Natsionalnoy Akademii Nauk Azerbaydjana, Seriya Fiz.-Tekh. i Math. Nauk: Informatika i Problemy Upravleniya,* Vol. XXXII, no. 6, pp. 3-9.

Received 22.11.17;
after revision 23.12.17

F.G. Feyziyev, M.R. Mekhtiyeva

MODIFICATION OF PETERSON-GORENSTEIN-ZIERLER METHOD, BRINGING THE MATRIX TO TRIANGULAR FORM

A modification of the Peterson-Gorenstein-Zierler method, based on the reduction of the matrix to triangular form, for detecting and correcting occurred errors in q-nary Bose-Chaudhuri-Hocquenghem codes has been proposed. The technique has been developed for accelerating calculation in accordance with this modification. An algorithm for decoding received messages based on the proposed modification is given.

K e y w o r d s: q-nary Bose-Chaudhuri-Hocquenghem code, Peterson-Gorenstein-Zierler method, triangular matrix, primitive element of finite field, error locator.

ФЕЙЗИЕВ Фикрат Гюлали оглы, д-р физ.-мат. наук, профессор, зав. кафедрой дифференциальных уравнений и оптимизации Сумгаитского госуниверситета. В 1978 г. окончил Азербайджанский госуниверситет. Область научных исследований — математическая кибернетика, теория конечных автоматов и теоретические вопросы информатики.

МЕХТИЕВА Марал Рзабала кызы, канд. физ.-мат. наук, доцент кафедры высшей математики Бакинского госуниверситета. В 1992 г. окончила Азербайджанский госуниверситет. Область научных исследований — математическая кибернетика, теория конечных автоматов и теоретические вопросы информатики.